kaspersky

Kaspersky Security Center 16.3 Linux

© 2026 AO Kaspersky Lab

Spis treści

System pomocy Kaspersky Security Center Linux

Nowości

Naprawione problemy

Informacje o Kaspersky Security Center Linux

- Pakiet dystrybucyjny
- Wymagania sprzętowe i programowe
  - Wymagania Serwera administracyjnego
  - Wymagania Web Console
  - Wymagania Agenta sieciowego
- Kompatybilne aplikacje i rozwiązania Kaspersky
- Informacje o kompatybilności składników Kaspersky Security Center Linux
- Porównanie Kaspersky Security Center: opartego na systemie Windows i opartego na systemie Linux
- Informacje o Kaspersky Next Expert View

Architektura i podstawowe pojęcia

- Architektura
- Schemat wdrożenia Serwera administracyjnego Kaspersky Security Center Linux i konsoli Kaspersky Security Center Web Console
- Porty używane przez Kaspersky Security Center Linux
- Porty używane przez Kaspersky Security Center Web Console
- Podstawowe pojęcia
  - Serwer administracyjny
  - Hierarchia Serwerów administracyjnych
  - Wirtualny Serwer administracyjny
  - Serwer sieciowy
  - Kaspersky Security Center Linux Web Server
  - Agent sieciowy
  - Grupy administracyjne
  - Zarządzane urządzenie
  - Urządzenie nieprzypisane
  - Stacja robocza administratora
  - Webowa wtyczka administracyjna
  - Zasady
  - Profile zasad
  - Zadania
  - Obszar zadania
  - Jak ustawienia lokalne aplikacji mają się do zasad
  - Punkt dystrybucji
  - Brama połączenia
  - Wirtualne Serwery administracyjne

Schematy ruchu sieciowego danych i użycia portów

- Serwer administracyjny i zarządzane urządzenia w sieci LAN
- Główny Serwer administracyjny w sieci LAN i dwa podrzędne Serwery administracyjne
- Serwer administracyjny w sieci LAN, zarządzane urządzenia w Internecie, odwrotny serwer proxy w użyciu

Serwer administracyjny w sieci LAN, zarządzane urządzenia w internecie, brama połączenia w użyciu
Serwer administracyjny w strefie DMZ, zarządzane urządzenia w Internecie
Interakcja komponentów Kaspersky Security Center Linux i aplikacji zabezpieczających: więcej informacji
Konwencje stosowane w schematach interakcji
Serwer administracyjny i DBMS
Serwer administracyjny i urządzenie klienckie: zarządzanie aplikacją zabezpieczająca
Aktualizowanie oprogramowania na urządzeniu klienckim poprzez punkt dystrybucji
Hierarchia Serwerów administracyjnych: główny Serwer administracyjny i podrzędny Serwer administracyjny
Hierarchia Serwerów administracyjnych z podrzędnym Serwerem administracyjnym w strefie DMZ
Serwer administracyjny, brama połączenia w segmencie sieci i urządzenie klienckie
Serwer administracyjny i dwa urządzenia w strefie DMZ: brama połączenia i urządzenie klienckie
Serwer administracyjny i Kaspersky Security Center Web Console
Pierwsze kroki
Przewodnik po zwiększaniu odporności
Lista kontrolna wzmocnienia zabezpieczeń
Wdrożenie Serwera administracyjnego
Bezpieczeństwo połączenia
Konta i uwierzytelnianie
Zarządzanie ochroną Serwera administracyjnego
Zarządzanie ochroną urządzeń klienckich
Konfigurowanie ochrony dla zarządzanych aplikacji
Konserwacja Serwera administracyjnego
Transfer zdarzeń do systemów innych producentów
Zalecenia dotyczące bezpieczeństwa systemów informatycznych innych firm
Zalecenia dotyczące korzystania z aplikacji zabezpieczających Kaspersky
Scenariusz: uwierzytelnianie serwera MySQL
Scenariusz: uwierzytelnianie serwera PostgreSQL
Przygotowanie do wdrożenia
Wybieranie konfiguracji Kaspersky Security Center Linux
Standardowa konfiguracja: Jedno biuro
Standardowa konfiguracja: Duże oddziały posiadające swoich administratorów
Standardowa konfiguracja: Małe zdalne biura
Wybieranie struktury ochrony firmy
Typowe schematy wdrażania systemu ochrony
Wybieranie systemu zarządzania bazą danych
Umożliwianie uzyskania dostępu do Serwera administracyjnego przez internet
Dostęp do internetu: Serwer administracyjny w sieci lokalnej
Dostęp do internetu: Serwer administracyjny w strefie DMZ
Instalacja
Konfigurowanie serwera MariaDB x64 do pracy z Kaspersky Security Center Linux
Konfigurowanie serwera PostgreSQL lub Postgres Pro do pracy z Kaspersky Security Center Linux
Konfigurowanie serwera MySQL x64 do pracy z Kaspersky Security Center Linux
Przygotowanie klastra DBMS o wysokiej dostępności do pracy z Kaspersky Security Center Linux
Instalowanie Kaspersky Security Center Linux
Instalowanie Kaspersky Security Center Linux w trybie cichym
Instalowanie Kaspersky Security Center Linux na Astra Linux w trybie zamkniętego środowiska oprogramowania

Instalowanie Kaspersky Security Center Web Console
Parametry instalacji Kaspersky Security Center Web Console
Instalowanie Kaspersky Security Center Web Console na Astra Linux w trybie zamkniętego środowiska oprogramowania
Instalowanie Kaspersky Security Center Linux za pomocą skryptu
Wdrażanie klastra trybu failover Kaspersky Security Center Linux
Klaster pracy awaryjnej Kaspersky Security Center Linux. Schematy wdrażania
Klaster pracy awaryjnej Kaspersky Security Center Linux
Scenariusz: Wdrażanie klastra trybu failover Kaspersky Security Center Linux
Klaster pracy awaryjnej Kaspersky Security Center Linux. Wymagania sprzętowe i programowe
Przygotowywanie serwera plików dla klastra trybu failover Kaspersky Security Center Linux
Przygotowywanie węzłów dla klastra trybu failover Kaspersky Security Center Linux
Instalowanie Kaspersky Security Center Linux na węzłach klastra trybu failover Kaspersky Security Center Linux
Ręczne uruchamianie i zatrzymywanie węzłów klastra
Ponowna instalacja węzła klastra trybu failover
Instalowanie Kaspersky Security Center Web Console połączonej z Serwerem administracyjnym zainstalowanym na węzłach klastra przełączania awaryjnego Kaspersky Security Center Linux
Geograficznie rozproszony klaster trybu failover Kaspersky Security Center Linux
Geograficznie rozproszony klaster z systemem Ubuntu i PostgreSQL DBMS
Przygotowanie system plików węzłów klastra
Konfigurowanie zreplikowanego systemu plików klastra
Instalowanie i konfigurowanie Corosync i Pacemaker na węzłach klastra
Instalowanie i konfigurowanie PostgreSQL DBMS
Instalowanie Kaspersky Security Center Linux na geograficznie rozproszonych węzłach klastra trybu failover
Geograficznie rozproszony klaster z systemem SberLinux i Platform V Pangolin DBMS
Przygotowanie system plików węzłów klastra
Konfigurowanie zreplikowanego systemu plików klastra
Instalowanie i konfigurowanie Corosync i Pacemaker na węzłach klastra
Instalowanie i konfigurowanie Platform V Pangolin DBMS
Instalowanie Kaspersky Security Center Linux na geograficznie rozproszonych węzłach klastra trybu failover
Instalowanie Kaspersky Security Center Web Console na geograficznie rozproszonych węzłach klastra trybu failover
Konta do pracy z DBMS
Konfiguracja konta DBMS do pracy z MySQL i MariaDB
Konfiguracja konta DBMS do pracy z PostgreSQL i Postgres Pro
Przenoszenie danych ze współdzielonej przestrzeni tabel do przestrzeni tabel typu plik-tabela w systemach DBMS MySQL lub MariaDB
Certyfikaty do pracy z Kaspersky Security Center Linux
Informacje o certyfikatach Kaspersky Security Center
Wymagania dotyczące niestandardowych certyfikatów stosowanych w Kaspersky Security Center Linux
Ponowne wystawianie certyfikatu dla Kaspersky Security Center Web Console
Zastępowanie certyfikatu dla Kaspersky Security Center Web Console
Konwersja certyfikatu PFX do formatu PEM
Scenariusz: Określanie niestandardowego certyfikatu Serwera administracyjnego
Zastępowanie certyfikatu Serwera administracyjnego za pomocą narzędzia klsetsrvcert
Podłączanie Agentów sieciowych do Serwera administracyjnego przy użyciu narzędzia klmover
Ponowne wystawianie certyfikatu serwera sieciowego
Zmiana domyślnego certyfikatu IAM na niestandardowy
Dodawanie adresu Serwera Administracyjnego do konfiguracji Serwera IAM

Określanie folderu współdzielonego
Logowanie do Kaspersky Security Center Web Console i wylogowywanie
Interfejs Kaspersky Security Center Web Console
Zmiana języka interfejsu oprogramowania Kaspersky Security Center Web Console
Zmiana strony głównej Kaspersky Security Center Web Console
Dodawanie i usuwanie z ulubionych
Usuwanie Kaspersky Security Center Web Console
Kreator wstępnej konfiguracji
Krok 1. Określenie ustawień połączenia internetowego
Krok 2. Pobieranie żądanych uaktualnień
Krok 3. Wybór elementów do zabezpieczenia
Krok 4. Wybieranie szyfrowania w rozwiązaniach
Krok 5. Konfigurowanie instalacji wtyczek dla zarządzanych aplikacji
Krok 6. Pobieranie pakietów dystrybucyjnych i tworzenie pakietów instalacyjnych
Krok 7. Konfigurowanie Kaspersky Security Network
Krok 8. Wybieranie metody aktywacji aplikacji
Krok 9. Określanie ustawień zarządzania aktualizacjami firm trzecich
Krok 10. Tworzenie podstawowej konfiguracji ochrony sieci
Krok 11. Konfigurowanie powiadomień e-mail
Krok 12. Zamykanie kreatora wstępnej konfiguracji
Kreator wdrażania ochrony
Krok 1. Uruchamianie kreatora wdrażania ochrony
Krok 2. Wybieranie pakietu instalacyjnego
Krok 3. Wybieranie metody rozsyłania pliku klucza lub kodu aktywacyjnego
Krok 4. Wybieranie wersji Agenta sieciowego
Krok 5. Wybór urządzeń
Krok 6. Określanie ustawień zadania zdalnej instalacji
Krok 7. Zarządzanie ponownym uruchomieniem
Krok 8. Usuwanie niekompatybilnych aplikacji przed instalacją
Krok 9. Przenoszenie urządzeń do grupy Zarządzane urządzenia
Krok 10. Wybieranie kont w celu uzyskania dostępu do urządzeń
Krok 11. Uruchamianie instalacji
Aktualizacja Kaspersky Security Center Linux
Aktualizacja Kaspersky Security Center Linux z wersji 16 lub nowszej
Aktualizowanie Kaspersky Security Center Linux z wersji 16 lub nowszej przy użyciu pliku instalatora
Aktualizacja Kaspersky Security Center Linux z wersji 16 lub nowszej za pomocą kopii zapasowej
Aktualizowanie Kaspersky Security Center Linux od wersji 16 lub nowszej na węzłach klastra trybu failover Kaspersky Security Center Linux
Aktualizacja Kaspersky Security Center Linux z wersji 15.4 lub starszej
Aktualizacja Kaspersky Security Center Linux z wersji 15.4 lub starszej przy użyciu pliku instalacyjnego
Aktualizowanie Kaspersky Security Center Linux z wersji 15.4 lub starszej poprzez kopię zapasową
Aktualizowanie Kaspersky Security Center Linux od wersji 15.4 lub starszej na węzłach klastra trybu failover Kaspersky Security Center Linux
Aktualizowanie Kaspersky Security Center Web Console
Aktualizowanie Kaspersky Security Center Web Console na Astra Linux w trybie zamkniętego środowiska oprogramowania

Migracja do Kaspersky Security Center Linux
Migracja do Kaspersky Security Center Linux przy użyciu kopii zapasowej danych Serwera administracyjnego
Film instruktażowy: Migracja do Kaspersky Security Center Linux przy użyciu kopii zapasowej danych Serwera administracyjnego
Migracji do Kaspersky Security Center Linux za pomocą Kreatora migracji
Eksportowanie obiektów grupowych z Kaspersky Security Center Windows
Importowanie pliku eksportowania do Kaspersky Security Center Linux
Przełączanie zarządzanych urządzeń na zarządzane przez Kaspersky Security Center Linux
Konfigurowanie Serwera administracyjnego
Konfigurowanie adresu połączenia Serwera administracyjnego
Konfigurowanie połączenia Kaspersky Security Center Web Console z Serwerem administracyjnym
Konfigurowanie listy dozwolonych adresów IP do łączenia się z Kaspersky Security Center Linux
Konfigurowanie ustawień dostępu do Internetu dla Serwera administracyjnego
Hierarchia Serwerów administracyjnych
Tworzenie hierarchii Serwerów administracyjnych: dodawanie podrzędnego Serwera administracyjnego
Przeglądanie listy podrzędnych Serwerów administracyjnych
Zarządzanie wirtualnymi Serwerami administracyjnymi
Tworzenie wirtualnego Serwera administracyjnego
Włączanie i wyłączanie wirtualnego Serwera administracyjnego
Przypisywanie administratora do wirtualnego Serwera administracyjnego
Zmienianie Serwera administracyjnego dla urządzeń klienckich
Usuwanie wirtualnego Serwera administracyjnego
Konfigurowanie rejestrowania zdarzeń połączenia serwera administracyjnego
Określanie maksymalnej liczby zdarzeń w repozytorium zdarzeń
Przenoszenie Serwera administracyjnego na inne urządzenie
Zmiana nazwy Serwera administracyjnego
Zachowanie połączeń przez dodanie nowego rekordu DNS
Zachowanie połączeń przez przełączenie na łączność opartą na adresie IP
Przywracanie przerwanych połączeń po zmianie nazwy serwera
Zmiana poświadczeń DBMS
Tworzenie kopii zapasowej i przywracanie danych Serwera administracyjnego
Tworzenie zadania kopii zapasowej danych Serwera administracyjnego
Używanie narzędzia klbackup do tworzenia kopii zapasowych i odzyskiwania danych
Korzystanie z narzędzia klbackup w celu przełączania zarządzanych urządzeń pod zarządzanie innego Serwera administracyjnego
Tworzenie kopii zapasowej i przywracanie danych Serwera administracyjnego podczas korzystania z MySQL lub MariaDB
Konserwacja Serwera administracyjnego
Usuwanie hierarchii Serwerów administracyjnych
Dostęp do publicznych serwerów DNS
Konfigurowanie interfejsu
Nawiązywanie szyfrowanego połączenia z Serwerem administracyjnym
Szyfrowanie komunikacji z TLS
Ustawienia sieciowe dotyczące interakcji z usługami zewnętrznymi
Globalna lista podsieci
Sprawdzanie integralności modułów za pomocą narzędzi klscmodchk i integrity_checker

Wykrywanie urządzeń w sieci
Scenariusz: Wykrywanie urządzeń w sieci
Przeszukiwanie sieci Windows
Przeszukiwanie zakresu IP
Dodawanie i modyfikowanie zakresu IP
Przeszukiwanie Zeroconf
Przeszukiwanie kontrolera domeny
Uwierzytelnianie i połączenie z kontrolerem domeny
Konfigurowanie kontrolera domeny Samba
Inwentaryzacja sprzętu
Dodawanie informacji o nowych urządzeniach
Konfigurowanie kryteriów wykorzystywanych do określania urządzeń firmowych
Używanie dynamicznego trybu VDI na urządzeniach klienckich
Włączanie dynamicznego trybu VDI we właściwościach pakietu instalacyjnego Agenta sieciowego
Przenoszenie urządzeń z VDI do grupy administracyjnej
Zarządzanie urządzeniami klienckimi
Ustawienia zarządzanego urządzenia
Ręczne sprawdzanie połączenia pomiędzy urządzeniem klienckim a Serwerem administracyjnym. Narzędzie klnagchk
Reguły przenoszenia urządzeń
Tworzenie reguł przenoszenia urządzeń
Kopiowanie reguł przenoszenia urządzeń
Warunki dla reguły przenoszenia urządzenia
Ręczne dodawanie urządzeń do grupy administracyjnej
Ręczne przenoszenie urządzeń lub klastrów do grupy administracyjnej
Informacje o klastrach i macierzach serwerowych
Właściwości klastra lub macierzy serwerowej
Dostosowanie punktów dystrybucji i bram połączenia
Informacje o punktach dystrybucji
Standardowa konfiguracja punktów dystrybucji: Jedno biuro
Standardowa konfiguracja punktów dystrybucji: Małe zdalne biura
Obliczanie liczby i konfigurowanie punktów dystrybucji
Automatyczne przypisywanie punktów dystrybucji
Ręczne przypisywanie punktów dystrybucji
Dodawanie bramy połączenia w strefie DMZ jako punktu dystrybucji
Modyfikowanie listy punktów dystrybucji dla grupy administracyjnej
Włączanie serwera push
Zwiększenie limitu deskryptorów plików dla usługi klnagent
Informacje o stanach urządzeń
Konfigurowanie przełączania stanów urządzeń
Wybory urządzeń
Przeglądanie listy urządzeń z wyboru urządzeń
Tworzenie kryteriów wyboru urządzeń
Konfigurowanie kryteriów wyboru urządzeń
Eksportowanie listy urządzeń z wyboru urządzeń
Usuwanie urządzeń z grup administracyjnych w wyborze

Znaczniki urządzeń
Tworzenie znacznika urządzenia
Zmienianie nazwy znacznika urządzenia
Usuwanie znacznika urządzenia
Przeglądanie urządzeń, do których przypisano znacznik
Przeglądanie znaczników przydzielonych do urządzenia
Ręczne oznaczanie urządzenia
Usuwanie przydzielonego znacznika z urządzenia
Wyświetlanie reguł automatycznego oznaczania urządzeń
Edytowanie reguły automatycznego znakowania urządzeń
Tworzenie reguły automatycznego znakowania urządzeń
Uruchamianie reguł automatycznego znakowania urządzeń
Usuwanie reguły automatycznego oznaczania urządzeń
Zarządzanie znacznikami urządzeń za pomocą narzędzia klscflag
Szyfrowanie i ochrona danych
Przeglądanie listy zaszyfrowanych dysków
Wyświetlanie listy zdarzeń szyfrowania
Tworzenie i przeglądanie raportów z szyfrowania
Udzielanie dostępu do zaszyfrowanego dysku w trybie offline
Przesyłanie kluczy szyfrowania między Serwerami administracyjnymi
Zmienianie Serwera administracyjnego dla urządzeń klienckich
Unikanie konfliktów między kilkoma Serwerami administracyjnymi
Przenoszenie urządzeń podłączonych do Serwera administracyjnego przez bramy połączeń na inny Serwer administracyjny
Przeglądanie i konfigurowanie działań, gdy urządzenia wykazują brak aktywności
Wysyłanie wiadomości na urządzenia użytkowników
Zdalne włączanie, wyłączanie i ponowne uruchamianie urządzeń klienckich
Zdalny dostęp do zarządzanych urządzeń
Zdalny dostęp z urządzenia opartego na systemie Linux za pomocą Kaspersky Security Center Web Console do urządzenia zarządzanego opartego na systemie Linux
Zdalny dostęp z urządzenia opartego na systemie Linux za pomocą Kaspersky Security Center Web Console do urządzenia zarządzanego opartego na systemie Windows
Zdalny dostęp z urządzenia opartego na systemie Windows za pomocą Kaspersky Security Center Web Console do urządzenia zarządzanego opartego na systemie Linux
Zdalny dostęp z urządzenia opartego na systemie Windows za pomocą Kaspersky Security Center Web Console do urządzenia zarządzanego opartego na systemie Windows
Zarządzanie urządzeniami mobilnymi
Korzystanie z Firebase Cloud Messaging
Integracja z infrastrukturą kluczy publicznych
Zarządzanie grupami administracyjnymi
Tworzenie grup administracyjnych
Automatyczna instalacja aplikacji na urządzeniach w grupie administracyjnej
Przenoszenie grup administracyjnych
Usuwanie grup administracyjnych
Wdrażanie aplikacji Kaspersky
Scenariusz: Wdrażanie aplikacji Kaspersky
Dodawanie wtyczek administracyjnych dla aplikacji Kaspersky

Pakiety instalacyjne
Pobieranie i tworzenie pakietów instalacyjnych dla aplikacji Kaspersky
Tworzenie pakietów instalacyjnych z pliku
Tworzenie autonomicznych pakietów instalacyjnych
Ustawienia pakietu instalacyjnego Agenta sieciowego
Uruchamianie pakietów autonomicznych utworzonych przez Kaspersky Security Center Linux
Instalowanie aplikacji przy pomocy pakietów autonomicznych
Aktualizowanie baz danych w pakiecie instalacyjnym aplikacji zabezpieczającej
Zmienianie ograniczenia rozmiaru danych niestandardowego pakietu instalacyjnego
Rozsyłanie pakietów instalacyjnych na podrzędne Serwery administracyjne
Przeglądanie listy autonomicznych pakietów instalacyjnych
Instalowanie Agenta sieciowego dla systemu Linux
Przygotowanie urządzenia z systemem Linux do zdalnej instalacji Agenta sieciowego
Przygotowanie urządzenia z systemem SUSE Linux Enterprise Server 15 do instalacji Agenta sieciowego
Przygotowanie urządzenia z systemem Astra Linux w trybie zamkniętego środowiska oprogramowania do instalacji Agenta sieciowego
Przygotowanie do instalacji Agenta sieciowego w systemie operacyjnym Linux z glibc 2.5 (starszy system operacyjny)
Przygotowanie do instalacji Agenta sieciowego w systemie operacyjnym Linux z OpenSSH w wersji 6.4 (starszy system operacyjny)
Zdalna instalacja Agenta sieciowego na urządzeniu z systemem Linux
Instalowanie Agenta sieciowego dla systemu Linux w trybie cichym (z plikiem odpowiedzi)
Instalowanie Agenta sieciowego dla systemu Linux w trybie interaktywnym
Obsługa przywracania systemu plików dla urządzeń z zainstalowanym Agentem sieciowym
Instalowanie Agenta sieciowego dla systemu Windows
Instalowanie Agenta sieciowego dla systemu Windows w trybie interaktywnym
Instalowanie Agenta sieciowego dla systemu Windows w trybie cichym
Wdrażanie poprzez przechwycenie i skopiowanie obrazu urządzenia
Tryb klonowania dysku Agenta sieciowego
Parametry instalacji Agenta sieciowego
Instalowanie aplikacji przy pomocy zadania zdalnej instalacji
Informacje o zadaniach zdalnej instalacji w Kaspersky Security Center Linux
Zdalna instalacja aplikacji
Instalacja zdalna aplikacji na urządzeniach z systemem macOS
Instalowanie aplikacji na podrzędnych Serwerach administracyjnych
Zdalna instalacja aplikacji na urządzeniach z zainstalowanym Agentem sieciowym
Zarządzanie ponownym uruchamianiem urządzeń w zadaniu zdalnej instalacji
Wymuszone wdrożenie przy użyciu zadania zdalnej instalacji z Kaspersky Security Center Linux
Instalowanie aplikacji w trybie cichym
Przygotowanie urządzenia macOS do zdalnej instalacji Agenta sieciowego
Infrastruktura wirtualna
Wskazówki dotyczące zmniejszenia obciążenia na maszynach wirtualnych
Obsługa dynamicznych maszyn wirtualnych
Obsługa kopiowania maszyn wirtualnych
Określanie ustawień zdalnej instalacji na urządzeniach z systemem Unix
Monitorowanie wdrożenia
Uruchamianie i zatrzymywania działania aplikacji Kaspersky
Zastępowanie aplikacji zabezpieczających firm trzecich

Zdalne usuwanie aplikacji lub aktualizacji oprogramowania
Przygotowanie urządzenia z systemem Windows do zdalnej instalacji
Tworzenie zadania zdalnego wykonywania skryptów
Tworzenie pakietu instalacyjnego na podstawie pliku manifestu
Przygotowanie archiwum dla zadania Zdalne wykonywanie skryptów
Zdalne instalowanie aplikacji na urządzeniach za pomocą zadania Zdalne wykonywanie skryptów
Konfigurowanie powiadomień i monitorowania dla zadania Zdalne wykonywanie skryptów
Licencjonowanie
Licencjonowanie Kaspersky Security Center Linux
Informacje o Umowie licencyjnej użytkownika końcowego
Informacje o licencji
Informacje o certyfikacie licencji
Informacje o kluczu licencyjnym
Przeglądanie Polityki prywatności
Opcje licencjonowania Kaspersky Security Center
Informacje o pliku klucza
Informacje o przekazywaniu danych
Informacje o subskrypcji
Aktywowanie Kaspersky Security Center Linux
Licencjonowanie zarządzanych aplikacji Kaspersky
Licencjonowanie zarządzanych aplikacji
Dodawanie klucza licencyjnego do repozytorium Serwera administracyjnego
Rozsyłanie klucza licencyjnego na urządzenia klienckie
Automatyczne rozsyłanie kluczy licencyjnych
Wyświetlanie informacji o używanych kluczach licencyjnych
Zdarzenia przekroczenia limitu licencji
Usuwanie klucza licencyjnego z repozytorium
Wycofanie zgody z Umową Licencyjną Użytkownika Końcowego
Odnawianie licencji dla aplikacji Kaspersky
Korzystanie z Kaspersky Marketplace do wyboru rozwiązań biznesowych firmy Kaspersky
Konfigurowanie aplikacji Kaspersky
Scenariusz: Konfigurowanie ochrony sieci
Informacje o metodach zarządzania ochroną skoncentrowaną na urządzeniu i użytkowniku
Konfiguracja i przydzielanie zasad: Metoda skoncentrowana na urządzeniu
Konfiguracja i przydzielanie zasad: Metoda skoncentrowana na użytkowniku
Zasady i profile zasad
Informacje o zasadach i profilach zasad
Informacje o blokadzie i zablokowanych ustawieniach
Dziedziczenie zasad i profili zasad
Hierarchia zasad
Profile zasad w hierarchii zasad
Implementacja ustawień na zarządzanym urządzeniu
Zarządzanie zasadami
Przeglądanie listy zasad
Tworzenie zasady
Ogólne ustawienia zasady
Modyfikowanie zasady

Włączanie i wyłączanie opcji dziedziczenia zasady
Kopiowanie zasady
Przenoszenie zasady
Eksportowanie zasady
Importowanie zasady
Wymuszona synchronizacja
Przeglądanie wykresu stanu dystrybucji zasad
Aktywowanie zasady automatycznie po wystąpieniu zdarzenia Ataku wirusa
Usuwanie zasady
Zarządzanie profilami zasad
Przeglądanie profili zasad
Zmiana priorytetu profilu zasad
Tworzenie profilu zasad
Kopiowanie profilu zasad
Tworzenie reguły aktywacji profilu zasad
Usuwanie profilu zasad
Eksportowanie i importowanie profilu zasad
Ustawienia zasady Agenta sieciowego
Korzystanie z Agenta sieciowego dla systemu Windows, Linux i macOS: Porównanie
Porównanie ustawień Agenta sieciowego według systemów operacyjnych
Włączanie i wyłączanie trybu niskiego zużycia zasobów dla Agenta sieciowego
Konfigurowanie ustawień ochrony aplikacji zarządzanych
Ręczna konfiguracja grupowego zadania aktualizacji dla Kaspersky Endpoint Security
Ręczna konfiguracja grupowego zadania skanowania urządzeń z zainstalowanym programem Kaspersky Endpoint Security
Kaspersky Security Network (KSN)
Informacje o KSN
Konfigurowanie dostępu do KSN
Włączanie i wyłączanie korzystania z KSN
Przeglądanie zaakceptowanego Oświadczenia KSN
Akceptowanie zaktualizowanego Oświadczenia KSN
Sprawdzanie, czy punkt dystrybucji działa jako serwer proxy KSN
Przeglądanie statystyk dotyczących serwera proxy KSN
Zarządzanie zadaniami
Informacje o zadaniach
Informacje o obszarze zadania
Tworzenie zadania
Ręczne uruchamianie zadania
Rozpoczęcie zadania dla wybranych urządzeń
Przeglądanie listy zadań
Ogólne ustawienia zadania
Eksportowanie zadania
Importowanie zadania
Uruchamianie kreatora zmiany haseł w zadaniach
Krok 1. Określanie danych uwierzytelniających
Krok 2. Wybieranie działania, jakie ma zostać podjęte
Krok 3. Sprawdzanie wyników
Przeglądanie wyników wykonywania zadań przechowywanych na Serwerze administracyjnym

Znaczniki aplikacji
Znaczniki aplikacji
Tworzenie znacznika aplikacji
Zmienianie nazwy znacznika aplikacji
Przydzielanie znaczników do aplikacji
Usuwanie przydzielonych znaczników z aplikacji
Usuwanie znacznika aplikacji
Użycie narzędzia klscflag do otwarcia portu 13291
Rejestrowanie interfejsu aplikacji Kaspersky Industrial CyberSecurity for Networks w Kaspersky Security Center Web Console
Zarządzanie użytkownikami i rolami użytkowników
Informacje o kontach użytkowników
Informacje o rolach użytkowników
Konfigurowanie praw dostępu do funkcji aplikacji. Kontrola dostępu oparta o rolę
Prawa dostępu do funkcji aplikacji
Informacje o rolach użytkowników
Nadawanie praw dostępu do określonych obiektów
Przydzielanie praw dostępu użytkownikom i grupom bezpieczeństwa
Dodawanie konta użytkownika wewnętrznego
Tworzenie grupy bezpieczeństwa
Edytowanie konta użytkownika wewnętrznego
Edytowanie grupy bezpieczeństwa
Przypisywanie roli do użytkownika lub grupy bezpieczeństwa
Dodawanie kont użytkowników do wewnętrznej grupy bezpieczeństwa
Wskazywanie użytkownika jako właściciela urządzenia
Przypisywanie użytkownika jako właściciela urządzenia podczas instalacji Agenta sieciowego
Przypisywanie użytkownika jako właściciela urządzenia z systemem Linux po instalacji Agenta sieciowego
Usuwanie użytkownika jako właściciela urządzenia
Włączanie ochrony konta przed nieautoryzowaną modyfikacją
Konfigurowanie uwierzytelniania dwuskładnikowego
Informacje o uwierzytelnianiu dwuskładnikowym konta
Konfigurowanie klucza tajnego uwierzytelniania dwuskładnikowego podczas logowania do Kaspersky Security Center Web Console
Zezwalanie użytkownikom na konfigurowanie uwierzytelniania dwuskładnikowego
Resetowanie i usuwanie klucza tajnego uwierzytelniania dwuskładnikowego
Wykluczanie kont z uwierzytelniania dwuskładnikowego
Edytowanie nazwy wystawcy kodu zabezpieczającego
Zmienianie liczby dozwolonych prób wprowadzenia hasła
Usuwanie użytkownika lub grupy bezpieczeństwa
Zmiana hasła do konta użytkownika
Tworzenie roli użytkownika
Edytowanie roli użytkownika
Edytowanie obszaru roli użytkownika
Usuwanie roli użytkownika
Kojarzenie profili zasad z rolami
Przydzielanie ról użytkownika do podrzędnych Serwerów administracyjnych
Zmiana hasła do konta

Wycofanie uprawnień lokalnego administratora
Konfigurowanie uwierzytelniania domeny Kerberos
Aktualizowanie baz danych i aplikacji Kaspersky
Scenariusz: Regularne aktualizowanie baz danych i aplikacji Kaspersky
Informacje o aktualizowaniu baz danych, modułów i aplikacji Kaspersky
Tworzenie zadania Pobierz aktualizacje do repozytorium serwera administracyjnego
Sprawdzanie pobranych uaktualnień
Tworzenie zadania pobierania aktualizacji do repozytoriów punktów dystrybucji
Dodawanie źródeł uaktualnień dla zadania Pobierz uaktualnienia do repozytorium Serwera administracyjnego
Zatwierdzanie i odrzucanie aktualizacji oprogramowania
Pobieranie pakietu instalacyjnego dla Kaspersky Endpoint Security for Windows
Informacje o używaniu plików diff do aktualizowania baz danych i modułów aplikacji Kaspersky
Włączanie funkcji Pobierz pliki diff
Pobieranie uaktualnień przez punkty dystrybucji
Aktualizowanie baz danych i modułów Kaspersky na urządzeniach offline
Monitorowanie, raportowanie i audyt
Scenariusz: Monitorowanie i raportowanie
Informacje o typach monitorowania i raportowania
Wywoływanie reguł w trybie Inteligentne uczenie
Przeglądanie i potwierdzanie obiektów wykrytych przy użyciu reguł Adaptacyjnej kontroli anomalii
Dodawanie wykluczeń z reguł Adaptacyjnej kontroli anomalii
Pulpit nawigacyjny i widżety
Korzystanie z pulpitu nawigacyjnego
Dodawanie widżetów do pulpitu nawigacyjnego
Ukrywanie widżetu na pulpicie nawigacyjnym
Przenoszenie widżetu na pulpicie nawigacyjnym
Zmiana wyglądu i rozmiaru widżetu
Zmiana ustawień widżetu
Informacje o trybie korzystania tylko z pulpitu
Konfigurowanie trybu korzystania tylko z pulpitu
Raporty administracyjne i ochrony
Korzystanie z raportów
Tworzenie szablonu raportu
Przeglądanie i edytowanie właściwości szablonu raportu
Eksportowanie raportu do pliku
Generowanie i przeglądanie raportu
Tworzenie zadania dostarczania raportu
Usuwanie szablonów raportu
Wskaźnik poziomu ochrony
Aplikacja zabezpieczająca jest zainstalowana
Zasada zastosowana
Aktualizacja antywirusowych baz danych skonfigurowana
Kopia zapasowa skonfigurowana
Konserwacja Serwera administracyjnego skonfigurowana
Szyfrowanie TLS włączone

Zdarzenia i wybory zdarzeń
Informacje o zdarzeniach w Kaspersky Security Center Linux
Zdarzenia składników Kaspersky Security Center Linux
Struktura danych opisu typu zdarzeń
Zdarzenia Serwera administracyjnego
Zdarzenia krytyczne Serwera administracyjnego
Zdarzenia błędu funkcjonalnego Serwera administracyjnego
Zdarzenia ostrzegające Serwera administracyjnego
Zdarzenia informacyjne Serwera administracyjnego
Zdarzenia Agenta sieciowego
Zdarzenia błędu funkcjonalnego Agenta sieciowego
Zdarzenia ostrzegające Agenta sieciowego
Zdarzenia informacyjne Agenta sieciowego
Używanie wyborów zdarzeń
Tworzenie kryterium wyboru zdarzenia
Edytowanie kryterium wyboru zdarzenia
Przeglądanie listy wyboru zdarzeń
Eksportowanie wyboru zdarzeń
Importowanie wyboru zdarzeń
Przeglądanie szczegółów zdarzenia
Eksportowanie zdarzeń do pliku
Przeglądanie historii obiektu ze zdarzenia
Usuwanie zdarzeń
Usuwanie wyborów zdarzeń
Ustawianie czasu przechowywania dla zdarzenia
Blokowanie często występujących zdarzeń
Informacje o blokowaniu często występujących zdarzeń
Zarządzanie blokowaniem często występujących zdarzeń
Usuwanie blokowania często występujących zdarzeń
Przetwarzanie i przechowywanie zdarzeń na Serwerze administracyjnym
Powiadomienia i stany urządzeń
Korzystanie z powiadomień
Przeglądanie powiadomień na ekranie
Informacje o stanach urządzeń
Konfigurowanie przełączania stanów urządzeń
Konfigurowanie dostarczania powiadomień
Sprawdzanie opcji wysyłania powiadomień
Wyświetlanie powiadomień o zdarzeniach po uruchomieniu pliku wykonywalnego
Ogłoszenia firmy Kaspersky
Informacje o ogłoszeniach firmy Kaspersky
Określanie ustawień ogłoszeń Kaspersky
Wyłączanie ogłoszeń Kaspersky
Przeglądanie informacji dotyczących wykrycia zagrożeń
Integracje umożliwiające reagowanie na alerty
Konfigurowanie integracji z usługą Active Directory w celu wykonywania działań reagowania
Konfigurowanie integracji z platformą Kaspersky Automated Security Awareness Platform
Konfigurowanie integracji z Kaspersky Threat Intelligence Portal Sandbox

Grupowanie alertów według atrybutów
Cloud Discovery
Włączanie funkcji Cloud Discovery za pomocą widżetu
Dodanie widżetu Cloud Discovery do pulpitu nawigacyjnego
Przeglądanie informacji o korzystaniu z usług w chmurze
Poziom ryzyka usługi w chmurze
Blokowanie dostępu do niechcianych usług w chmurze
Eksportowanie zdarzeń do systemów SIEM
Konfigurowanie eksportowania zdarzeń do systemów SIEM
Czynności niezbędne do wykonania przed rozpoczęciem pracy
Informacje o eksportowaniu zdarzeń
Informacje o konfigurowaniu eksportowania zdarzeń w systemie SIEM
Informacje dotyczące eksportowania zdarzeń przy użyciu formatów CEF i LEEF
Konwersja zdarzeń do formatu CEF lub LEEF
Oznaczenie zdarzeń do wyeksportowania do systemów SIEM w formacie Syslog
Oznaczanie zdarzeń aplikacji Kaspersky do eksportowania w formacie Syslog
Oznaczanie ogólnych zdarzeń do eksportu w formacie Syslog
Informacje dotyczące eksportowania zdarzeń przy użyciu formatu Syslog
Konfigurowanie Kaspersky Security Center Linux do wyeksportowania zdarzeń do systemu SIEM
Monitorowanie zmian zasad i profilów zasad
Eksportowanie zdarzeń bezpośrednio z bazy danych
Tworzenie zapytania SQL przy użyciu narzędzia klsql2
Przykład zapytania SQL w narzędziu klsql2
Sprawdzanie nazwy bazy danych Kaspersky Security Center Linux
Przeglądanie wyników eksportowania
Zarządzanie rewizjami obiektów
Wyświetlanie i zapisywanie rewizji zasady
Porównanie rewizji zasad
Przywracanie poprzedniej wersji obiektu
Aktywne zagrożenia
Leczenie nieprzetworzonego pliku
Pobieranie nieprzetworzonego pliku
Usuwanie plików z sekcji „Aktywne zagrożenia”
Usuwanie obiektów
Pobieranie i usuwanie plików z Kwarantanny i Kopie zapasowe plików
Pobieranie plików z Kwarantanny i Kopii zapasowej
Informacje o usuwaniu obiektów z repozytoriów Kwarantanny, Kopii zapasowej plików lub Aktywnych zagrożeń
Zarządzanie aplikacją przez SNMP
Konfigurowanie usługi snmpd w systemie operacyjnym
Włączanie i wyłączanie powiadomień przez SNMP
Włączanie i wyłączanie protokołu SNMP w Kaspersky Security Center Linux
Wartości identyfikatorów obiektów dla SNMP

Praca z Kaspersky Security Center Linux w ramach licencji Kaspersky Next XDR Optimum
Integracje umożliwiające reagowanie na alerty
Konfigurowanie integracji z usługą Active Directory w celu wykonywania działań reagowania
Konfigurowanie integracji z platformą Kaspersky Automated Security Awareness Platform
Konfigurowanie integracji z Kaspersky Threat Intelligence Portal Sandbox
Grupowanie alertów według atrybutów
Interakcja Kaspersky Security Center Web Console i innych rozwiązań Kaspersky
Nawiązywanie połączenia w tle
Konfigurowanie połączenia z serwerem proxy
Zdalna diagnostyka urządzeń klienckich
Otwieranie okna zdalnej diagnostyki
Włączanie i wyłączanie śledzenia dla aplikacji
Pobieranie plików śledzenia aplikacji
Usuwanie plików śledzenia
Pobierania ustawień aplikacji
Pobieranie informacji systemowych z urządzenia klienckiego
Pobierania dzienników zdarzeń
Uruchamianie, zatrzymywanie, ponowne uruchamianie aplikacji
Uruchamianie zdalnej diagnostyki Agenta sieciowego Kaspersky Security Center Linux i pobieranie wyników
Uruchamianie aplikacji na urządzeniu klienckim
Uruchamianie zdalnej diagnostyki na urządzeniu klienckim z systemem Linux
Zarządzanie aplikacjami i plikami wykonywalnymi firm trzecich na urządzeniach klienckich
Korzystanie z Kontroli aplikacji do zarządzania plikami wykonywalnymi
Uzyskiwanie i przeglądanie listy plików wykonywalnych przechowywanych na urządzeniach klienckich
Tworzenie kategorii aplikacji z zawartością dodaną ręcznie
Tworzenie kategorii aplikacji, która zawiera pliki wykonywalne z wybranych urządzeń
Tworzenie kategorii aplikacji, która zawiera pliki wykonywalne z wybranego folderu
Przeglądanie listy kategorii aplikacji
Dodawanie plików wykonywalnych dotyczących zdarzeń do kategorii aplikacji
Konfigurowanie Kontroli aplikacji w zasadzie Kaspersky Endpoint Security for Windows
Uzyskiwanie i przeglądanie listy aplikacji zainstalowanych na urządzeniach klienckich
Informacje o aplikacjach innych firm
Instalowanie aktualizacji oprogramowania firm trzecich
Scenariusz: Aktualizowanie oprogramowania innej firmy
Opcje instalacji aktualizacji oprogramowania innej firmy
Ustawienia zadania Wyszukiwanie luk i wymaganych aktualizacji
Tworzenie zadania Wyszukiwanie luk i wymaganych aktualizacji
Przeglądanie informacji o dostępnych aktualizacjach oprogramowania firm trzecich
Eksportowanie listy dostępnych aktualizacji oprogramowania do pliku
Zatwierdzanie oraz odrzucanie aktualizacji oprogramowania firm trzecich
Tworzenie zadania Zainstaluj wymagane aktualizacje i napraw luki
Dodawanie reguł dla instalacji aktualizacji
Ustawienia zadania Zainstaluj wymagane aktualizacje i napraw luki określone po utworzeniu zadania
Automatyczne aktualizowanie aplikacji innych firm
Eliminowanie luk w oprogramowaniu innych firm
Informacje o wyszukiwaniu i eliminowaniu luk w oprogramowaniu
Scenariusz: Wyszukiwanie i usuwanie luk w oprogramowaniu firm trzecich

Eliminowanie luk w oprogramowaniu innych firm
Tworzenie zadania Napraw luki
Wybieranie poprawek użytkownika dla luk w programach innych firm
Przeglądanie informacji o lukach w oprogramowaniu wykrytych na wszystkich zarządzanych urządzeniach
Przeglądanie informacji o lukach w oprogramowaniu wykrytych na wybranym zarządzanym urządzeniu
Przeglądanie statystyk dotyczących luk na zarządzanych urządzeniach
Eksportowanie listy luk w oprogramowaniu do pliku
Ignorowanie luk w oprogramowaniu
Tworzenie pakietu instalacyjnego aplikacji innej firmy z bazy danych Kaspersky
Przeglądanie i modyfikowanie ustawienia pakietu instalacyjnego aplikacji innej firmy z bazy danych Kaspersky
Ustawienia pakietu instalacyjnego aplikacji innej firmy z bazy danych Kaspersky
Naprawianie luk w odizolowanej sieci
Scenariusz: Eliminowanie luk w oprogramowaniu innych firm w odizolowanej sieci
Eliminowanie luk w oprogramowaniu innych firm w odizolowanej sieci
Konfigurowanie serwera administracyjnego z dostępem do internetu w celu usunięcia luk w odizolowanej sieci
Konfigurowanie izolowanych Serwerów administracyjnych w celu usunięcia luk w odizolowanej sieci
Przesyłanie poprawek i instalowanie aktualizacji w odizolowanej sieci
Wyłączenie przesyłania poprawek i instalacji aktualizacji w sieci izolowanej
Dokumentacja API
Praktyczne zastosowanie aplikacji dla dostawców usługi
Planowanie wdrożenia Kaspersky Security Center Linux
Umożliwianie uzyskania dostępu do Serwera administracyjnego przez internet
Standardowa konfiguracja Kaspersky Security Center Linux
Informacje o punktach dystrybucji
Hierarchia Serwerów administracyjnych
Wirtualne Serwery administracyjne
Instalacja i wstępna konfiguracja
Zalecenia dotyczące instalacji Serwera administracyjnego
Tworzenie kont dla usług Serwera administracyjnego na klastrze typu failover
Wybieranie systemu zarządzania bazą danych
Określanie adresu Serwera administracyjnego
Utrzymywanie bezczynnych połączeń
Wdrażanie Agenta sieciowego i aplikacji zabezpieczających
Konfigurowanie ochrony w sieci organizacji klienta
Ręczna konfiguracja zasady Kaspersky Endpoint Security
Konfigurowanie zasady w sekcji Zaawansowana ochrona przed zagrożeniami
Konfigurowanie zasady w sekcji Podstawowa ochrona przed zagrożeniami
Konfigurowanie zasady w sekcji Ustawienia ogólne
Konfigurowanie zasad w sekcji Konfiguracja zdarzenia
Ręczna konfiguracja grupowego zadania aktualizacji dla Kaspersky Endpoint Security
Ręczna konfiguracja grupowego zadania skanowania urządzeń z zainstalowanym programem Kaspersky Endpoint Security
Konfigurowanie terminarza zadania Wyszukiwanie luk i wymaganych aktualizacji
Ręczna konfiguracja grupowego zadania instalacji uaktualnień i naprawy luk
Tworzenie struktury grup administracyjnych i przydzielanie punktów dystrybucji
Standardowa konfiguracja klienta MSP: Jedno biuro
Standardowa konfiguracja klienta MSP: Wiele małych, zdalnych biur

Hierarchia zasad i korzystanie z zasad
Hierarchia zasad
Profile zasad
Zadania
Reguły przenoszenia urządzeń
Kategoryzacja oprogramowania
Tworzenie kopii zapasowej i przywracanie ustawień Serwera administracyjnego
Urządzenie z zainstalowanym Serwerem administracyjnym nie działa
Ustawienia Serwera administracyjnego lub bazy danych są uszkodzone
Informacje o profilach połączenia dla użytkowników mobilnych
Informacje o przełączaniu Agenta sieciowego na inne Serwery administracyjne
Tworzenie profilu połączenia dla użytkowników mobilnych
Zdalny dostęp do zarządzanych urządzeń
Korzystanie z opcji „Nie odłączaj od Serwera administracyjnego" w celu zapewnienia ciągłej łączności między zarządzanym urządzeniem a Serwerem administracyjnym
Informacje o sprawdzaniu czasu połączenia pomiędzy urządzeniem a Serwerem administracyjnym
Informacje o wymuszonej synchronizacji
Poradnik dotyczący rozmiarów
Informacje o podręczniku
Wyliczenia dla Serwerów administracyjnych
Obliczanie zasobów sprzętowych dla Serwera administracyjnego
Wymagania sprzętowe dla systemu zarządzania bazą danych i Serwera administracyjnego
Obliczanie pojemności bazy danych
Obliczanie miejsca na dysku
Obliczanie liczby i konfigurowanie Serwerów administracyjnych
Zalecenia dotyczące łączenia dynamicznych maszyn wirtualnych z Kaspersky Security Center
Wyliczenia dla punktów dystrybucji i bram połączenia
Wymagania wobec punktu dystrybucji
Obliczanie liczby i konfigurowanie punktów dystrybucji
Obliczanie liczby bram połączenia
Zapisywanie informacji o zdarzeniach dla zadań i zasad
Najlepsze praktyki dla Serwera administracyjnego zarządzającego dużą liczbą urządzeń
Szczególne względy i optymalne ustawienia określonych zadań
Częstotliwość wykrywania urządzeń
Zadanie tworzenia kopii zapasowej danych Serwera administracyjnego i zadanie konserwacji baz danych
Grupowe zadania aktualizacji Kaspersky Endpoint Security
Zadanie inwentaryzacji
Szczegóły dotyczące obciążenia sieci pomiędzy Serwerem administracyjnym a chronionymi urządzeniami
Zużycie ruchu sieciowego w różnych scenariuszach
Przeciętne zużycie ruchu sieciowego w ciągu 24 godzin
Znane problemy
Kontakt z działem pomocy technicznej
Jak uzyskać pomoc techniczną
Pomoc techniczna poprzez Kaspersky CompanyAccount
Uzyskiwanie plików zrzutu Serwera administracyjnego
Źródła informacji o aplikacji

Słownik
Administrator dostawcy usługi
Administrator Kaspersky Security Center Linux
Administrator klienta
Agent autoryzacji
Agent sieciowy
Aktualizacja
Aktywny klucz
Antywirusowe bazy danych
Atak wirusa
Bezpośrednie zarządzanie aplikacjami
Brama połączenia
Certyfikat współdzielony
Certyfikatu Serwera administracyjnego
Cloud Discovery
Dodatkowy (lub rezerwowy) klucz licencyjny
Domena rozgłoszeniowa
Dostawca usługi ochrony antywirusowej
Dostępne aktualizacje
FileTransferBridge
Folder Kopia zapasowa
Funkcja rozpoznawania lokalizacji w sieci (NLA)
Grupa administracyjna
Grupa ról
HTTPS
Instalacja lokalna
Instalacja ręczna
Instalacja zdalna
Istotność poprawki
JavaScript
Kaspersky Private Security Network (KPSN)
Kaspersky Security Center Linux Web Server
Kaspersky Security Center System Health Validator (SHV)
Klient Serwera administracyjnego (urządzenie klienckie)
Konsola administracyjna
Kopia zapasowa danych Serwera administracyjnego
Lightweight Nagent (LWNGT)
Luka
Macierzysty Serwer administracyjny
Menedżer tożsamości i dostępu (IAM)
Niekompatybilna aplikacja
Ochrona antywirusowa sieci
Okres licencji
Operator Kaspersky Security Center
Pakiet instalacyjny
Plik klucza
Priorytet zdarzenia

Profil
Profil informacyjny
Profil konfiguracyjny
Przywracanie
Przywrócenie danych Serwera administracyjnego
Punkt dystrybucji
Repozytorium zdarzeń
Scentralizowane zarządzanie aplikacjami
Serwer administracyjny
Serwer iOS MDM
Serwery aktualizacji Kaspersky
Sklep aplikacji
SSL
Stacja robocza administratora
Stan ochrony
Stan ochrony sieci
Strefa zdemilitaryzowana (DMZ)
Uprawnienia administracyjne
Urządzenie iOS MDM
Ustawienia programu
Ustawienia zadania
Użytkownicy wewnętrzni
Wirtualny Serwer administracyjny
Właściciel urządzenia
Zadanie
Zadanie dla określonych urządzeń
Zadanie grupowe
Zadanie lokalne
Zarządzane urządzenia
Zasada
Informacje o kodzie firm trzecich
Informacje o znakach towarowych

System pomocy Kaspersky Security Center Linux

Nowe funkcje

- Nowości

Wymagania sprzętowe i programowe

- Wymagania Serwera administracyjnego
- Wymagania Web Console
- Wymagania Agenta sieciowego

Pierwsze kroki

- Instalacja
- Kreator wstępnej konfiguracji
- Kreator wdrażania ochrony

Licencjonowanie i aktywacja

- Aktywowanie Kaspersky Security Center Linux
- Licencjonowanie zarządzanych aplikacji

Wdrożenie i konfiguracja

- Wykrywanie urządzeń w sieci
- Dostosowanie punktów dystrybucji i/lub bram połączenia
- Zastępowanie aplikacji zabezpieczających firm trzecich

- Aplikacje Kaspersky. Scentralizowane wdrażanie
- Konfigurowanie ochrony sieci
- Aplikacje Kaspersky. Aktualizowanie baz danych i modułów aplikacji
- Konfigurowanie adresu połączenia Serwera administracyjnego
- Migracja do Kaspersky Security Center Linux
- Informacje o aktualizacji Kaspersky Security Center Linux

Monitorowanie

- Monitorowanie i raportowanie
- Cloud Discovery

Zarządzanie urządzeniami klienckimi

- Zdalny dostęp do zarządzanych urządzeń

Zarządzanie lukami i poprawkami

- Wyszukiwanie i usuwanie luk w oprogramowaniu firm trzecich

Dodatkowe funkcje

- Eksportowanie zdarzeń do systemów SIEM
- Przeglądanie statystyk dotyczących serwera proxy KSN
- Podręcznik szacowania rozmiaru (tylko pomoc online)

Nowości

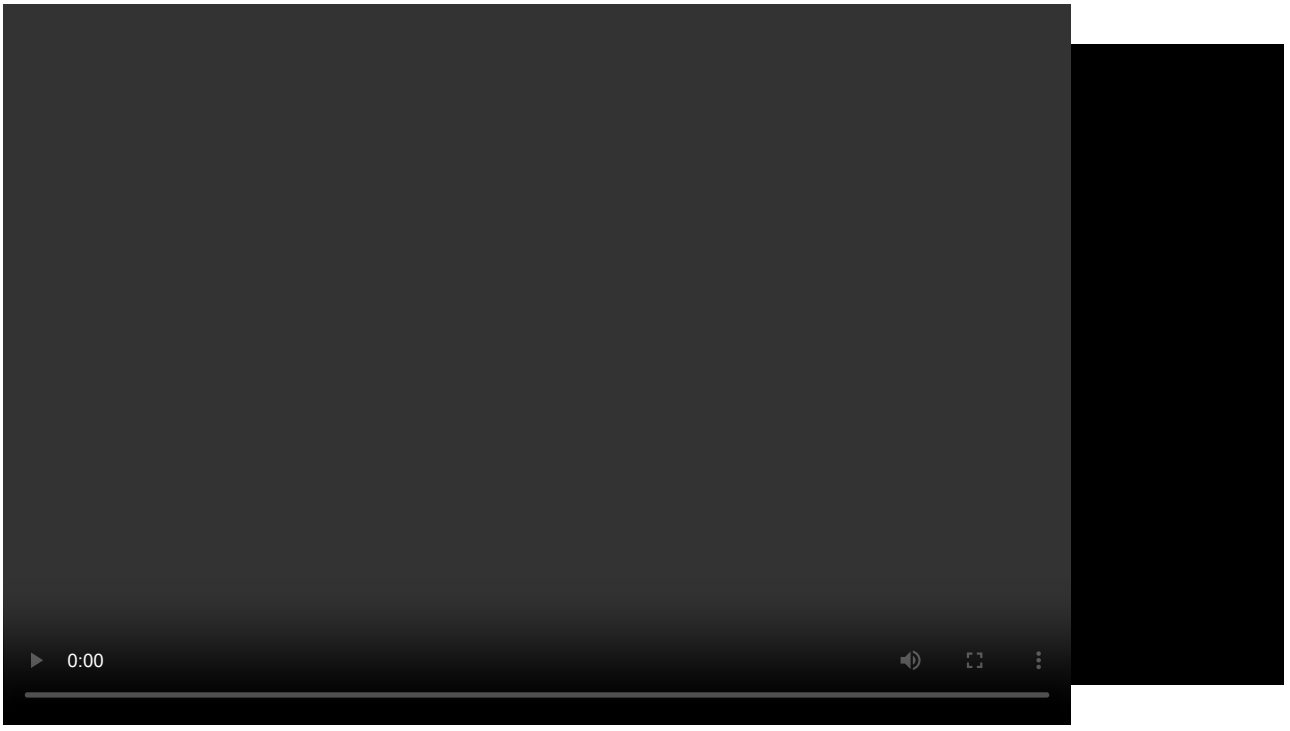
Kaspersky Security Center 16.3 Linux

Kaspersky Security Center 16.3 Linux posiada kilka nowych funkcji i ulepszeń:

- W przypadku zmodyfikowania zasady dla każdego zmienionego parametru tworzone jest osobne zdarzenie audytu. Zdarzenia są eksportowane do systemu SIEM.
- Do funkcji eksportu zdarzeń do systemów SIEM dodano obsługę **Kaspersky SIEM** (KUMA).
- Kaspersky Security Center Linux obsługuje teraz współpracę z rozwiązaniem Kaspersky Vulnerability Management.
- W celu zapewnienia zgodności z Przewodnikiem po zwiększaniu odporności opracowaliśmy zoptymalizowaną konfigurację Kaspersky Endpoint Security for Linux do instalacji na urządzeniach z komponentami Serwer administracyjny, Web Console i DBMS, a także do wdrażania klastra pracy awaryjnej Kaspersky Security Center Linux.
- Można teraz określić niestandardowy schemat bazy danych podczas instalacji Kaspersky Security Center Linux.
- W sekcji **Monitorowanie** → **Pulpit nawigacyjny**, wskaźnik poziomu ochrony pomaga ocenić bezpieczeństwo Serwera administracyjnego i punktów dystrybucji. Jeśli wskaźnik ma kolor żółty lub czerwony, należy podjąć działania w celu rozwiązania problemów i zmiany stanu wskaźnika na zielony.
- Dostępna jest uproszczona metoda wdrażania Kaspersky Security Center Linux: można teraz użyć skryptu instalacyjnego.
- Dostępny jest specjalny pakiet dystrybucyjny dla Kaspersky Network Agent for Linux Legacy z biblioteką glibc w wersji 2.5, który zapewnia obsługę następujących przestarzałych systemów operacyjnych:
  - CentOS 5.2
  - CentOS 5.4
  - CentOS 6.4
  - CentOS 6.6
  - Astra Linux Special Edition RUSB.10015-01 (aktualizacja operacyjna 1.4) 64-bitowy
- Agent sieciowy obsługuje teraz następujące nowe wersje systemów operacyjnych:
  - Microsoft Windows 11 IoT Enterprise, wersja 25H2, 64-bitowy
  - SberOS 3.6.1
  - Ubuntu Server 26.04 LTS

- Następujące systemy DBMS nie są już obsługiwane:
  - MySQL 5.7
  - MariaDB 10.1.30
- Rozwiązania podwyższająca poziom komfortu użytkownika:
  - Ulepszone filtrowanie w tabelach **Zadania** i **Zasady**. Teraz można dodawać wiele warunków przy użyciu logiki `OR`, a także korzystać z nowego operatora, który umożliwia wybranie wielu wartości dla jednej właściwości i wyświetlenie rekordów spełniających co najmniej jedno z określonych kryteriów.
  - W menu głównym:
    - Dostępna jest nowa sekcja **Zarządzanie oprogramowaniem**. Następujące sekcje zostały przeniesione do sekcji **Zarządzanie oprogramowaniem**: **Pakiety instalacyjne**, **Aplikacje Kaspersky**, **Aplikacje innych firm**, **Aktualne wersje aplikacji** i **Zarządzanie poprawkami**.
    - Sekcje **Urządzenia nieprzypisane** i **Sprzęt** zostały przeniesione do sekcji **Zarządzanie zasobami**.
    - Sekcje **Zadania** i **Repozytoria** zostały przeniesione na pierwszy poziom menu.
    - Sekcja **Kopie zapasowe wtyczek webowych** nie jest już używana i została usunięta z konsoli Web Console.

Kaspersky Security Center 16.2 Linux



Przegląd nowych funkcji w wersji 16.2. Film wideo

Kaspersky Security Center 16.2 Linux posiada kilka nowych funkcji i ulepszeń:

- W Kaspersky Security Center Web Console można teraz skonfigurować bramę połączenia w strefie zdemilitaryzowanej (DMZ).

  Użyj opcji **Użyj bramy połączenia DMZ przy użyciu adresu**, aby skonfigurować bramę połączenia.

- Ulepszono algorytm służący do zachowywania identyfikatora urządzenia Agenta sieciowego (parametr `Device ID`) na urządzeniach z systemem Linux. Jeśli numer seryjny BIOS-u urządzenia, numer seryjny płyty głównej, identyfikatory dysków pamięci masowej lub adres MAC pasują do wcześniej znanych wartości, Serwer administracyjny poprawnie identyfikuje urządzenie jako wcześniej wykryte po aktualizacji systemu operacyjnego lub zmianie adresu MAC.

- Dodano obsługę rozproszonego geograficznie klastra trybu failover Kaspersky Security Center Linux z węzłami zlokalizowanymi w różnych centrach danych. W konfiguracji klastra rozproszonego geograficznie wszystkie komponenty są przełączane awaryjnie.

- Możesz teraz eksportować zdarzenia do systemu SIEM w formatach CEF lub LEEF.

- Dodano obsługę klastra PostgreSQL o wysokiej dostępności z Patroni do automatycznego przełączania awaryjnego i HAProxy do równoważenia obciążenia.

- Możesz porównać rewizje zasady. Opcja ta jest dostępna dla zasad Serwera administracyjnego, Agenta sieciowego, Kaspersky Endpoint Security for Windows (od wersji 14.0 wtyczki webowej) oraz Kaspersky Endpoint Security for Mac (od wersji 12.2.1 z poprawką A wtyczki webowej). Lista aplikacji Kaspersky obsługujących tę funkcję zostanie rozszerzona w przyszłych wersjach.

- Protokół SNMP jest teraz obsługiwany. Za pomocą protokołu SNMP można udostępniać informacje, statystyki i zdarzenia dotyczące Serwera administracyjnego aplikacjom klienckim firm trzecich.

- Przeszukiwanie sieci Windows jest teraz obsługiwane dla punktów dystrybucji opartych na systemie Windows.

- Pojedynczy pakiet instalacyjny Agenta sieciowego dla systemu Linux jest już dostępny. Ten pakiet instalacyjny zawiera wersje dla różnych menedżerów pakietów i architektur procesorów. Podczas instalacji środowisko jest automatycznie wykrywane i instalowany jest odpowiedni pakiet Agenta sieciowego.

- Zdarzenia obejmują teraz informacje o inicjatorze poleceń wykonywanych na urządzeniach mobilnych.

- Komponent NSQ został usunięty z pakietu dystrybucyjnego Kaspersky Security Center Web Console. Usługa KSCWebConsoleMessageQueue.service nie jest już używana i zostanie usunięta po aktualizacji Kaspersky Security Center Web Console.

- W odizolowanych sieciach tworzenie pakietów instalacyjnych dla urządzeń z systemem Windows wymaga teraz pobrania dodatkowych modułów ze strony internetowej Kaspersky (archiwa ri_utils_win32.zip oraz ri_utils_arm64.zip).

- Agent sieciowy dla systemu Linux obsługuje teraz architekturę Windows ARM 64-bit. Zgodność z zarządzanymi aplikacjami można sprawdzić w odpowiedniej dokumentacji pomocy.

- Kaspersky Security Center Linux obsługuje współpracę z Kaspersky Sandbox.

- Rozwiązania podwyższająca poziom komfortu użytkownika:

  - Możesz teraz usunąć wszystkie zdarzenia z wyboru zdarzeń i z listy zdarzeń urządzenia jednocześnie.

    Opcje **Wybierz wszystkie** i **Wybierz wszystko na bieżącej stronie** są dostępne w wyborze zdarzeń i na liście zdarzeń urządzenia.

- Możesz teraz ręcznie określić priorytet reguł przenoszenia.

  Przycisk **Zmień priorytet** staje się dostępny po wybraniu reguły przenoszenia i umożliwia określenie nowego priorytetu.

- Kaspersky Security Center Linux obsługuje współpracę z Platform V SberLinux OS Server (SLO) 9.6.

- Kaspersky Security Center Linux obsługuje teraz pracę z następującymi systemami DBMS:

  - MySQL Standard Edition 8.4

  - MySQL Enterprise Edition 8.4

  - PostgreSQL 18

  - Postgres Pro 18 (wszystkie wersje)

  - Postgres Pro 18 Enterprise (wbudowany klaster o wysokiej dostępności)

- Agent sieciowy obsługuje teraz następujące nowe wersje systemów operacyjnych:

  - Microsoft Windows 11 Home/Pro/Pro for Workstations/Enterprise/Education ARM

  - Platform V SberLinux OS Server (SLO) 9.6

Kaspersky Security Center 16.1 Linux

Kaspersky Security Center 16.1 Linux posiada kilka nowych funkcji i ulepszeń:

- Uwierzytelnianie dwuskładnikowe jest teraz domyślnie włączone. Globalna opcja wyłączenia uwierzytelniania dwuskładnikowego nie jest już dostępna. Aby mieć pewność, że użytkownicy mogą zalogować się do Kaspersky Security Center Web Console i kontynuować korzystanie ze skryptów automatyzacji OpenAPI, przed uaktualnieniem należy włączyć uwierzytelnianie dwuskładnikowe dla wszystkich użytkowników.

- Możesz teraz zapisać profil zasad w pliku KLPROF bez eksportowania zasad, a następnie użyć tego pliku KLPROF do zaimportowania zapisanego profilu do zasad.

- Agent sieciowy działa teraz na urządzeniu z systemem operacyjnym ALT OS w zamkniętym trybie środowiska oprogramowania.

- Dodano obsługę uwierzytelniania domeny opartego na protokole Kerberos dla użytkowników domeny bez hasła przy użyciu protokołu SCRIL, umożliwiając pojedyncze logowanie (SSO) oparte na certyfikatach.

- Rozwiązania podwyższająca poziom komfortu użytkownika:

  - Filtrowanie urządzeń klienckich według wersji systemu operacyjnego i menedżera pakietów obejmuje teraz wersje systemu operacyjnego Linux.

  - Ulepszono mechanizm stronicowania tabel w Kaspersky Security Center Web Console: domyślna liczba wyświetlanych elementów została zwiększona do 50, a niestandardowa liczba wyświetlanych elementów jest teraz zachowywana między sesjami.

- Komentarze dotyczące kategorii aplikacji umożliwiają dodawanie opisów reguł uwzględniania i wykluczania aplikacji w ramach kategorii.
- Domyślnie lista dostępnych pakietów instalacyjnych wyświetla teraz tylko pakiety instalacyjne aplikacji Kaspersky w języku interfejsu Kaspersky Security Center Web Console oraz w języku angielskim.

- Kaspersky Security Center Linux obsługuje współpracę z Kaspersky Endpoint Security for Linux 12.4.
- Kaspersky Security Center Linux obsługuje teraz następujące nowe wersje systemów operacyjnych:
  - Debian GNU/Linux 13 (Trixie)
  - CentOS Stream 10
  - Red Hat Enterprise Linux Server 10.x
- Agent sieciowy obsługuje teraz następujące nowe wersje systemów operacyjnych:
  - ALT Workstation 11
  - ALT Server 11
  - ALT Education 11
  - AlterOS 2025
  - SberOS 3.4.0
  - SberOS 3.5.0
  - OSnova 3.*

Kaspersky Security Center 16 Linux

Kaspersky Security Center 16 Linux posiada kilka nowych funkcji i ulepszeń:

- Obsługiwane są kontrolery domeny FreeIPA i ALD Pro.
- Uwierzytelnianie domeny (pojedyncze logowanie) jest wdrożone. Funkcja pojedynczego logowania umożliwia Ci włączenie bezpiecznego uwierzytelniania w Kaspersky Security Center 16 Web Console bez konieczności ponownego wprowadzania hasła w sieci firmowej. Aby korzystać z uwierzytelniania domeny, należy określić dodatkowe parametry w pliku odpowiedzi podczas instalacji Kaspersky Security Center Web Console.
- Serwer administracyjny Kaspersky Security Center 16 Linux jest kompatybilny tylko z Kaspersky Security Center 16 Web Console. Nie można używać wcześniejszych wersji Kaspersky Security Center Web Console.
- Możesz teraz korzystać z funkcjonalności Kaspersky Next XDR Optimum w ramach licencji próbnej, pod warunkiem że dodałeś podrzędny Serwer administracyjny, aktywowałeś ten serwer w ramach licencji próbnej i wdrożyłeś klucz licencyjny na urządzenia zarządzane przez podrzędny Serwer administracyjny.

- Rozwiązania podwyższająca poziom komfortu użytkownika:
  - Zaktualizowano nawigację po grupach administracyjnych i Serwerach administracyjnych: można łatwo przełączać się między grupami i Serwerami z poziomu jednego panelu nawigacyjnego.
  - Ustawienia Twojego profilu przeniesiono do górnego panelu.
  - Nazwy niektórych sekcji menu głównego zostały zmienione:
    - Sekcja **Zasoby (Urządzenia)** nosi teraz nazwę **Zarządzanie zasobami**.
    - **Zarządzane urządzenia** nazywają się teraz **Zasoby (urządzenia)**.
    - **Szybkie odnośniki** zostały zmienione na **Poruszanie się po konsoli**.
  - W razie potrzeby można zminimalizować menu główne do ikon.
  - Sekcja **Aktualności Kaspersky** została usunięta z sekcji **Monitorowanie** → **Powiadomienia**.
- Filtry, które stosujesz do tabel w sekcjach **Operacje** → **Zarządzanie poprawkami** → **Luki w oprogramowaniu** oraz **Operacje** → **Zarządzanie poprawkami** → **Aktualizacje oprogramowania**, są teraz pomyślnie zapisywane i nie są resetowane.
- Kaspersky Security Center Linux współpracuje:
  - Z Kaspersky NGFW
  - Z następującymi wersjami systemu operacyjnego (dla zarządzanych urządzeń):
    - MosOS 15.5 Arbat
    - Microsoft Windows 11 25H2
    - CentOS 6.4
    - CentOS 6.6

Kaspersky Security Center 15.4 Linux w ramach licencji Kaspersky Next XDR Optimum

Jeśli aktywowałeś Serwer administracyjny w ramach licencji Kaspersky Next XDR Optimum i wdrożyłeś klucz licencyjny Kaspersky Next XDR Optimum w zarządzanych aplikacjach, możesz wykonać następujące czynności:

- Grupuj alerty według atrybutów.
- Skonfiguruj integracje w celu reagowania na zagrożenia.

Kaspersky Security Center 15.4 Linux

Kaspersky Security Center 15.4 Linux posiada kilka nowych funkcji i ulepszeń:

- Profile połączenia dla użytkowników mobilnych urządzeń z systemem Linux są już dostępne. Korzystając z profili połączeń, możesz skonfigurować reguły dla Agentów sieciowych na urządzeniach Linux, aby łączyły się z tym samym lub różnymi Serwerami administracyjnymi, w zależności od lokalizacji urządzenia.
- Przesyłanie kluczy szyfrowania pomiędzy Serwerami administracyjnymi jest teraz dostępne.
- Kaspersky Thin Client jest teraz obsługiwany.
- Wbudowany klaster o wysokiej dostępności Platform V Pangolin jest teraz obsługiwany.
- Wbudowany klaster o wysokiej dostępności Postgres Pro jest teraz obsługiwany. Węzły tego klastra DBMS są określane w parametrach połączenia w trakcie instalacji Kaspersky Security Center Linux.
- Kaspersky Security Center Linux obsługuje teraz pracę z następującymi systemami DBMS:
  - Platform V Pangolin 6.5.1
  - Tantor SE 1C dla Astra Linux Special Edition RUSB.10015-01 (aktualizacja operacyjna 1.8)
  - Jatoba 5
- Obsługa wersji 8.10.1, 9.0.1, 9.5.1 Platform V SberLinux OS Server (SLO).
- Archiwum KlAkOAPI.tar.gz zostało usunięte z Pomocy. Archiwum KlAkOAPI.tar.gz znajduje się w folderze instalacyjnym Kaspersky Security Center Linux.
- Przycisk **Skanuj** został usunięty z sekcji **Kwarantanna**.
- Informacje o rozmiarze, hash pliku i ścieżce nie są dostępne na liście pakietów instalacyjnych dla pakietu autonomicznego Agenta sieciowego ani dla żadnych pakietów utworzonych na wirtualnych Serwerach administracyjnych, ponieważ te pakiety autonomiczne są generowane w momencie pobierania.

Kaspersky Security Center 15.3 Linux

Kaspersky Security Center 15.3 Linux posiada kilka nowych funkcji i ulepszeń:

- Narzędzie klcsngtgui zostało usunięte z zestawu dystrybucyjnego Kaspersky Security Center Linux. Zalecamy używanie narzędzia klnagchk zamiast klcsngtgui.
- Agent sieciowy obsługuje teraz następujące nowe wersje systemów operacyjnych:
  - Windows Server 2025
  - Fedora Linux Server 41
  - Fedora Linux Workstation 41

- Kaspersky Security Center Linux obsługuje teraz pracę z następującymi systemami DBMS:
  - PostgreSQL 17
  - Postgres Pro 17
- Teraz możesz pobierać tylko wymagane aktualizacje baz danych i modułów oprogramowania dla aplikacji zabezpieczających Kaspersky, korzystając z Kaspersky Update Utility. W oknie właściwości zadania **Pobierz aktualizacje do repozytorium Serwera administracyjnego** włącz opcję **Pobierz plik żądania aktualizacji automatycznie**, a następnie określ ścieżkę, w której Kaspersky Security Center Linux utworzy plik żądania aktualizacji zawierający informacje o aktualizacjach, które mają zostać pobrane.
- Możliwość przeglądania statystyk wykorzystania serwera proxy KSN jest już dostępna.
- Zaktualizowano możliwość przenoszenia danych z Serwera administracyjnego Kaspersky Security Center Windows do Kaspersky Security Center Linux przy użyciu narzędzia klbackup. Teraz możesz przenieść dane Serwera administracyjnego przechowywane w bazie danych Microsoft SQL Server do bazy danych PostgreSQL lub Postgres Pro.
- Można teraz skonfigurować adres połączenia z Serwerem administracyjnym. Adres połączenia z Serwerem administracyjnym jest używany jako adres domyślny podczas tworzenia pakietów instalacyjnych Agenta sieciowego oraz jako adres serwera proxy KSN podczas łączenia zarządzanych urządzeń z KSN.
- Możesz teraz centralnie ponownie uruchamiać zarządzane urządzenia.
- Informacje o użytkownikach aktualnie zalogowanych na zarządzanym urządzeniu Linux są teraz wyświetlane w sekcji **Ogólne** → **Sesje** okna właściwości urządzenia.
- Możesz teraz uzyskać zdalny dostęp do zarządzanych urządzeń Linux i Windows za pośrednictwem Agenta sieciowego zainstalowanego na tych urządzeniach. Połączenie jest nawiązywane za pomocą protokołu RDP, VNC lub WDS. Po nawiązaniu połączenia z urządzeniem, administrator uzyskuje pełny dostęp do informacji przechowywanych na tym urządzeniu, dzięki czemu może zarządzać aplikacjami, które są na nim zainstalowane.
- Prześlij i uruchom aplikację (lub skrypt) do diagnostyki na zarządzanym urządzeniu. Możesz teraz przesłać katalog lub archiwum zawierające plik wykonywalny albo sam plik wykonywalny. Po pomyślnym uruchomieniu aplikacji możesz pobrać wyniki działania.
- Ulepszenia w zakresie użytkowania, w tym nowa sekcja **Szybkie odnośniki**. W tej sekcji wyświetlana jest mapa menu głównego, a także można uzyskać szybki dostęp do wszystkich sekcji Kaspersky Security Center Web Console. Domyślnie **Szybkie odnośniki** ustawione są jako strona główna.

Kaspersky Security Center 15.2 Linux

Kaspersky Security Center 15.2 Linux posiada kilka nowych funkcji i ulepszeń:

- Nowe funkcje zarządzania hasłami kont użytkowników wewnętrznych:
  - Teraz możesz wymusić na użytkowniku wewnętrznym zmianę hasła przy pierwszej (lub kolejnej) próbie zalogowania się do Kaspersky Security Center Web Console.
  - Nowa opcja umożliwiająca konfigurację okresu ważności hasła dla kont użytkowników wewnętrznych.

- Teraz możesz wykonać kopię zapasową danych Serwera administracyjnego Kaspersky Security Center Windows i przywrócić je w Kaspersky Security Center Linux, korzystając z narzędzia klbackup. Migrację można przeprowadzić bez utraty danych pomiędzy systemami DBMS tego samego typu lub Microsoft SQL Server → MySQL lub MariaDB.

- Kaspersky Security Center Linux obsługuje teraz pracę z następującymi systemami DBMS:

  - PostgreSQL 16.x

  - Postgres Pro 16.x

- Kaspersky Security Center Linux obsługuje teraz niektóre typy klastrów PostgreSQL i Postgres Pro.

- Wsparcie dla nowych systemów operacyjnych i nowych wersji systemów operacyjnych, w tym nowych wersji OS MES (Moscow Electronic School), MosTech i MosTech Server.

- Rozwiązania podwyższająca poziom komfortu użytkownika, w tym:

  - Nowy przycisk **Zapisz** w oknie ustawień zasad. Kliknij ten przycisk, jeśli chcesz zapisać zmiany bez zamykania okna ustawień zasad.

- Teraz możesz zarządzać wysyłaniem plików na urządzenia z systemem Android, usuwać wcześniej wysłane pliki i konfigurować ich ustawienia w nowej sekcji „Aplikacje i pliki" wtyczki zarządzającej Kaspersky Mobile Devices Protection and Management.

- Teraz możesz przesyłać pakiety instalacyjne aplikacji i profile zarządzania urządzeniami na urządzenia mobilne, nie łącząc ich bezpośrednio z Serwerem administracyjnym, korzystając z nowej usługi serwera sieciowego na bramie połączeń.

Kaspersky Security Center 15.1 Linux

Kaspersky Security Center 15.1 Linux posiada kilka nowych funkcji i ulepszeń:

- Kaspersky Security Center Web Console obsługuje teraz zarządzanie urządzeniami mobilnymi za pośrednictwem wtyczki zarządzającej Kaspersky Mobile Devices Protection and Management.

- Możesz teraz instalować i konfigurować serwery iOS MDM za pomocą wtyczki ustawień serwera iOS MDM, co pozwala na zarządzanie urządzeniami iOS MDM.

- Teraz możesz zarządzać certyfikatami urządzeń mobilnych.

- Kaspersky Endpoint Security for Android jest teraz obsługiwany.

- Kaspersky Security for iOS jest teraz obsługiwany.

- Kaspersky Endpoint Security for Aurora jest teraz obsługiwany.

- Zarządzanie lukami i poprawkami dla zarządzanych urządzeń z systemem Windows. Możesz zarządzać aktualizacjami oprogramowania innych firm zainstalowanymi na zarządzanych urządzeniach i naprawiać luki w zabezpieczeniach takiego oprogramowania poprzez instalację wymaganych aktualizacji.

- Kaspersky Security Center Linux przeszukuje teraz kontrolery domeny strona po stronie, zamiast przeszukiwać cały kontroler domeny na raz. Umożliwia to przeszukiwanie kontrolerów domeny zawierających dużą liczbę wpisów.

- Adaptacyjna kontrola anomalii. Jest to funkcja Kaspersky Endpoint Security for Windows, która wykorzystuje zestaw reguł do śledzenia nietypowych zachowań na urządzeniach klienckich i umożliwia blokowanie nieprawidłowych działań.

- Bezproblemowe aktualizacje zarządzanych aplikacji Kaspersky zainstalowanych na urządzeniach z systemem Windows i Agenta sieciowego dla systemu Linux. Możesz zarządzać procesem instalacji aktualizacji, zatwierdzając aktualizacje, których zainstalowanie jest obowiązkowe i odrzucając aktualizacje, których instalowanie jest zabronione.

- Rozszerzony audyt zasad. Możesz teraz wyświetlić treść rewizji zasad i zapisać ją w pliku. Obecnie te funkcje są dostępne tylko dla zasady Serwera administracyjnego i zasady Agenta sieciowego.

- Cloud Discovery. Jest to nowa funkcja, która pozwala monitorować korzystanie z usług w chmurze na zarządzanych urządzeniach z systemem Windows i blokować dostęp do niechcianych usług w chmurze.

- Nowa podsekcja **Alerty** w sekcji **Monitorowanie** menu głównego. W podsekcji **Alerty** możesz przejrzeć informacje dotyczące wykrytych zagrożeń na urządzeniach końcowych. Zagrożenia są wykrywane przez aplikacje zabezpieczające Kaspersky.

- Kaspersky Security Center Linux może teraz działać jako komponent rozwiązania Kaspersky Managed Detection and Response.

- Pomoc techniczna dla Kaspersky Security for Virtualization Light Agent

- Rozszerzona inwentaryzacja sprzętu urządzeń macOS. Agent sieciowy na urządzeniu z systemem macOS wysyła adres MAC i numer seryjny urządzenia do Serwera administracyjnego.

- W przypadku instalacji oprogramowania na zarządzanych urządzeniach za pomocą niestandardowych skryptów możesz teraz otrzymać raport dotyczący instalacji zdalnej.

- Jeśli wykonujesz kilka niestandardowych skryptów na zarządzanym urządzeniu, możesz ustawić priorytet dla każdego skryptu, aby określić kolejność wykonywania. Skrypty będą wykonywane od tego o najwyższym priorytecie do tego o najniższym priorytecie.

- Aby zmniejszyć ilość pamięci RAM zużywanej przez Kaspersky Endpoint Security for Linux i Agenta sieciowego dla systemu Linux, możesz włączyć specjalny tryb pracy dla Agenta sieciowego dla systemu Linux. W tym trybie Agent sieciowy dla systemu Linux wymaga mniej pamięci RAM, ale jego funkcjonalność jest ograniczona.

- Możesz odinstalować niekompatybilne oprogramowanie z zarządzanych urządzeń, korzystając z zadania *Zdalna dezinstalacja aplikacji*.

- Raport o atakach sieciowych zawiera teraz adres MAC i port atakującego urządzenia.

- Maksymalna długość hasła dla użytkownika wewnętrznego została zwiększona do 256 znaków.

- Rozwiązania podwyższająca poziom komfortu użytkownika, w tym:
  - Personalizacja menu głównego poprzez przypinanie sekcji Kaspersky Security Center Web Console w celu szybkiego dostępu z sekcji **Zakładki**.
  - Zoptymalizowana praca z tabelami. Domyślny widok każdej tabeli zawiera teraz najczęściej używane kolumny. Obecnie możesz zaznaczyć wszystkie elementy na bieżącej stronie lub w całej tabeli, a także posortować elementy w całej tabeli.
  - Lepsza konfiguracja funkcja dostarczania raportów. Możesz teraz określić maksymalnie 20 adresów e-mail, na które chcesz wysłać raport, oraz harmonogram dostarczania raportu.
- Obsługa szerokiej gamy systemów operacyjnych i nowych wersji systemów operacyjnych.
- Opracowano i opublikowano nowy poradnik dotyczący rozmiarów w pomocy online.
- W wyniku przeglądu interfejsu użytkownika rozwiązano problem, który powodował pojawianie się sekcji **Zdalna diagnostyka** w oknie właściwości Serwera administracyjnego.
- Możesz utworzyć zadanie *Zdalne wykonanie skryptu*, aby wykonać pakiet instalacyjny na urządzeniu klienckim i zdalnie zainstalować aplikację.
- Użytkownik może zostać przypisany jako właściciel urządzenia podczas lub po instalacji Agenta sieciowego na urządzeniu klienckim w systemie Linux.
- Można skonfigurować wybór urządzeń lub utworzyć regułę przenoszenia urządzeń na podstawie właściciela urządzenia, członkostwa właściciela urządzenia w grupie zabezpieczeń i roli właściciela urządzenia.
- Możesz wycofać uprawnienia administratora lokalnego z kont. Zapewnia to dodatkową warstwę kontroli nad kontami użytkowników. Można na przykład wycofać uprawnienia administratora lokalnego po zakończeniu jednorazowego przypisania.
- Możesz zmienić hasło do konta lokalnego, na przykład gdy użytkownik zapomni hasła do tego konta lub w celu wykonania zaplanowanej zmiany hasła.
- W podsekcji **Zarządzanie certyfikatami użytkownika** możesz określić, które certyfikaty główne mają zostać zainstalowane. Certyfikaty te mogą służyć np. do weryfikacji autentyczności stron internetowych czy serwerów internetowych.

Kaspersky Security Center 15 Linux

Kaspersky Security Center 15 Linux posiada kilka nowych funkcji i ulepszeń:

- Przeszukiwanie kontrolera domeny umożliwia przeszukiwanie kontrolera domeny Microsoft Active Directory i kontrolera domeny Samba. Do przeszukiwania Microsoft Active Directory możesz użyć Serwera administracyjnego lub punktu dystrybucji. Kontroler domeny Samba można przeszukiwać tylko za pośrednictwem punktu dystrybucji opartego na systemie Linux. Kiedy przeszukujesz kontroler domeny, Serwer administracyjny lub punkt dystrybucji pobiera informacje o strukturze domeny, kontach użytkowników, grupach zabezpieczeń i nazwach DNS urządzeń znajdujących się w domenie.

- Kaspersky Security Center Linux obsługuje teraz pracę z następującymi systemami DBMS:

  - PostgreSQL 15.x

  - Postgres Pro 15.x

- Jeśli używasz PostgreSQL lub Postgres Pro jako systemu DBMS, Kaspersky Security Center Linux obsługuje do 50 000 zarządzanych urządzeń.

- Migracja z Kaspersky Security Center Windows do Kaspersky Security Center Linux. Możesz uruchomić kreatora w celu migracji obiektów Kaspersky Security Center, w tym zadań, zasad i struktury grup administracyjnych. Następnie możesz przenieść zaimportowane zarządzane urządzenia, aby znalazły się pod zarządzaniem Kaspersky Security Center Linux.

- Kaspersky Security Center Linux obsługuje teraz pracę z następującymi aplikacjami Kaspersky:

  - Kaspersky Security for Virtualization Light Agent

  - Kaspersky Embedded Systems Security for Windows

  - Kaspersky Embedded Systems Security for Linux

  - Kaspersky Industrial CyberSecurity for Nodes

  - Kaspersky Industrial CyberSecurity for Networks

  - Kaspersky Endpoint Security for Mac

  - Kaspersky Endpoint Agent

  - Kaspersky Security for Virtualization Light Agent

- Zdalna diagnostyka zarządzanych urządzeń z systemem Windows i Linux.

- Ulepszony komponent Kontrola aplikacji. Możesz teraz utworzyć kategorię aplikacji w oparciu o listę plików wykonywalnych z wybranego folderu lub w oparciu o kategorię aplikacji Kaspersky. Następnie możesz określić, czy chcesz zezwolić, czy zablokować aplikacje z utworzonej kategorii w organizacji.

- Eksport i import wybranych wydarzeń. Możesz wyeksportować wybór zdarzeń zdefiniowany przez użytkownika i jego ustawienia do pliku KLO, a następnie zaimportować zapisany wybór zdarzeń do Kaspersky Security Center Windows lub Kaspersky Security Center Linux.

- W Raporcie o zagrożeniach możesz teraz otworzyć łańcuch rozprzestrzeniania się zagrożeń, klikając odnośnik **Wyświetl alert**.

- Kaspersky Security Center Linux obsługuje teraz technologię klastra. Jeśli grupa administracyjna zawiera klastry lub macierze serwerowe, na stronie **Zasoby (urządzenia)** są wyświetlane dwie zakładki — jedna dla poszczególnych urządzeń, a druga dla klastrów i macierzy serwerowych. Po wykryciu zarządzanych urządzeń jako węzłów klastra, klaster jest dodawany jako pojedynczy obiekt na karcie **Klastry i grupy serwerów**. Węzły klastra są wymienione na zakładce **Urządzenia** wraz z innymi zarządzanymi urządzeniami.

- Wsparcie dla niektórych platform przez Kaspersky Security Center Linux zostało zakończone, ponieważ platformy te nie są już obsługiwane przez ich dostawców.

Kaspersky Security Center 14.2 Linux

Kaspersky Security Center 14.2 Linux posiada kilka nowych funkcji i ulepszeń:

- W hierarchii Serwerów administracyjnych Serwer administracyjny oparty na systemie Linux może teraz działać jako Serwer podstawowy i może zarządzać Serwerami opartymi na systemie Linux lub Windows działającymi jako serwer pomocniczy.

- Kaspersky Security Center Linux obsługuje teraz Kaspersky Security Network (KSN), usługę KSN Proxy oraz Kaspersky Private Security Network (KPSN).

- Kaspersky Security Center Linux obsługuje teraz Kaspersky Endpoint Security for Windows jako aplikację zarządzaną.

  Zdalna instalacja Agenta sieciowego dla systemu Windows na urządzeniach klienckich jest możliwa tylko przy użyciu narzędzi systemu operacyjnego za pośrednictwem punktów dystrybucji opartych na systemie Windows.

- Dane na zarządzanych urządzeniach z systemem Windows można teraz szyfrować, aby zmniejszyć ryzyko niezamierzonego wycieku poufnych i firmowych danych w przypadku kradzieży lub zagubienia laptopa lub dysku twardego. Ta funkcja jest implementowana przez Kaspersky Endpoint Security for Windows.

- Kaspersky Security Center Linux umożliwia pobieranie i aktualizowanie zarówno pakietów dystrybucyjnych aplikacji Kaspersky, jak i webowych wtyczek administracyjnych bezpośrednio w interfejsie użytkownika Kaspersky Security Center Linux.

- Domyślnie informacje o aplikacjach zainstalowanych na urządzeniach zarządzanych z systemem Linux i Windows są wysyłane do Serwera administracyjnego.

- Dostęp do serwerów Kaspersky jest teraz weryfikowany automatycznie. Jeżeli dostęp do serwerów za pomocą systemowego DNS nie jest możliwy, aplikacja korzysta z publicznego DNS.

- Wrażliwe dane przesyłane między głównym Serwerem administracyjnym, podrzędnymi Serwerami administracyjnymi i Agentami sieciowymi są teraz chronione algorytmem szyfrowania AES.

- Uprawnienia użytkownika na wirtualnym Serwerze administracyjnym są dostępne do konfiguracji w dowolnym momencie niezależnie od podstawowego Serwera administracyjnego. Użytkownikom Serwera podstawowego można również przypisać prawa do zarządzania Serwerem wirtualnym.

- Kaspersky Security Center Linux obsługuje teraz pracę z następującymi systemami DBMS:
  - PostgreSQL 13.x
  - PostgreSQL 14.x
  - Postgres Pro 13.x (wszystkie wersje)
  - Postgres Pro 14.x (wszystkie wersje)
- Możesz użyć Kaspersky Security Center Web Console do wyeksportowania zasad i zadań do pliku, a następnie zaimportowania zasad i zadań do Kaspersky Security Center Windows lub Kaspersky Security Center Linux.
- Opcja **Nie używaj serwera proxy** została usunięta z następujących zadań:
  - *Pobierz aktualizacje do repozytorium Serwera administracyjnego*
  - *Pobierz aktualizacje do repozytoriów punktów dystrybucji*

Kaspersky Security Center 14 Linux

Kaspersky Security Center Linux posiada kilka nowych funkcji i ulepszeń:

- Oprócz zadania *Pobierz aktualizacje do repozytorium Serwera administracyjnego* antywirusowe bazy danych dla aplikacji zabezpieczających firmy Kaspersky można teraz pobierać za pomocą zadania *Pobierz aktualizacje do repozytoriów punktów dystrybucji*.
- Antywirusowe bazy danych i moduły aplikacji na zarządzanych urządzeniach mogą być propagowane i aktualizowane za pośrednictwem Serwera administracyjnego lub punktów dystrybucji. Możesz wybrać schemat aktualizacji optymalny dla Twojej organizacji, aby zmniejszyć obciążenie Serwera administracyjnego i zoptymalizować ruch danych w sieci firmowej.
- Kaspersky Security Center Linux pobiera z serwerów aktualizacji Kaspersky tylko te aktualizacje, których żądają aplikacje zabezpieczające firmy Kaspersky. Zmniejsza to rozmiar pobieranych danych.
- Możesz teraz używać funkcji plików diff do pobierania antywirusowych baz danych i modułów oprogramowania. Plik diff opisuje różnice między dwoma wersjami pliku bazy danych lub modułu programu. Użycie plików diff oszczędza ruch sieciowy w sieci firmowej, ponieważ pliki diff zajmują mniej miejsca niż całe pliki baz danych i modułów programu.
- Dodano zadanie *Weryfikacja aktualizacji*. Korzystając z tego zadania, możesz automatycznie sprawdzić pobrane aktualizacje pod kątem działania i błędów przed zainstalowaniem aktualizacji na zarządzanych urządzeniach.
- Kaspersky Security Center Linux obsługuje teraz Kaspersky Industrial CyberSecurity for Linux Nodes 1.3 jako aplikację zarządzaną.

Naprawione problemy

Poniższa tabela zawiera listę wszystkich problemów znalezionych w poprzednich wersjach Kaspersky Security Center Linux i naprawionych w obecnej wersji.

Lista problemów naprawionych w Kaspersky Security Center Linux 16.3

Wersja Kaspersky Security Center Linux, w której problem pojawił się po raz pierwszy	Identyfikator problemu	Opis problemu
16,2	9959974	Naprawiono problem, w wyniku którego karta **Zdarzenia** w oknie właściwości urządzenia zawierała opcję **Wybierz wszystkie**, która mogła usunąć wszystkie zdarzenia z bazy danych Serwera administracyjnego.
16,2	9392997	Naprawiono problem, w wyniku którego po pomyślnym odpytywaniu kontrolera domeny ALD Pro lub FreeIPA do dziennika zdarzeń dodawany był komunikat o błędzie.
16,2	9504495	Naprawiono problem, który mógł powodować nieprawidłowe przypisanie użytkownika, jeśli właściciel urządzenia został przypisany za pomocą parametrów pakietu instalacyjnego Agenta sieciowego.
16,1	9316206	Naprawiono problem, w wyniku którego przyciski sterujące mogły znikać z karty **Uwierzytelnianie dwuskładnikowe** podczas odświeżania przeglądarki po otwarciu tej karty.
16,1	7555541	Naprawiono problem powodujący niepowodzenie logowania do Web Console w przypadku włączenia opcji **Ustaw jako hasło jednorazowe (użytkownik musi zmienić hasło po pierwszym zalogowaniu)** podczas tworzenia zadania *Zmień hasło konta (tylko Linux)*.
15,4	7555788	Naprawiono problem, w wyniku którego zadanie *Zmień hasło konta* mogło nie działać prawidłowo, jeśli na urządzeniu użytkownika włączono SELinux.
16,2	9603496	Naprawiono problem, w wyniku którego konieczne było zainstalowanie Agenta sieciowego na urządzeniu Serwera administracyjnego w celu uzyskania informacji diagnostycznych dotyczących tego urządzenia.
16,2	9704308	Naprawiono problem, w wyniku którego otwarcie sekcji **Hierarchia grup** podczas ładowania strony w środowiskach z dużą liczbą grup administracyjnych mogło spowodować błąd `429 Too Many Requests`, przerwać połączenie z Serwerem administracyjnym i przekierować użytkowników na stronę logowania.
16,2	9989231	Naprawiono problem, w wyniku którego filtrowanie urządzeń według adresu IP połączenia mogło zwracać nieprawidłowe wyniki.
16,2	9990025	Naprawiono problem, w wyniku którego ustawienia widoku tabeli w sekcjach **Zasady** i **Zadania** nie były zachowywane podczas przechodzenia między stronami.
15,3	9632613	Naprawiono problem, w wyniku którego logowanie użytkownika domeny do Web Console mogło być znacznie opóźnione, gdy kontrolery domeny LDAP były niedostępne lub nie zawierały konta użytkownika.
15,1	9829027	Naprawiono problem, w wyniku którego skonfigurowanie filtra **Stan aktualizacji** w raporcie **Raport o używanych antywirusowych bazach danych** mogło spowodować błąd.
15,1	9844707	Kaspersky Security Center i FCM (Firebase Cloud Messaging) komunikowały się bezpośrednio, nawet jeśli skonfigurowano serwer proxy.

Lista problemów naprawionych w Kaspersky Security Center Linux 16.2

Wersja Kaspersky Security Center Linux, w której problem pojawił się po raz pierwszy	Identyfikator problemu	Opis problemu
15,1	10071566	Naprawiono problem, w wyniku którego zmiany wprowadzone w harmonogramie zadań nie były propagowane do zarządzanych urządzeń, jeśli w harmonogramie zastosowano ustawienie „Według dni tygodnia".
15,4	9067754	Naprawiono problem, który powodował nieprawidłowe wyświetlanie nowych zdarzeń we wcześniej utworzonej zasadzie po aktualizacji wtyczki Kaspersky Mobile Devices Protection and Management.
16	9329729	Naprawiono problem, który powodował pojawianie się błędu w Dzienniku zdarzeń aplikacji Kaspersky po aktualizacji Kaspersky Security Center Linux z wersji 16 do wersji 16.1, jeśli uwierzytelnianie dwuskładnikowe zostało skonfigurowane dla niektórych użytkowników przed aktualizacją.
16,1	9256000	Naprawiono problem, w którym informacje o komponentach zarządzanych aplikacji nie były dostępne, jeśli Agent sieciowy był zainstalowany w systemie Microsoft Windows XP.
16,1	9251629	Naprawiono problem, w wyniku którego niektóre wymagane nagłówki odpowiedzi HTTP nie były dodawane podczas logowania do Kaspersky Security Center Web Console.

Informacje o Kaspersky Security Center Linux

Sekcja zawiera informacje o przeznaczeniu Kaspersky Security Center Linux, jego głównych funkcjach i komponentach oraz sposobach zakupu Kaspersky Security Center Linux.

Kaspersky Security Center Linux (nazywany również Kaspersky Security Center) jest przeznaczony do wdrażania i zarządzania ochroną urządzeń klienckich przy użyciu Serwera administracyjnego opartego na systemie Linux.

Kaspersky Security Center Linux umożliwia instalację aplikacji zabezpieczających firmy Kaspersky na urządzeniach w sieci firmowej, zdalne uruchamianie zadań skanowania i aktualizacji oraz zarządzanie zasadami zabezpieczeń zarządzanych aplikacji. Jako Administrator, możesz użyć szczegółowego pulpitu nawigacyjnego, który zawiera migawkę stanów urządzeń firmowych, szczegółowe raporty i szczegółowe ustawienia w zasadach ochrony.

W porównaniu z Kaspersky Security Center, które posiada Serwer administracyjny oparty na systemie Windows®, Kaspersky Security Center Linux ma inny zestaw funkcji.

Kaspersky Security Center Linux jest aplikacją przeznaczoną dla administratorów sieci firmowych oraz dla pracowników odpowiedzialnych za ochronę urządzeń w różnych organizacjach.

Korzystając z Kaspersky Security Center, możesz:

- Utworzyć hierarchię Serwerów administracyjnych, aby zarządzać siecią firmy oraz sieciami odległych biur lub organizacji klienta.

  Organizacja klienta to organizacja, której ochrona antywirusowa jest zapewniana przez dostawcę usługi.

- Utworzyć hierarchię grup administracyjnych, aby zarządzać wyborem urządzeń klienckich jako całością.
- Zarządzać systemem ochrony antywirusowej zbudowanym w oparciu o aplikacje Kaspersky.
- Wykonywać zdalną instalację aplikacji Kaspersky i innych producentów oprogramowania.
- Wykonywać scentralizowane wdrażanie kluczy licencyjnych dla aplikacji Kaspersky na urządzenia klienckie, monitorowanie ich wykorzystania i odnawianie licencji.
- Otrzymywać statystyki i raporty dotyczące pracy aplikacji i urządzeń.
- Otrzymywać powiadomienia na temat zdarzeń krytycznych występujących podczas działania aplikacji Kaspersky.
- Zarządzaj szyfrowaniem informacji przechowywanych na dyskach twardych urządzeń z systemem Windows i dyskach wymiennych.
- Zarządzaj dostępem użytkowników do zaszyfrowanych danych na urządzeniach z systemem Windows.
- Wykonywać inwentaryzację sprzętu podłączonego do sieci firmy.
- Centralnie zarządzać plikami umieszczonymi w Kwarantannie lub Kopii zapasowej przez aplikacje zabezpieczające, a także zarządzać plikami, których przetwarzanie zostało odroczone.

Możesz kupić Kaspersky Security Center Linux za pośrednictwem Kaspersky (na przykład na stronie https://www.kaspersky.com) lub za pośrednictwem firm partnerskich.

Jeśli Kaspersky Security Center Linux zakupiono za pośrednictwem Kaspersky, możesz skopiować aplikację z naszej strony internetowej. Informacje wymagane do aktywacji aplikacji są wysyłane do Ciebie e-mailem po przetworzeniu płatności.

Aktualizuje funkcje (obejmuje aktualizacje sygnatur wirusów oraz aktualizacje bazy kodu), przy czym funkcja KSN może nie być dostępna w oprogramowaniu na terytorium Stanów Zjednoczonych.

Pakiet dystrybucyjny

Na stronie internetowej Kaspersky można pobrać wszystkie niezbędne pakiety dystrybucyjne aplikacji.

Zestaw dystrybucyjny Kaspersky Security Center Linux zawiera następujące pliki:

Serwer administracyjny Kaspersky Security Center Linux:

- Serwer administracyjny, który ma zostać zainstalowany na urządzeniu z systemem operacyjnym Debian:

  ksc64_16.3.0-<kompilacja>_amd64.deb

- Serwer administracyjny, który ma zostać zainstalowana na urządzeniu z systemem operacyjnym Red Hat Enterprise Linux:

  ksc64-16.3.0-<build>.x86_64.rpm

Kaspersky Security Center Web Console:

- Web Console, która ma zostać zainstalowana na urządzeniu z systemem operacyjnym Debian:

  ksc-web-console-16.3.<kompilacja>.x86_64.deb

- Web Console, która ma zostać zainstalowana na urządzeniu z systemem operacyjnym Red Hat Enterprise Linux:

  ksc-web-console-16.3.<kompilacja>.x86_64.rpm

Skrypt instalacyjny Kaspersky Security Center:

- ksc_fast_install.tar.gz

Agent sieciowy dla systemu Windows:

- Agent sieciowy do zainstalowania na urządzeniu z architekturą Arm:

  klnagent_winarm64-16.3.0.<build>-win_<localization>.zip

- Pliki do instalacji zdalnej Agenta sieciowego na urządzeniu z architekturą x86-32 lub x64:

  ksc_16_16.3.0.<kompilacja>_NetAgent_<lokalizacja>.zip

- Pliki do instalacji zdalnej Agenta sieciowego na urządzeniu z architekturą Arm:

  ksc_16_16.3.0.<build>_NetAgent_arm64_<localization>.zip

- Pliki do instalacji zdalnej za pośrednictwem Kaspersky Security Center na urządzeniu z architekturą Arm:

  ri_utils_arm64.zip

- Pliki do instalacji zdalnej za pośrednictwem Kaspersky Security Center na urządzeniu z architekturą x86-32 lub x64:

  ri_utils_win32.zip

Agent sieciowy dla systemu Linux:

- Agent sieciowy, który należy zainstalować na urządzeniu z systemem operacyjnym Debian:

  klnagent64_16.3.0-<kompilacja>_<architektura>.deb

- Agent sieciowy, który należy zainstalować na urządzeniu z systemem operacyjnym Red Hat Enterprise Linux:

  klnagent64-16.3.0-<build>_<architecture>.rpm

- Pliki do zdalnej instalacji Agenta sieciowego na urządzeniu z systemem operacyjnym Debian:

  klnagent-<architecture>-16.3.0.<build>-deb_<localization>.tar.gz

- Pliki do zdalnej instalacji Agenta sieciowego na urządzeniu z systemem operacyjnym Red Hat Enterprise Linux:

  klnagent-<architecture>-16.3.0.<build>-rpm_<localization>.tar.gz

- Pojedynczy pakiet dystrybucyjny do instalacji zdalnej Agentów sieciowych dla systemu Linux:

  klnagent-all-16.3.0.<build>-all_<localization>.tar.gz

  Pojedynczy pakiet dystrybucyjny może być przydatny, jeśli posiadasz wiele urządzeń klienckich o różnej architekturze procesora i różnych systemach operacyjnych opartych na systemie Linux. Wymagane wersje Agentów sieciowych zostaną automatycznie wybrane do dalszej instalacji na urządzeniach.

- Pliki do instalacji zdalnej Agenta sieciowego na urządzeniu ze starszym systemem operacyjnym opartym na Debianie lub Red Hat Enterprise Linux z biblioteką glibc 2.5:

  klnagent-all-16.3.0.<build>-glibc2.5-all-<localization>.tar.gz

Wtyczka webowa Kaspersky Endpoint Detection and Response Optimum:

- signed_irp.zip

  Możesz pobrać wtyczkę webową tylko z Repozytorium pakietów dystrybucyjnych aplikacji do instalacji zdalnej.

Jeśli masz trudności z wyborem pakietu instalacyjnego dla Agenta sieciowego dla systemu Linux, zapoznaj się z artykułem: Jak wybrać pakiet instalacyjny dla Agenta sieciowego dla systemu Linux.

Wymagania sprzętowe i programowe

- Wymagania Serwera administracyjnego
- Wymagania Web Console
- Wymagania Agenta sieciowego

Wymagania dotyczące wersji systemu Android i iOS w zakresie wdrażania ochrony i zarządzania urządzeniami mobilnymi można znaleźć w Pomocy dla Kaspersky Security for Mobile i Pomocy dla Kaspersky Secure Mobility Management.

Wymagania Serwera administracyjnego

Minimalne wymagania sprzętowe:

- Procesor o częstotliwości taktowania 2,5 GHz lub większej, 2 rdzenie.
- Pamięć RAM: 6 GB.

  Należy włączyć plik wymiany na urządzeniu z zainstalowanym Serwerem administracyjnym. Minimalny rozmiar pliku wymiany musi być 1,5 raza większy niż ilość pamięci RAM.
- Dostępne miejsce na dysku: 10 GB wymagane na folder, w którym przechowywane są dane Serwera administracyjnego (/var/opt/kaspersky/klnagent_srv).

Zalecamy, aby po zainstalowaniu Serwera administracyjnego na urządzeniu zainstalować na tym urządzeniu program Kaspersky Endpoint Security for Linux.
W przypadku instalacji jednoczesnej konieczne jest zapewnienie co najmniej 300 IOPS oraz zwiększenie wymagań Serwera administracyjnego o 1,5 GB pamięci RAM i 15% mocy procesora.
Informacje o wymaganiach sprzętowych Kaspersky Endpoint Security można znaleźć w Pomocy Kaspersky Endpoint Security for Linux.
Informacje o zalecanych minimalnych ustawieniach zabezpieczeń wymaganych do pracy z Serwerem administracyjnym można znaleźć w Pomocy Kaspersky Endpoint Security for Linux.

Obsługiwane są następujące systemy operacyjne:

Do komunikacji międzyprocesowej w systemie operacyjnym musi być dostępny interfejs pętli zwrotnej.

- Debian GNU/Linux 12 (Bookworm) 64-bitowy
- Debian GNU/Linux 13 (Trixie) 64-bitowy
- Ubuntu Server 22.04 LTS (Jammy Jellyfish) 64-bitowy
- Ubuntu Server 24.04 LTS (Noble Numbat) 64-bitowy
- Ubuntu Server 26.04 LTS (Resolute Raccoon) 64-bitowy
- CentOS Stream 9 64-bitowy
- CentOS Stream 10 64-bitowy
- Red Hat Enterprise Linux Server 7.x 64-bitowy
- Red Hat Enterprise Linux Server 8.x 64-bitowy
- Red Hat Enterprise Linux Server 9.x 64-bitowy
- Red Hat Enterprise Linux Server 10.x 64-bitowy
- SUSE Linux Enterprise Server 12 (wszystkie pakiety Service Pack) 64-bitowy

- SUSE Linux Enterprise Server 15 (wszystkie pakiety Service Pack) 64-bitowy
- Astra Linux Special Edition RUSB.10015-01 (aktualizacja operacyjna 1.6) 64-bitowy
- Astra Linux Special Edition RUSB.10015-01 (aktualizacja operacyjna 1.7) 64-bitowy
- Astra Linux Special Edition RUSB.10015-01 (aktualizacja operacyjna 1.8) 64-bitowy
- Astra Linux Special Edition RUSB.10015-16 (wydanie 1) (aktualizacja operacyjna 1.6) 64-bitowy
- Astra Linux Special Edition RUSB.10015-17 (aktualizacja operacyjna 1.7.3) 64-bitowy
- Astra Linux Special Edition RUSB.10015-03 (aktualizacja operacyjna 7.6) 64-bitowy
- Astra Linux Special Edition RUSB.10015-37 (aktualizacja operacyjna 7.7) 64-bitowy
- Astra Linux Common Edition (aktualizacja operacyjna 2.12) 64-bitowy
- ALT SP Server 10 64-bitowy
- ALT SP Workstation 10 64-bitowy
- Oracle Linux 7 64-bitowy
- Oracle Linux 8 64-bitowy
- Oracle Linux 9 64-bitowy
- Platform V SberLinux OS Server (SLO) 8.10.1 64-bitowy
- Platform V SberLinux OS Server (SLO) 9.5.1 64-bitowy
- Platform V SberLinux OS Server (SLO) 9.6 64-bitowy
- Platform V SberLinux OS Server (SLO) 9.7 64-bitowy
- RED OS 7.3 Server 64-bitowy
- RED OS 7.3 Certified Edition 64-bitowy
- RED OS 8 64-bitowy
- ROSA COBALT 7.9 64-bitowy
- M OS (Moscow Electronic School) 12 Server 64-bitowy
- Mostech Server 64-bitowy
- MosOS 15.5 Arbat 64-bitowy

Zalecamy używanie systemu plików EXT4 z jego ustawieniami domyślnymi.

Obsługiwane są następujące serwery baz danych (można zainstalować na innym urządzeniu):

- MySQL Standard Edition 8.0 (wersja 8.0.20 i nowsze) 32-bitowy/64-bitowy
- MySQL Enterprise Edition 8.0 (wersja 8.0.20 i nowsze) 32-bitowy/64-bitowy
- MySQL Standard Edition 8.4 32-bitowy/64-bitowy
- MySQL Enterprise Edition 8.4 32-bitowy/64-bitowy
- MariaDB 10.3 (kompilacja 10.3.22 i nowsze) 32-bitowe/64-bitowe
- MariaDB 10.4 (kompilacja 10.4.20 i nowsze) 32-bitowe/64-bitowe
- MariaDB 10.5 (kompilacja 10.5.27 i nowsze) 32-bitowe/64-bitowe
- MariaDB 10.6 (kompilacja 10.6.20 i nowsze) 32-bitowe/64-bitowe
- MariaDB 10.11 (kompilacja 10.11.10 i nowsze) 32-bitowe/64-bitowe
- MariaDB Galera Cluster 10.3 32-bitowy/64-bitowy z silnikiem magazynowania InnoDB
- PostgreSQL 13.x 64-bitowy
- PostgreSQL 14.x 64-bitowy
- PostgreSQL 15.x 64-bitowy
- PostgreSQL 15.x 64-bitowy (klaster Corosync/Pacemaker)
- PostgreSQL 16.x 64-bitowy
- PostgreSQL 17 64-bitowy
- PostgreSQL 18 64-bitowy
- Postgres Pro 13.x 64-bitowy (wszystkie wersje)
- Postgres Pro 14.x 64-bitowy (wszystkie wersje)
- Postgres Pro 15.x 64-bitowy (wszystkie wersje)
- Postgres Pro 15.x 64-bitowy (klaster Corosync/Pacemaker)
- Postgres Pro 16.x 64-bitowy (wszystkie wersje)
- Postgres Pro 16.x Enterprise 64-bitowy (wbudowany klaster o wysokiej dostępności)
- Postgres Pro 17 64-bitowy (wszystkie wersje)
- Postgres Pro 17 Enterprise 64-bitowy (wbudowany klaster o wysokiej dostępności)
- Postgres Pro 18 64-bitowy (wszystkie wersje)
- Postgres Pro 18 Enterprise 64-bitowy (wbudowany klaster o wysokiej dostępności)

- Platform V Pangolin 6.5.1 64-bitowa
- Platform V Pangolin 6.5.1 64-bitowa (wbudowany klaster o wysokiej dostępności)
- Jatoba 4 wersja 64-bitowa
- Jatoba 5 wersja 64-bitowa
- Tantor SE 1C 64-bitowy

Obsługiwane są klastry PostgreSQL o wysokiej dostępności. Aby uzyskać szczegółowe informacje, zapoznaj się z następującym artykułem: Przygotowanie klastra DBMS o wysokiej dostępności do pracy z Kaspersky Security Center Linux.

Informacje o obsługiwanych platformach wirtualizacji można znaleźć w Pomocy online Kaspersky Security for Virtualization Light Agent.

Wymagania Web Console

Kaspersky Security Center Web Console Server

Minimalne wymagania sprzętowe:

- Procesor: 2 rdzenie, częstotliwość taktowania wynosząca 2,5 GHz.
- Pamięć RAM: 4 GB.
- Dostępne miejsce na dysku: 40 GB wymagane na folder, w którym przechowywane są dane Web Console (/var/opt/kaspersky).

Zalecamy, aby po zainstalowaniu Kaspersky Security Center Web Console na urządzeniu zainstalować na nim Kaspersky Endpoint Security for Linux. Informacje o wymaganiach sprzętowych Kaspersky Endpoint Security można znaleźć w Pomocy Kaspersky Endpoint Security for Linux.

Jeden z następujących systemów operacyjnych (**tylko wersje 64-bitowe**):

> Do komunikacji międzyprocesowej w systemie operacyjnym musi być dostępny interfejs pętli zwrotnej.

- Debian GNU/Linux 12 (Bookworm)
- Debian GNU/Linux 13 (Trixie)
- Ubuntu Server 22.04 LTS (Jammy Jellyfish)
- Ubuntu Server 24.04 LTS (Noble Numbat)
- Ubuntu Server 26.04 LTS (Resolute Raccoon) 64-bitowy
- CentOS Stream 9

- CentOS Stream 10
- Red Hat Enterprise Linux Server 7.x
- Red Hat Enterprise Linux Server 8.x
- Red Hat Enterprise Linux Server 9.x
- Red Hat Enterprise Linux Server 10.x
- SUSE Linux Enterprise Server 12 (wszystkie pakiety Service Pack)
- SUSE Linux Enterprise Server 15 (wszystkie pakiety Service Pack)
- Astra Linux Special Edition RUSB.10015-01 (aktualizacja operacyjna 1.6)
- Astra Linux Special Edition RUSB.10015-16 (wydanie 1) (aktualizacja operacyjna 1.6)
- Astra Linux Special Edition RUSB.10015-01 (aktualizacja operacyjna 1.7)
- Astra Linux Special Edition RUSB.10015-17 (aktualizacja operacyjna 1.7.3)
- Astra Linux Special Edition RUSB.10015-01 (aktualizacja operacyjna 1.8)
- Astra Linux Special Edition RUSB.10015-03 (aktualizacja operacyjna 7.6)
- Astra Linux Special Edition RUSB.10015-37 (aktualizacja operacyjna 7.7)
- Astra Linux Common Edition (aktualizacja operacyjna 2.12)
- ALT SP Server 10
- ALT SP Workstation 10
- Oracle Linux 7
- Oracle Linux 8
- Oracle Linux 9
- Platform V SberLinux OS Server (SLO) 8.10.1
- Platform V SberLinux OS Server (SLO) 9.5.1
- Platform V SberLinux OS Server (SLO) 9.6 64-bitowy
- Platform V SberLinux OS Server (SLO) 9.7 64-bitowy
- RED OS 7.3 Server
- RED OS 7.3 Certified Edition
- RED OS 8
- ROSA COBALT 7.9

- M OS (Moscow Electronic School) 12 Server
- Mostech Server
- MosOS 15.5 Arbat

Informacje o obsługiwanych platformach wirtualizacji można znaleźć w Pomocy online Kaspersky Security for Virtualization Light Agent.

Urządzenia klienckie

W przypadku urządzenia klienckiego do korzystania z Kaspersky Security Center Web Console wymagana jest tylko przeglądarka internetowa.

Minimalna rozdzielczość ekranu wynosi 1366x768 pikseli.

Wymagania sprzętowe i programowe urządzenia są takie same, jak wymagania dotyczące przeglądarki używanej do pracy z Kaspersky Security Center Web Console.

Przeglądarki:

- Google Chrome w wersji 149.0.7827.115 lub nowszej
- Microsoft Edge w wersji 149.0.4022.62 lub nowszej
- Safari 18.6 (20621.3.11.11.3) w systemie macOS
- Przeglądarka Yandex w wersji 26.4.4.799 lub nowszej
- Wydłużone wsparcie techniczne Mozilla Firefox w wersji 140.11.0 lub nowszej

Wymagania Agenta sieciowego

Minimalne wymagania sprzętowe:

- Procesor o częstotliwości taktowania 1 GHz lub większej. W przypadku 64-bitowych systemów operacyjnych minimalna częstotliwość taktowania procesora to 1.4 GHz.
- Pamięć RAM: 512 MB.
- Dostępne miejsce na dysku: 1 GB.

Wymagania dotyczące oprogramowania dla urządzeń opartych na systemie Linux: musi być zainstalowany interpreter języka Perl w wersji 5.10 lub nowszej.

Agent sieciowy. Obsługiwane platformy

Systemy operacyjne. Stacje robocze Microsoft Windows	Microsoft Windows Embedded POSReady 2009 z najnowszym pakietem Service Pack 32-bitowy Microsoft Windows Embedded Standard 7 z dodatkiem Service Pack 1 32-bitowy/64-bitowy Microsoft Windows Embedded 8.1 Industry Pro 32-bitowy/64-bitowy Microsoft Windows 10 Enterprise 2015 LTSB 32-bitowy/64-bitowy Microsoft Windows 10 Enterprise 2016 LTSB 32-bitowy/64-bitowy Microsoft Windows 10 IoT Enterprise 2015 LTSB 32-bitowy/64-bitowy Microsoft Windows 10 IoT Enterprise 2016 LTSB 32-bitowy/64-bitowy Microsoft Windows 10 Enterprise 2019 LTSC 32-bitowy/64-bitowy Microsoft Windows 10 IoT Enterprise w wersji 1703, 1709, 1803, 1809, 32-bitowy/64-bitowy Microsoft Windows 10 20H2, 21H2 IoT Enterprise 32-bitowy/64-bitowy Microsoft Windows 10 IoT Enterprise 32-bitowy/64-bitowy Microsoft Windows 10 IoT Enterprise version 1909 32-bitowy/64-bitowy Microsoft Windows 10 IoT Enterprise LTSC 2021 32-bitowy/64-bitowy Microsoft Windows 10 IoT Enterprise version 1607 32-bitowy/64-bitowy Microsoft Windows 10 TH1 (lipiec 2015 r.) Home/Pro/Pro for Workstations/Enterprise/Education 32-bitowy/64-bitowy Microsoft Windows 10 TH2 (listopad 2015 r.) Home/Pro/Pro for Workstations/Enterprise/Education 32-bitowy/64-bitowy Microsoft Windows 10 RS1 (sierpień 2016 r.) Home/Pro/Pro for Workstations/Enterprise/Education 32-bitowy/64-bitowy Microsoft Windows 10 RS2 (kwiecień 2017 r.) Home/Pro/Pro for Workstations/Enterprise/Education 32-bitowy/64-bitowy Microsoft Windows 10 RS3 (Fall Creators Update, v1709) Home/Pro/Pro for Workstations/Enterprise/Education 32-bitowy/64-bitowy Microsoft Windows 10 RS4 (aktualizacja z kwietnia 2018 r., 17134) Home/Pro/Pro for Workstations/Enterprise/Education 32-bitowy/64-bitowy Microsoft Windows 10 RS5 (październik 2018 r.) Home/Pro/Pro for Workstations/Enterprise/Education 32-bitowy/64-bitowy Microsoft Windows 10 RS6 (maj 2019 r.) Home/Pro/Pro for Workstations/Enterprise/Education 64-bitowy Microsoft Windows 10 19H1, 19H2 Home/Pro/Pro for Workstations/Enterprise/Education 32-bitowy/64-bitowy Microsoft Windows 10 20H1 (aktualizacja z maja 2020 r.) Home/Pro/Pro for Workstations/Enterprise/Education 32-bitowy/64-bitowy Microsoft Windows 10 20H2 (aktualizacja z października 2020 r.) Home/Pro/Pro for Workstations/Enterprise/Education 32-bitowy/64-bitowy Microsoft Windows 10 21H1 (aktualizacja z maja 2021 r.) Home/Pro/Pro for Workstations/Enterprise/Education 32-bitowy/64-bitowy Microsoft Windows 10 21H2 (aktualizacja z października 2021 r.) Home/Pro/Pro for Workstations/Enterprise/Education 32-bitowy/64-bitowy Microsoft Windows 10 22H2 (aktualizacja z października 2023 r.) Home/Pro/Pro for Workstations/Enterprise/Education 32-bitowy/64-bitowy Microsoft Windows 11 Home/Pro/Pro for Workstations/Enterprise/Education ARM 64-bitowy Microsoft Windows 11 Home/Pro/Pro for Workstations/Enterprise/Education 64-bitowy Microsoft Windows 11 IoT Enterprise w wersji 25H2 64-bitowy Microsoft Windows 11 22H2 Home/Pro/Pro for Workstations/Enterprise/Education 64-bitowy Microsoft Windows 11 23H2 Home/Pro/Pro for Workstations/Enterprise/Education 64-bitowy Microsoft Windows 11 24H2 Home/Pro/Pro for Workstations/Enterprise/Education 64-bitowy Microsoft Windows 11 25H2 Home/Pro/Pro for Workstations/Enterprise/Education 64-bitowy Microsoft Windows 8.1 Pro/Enterprise 32-bitowy/64-bitowy Microsoft Windows 8 Pro/Enterprise 32-bitowy/64-bitowy Microsoft Windows 7 Professional/Enterprise/Ultimate/Home Basic/Premium z pakietem Service Pack 1 i nowszym, 32-bitowy/64-bitowy Microsoft Windows XP Professional z Service Pack 2 32-bit/64-bit (obsługiwany tylko przez Agenta sieciowego w wersji 10.5.1781) Microsoft Windows XP Professional z dodatkiem Service Pack 3 i nowszym 32-bitowym (obsługiwany przez Agenta sieciowego w wersji 14.0.0.20023, wymaga aktualizacji zabezpieczeń dla Windows XP KB2868626) Microsoft Windows XP Professional dla systemów wbudowanych z dodatkiem Service Pack 3 32-bit (obsługiwany przez Agenta sieciowego w wersji 14.0.0.20023)

Systemy operacyjne. Serwery Microsoft Windows	Microsoft Windows MultiPoint Server 2011 Standard/Premium 64-bitowy Microsoft Windows Server 2003 SP1 32-bitowy/64-bitowy (obsługiwany tylko przez Agenta sieciowego w wersji 10.5.1781, o który można poprosić za pośrednictwem pomocy technicznej) Microsoft Windows Server 2003 SP2 Standard/Enterprise 32-bitowy/64-bitowy (obsługiwany tylko przez Agenta sieciowego w wersji 10.5.1781) Microsoft Windows Server 2003 R2 Standard/Enterprise z dodatkiem SP2 32-bitowy/64-bitowy (obsługiwany tylko przez Agenta sieciowego w wersji 10.5.1781) Microsoft Windows Server 2008 Foundation z pakietem Service Pack 2 32-bitowy/64-bitowy Microsoft Windows Server 2008 Standard/Enterprise/Datacenter z pakietem Service Pack 2 32-bitowy/64-bitowy Microsoft Windows Server 2008 R2 Datacenter/Enterprise/Foundation/Standard z pakietem Service Pack 1 i nowszym 64-bitowy Microsoft Windows Server 2012 Server Core/Datacenter/Essentials/Foundation/Standard 64-bitowy Microsoft Windows Server 2012 R2 Server Core/Datacenter/Essentials/Foundation/Standard 64-bitowy Microsoft Windows Server 2016 Datacenter/Standard/Server Core (opcja instalacji) (LTSB) 64-bitowy Microsoft Windows Server 2019 Standard/Datacenter/Core 64-bitowy Microsoft Windows Server 2019 RS5 Essentials/Standard 64-bitowy Microsoft Windows Server 2022 Standard/Datacenter/Core 64-bitowy Microsoft Windows Server 2025 Standard/Datacenter/Core 64-bitowy Microsoft Windows Server 2022 21H2 Standard/Datacenter 64-bitowy Microsoft Windows Storage Server 2019 64-bitowy Microsoft Windows Small Business Server 2011 Standard 64-bitowy Microsoft Windows Small Business Server 2011 Essentials 64-bitowy Microsoft Windows Small Business Server 2011 Premium Add-on 64-bitowy

Systemy operacyjne. Linux	Debian GNU/Linux 10.x (Buster) 32-bitowy/64-bitowy Debian GNU/Linux 11.x (Bullseye) 32-bitowy/64-bitowy Debian GNU/Linux 12 (Bookworm) 32-bitowy/64-bitowy Debian GNU/Linux 13 (Trixie) 64-bitowy Ubuntu Server 10.04 LTS (Lucid Lynx) 32-bitowy/64-bitowy Ubuntu Server 16.04 LTS (Xenial Xerus) 32-bitowy/64-bitowy Ubuntu Server 18.04 LTS (Bionic Beaver) 64-bitowy Ubuntu Server 20.04 LTS (Focal Fossa) 64-bitowy Ubuntu Server 22.04 LTS (Jammy Jellyfish) 64-bitowy Ubuntu Server 22.04 LTS ARM 64-bitowy Ubuntu Server 24.04 LTS (Noble Numbat) 64-bitowy Ubuntu Server 26.04 LTS (Resolute Raccoon) 64-bitowy Ubuntu Server 26.04 LTS ARM 64-bitowy Ubuntu Desktop 10.04 LTS (Lucid Lynx) 32-bitowy/64-bitowy Ubuntu Desktop 16.04 LTS (Xenial Xerus) 32-bitowy/64-bitowy CentOS 5.2 32-bitowy/64-bitowy (obsługiwany wyłącznie przez Agenta sieciowego for Linux Legacy, którego można pobrać za pomocą interfejsu Web Console lub z witryny Kaspersky) CentOS 5.4 32-bitowy/64-bitowy (obsługiwany wyłącznie przez Agenta sieciowego for Linux Legacy, którego można pobrać za pomocą interfejsu Web Console lub z witryny Kaspersky) CentOS 6.4 32-bitowy/64-bitowy (obsługiwany wyłącznie przez Agenta sieciowego for Linux Legacy, którego można pobrać za pomocą interfejsu Web Console lub z witryny Kaspersky) CentOS 6.6 32-bitowy/64-bitowy (obsługiwany wyłącznie przez Agenta sieciowego for Linux Legacy, którego można pobrać za pomocą interfejsu Web Console lub z witryny Kaspersky) CentOS 7.2 i nowszy 64-bitowy CentOS Stream 8 64-bitowy CentOS Stream 9 64-bitowy CentOS Stream 9 ARM 64-bitowy CentOS Stream 10 64-bitowy Red Hat Enterprise Linux Server 6.x 32-bitowy/64-bitowy Red Hat Enterprise Linux Server 7.2 i nowszy 64-bitowy Red Hat Enterprise Linux Server 8.x 64-bitowy Red Hat Enterprise Linux Server 9.x 64-bitowy Red Hat Enterprise Linux Server 10.x 64-bitowy SUSE Linux Enterprise Server 12.5 i nowszy (wszystkie pakiety Service Pack) 64-bitowy SUSE Linux Enterprise Server 15 (wszystkie pakiety Service Pack) 64-bitowy SUSE Linux Enterprise Server 15 (wszystkie pakiety Service Pack) ARM 64-bitowy openSUSE Leap 15 64-bitowy EulerOS 2.0 SP10 64-bitowy EulerOS 2.0 SP10 ARM 64-bitowy Astra Linux Special Edition RUSB.10015-01 (aktualizacja operacyjna 1.4) 32-bitowy Astra Linux Special Edition RUSB.10015-01 (aktualizacja operacyjna 1.4) 64-bitowy (obsługiwany wyłącznie przez Agenta sieciowego dla systemu Linux Legacy, którego można pobrać za pomocą interfejsu Web Console lub z witryny internetowej Kaspersky) Astra Linux Special Edition RUSB.10015-01 (aktualizacja operacyjna 1.5), 64-bit Astra Linux Special Edition RUSB.10015-01 (aktualizacja operacyjna 1.6) 64-bitowy Astra Linux Special Edition RUSB.10015-16 (wydanie 1) (aktualizacja operacyjna 1.6) 64-bitowy Astra Linux Special Edition RUSB.10015-17 (aktualizacja operacyjna 1.7.3) 64-bitowy Astra Linux Special Edition RUSB.10015-01 (aktualizacja operacyjna 1.7) 64-bitowy Astra Linux Special Edition RUSB.10015-01 (aktualizacja operacyjna 1.8) 64-bitowy Astra Linux Special Edition RUSB.10015-03 (aktualizacja operacyjna 7.6) 64-bitowy Astra Linux Special Edition RUSB.10015-37 (aktualizacja operacyjna 7.7) 64-bitowy Astra Linux Special Edition RUSB.10152-02 (aktualizacja operacyjna 4.7) ARM 64-bitowy Astra Linux Common Edition (aktualizacja operacyjna 2.12) 64-bitowy ALT Workstation 11 64-bitowy ALT Server 11 64-bitowy ALT Education 11 64-bitowy ALT Workstation 10.1 64-bitowy

ALT Server 10.1 64-bitowy
ALT Education 10.1 64-bitowy
ALT SP Server 10 32-bit/64-bitowy
ALT SP Server 10 ARM 64-bitowy
ALT SP Workstation 10 32-bit/64-bitowy
ALT SP Workstation 10 ARM 64-bitowy
ALT 8 SP Server (LKNV.11100-01) 32-bitowy/64-bitowy
ALT 8 SP Server (LKNV.11100-02) 32-bitowy/64-bitowy
ALT 8 SP Server (LKNV.11100-03) 32-bitowy/64-bitowy
ALT 8 SP Workstation (LKNV.11100-01) 32-bitowy/64-bitowy
ALT 8 SP Workstation (LKNV.11100-02) 32-bitowy/64-bitowy
ALT 8 SP Workstation (LKNV.11100-03) 32-bitowy/64-bitowy
Oracle Linux 7 64-bitowy
Oracle Linux 8 64-bitowy
Oracle Linux 9 64-bitowy
Linux Mint 21.1 i nowsze wersje 64-bitowe
Linux Mint 22.x 64-bitowy
AlterOS 7.5 i nowszy 64-bitowy
AlterOS 2025 64-bitowy
GosLinux IC6/7.17 64-bitowy
GosLinux IC6/7.2 64-bitowy
SberOS 3.4.0 64-bitowy
SberOS 3.5.0 64-bitowy
SberOS 3.6.1 64-bitowy
Platform V SberLinux OS Server (SLO) 8.10.1 64-bitowy
Platform V SberLinux OS Server (SLO) 9.1 64-bitowy
Platform V SberLinux OS Server (SLO) 9.5.1 64-bitowy
Platform V SberLinux OS Server (SLO) 9.6 64-bitowy
Platform V SberLinux OS Server (SLO) 9.7 64-bitowy
RED OS 7.3 Server 64-bitowy
RED OS 7.3 Certified Edition 64-bitowy
RED OS 8 64-bitowy
RED OS 8 ARM 64-bitowy
ROSA Enterprise Linux Server 7.9 64-bitowy
ROSA Enterprise Linux Desktop 7.9 64-bitowy
ROSA COBALT 7.9 64-bitowy
ROSA CHROME 12 64-bitowy
AlmaLinux 8 i nowszy 64-bitowy
AlmaLinux 9 i nowszy 64-bitowy
Rocky Linux 8 i nowszy 64-bitowy
Rocky Linux 9 i nowszy 64-bitowy
Atlant, kompilacja Alcyone, wersja 2022.02 64-bitowy
MSVSPHERE 9.2 SERVER 64-bitowy
MSVSPHERE 9.2 ARM 64-bitowy
MSVSPHERE SERVER 9.4 64-bitowy
MSVSPHERE 9.4 ARM 64-bitowy
SynthesisM Server 8.6 64-bitowy
SynthesisM Client 8.6 64-bitowy
OSnova 2.* 64-bitowy
OSnova 3.* 64-bitowy
Kylin 10 64-bitowy
EMIAS 1.0 64-bitowy
Amazon Linux 2 64-bitowy
MosOS 15.5 Arbat 64-bitowy
OS MES (Moscow Electronic School) 12 (dla komputerów i laptopów) 64-bitowy
OS MES (Moscow Electronic School) 12 (dla paneli interaktywnych) 64-bitowy

	M OS (Moscow Electronic School) 12 Server 64-bitowy Mostech 64-bitowy Mostech Server 64-bitowy Fedora Linux Server 41 64-bitowy Fedora Linux Workstation 41 64-bitowy
Systemy operacyjne. macOS	Listę obsługiwanych systemów operacyjnych znajdziesz w Pomocy Kaspersky Endpoint Security for Mac.
Platformy wirtualizacji	Informacje o obsługiwanych platformach wirtualizacji można znaleźć w Pomocy online Kaspersky Security for Virtualization Light Agent.

W wersjach systemu Windows starszych niż Microsoft Windows Server 2008 R2 (wersje serwerowe) i Microsoft Windows 7 (wersje na komputery stacjonarne) Agent sieciowy nie obsługuje następujących funkcji:

- Ponowna translacja aktualizacji (używana przez punkty dystrybucji)
- Serwer proxy KSN (używany przez punkty dystrybucji)
- Zadanie wykrywania luk w zabezpieczeniach

Na urządzeniach działających pod kontrolą systemu Microsoft Windows 10 w wersji RS4 lub RS5, Kaspersky Security Center może nie wykrywać niektórych luk w folderach, w których włączono uwzględnianie wielkości liter.

Przed zainstalowaniem Agenta sieciowego na urządzeniach z systemem Windows 7, Windows Server 2008, Windows Server 2008 R2 lub Windows MultiPoint Server 2011 upewnij się, że została zainstalowana aktualizacja zabezpieczeń KB3063858 dla systemu operacyjnego Windows (Aktualizacja zabezpieczeń dla systemu Windows 7 (KB3063858), Aktualizacja zabezpieczeń dla systemu Windows 7 dla komputerów z procesorem x64 (KB3063858), Aktualizacja zabezpieczeń dla systemu Windows Server 2008 (KB3063858), Aktualizacja zabezpieczeń dla systemu Windows Server 2008 x64 Edition (KB3063858), Aktualizacja zabezpieczeń dla systemu Windows Server 2008 R2 x64 Edition (KB3063858)).

W Microsoft Windows XP Agent sieciowy może nie wykonać niektórych działań poprawnie.

Możesz zainstalować lub zaktualizować Agenta sieciowego dla Windows XP tylko w systemie Microsoft Windows XP. Obsługiwane edycje systemu Microsoft Windows XP i odpowiadające im wersje Agenta sieciowego są wymienione na liście obsługiwanych systemów operacyjnych. Z tej strony możesz pobrać wymaganą wersję Agenta sieciowego dla systemu Microsoft Windows XP.

Zalecamy zainstalowanie tej samej wersji Agenta sieciowego dla systemu Linux, co Kaspersky Security Center Linux.

Kaspersky Security Center Linux w pełni obsługuje Agenta sieciowego w tej samej lub nowszej wersji.

Agent sieciowy dla systemu macOS jest dostarczany wraz z aplikacją zabezpieczającą Kaspersky dla tego systemu operacyjnego.

Kompatybilne aplikacje i rozwiązania Kaspersky

Kaspersky Security Center Linux obsługuje scentralizowane wdrażanie i zarządzanie wszystkimi aplikacjami i rozwiązaniami firmy Kaspersky, które są obecnie obsługiwane. Aby poznać wersje aplikacji i rozwiązań, odwiedź stronę internetową zawierającą czas trwania wsparcia technicznego aplikacji.

Obsługiwane aplikacje Kaspersky:

- Kaspersky Endpoint Security for Windows (obsługuje serwery plików):
- Kaspersky Endpoint Security for Linux (obsługuje serwery plików)
- Kaspersky Endpoint Security for Linux Elbrus Edition
- Kaspersky Endpoint Security for Mac
- Kaspersky Endpoint Security for Android
- Kaspersky Endpoint Security for Aurora
- Kaspersky Security for iOS
- Kaspersky Industrial CyberSecurity for Linux Nodes
- Kaspersky Industrial CyberSecurity for Nodes
- Kaspersky Industrial CyberSecurity for Networks
- Kaspersky Endpoint Agent
- Kaspersky Embedded Systems Security for Windows
- Kaspersky Embedded Systems Security for Linux
- Kaspersky Security for Virtualization Light Agent
- KATA Sandbox (jeden ze składników Kaspersky Anti Targeted Attack Platform)
- Kaspersky Thin Client
- Kaspersky NGFW
- Kaspersky Sandbox
- Kaspersky Password Manager for Business
- Kaspersky Vulnerability Management

Kaspersky Security Center Linux jest zawarty w następujących rozwiązaniach:

- Kaspersky Endpoint Detection and Response Optimum
- Kaspersky Managed Detection and Response
- Kaspersky Next XDR Optimum

Zapoznaj się ze stroną internetową dotyczącą cyklu wsparcia technicznego produktów dla wersji aplikacji.

Znane problemy

Pojedyncze logowanie (SSO) nie jest obsługiwane w Kaspersky Industrial CyberSecurity for Networks.

Informacje o kompatybilności składników Kaspersky Security Center Linux

W poniższej tabeli znajdziesz informacje dotyczące kompatybilności składników Kaspersky Security Center Linux.

Kompatybilność składników Kaspersky Security Center Linux

Moduł	Kompatybilny z
Serwer administracyjny Kaspersky Security Center 16.3 Linux	• Kaspersky Security Center Web Console w następujących wersjach: 16.3, 16.2, 16.1 • Agent sieciowy Kaspersky Security Center w następujących wersjach: 16.3, 16.2, 16.1, 16, 15.4, 15.3, 15.2, 15.1, 15, 14*, 10.5**
Kaspersky Security Center 16.3 Web Console	Serwer administracyjny Kaspersky Security Center Linux w następujących wersjach: 16.3, 16.2, 16.1, 16
Główny Serwer administracyjny Kaspersky Security Center 16.3 Linux	Podrzędne Serwery administracyjne: • Kaspersky Security Center Linux w następujących wersjach: 16.3, 16.2, 16.1, 16, 15.4, 15.3, 15.2, 15.1, 15 • Kaspersky Security Center Windows w następujących wersjach: 15.1
Podrzędny Serwer administracyjny Kaspersky Security Center 16.3 Linux	Główny Serwery administracyjny: • Kaspersky Security Center Linux w następujących wersjach: 16.3, 16.2, 16.1, 16, 15.4, 15.3, 15.2, 15.1, 15 • Kaspersky Security Center Windows w następujących wersjach: 15.1
Agent sieciowy Kaspersky Security Center 16.3	Serwery administracyjne: • Kaspersky Security Center Linux w następujących wersjach: 16.3, 16.2, 16.1, 16, 15.4, 15.3, 15.2, 15.1, 15 • Kaspersky Security Center Windows w następujących wersjach: 15.1
Tworzenie kopii zapasowej i przywracanie danych Serwera administracyjnego Kaspersky Security Center	Tworzenie kopii zapasowej i przywracanie danych jest obsługiwane przez następujące wersje Serwera administracyjnego Kaspersky Security Center Linux: 16.2, 16.1, 16, 15.4, 15.3, 15.2, 15.1, 15

*Ta wersja obsługuje system Microsoft Windows XP Professional z dodatkiem Service Pack 3. Możesz pobrać tę wersję Agenta sieciowego z tej strony.

**Ta wersja obsługuje system Microsoft Windows XP Professional z dodatkiem Service Pack 2. Możesz poprosić o tę wersję Agenta sieciowego za pośrednictwem Pomocy technicznej.

Zalecamy korzystanie z najnowszej wersji Serwera administracyjnego Kaspersky Security Center i Kaspersky Security Center Web Console. W przeciwnym razie funkcjonalność Kaspersky Security Center może być ograniczona. Możesz niezależnie zainstalować i uaktualnić Serwer administracyjny Kaspersky Security Center i Kaspersky Security Center Web Console. W takim przypadku, musisz upewnić się, że wersja zainstalowanej konsoli Kaspersky Security Center Web Console jest zgodna z wersją Serwera administracyjnego, z którym się łączysz.

Jeśli posiadasz najnowszą wersję Kaspersky Security Center Web Console i poprzednią wersję Kaspersky Security Center i podczas uwierzytelniania domeny wystąpi błąd, tekst błędu będzie zawierał domyślny komunikat.

Porównanie Kaspersky Security Center: opartego na systemie Windows i opartego na systemie Linux

Kaspersky dostarcza Kaspersky Security Center jako rozwiązanie lokalne dla dwóch platform — Windows i Linux. W rozwiązaniu opartym na systemie Windows Serwer administracyjny jest instalowany na urządzeniu z systemem Windows, a rozwiązanie oparte na systemie Linux ma wersję Serwera administracyjnego zaprojektowaną do zainstalowania na urządzeniu z systemem Linux. Ta pomoc online zawiera informacje o Kaspersky Security Center. Szczegółowe informacje na temat rozwiązania opartego na systemie Windows można znaleźć w Pomocy online Kaspersky Security Center Windows.

Poniższa tabela umożliwia porównanie głównych funkcji Kaspersky Security Center jako rozwiązania opartego na systemie Windows i jako rozwiązania opartego na systemie Linux.

Porównanie funkcji Kaspersky Security Center działającego jako rozwiązanie oparte na systemie Windows i rozwiązanie oparte na systemie Linux

Funkcja lub właściwość	Kaspersky Security Center 15.1 Windows	Kaspersky Security Center 16.3 Linux
Serwer administracyjny		
Lokalizacja systemu zarządzania bazą danych (DBMS)	Lokalnie	Lokalnie (Microsoft SQL nie jest obsługiwany)
System operacyjny do zainstalowania Serwera administracyjnego	Windows	Linux
Hierarchia Serwerów administracyjnych	✓	✓
Obsługa wirtualnych Serwerów administracyjnych	✓	✓
Wdrażanie klastra trybu failover Kaspersky Security Center	✓ Dotyczy to tylko klastra jednolokalizacyjnego	✓ Począwszy od wersji 16.2 Kaspersky Security Center Linux, geograficznie rozproszony klaster trybu failover jest obsługiwany
Używanie SNMP do wysyłania statystyk Serwera administracyjnego do aplikacji innych firm	✓	✓
Serwer sieciowy do publikowania pakietów instalacyjnych i innych plików	✓	✓
Konsola administracyjna		
Typ Konsoli administracyjnej	Oparte na MMC i oparte na sieci Web	Internetowe

Funkcja lub właściwość	Kaspersky Security Center 15.1 Windows	Kaspersky Security Center 16.3 Linux
System operacyjny do zainstalowania konsoli administracyjnej opartej na sieci Web	Windows lub Linux	Linux
Zaloguj się do konsoli, korzystając z uwierzytelniania domeny	✓	✓
Zarządzanie urządzeniami klienckimi i grupami administracyjnymi		
Maksymalna liczba zarządzanych urządzeń (na jeden Serwer administracyjny)	100 000 (z Microsoft SQL Server)	50 000 (z PostgreSQL i Postgres Pro)
Przeszukiwanie sieci	✓	✓
Ochrona urządzeń zarządzanych przez systemy Windows, macOS i Linux	✓	✓
Ochrona urządzeń mobilnych	✓ Podstawowe zarządzanie urządzeniami mobilnymi	✓ MDM i korzystanie z funkcjonalności Kaspersky Secure Mobility Management (w ramach licencji)
Zarządzenie ochroną maszyn wirtualnych	✓	✓
Ochrona infrastruktury chmury publicznej	✓	—
Zdalne połączenie z pulpitem urządzenia klienckiego	✓	✓
Szyfrowanie i ochrona danych	✓ (Na zarządzanych urządzeniach z systemem Windows, na których zainstalowano Kaspersky Endpoint Security for Windows lub Kaspersky Endpoint Security for Mac)	✓ (Na zarządzanych urządzeniach z systemem Windows, na których zainstalowano Kaspersky Endpoint Security for Windows lub Kaspersky Endpoint Security for Mac)
Wsparcie klastrów i macierzy serwerów w grupach administracyjnych	✓	✓
Hierarchia Grupy administracyjnej	✓	✓
Dodawanie bramy połączenia w strefie DMZ jako punktu dystrybucji	✓ (nieobsługiwane w przypadku Web Console)	✓
Praca z użytkownikami		
Tworzenie i zarządzanie kontami użytkowników	✓	✓
Zarządzanie aplikacjami Kaspersky		
Zasady aplikacji	✓	✓
Zadania dla aplikacji Kaspersky	✓	✓
Kaspersky Security Network	✓	✓
KSN Proxy	✓	✓
Kaspersky Private Security Network	✓	✓
Scentralizowane wdrażanie kluczy licencyjnych dla aplikacji Kaspersky	✓	✓
Zdalna diagnostyka urządzeń klienckich	✓	✓
Automatyczna aktualizacja aplikacji Kaspersky	✓	✓
Obsługa adaptacyjnej kontroli anomalii	✓	✓
Zarządzanie bezpieczeństwem zorientowane na urządzenie	✓	✓
Zarządzanie bezpieczeństwem zorientowane na użytkownika	✓	✓
Zarządzanie systemami		

Funkcja lub właściwość	Kaspersky Security Center 15.1 Windows	Kaspersky Security Center 16.3 Linux
Wdrażanie systemów operacyjnych na urządzeniach klienckich	✓	—
Zarządzanie licencjami stron trzecich	✓	Do wdrożenia w 2026 roku
Używanie Serwera administracyjnego jako serwera WSUS	✓	✓ (tylko w trybie pasywnego wyszukiwania w usłudze Windows Update)
Zarządzanie aplikacjami firm trzecich na urządzeniach klienckich		
Instalowanie aktualizacji oprogramowania innych firm i usuwanie luk w zabezpieczeniach oprogramowania innych firm	✓	✓
Importowanie i eksportowanie kategorii aplikacji	✓ (nieobsługiwane w przypadku Web Console)	Do wdrożenia w 2026 roku
Monitorowanie, raportowanie i audyt		
Zarządzanie rewizjami obiektów	✓	✓
Porównanie rewizji zasad	✓	✓
Wyświetlanie i praca z alertami wykrytymi przez Kaspersky Endpoint Detection and Response Optimum	✓	✓
Powiadomienia o zdarzeniach, które wystąpiły na zarządzanych urządzeniach	✓	✓
Monitorowanie statusu zasad i status zadań	✓	✓
Integracje		
Integracja z Kaspersky Managed Detection and Response	✓	✓
Integracja z systemami SIEM	✓	✓
Agregowanie alertów i wykonywanie działań reagowania za pośrednictwem usługi Active Directory, KASAP i Kaspersky TIP Sandbox	—	✓ (Musisz aktywować Serwer administracyjny w ramach licencji Kaspersky Next XDR Optimum, a następnie zainstalować klucz licencyjny Kaspersky Next XDR Optimum w zarządzanych aplikacjach)

Informacje o Kaspersky Next Expert View

Używanie Kaspersky Security Center jako lokalnej aplikacji oznacza zainstalowanie Kaspersky Security Center, w tym Serwera administracyjnego, na urządzeniu lokalnym i zarządzanie systemem ochrony sieci za pośrednictwem Konsoli administracyjnej opartej o konsolę Microsoft Management Console (dostępnej wyłącznie w Kaspersky Security Center Windows) lub Kaspersky Security Center Web Console.

Jednakże możesz użyć Kaspersky Security Center jako usługi w chmurze. W tym przypadku Kaspersky Security Center jest instalowany i utrzymywany dla Ciebie przez ekspertów z Kaspersky w środowisku chmury, a Kaspersky zapewnia dostęp do Serwera administracyjnego jako usługi. Systemem ochrony sieci zarządzasz za pośrednictwem działającej w chmurze Konsoli administracyjnej o nazwie Kaspersky Next Expert View. Ta konsola posiada interfejs podobny do interfejsu Kaspersky Security Center Web Console.

Interfejs i dokumentacja Kaspersky Next Expert View są dostępne w następujących językach:

- angielskim
- francuskim

- niemieckim
- włoskim
- japońskim
- portugalskim (Brazylijski)
- rosyjskim
- Chiński uproszczony
- hiszpańskim
- hiszpańskim (LATAM)
- Chiński tradycyjny

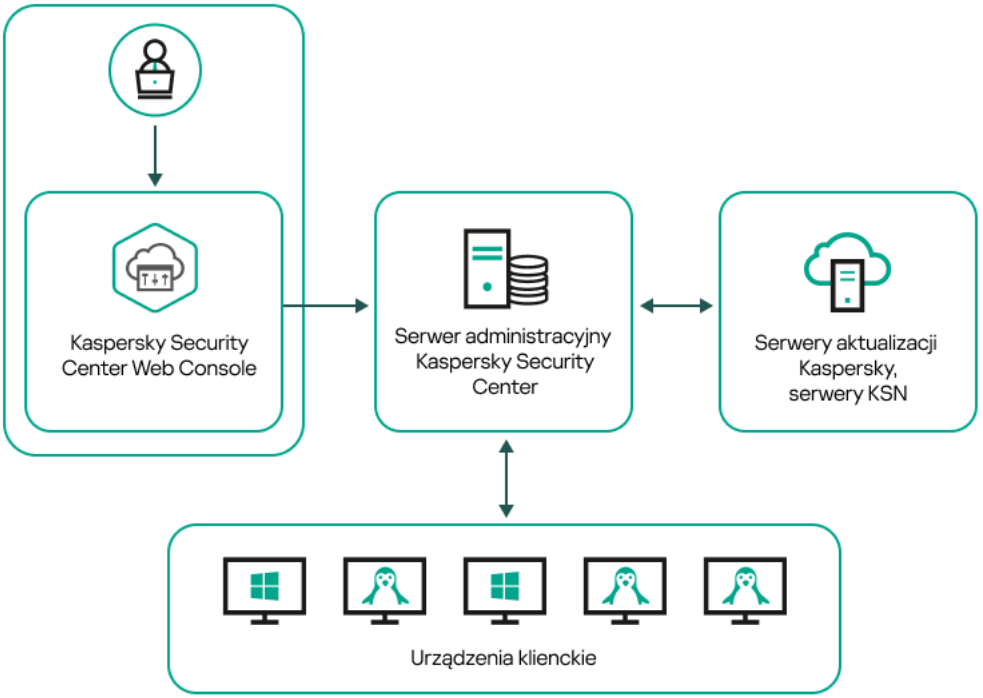
Więcej informacji o Kaspersky Next Expert View i jego funkcjach można znaleźć w dokumentacji Kaspersky Next Expert View oraz w dokumentacji Kaspersky Endpoint Security for Business.

Architektura i podstawowe pojęcia

W tej sekcji wyjaśniono architekturę aplikacji i podstawowe pojęcia związane z oprogramowaniem Kaspersky Security Center Linux.

Architektura

Ta sekcja zawiera opis komponentów Kaspersky Security Center i ich interakcji.



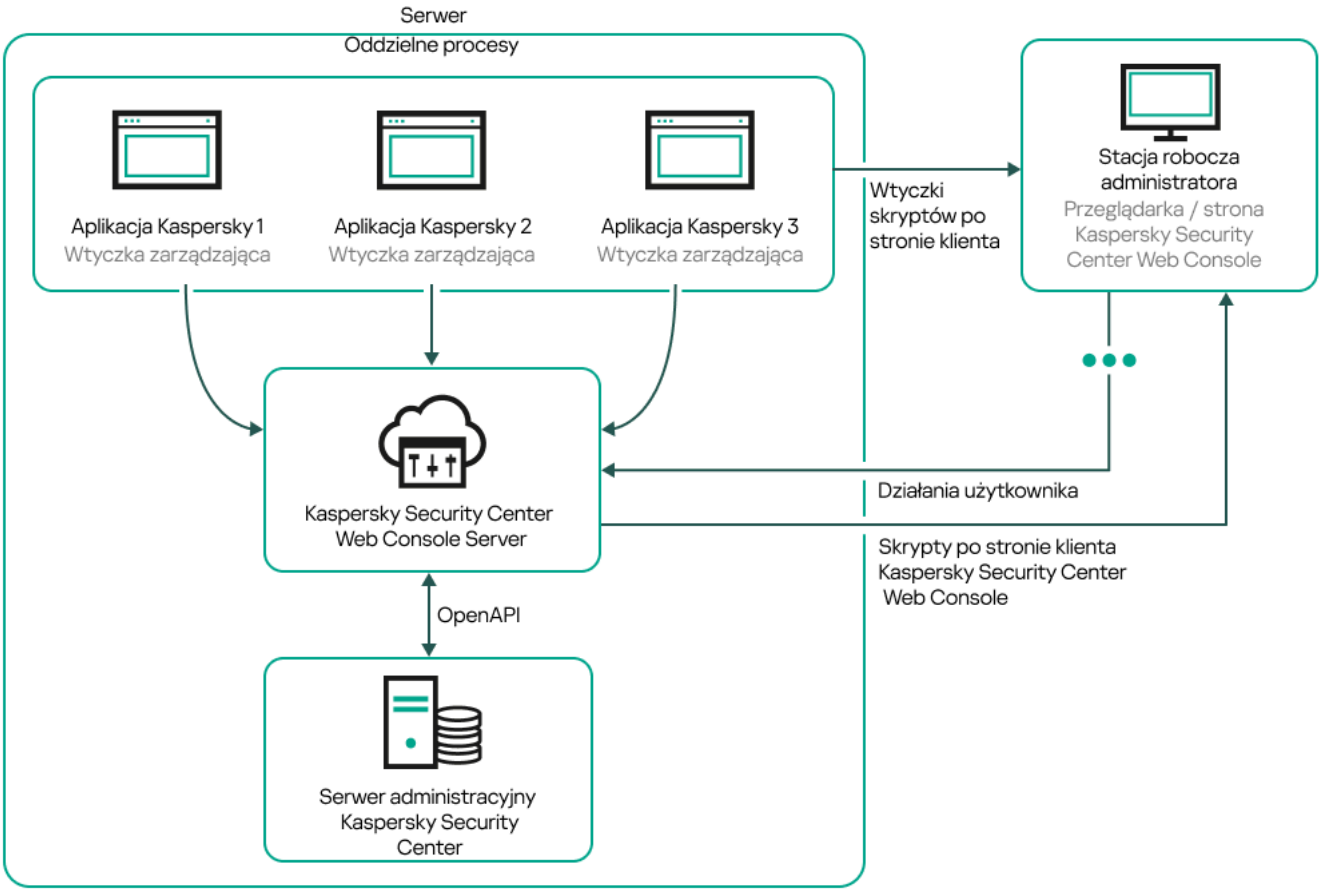
Architektura Kaspersky Security Center Linux

Kaspersky Security Center Linux zawiera następujące główne składniki:

- **Kaspersky Security Center Web Console**. Oferuje interfejs webowy do tworzenia i utrzymania systemu ochrony sieci organizacji klienta zarządzanej przez Kaspersky Security Center.
- **Serwer administracyjny Kaspersky Security Center** (zwany również *Serwer*). Scentralizowane repozytorium informacji dotyczących aplikacji zainstalowanych w sieci firmowej oraz informacji dotyczących sposobu zarządzania tymi aplikacjami.
- **Serwery aktualizacji Kaspersky**. Serwery HTTP(S) firmy Kaspersky, z których aplikacje Kaspersky pobierają uaktualnienia baz danych i modułów aplikacji.
- **Serwery KSN**. Serwery, które zawierają bazę danych firmy Kaspersky, zawierającej ciągle aktualizowane informacje o reputacji plików, zasobach sieciowych oraz oprogramowaniu. Kaspersky Security Network zapewnia przyspieszenie czasu odpowiedzi aplikacji Kaspersky po wykryciu zagrożenia, ulepszenie działania niektórych składników ochrony oraz zmniejszenie ryzyka wystąpienia fałszywych alarmów.
- **Urządzenia klienckie.** Urządzenia klienckie firmy chronione przez Kaspersky Security Center Linux. Każde urządzenie, które musi być chronione, musi posiadać zainstalowaną jedną z aplikacji zabezpieczających Kaspersky.

Schemat wdrożenia Serwera administracyjnego Kaspersky Security Center Linux i konsoli Kaspersky Security Center Web Console

Rysunek poniżej przedstawia schemat wdrożenia Serwera administracyjnego Kaspersky Security Center Linux i konsoli Kaspersky Security Center Web Console.



Schemat wdrożenia Serwera administracyjnego Kaspersky Security Center Linux i konsoli Kaspersky Security Center Web Console

Wtyczki administracyjne dla aplikacji Kaspersky zainstalowanych na chronionych urządzeniach (jedna wtyczka dla każdej aplikacji) są wdrażane razem z Kaspersky Security Center Web Console Server.

Jako administrator uzyskujesz dostęp do Kaspersky Security Center Web Console przy użyciu przeglądarki na swojej stacji roboczej.

Jeśli wykonujesz określone działania w Kaspersky Security Center Web Console, Kaspersky Security Center Web Console Server komunikuje się z serwerem administracyjnym Kaspersky Security Center Linux poprzez interfejs OpenAPI. Kaspersky Security Center Web Console Server żąda wymaganych informacji z serwera administracyjnego Kaspersky Security Center Linux i wyświetla wyniki Twoich działań w Kaspersky Security Center Web Console.

Porty używane przez Kaspersky Security Center Linux

Poniższe tabele przedstawiają domyślne porty używane przez Serwer administracyjny i urządzenia klienckie. Jeśli chcesz, możesz zmienić każdy z tych domyślnych numerów portów.

Porty używane przez Serwer administracyjny Kaspersky Security Center Linux

Numer portu	Nazwa procesu, który otwiera port	Protokół	Przeznaczenie portu	Obszar
8060	klcsweb	TCP	Przesyłanie opublikowanych pakietów instalacyjnych na urządzenia klienckie	Publikowanie pakietów instalacyjnych. Możesz zmienić numer domyślnego portu w sekcji **Serwer WWW** w oknie właściwości Serwera administracyjnego. Ten parametr jest opcjonalny. Ze względów bezpieczeństwa zalecamy używanie portu TCP 8061.
8061	klcsweb	TCP (TLS)	Przesyłanie opublikowanych pakietów instalacyjnych na urządzenia klienckie	Publikowanie pakietów instalacyjnych. Możesz zmienić numer domyślnego portu w sekcji **Serwer WWW** w oknie właściwości Serwera administracyjnego.
13000	klserver	TCP (TLS)	Odbieranie połączeń od Agentów sieciowych i podrzędnych Serwerów administracyjnych; używany także na podrzędnych Serwerach administracyjnych do odbierania połączeń od głównego Serwera administracyjnego (na przykład, jeśli podrzędny Serwer administracyjny znajduje się w strefie DMZ)	Zarządzanie urządzeniami klienckimi i podrzędnymi Serwerami administracyjnymi. Możesz zmienić numer domyślnego portu do odbierania połączeń od Agentów sieciowych podczas konfigurowania portów połączeń podczas instalacji Kaspersky Security Center Linux; możesz zmienić numer domyślnego portu do odbierania połączeń z podrzędnych Serwerów administracyjnych podczas tworzenia hierarchii Serwerów administracyjnych.
13000	klserver	UDP	Pobieranie informacji o urządzeniach, które zostały wyłączone, z Agentów sieciowych	Zarządzanie urządzeniami klienckimi. Możesz zmienić numer domyślnego portu w ustawieniach zasady Agenta sieciowego.
13291	klserver	TCP (TLS)	Korzystanie z narzędzia klakaut w celu zautomatyzowania działania Kaspersky Security Center Linux	Praca z narzędziem klakaut. Narzędzie klakaut i jego system pomocy znajdują się w folderze instalacyjnym Kaspersky Security Center Linux. Ten port jest domyślnie zamknięty. Jeśli chcesz użyć narzędzia klakaut w celu zautomatyzowania działania Kaspersky Security Center Linux, otwórz port 13291 przy użyciu narzędzia klscflag.
13299	klserver	TCP (TLS)	Odbieranie połączeń od Menadżera tożsamości i dostępu (IAM) do Serwera administracyjnego; odbieranie połączeń do Serwera administracyjnego poprzez OpenAPI	Zarządzanie Serwerem administracyjnym przy użyciu Kaspersky Security Center Web Console; praca z OpenAPI. Domyślny numer portu można zmienić w oknie właściwości Serwera administracyjnego (w podsekcji **Porty połączeń** w sekcji **Ogólne**) lub podczas tworzenia hierarchii Serwerów administracyjnych.

Numer portu	Nazwa procesu, który otwiera port	Protokół	Przeznaczenie portu	Obszar
14000	klserver	TCP	Odbieranie połączeń od Agentów sieciowych	Zarządzanie urządzeniami klienckimi. Możesz zmienić numer domyślnego portu podczas konfigurowania portów połączeń podczas instalacji Kaspersky Security Center Linux lub podczas ręcznego łączenia urządzenia klienckiego z Serwerem administracyjnym. Ten port jest opcjonalny i domyślnie jest zamknięty. Ze względów bezpieczeństwa zalecamy używanie portu TCP 13000.
13111 (tylko wtedy, gdy usługa KSN proxy jest uruchomiona na urządzeniu)	ksnproxy	TCP	Odbieranie żądań od zarządzanych urządzeń do serwera KSN proxy	Serwer KSN proxy. Możesz zmienić numer domyślnego portu w oknie właściwości Serwera administracyjnego.
15111 (tylko wtedy, gdy usługa KSN proxy jest uruchomiona na urządzeniu)	ksnproxy	UDP	Odbieranie żądań od zarządzanych urządzeń do serwera KSN proxy	Serwer KSN proxy. Możesz zmienić numer domyślnego portu w oknie właściwości Serwera administracyjnego.
17111 (tylko wtedy, gdy usługa KSN proxy jest uruchomiona na urządzeniu)	ksnproxy	HTTPS	Odbieranie żądań od zarządzanych urządzeń do serwera KSN proxy	Serwer KSN proxy. Możesz zmienić numer domyślnego portu w oknie właściwości Serwera administracyjnego.
17000	klactprx	TCP (TLS)	Odbieranie połączeń dla aktywacji aplikacji od zarządzanych urządzeń	Aktywacja przy użyciu serwera proxy dla zarządzanych urządzeń. Możesz zmienić numer domyślnego portu w oknie właściwości Serwera administracyjnego (w podsekcji **Dodatkowe porty** sekcji **Ogólne**).
13292 (tylko wtedy, gdy zarządzasz urządzeniami mobilnymi)	klserver	TCP (TLS)	Obieranie połączeń od urządzeń mobilnych	Zarządzanie urządzeniami mobilnymi. Możesz zmienić numer domyślnego portu w oknie właściwości Serwera administracyjnego w Konsoli administracyjnej lub w konsoli Kaspersky Security Center Web Console.
19170	klserver	HTTPS (TLS)	Tunelowanie połączeń z zarządzanymi urządzeniami przy użyciu narzędzia klsctunnel	Zdalne nawiązywanie połączenia z zarządzanymi urządzeniami przy użyciu Kaspersky Security Center Web Console. Domyślny numer portu można zmienić w oknie właściwości Serwera administracyjnego (**Ogólne** → **Porty połączenia** → **Tunelowanie połączenia RDP**).
4444	kliam	HTTPS	Uwierzytelnianie przy użyciu protokołu OpenID Connect	Wymiana tokenów uwierzytelniających między przeglądarką a Menedżerem tożsamości i dostępu (IAM).
9050	kliam	HTTPS	Połączenie z Serwerem administracyjnym przy użyciu IAM	Wymiana tokenów uwierzytelniania między Kaspersky Security Center Web Console a IAM.

Jeśli instalujesz Serwer administracyjny i bazę danych na różnych urządzeniach, musisz udostępnić potrzebne porty na urządzeniu, na którym znajduje się baza danych (na przykład: port 3306 dla MariaDB). Odpowiednie informacje można znaleźć w dokumentacji do DBMS.

Poniższa tabela wyświetla port, który musi zostać otwarty na serwerze iOS™ MDM Server (tylko wtedy, gdy zarządzasz urządzeniami mobilnymi).

Port używany przez serwer iOS MDM

Numer portu	Nazwa procesu, który otwiera port	Protokół	Przeznaczenie portu	Obszar
443	kliosmdmservicesrv	TCP (TLS)	Obieranie połączeń od urządzeń mobilnych iOS	Zarządzanie urządzeniami mobilnymi. Możesz zmienić numer domyślnego portu podczas instalowania serwera iOS MDM.

Poniższa tabela wyświetla port, który musi zostać otwarty na serwerze Kaspersky Security Center Web Console Server. To może być to samo urządzenie, na którym jest zainstalowany Serwer administracyjny, lub inne urządzenie.

Port używany przez Kaspersky Security Center Web Console Server

Numer portu	Nazwa procesu, który otwiera port	Protokół	Przeznaczenie portu	Obszar
8080	Node.js: Server-side JavaScript	TCP (TLS)	Odbieranie połączeń z przeglądarki do Kaspersky Security Center Web Console	Kaspersky Security Center Web Console. Podczas instalacji Kaspersky Security Center Web Console możesz zmienić domyślny numer portu. Jeśli instalujesz konsolę Kaspersky Security Center Web Console w systemie operacyjnym Linux ALT, musisz określić numer portu inny niż 8080, ponieważ port 8080 jest używany przez system operacyjny.

Poniższa tabela wyświetla port, który musi być otwarty na zarządzanych urządzeniach, na których jest zainstalowany Agent sieciowy.

Porty używane przez Agenta sieciowego

Numer portu	Nazwa procesu, który otwiera port	Protokół	Przeznaczenie portu	Obszar
15000	klnagent	UDP	Sygnały zarządzania z Serwera administracyjnego lub punktów dystrybucji do Agentów sieciowych	Zarządzanie urządzeniami klienckimi. Możesz zmienić numer domyślnego portu w ustawieniach zasady Agenta sieciowego.
15000	klnagent	Transmisja UDP	Uzyskiwanie danych o innych Agentach sieciowych w obrębie tej samej domeny broadcastowej (dane są następnie wysyłane do Serwera administracyjnego)	Dostarczanie uaktualnień i pakietów instalacyjnych.
15001	klnagent	UDP	Odbieranie żądań multiemisji z punktu dystrybucji (jeśli jest używany)	Odbieranie aktualizacji i pakietów instalacyjnych z punktu dystrybucji. Możesz zmienić numer domyślnego portu w oknie właściwości punktu dystrybucji.
30522, 30523 (porty na interfejsie localhost)	klnagent	TCP	Przesyłanie aktualizacji aplikacji z Agenta sieciowego do lokalnie zainstalowanych aplikacji Kaspersky przy użyciu komponentu FileTransferBridge	Zarządzane urządzenia, które otrzymują aktualizacje aplikacji Kaspersky z Serwera administracyjnego określonego jako źródło aktualizacji bazy danych.

Należy pamiętać, że proces klnagent może również żądać wolnych portów z dynamicznego zakresu portów systemu operacyjnego punktu końcowego. Porty te są automatycznie przydzielane procesowi klnagent przez system operacyjny, więc proces klnagent może korzystać z niektórych portów używanych przez inne oprogramowanie. Jeśli proces klnagent wpływa na działanie tego oprogramowania, zmień ustawienia portu w tym oprogramowaniu lub zmień domyślny dynamiczny zakres portów w systemie operacyjnym, aby wykluczyć port używany przez oprogramowanie, którego dotyczy problem.

Należy również wziąć pod uwagę, że zalecenia dotyczące kompatybilności Kaspersky Security Center Linux z oprogramowaniem innych firm zostały opisane wyłącznie w celach informacyjnych i mogą nie mieć zastosowania do nowych wersji oprogramowania innych firm. Opisane zalecenia dotyczące konfiguracji portów zostały oparte na doświadczeniach działu pomocy technicznej i naszych najlepszych praktykach.

Poniższa tabela wyświetla porty, które muszą być otwarte na zarządzanym urządzeniu z zainstalowanym Agentem sieciowym pełniącym rolę punktu dystrybucji. Wymienione porty muszą być otwarte na urządzeniach punktu dystrybucji oprócz portów używanych przez Agentów sieciowych (patrz tabela powyżej).

Porty używane przez Agenta sieciowego pełniącego rolę punktu dystrybucji

Numer portu	Nazwa procesu, który otwiera port	Protokół	Przeznaczenie portu	Obszar
13000	klnagent	TCP (TLS)	Odbieranie połączeń z Agentów sieciowych i bram połączeń	Zarządzanie urządzeniami klienckimi, dostarczanie uaktualnień i pakietów instalacyjnych. Możesz zmienić numer domyślnego portu we właściwościach punktu dystrybucji.
13111 (tylko wtedy, gdy usługa KSN proxy jest uruchomiona na urządzeniu)	ksnproxy	TCP	Odbieranie żądań od zarządzanych urządzeń do serwera KSN proxy	Serwer KSN proxy. Możesz zmienić numer domyślnego portu we właściwościach punktu dystrybucji.
15111 (tylko wtedy, gdy usługa KSN proxy jest uruchomiona na urządzeniu)	ksnproxy	UDP	Odbieranie żądań od zarządzanych urządzeń do serwera KSN proxy	Serwer KSN proxy. Możesz zmienić numer domyślnego portu we właściwościach punktu dystrybucji.
17111 (tylko wtedy, gdy usługa KSN proxy jest uruchomiona na urządzeniu)	ksnproxy	HTTPS	Odbieranie żądań od zarządzanych urządzeń do serwera KSN proxy	Serwer KSN proxy. Możesz zmienić numer domyślnego portu we właściwościach punktu dystrybucji.
13295 (tylko wtedy, gdy używasz punktu dystrybucji jako serwera push)	klnagent	TCP (TLS)	Obieranie połączeń od urządzeń klienckich	Serwer push. Możesz zmienić numer domyślnego portu we właściwościach punktu dystrybucji.
8060	klcsweb	TCP	Przesyłanie opublikowanych pakietów instalacyjnych na urządzenia klienckie	Publikowanie pakietów instalacyjnych. Możesz zmienić numer domyślnego portu w Sekcji **Serwer WWW** w oknie właściwości Serwera administracyjnego.
8061	klcsweb	TCP (TLS)	Przesyłanie opublikowanych pakietów instalacyjnych na urządzenia klienckie	Publikowanie pakietów instalacyjnych. Możesz zmienić numer domyślnego portu w Sekcji **Serwer WWW** w oknie właściwości Serwera administracyjnego.

Poniższa tabela przedstawia porty używane na urządzeniu kontrolera domeny.

Porty używane na urządzeniu kontrolera domeny

Numer portu	Protokół	Przeznaczenie portu	Obszar
389	LDAP przez TCP lub UDP	Łączenie z serwerem LDAP	Przeszukiwanie kontrolera domeny
636	LDAP przez TLS	Łączenie z serwerem LDAP	Przeszukiwanie kontrolera domeny

Poniższa tabela zawiera port, który musi być otwarty na urządzeniach klienckich, na których jest zainstalowany Agent sieciowy.

Port używany na nieprzypisanym urządzeniu klienckim

Numer portu	Protokół	Przeznaczenie portu	Obszar
22	SSH	Łączenie się z urządzeniem klienckim przez SSH	Instalacja zdalna aplikacji Kaspersky.

Porty używane przez Kaspersky Security Center Web Console

W tabeli poniżej przedstawiono porty, które muszą być otwarte na urządzeniu, na którym jest zainstalowany Kaspersky Security Center Web Console Server (zwany również Kaspersky Security Center Web Console).

Porty używane przez Kaspersky Security Center Web Console

Numer portu	Nazwa usługi	Protokół	Przeznaczenie portu	Obszar
2001	Kaspersky Security Center Product Plugins Server	HTTPS	Port API, który jest używany przez procesy wtyczki zarządzającej do otrzymywania żądań z „Usługi zarządzania Kaspersky Security Center Web Console".	Uruchamianie procesów node wtyczek zarządzania
1329, 2003	Usługa zarządzania Kaspersky Security Center Web Console	HTTPS	Porty API, które są używane do otrzymywania żądań z „Usługi zarządzania Kaspersky Security Center Web Console" działającej na tym samym urządzeniu.	Aktualizowanie składników Kaspersky Security Center Web Console
2005	Kaspersky Security Center Web Console	HTTPS	Port API, który jest używany do otrzymywania żądań z „Usługi zarządzania Kaspersky Security Center Web Console" działającej na tym samym urządzeniu.	Uruchamianie procesów node Kaspersky Security Center Web Console
8200	—	HTTP	Port API, który jest używany do generowania certyfikatów przy użyciu magazynu HashiCorp Vault (więcej informacji znajdziesz na stronie internetowej HashiCorp Vault).	Instalowanie Kaspersky Security Center Web Console i aktualizowanie składników Kaspersky Security Center Web Console
4222	Kaspersky Security Center Web Console Server NATS	HTTPS	Porty API brokera komunikatów opartego na NATS, które są używane do komunikacji między procesami Kaspersky Security Center Web Console oraz wtyczek zarządzających. Port 8222 służy do monitorowania NATS.	Interakcja Kaspersky Security Center Web Console i wtyczek administracyjnych
4444	Menedżer tożsamości i dostępu (IAM)	HTTPS	Port używany przez protokół uwierzytelniania OpenID Connect.	Wymiana tokenów uwierzytelniających między Kaspersky Security Center Web Console a Menedżerem tożsamości i dostępu (IAM)
9050	IAM	HTTPS	Port używany przez IAM.	Interakcja pomiędzy Kaspersky Security Center Web Console a IAM

Podstawowe pojęcia

W tej sekcji wyjaśniono podstawowe pojęcia związane z Kaspersky Security Center Linux.

Serwer administracyjny

Komponenty Kaspersky Security Center Linux umożliwiają zdalne zarządzanie aplikacjami firmy Kaspersky zainstalowanymi na urządzeniach klienckich.

Urządzenia z zainstalowanym komponentem Serwer administracyjny będą nazywane *Serwerami administracyjnymi* (zwane również *Serwerami*). Serwery administracyjne muszą być chronione, włączając w to ochronę fizyczną, przed wszelkim nieautoryzowanym dostępem.

Serwer administracyjny jest instalowany na urządzeniu jako usługa z następującym zestawem atrybutów:

- O nazwie `kladminserver_srv`
- Ustawiony do automatycznego uruchamiania po załadowaniu systemu operacyjnego
- Posiada konto `ksc` lub konto użytkownika wybrane podczas instalacji Serwera administracyjnego

Pełną listę ustawień instalacji można znaleźć w następującym artykule: Instalacja Kaspersky Security Center Linux.

Serwer administracyjny pełni następujące funkcje:

- Przechowuje strukturę grup administracyjnych
- Przechowuje informacje o konfiguracji urządzeń klienckich
- Organizuje repozytoria dla pakietów dystrybucyjnych aplikacji
- Służy do zdalnej instalacji aplikacji na urządzeniach klienckich oraz do usuwania aplikacji
- Aktualizuje bazy danych i moduły aplikacji firmy Kaspersky
- Zarządza zasadami i zadaniami na urządzeniach klienckich
- Przechowuje informacje o zdarzeniach, które wystąpiły na urządzeniach klienckich
- Generuje raporty z działania aplikacji Kaspersky
- Wdraża klucze licencyjne na urządzenia klienckie oraz przechowuje informacje o kluczach licencyjnych
- Wysyła komunikaty o postępie zadań (na przykład o wykryciu wirusów na urządzeniu klienckim)

Nadawanie nazw Serwerom administracyjnym w interfejsie aplikacji

W interfejsie użytkownika konsoli Kaspersky Security Center Web Console Serwery administracyjne mogą posiadać następujące nazwy:

- Nazwę urządzenia z Serwerem administracyjny, na przykład: „*nazwa_urządzenia*" lub „Serwer administracyjny: *nazwa_urządzenia*".
- Adres IP urządzenia z Serwerem administracyjny, na przykład: „*adres_IP*" lub „Serwer administracyjny: *adres_IP*".
- Podrzędne Serwery administracyjne i wirtualne Serwery administracyjne posiadają niestandardowe nazwy, które określasz podczas podłączania wirtualnego lub podrzędnego Serwera administracyjnego do głównego Serwera administracyjnego.
- Jeśli używasz konsoli Kaspersky Security Center Web Console zainstalowanej na urządzeniu z systemem Linux, aplikacja wyświetli nazwy Serwerów administracyjnych, które zostały określone jako zaufane w pliku odpowiedzi.

Możesz nawiązać połączenie z Serwerem administracyjnym poprzez Kaspersky Security Center Web Console.

Hierarchia Serwerów administracyjnych

Serwery administracyjne można zorganizować w hierarchię. Każdy Serwer administracyjny może mieć kilka podrzędnych Serwerów administracyjnych (zwanych *Serwerami podrzędnymi*) na różnych poziomach zagnieżdżenia w obrębie hierarchii. Poziom zagnieżdżenia Serwerów podrzędnych nie jest ograniczony. Grupy administracyjne głównego Serwera administracyjnego będą obejmować urządzenia klienckie wszystkich podrzędnych Serwerów administracyjnych. Z tego powodu odizolowane i niezależne sekcje sieci mogą być zarządzane przez różne Serwery administracyjne, które z kolei są zarządzane przez Serwer główny.

W hierarchii serwer administracyjny oparty na systemie Linux może działać zarówno jako serwer podstawowy, jak i serwer pomocniczy. Podstawowy serwer oparty na systemie Linux może zarządzać serwerami pomocniczymi opartymi na systemie Linux i Windows. Podstawowy serwer oparty na systemie Windows może zarządzać dodatkowym serwerem opartym na systemie Linux.

Wirtualne Serwery administracyjne są szczególnym przypadkiem podrzędnych Serwerów administracyjnych.

Hierarchii Serwerów administracyjnych można użyć w celu:

- Zmniejszenia obciążenia na Serwerze administracyjnym (w porównaniu do pojedynczego Serwera działającego dla całej sieci).
- Zmniejszenia ruchu w sieci wewnętrznej i uproszczenia pracy ze zdalnymi komputerami firmowymi. Nie ma konieczności nawiązywania połączenia pomiędzy głównym Serwerem administracyjnym a wszystkimi urządzeniami sieciowymi, które mogą znajdować się, na przykład, w innych regionach. W każdym segmencie sieci wystarczy zainstalować podrzędny Serwer administracyjny, przydzielić urządzenia do grup administracyjnych Serwerów podrzędnych i ustanowić połączenia między Serwerami podrzędnymi a Serwerem głównym na kanałach szybkiej komunikacji.
- Rozdzielenia obowiązków pomiędzy administratorami ochrony antywirusowej. Wszystkie możliwości scentralizowanego zarządzania i monitorowania stanu ochrony antywirusowej w sieciach korporacyjnych pozostają dostępne.
- Używania Kaspersky Security Center Linux przez dostawców usług. Dostawca usługi musi tylko zainstalować Kaspersky Security Center Linux i Kaspersky Security Center Web Console. Aby zarządzać dużą liczbą urządzeń klienckich różnych organizacji, dostawca usług może dodać pomocnicze Serwery administracyjne (w tym Serwery wirtualne) do hierarchii Serwerów administracyjnych.

Każde urządzenie wchodzące w skład hierarchii grup administracyjnych może być podłączone tylko do jednego Serwera administracyjnego. Należy monitorować połączenia urządzeń z Serwerami administracyjnymi. Użyj funkcji wyszukiwania urządzeń w grupach administracyjnych różnych Serwerów w oparciu o atrybuty sieciowe.

Wirtualny Serwer administracyjny

Wirtualny Serwer administracyjny (zwany również *Serwerem wirtualnym*) jest to moduł z Kaspersky Security Center Linux służący do zarządzania ochroną antywirusową sieci organizacji klienta.

Wirtualny Serwer administracyjny jest szczególnym przypadkiem podrzędnego Serwera administracyjnego i ma następujące ograniczenia w porównaniu z fizycznym Serwerem administracyjnym:

- Wirtualny Serwer administracyjny można utworzyć tylko na głównym Serwerze administracyjnym.
- Podczas działania wirtualny Serwer administracyjny używa bazy danych głównego Serwera administracyjnego. Zadania tworzenia kopii zapasowych i przywracania danych, a także zadania pobierania i skanowania aktualizacji nie są obsługiwane na wirtualnym Serwerze administracyjnym.
- Serwer wirtualny nie obsługuje tworzenia podrzędnych Serwerów administracyjnych (łącznie z Serwerami wirtualnymi).

Dodatkowo, wirtualny Serwer administracyjny posiada następujące ograniczenia:

- W oknie właściwości wirtualnego Serwera administracyjnego ograniczona jest liczba sekcji.
- Aby zdalnie zainstalować aplikacje firmy Kaspersky na urządzeniach klienckich zarządzanych przez wirtualny Serwer administracyjny, upewnij się, że Agent sieciowy jest zainstalowany na jednym z urządzeń klienckich w celu zapewnienia komunikacji z wirtualnym Serwerem administracyjnym. Przy pierwszym połączeniu z wirtualnym Serwerem administracyjnym to urządzenie jest automatycznie przypisywane jako punkt dystrybucji, pełniąc rolę bramy połączenia pomiędzy urządzeniami klienckimi a wirtualnym Serwerem administracyjnym.
- Serwery wirtualne mogą odpytywać sieć wyłącznie za pośrednictwem punktów dystrybucji.
- Aby uruchomić ponownie nieprawidłowo działający Serwer wirtualny, Kaspersky Security Center Linux uruchamia ponownie główny Serwer administracyjny i wszystkie wirtualne Serwery administracyjne.
- Użytkownikom utworzonym na Serwerze wirtualnym nie można przypisać roli na Serwerze administracyjnym.

Administrator wirtualnego Serwera administracyjnego posiada wszystkie uprawnienia na tym konkretnym Serwerze wirtualnym.

Serwer sieciowy

Kaspersky Security Center *Web Server* (zwany również *serwer sieciowy, serwer WWW*) jest składnikiem Kaspersky Security Center, który jest instalowany wraz z Serwerem administracyjnym. Serwer WWW został zaprojektowany do przesyłania za pośrednictwem sieci autonomicznych pakietów instalacyjnych oraz plików z folderu współdzielonego.

Po utworzeniu autonomicznego pakietu instalacyjnego, jest on automatycznie publikowany na serwerze sieciowym. Odnośnik do pobrania pakietu autonomicznego jest wyświetlany na liście utworzonych autonomicznych pakietów instalacyjnych. Jeśli jest to konieczne, możesz anulować publikację pakietu autonomicznego lub opublikować go ponownie na serwerze sieciowym.

Folder współdzielony jest używany do przechowywania informacji dostępnych dla wszystkich użytkowników, których urządzenia są zarządzane poprzez Serwer administracyjny. Jeśli użytkownik nie ma bezpośredniego dostępu do folderu współdzielonego, nie może uzyskać informacji z folderu przy pomocy serwera sieciowego.

Aby udostępnić użytkownikom informacje z folderu współdzielonego przy pomocy serwera WWW, administrator musi utworzyć w folderze współdzielonym podfolder o nazwie "public" i wkleić do niego odpowiednie informacje.

Składnia odnośnika do przesłania informacji wygląda następująco:

```
https://<Web Server name>:<HTTPS port>/public/<object>
```

gdzie:

- `<Web Server name>` to nazwa serwera sieciowego Kaspersky Security Center Web Server.
- `<HTTPS port>` to port HTTPS serwera sieciowego, który został zdefiniowany przez Administratora. Port HTTPS można ustawić w sekcji **Serwer WWW** okna właściwości Serwera administracyjnego. Domyślny numer portu to 8061.
- `<object>` to podfolder lub plik, do którego użytkownik posiada dostęp.

Administrator może wysłać użytkownikowi nowy odnośnik w dowolny sposób, na przykład za pośrednictwem poczty elektronicznej.

Klikając odnośnik, użytkownik może pobrać żądane informacje na urządzenie lokalne.

Kaspersky Security Center Linux Web Server

Kaspersky Security Center Linux Web Server (zwany również serwerem sieciowym) jest składnikiem Kaspersky Security Center Linux. Serwer sieciowy został zaprojektowany do publikowania autonomicznych pakietów instalacyjnych oraz plików z folderu współdzielonego.

Pakiety instalacyjne są automatycznie publikowane na serwerze sieciowym, a następnie są usuwane po pierwszym pobraniu. Administrator może wysłać użytkownikowi nowy odnośnik w dowolny sposób, na przykład za pośrednictwem poczty elektronicznej.

Klikając odnośnik, użytkownik może pobrać żądane informacje na urządzenie mobilne.

Ustawienia serwera sieciowego

Jeśli wymagane jest dostrojenie serwera WWW, jego właściwości umożliwiają zmiany portów dla HTTP (8060) i HTTPS (8061). Oprócz zmiany portów, możesz zastąpić certyfikat serwera dla HTTPS i zmienić FQDN serwera sieciowego dla HTTP.

Ustawienia serwera sieciowego w bramie połączenia

Oddzielna usługa serwera sieciowego jest implementowana w punkcie dystrybucji w trybie bramy połączenia, co pozwala na pracę z urządzeniami mobilnymi podłączonymi do Kaspersky Security Center Linux. Usługa ta odpowiada za przesyłanie pakietów instalacyjnych aplikacji i profili zarządzania urządzeniami na urządzenia bez konieczności bezpośredniego łączenia ich z Serwerem administracyjnym. Pliki są przesyłane w trakcie przetwarzania przez usługę żądań plików HTTP/HTTPS na bramie połączenia.

Usługa serwera sieciowego na bramie połączenia jest instalowana razem z Agentem sieciowym Linux. Aby skorzystać z tej funkcjonalności, należy przypisać urządzenie, które będzie działać jako punkt dystrybucji w trybie bramy połączenia, a następnie określić odpowiednie ustawienia. Szczegółowe informacje dotyczące konfigurowania ustawień serwera sieciowego na bramie połączenia można znaleźć w pomocy programu Kaspersky Secure Mobility Management.

Agent sieciowy

Interakcja między Serwerem administracyjnym a urządzeniami odbywa się przy użyciu komponentu *Agent sieciowy* programu Kaspersky Security Center Linux. Agent sieciowy powinien być zainstalowany na wszystkich urządzeniach, na których do zarządzania aplikacjami Kaspersky wykorzystywany jest Kaspersky Security Center Linux.

Urządzenie, na którym jest zainstalowany Agent sieciowy, nazywa się *zarządzane urządzenie* lub *urządzenie*. Pakiet instalacyjny Agenta sieciowego można pobrać z następujących źródeł:

- Pakiet instalacyjny w magazynie Serwera administracyjnego (należy posiadać zainstalowany Serwer administracyjny)
- Strona internetowa Kaspersky

Agent sieciowy dla Linux jest instalowany na urządzeniu jako usługa z następującym zestawem atrybutów:

- Nazwa „Agent sieciowy Kaspersky"
- Ustawiony do automatycznego uruchamiania po załadowaniu systemu operacyjnego
- Korzysta z konta root

Agent sieciowy dla Windows jest instalowany na urządzeniu jako usługa z następującym zestawem atrybutów:

- Nazwa „Agent sieciowy Kaspersky Security Center"
- Ustawiony do automatycznego uruchamiania po załadowaniu systemu operacyjnego
- Korzysta z konta LocalSystem

Agent sieciowy dla systemu macOS jest instalowany na urządzeniu jako usługa z następującym zestawem atrybutów:

- Nazwa „com.kaspersky.klnagent.core"
- Ustawiony do automatycznego uruchamiania po załadowaniu systemu operacyjnego
- Korzysta z konta root

Nazwy procesów usługowych:

- Dla systemu Linux:
  - klnagent64.service (dla 64-bitowego systemu operacyjnego)
  - klnagent.service (dla 32-bitowego systemu operacyjnego)
- Dla systemu Windows:
  - klnagent
- W przypadku macOS:
  - com.kaspersky.klnagent

Domyślnie Agent sieciowy instalowany jest w następujących lokalizacjach:

- Dla systemu Linux:
  - Systemy 32-bitowe: /opt/kaspersky/klnagent/
  - Systemy 64-bitowe: /opt/kaspersky/klnagent64/
- Dla systemu Windows:
  - Systemy 32-bitowe: C:\Program Files\Kaspersky Lab\NetworkAgent
  - Systemy 64-bitowe: C:\Program Files (x86)\Kaspersky Lab\NetworkAgent
- W przypadku macOS:
  - Systemy 64-bitowe: /Library/Application Support/Kaspersky Lab/klnagent/Binaries/klnagent

W przypadku urządzeń z systemem Windows w ustawieniach pakietu instalacyjnego można określić inny folder do instalacji Agenta sieciowego. Jednak w przypadku urządzeń z systemem Linux Agenta sieciowego można zainstalować jedynie w domyślnym katalogu.

Folder instalacyjny Agenta sieciowego zawiera również narzędzia do zarządzania i diagnostyki działania Agenta sieciowego, takie jak narzędzia klmover i klnagchk.

Podczas instalacji Serwera administracyjnego, serwerowa wersja Agenta sieciowego jest automatycznie instalowana razem z Serwerem administracyjnym. Niemniej jednak, aby zarządzać urządzeniem Serwera administracyjnego jak każdym innym zarządzanym urządzeniem, zainstaluj Agenta sieciowego dla systemu Linux na urządzeniu Serwera administracyjnego. W takim przypadku Agent sieciowy dla systemu Linux jest instalowany i działa niezależnie od wersji serwerowej Agenta sieciowego zainstalowanego wraz z Serwerem administracyjnym.

Agent sieciowy synchronizuje zarządzane urządzenie z Serwerem administracyjnym. Zalecane jest ustawienie okresu synchronizacji (zwanego także *puls*) na 15 minut dla 10 000 zarządzanych urządzeń.

Grupy administracyjne

Grupa administracyjna (zwana dalej również *grupą*) jest logicznym zestawem zarządzanych urządzeń połączonych na podstawie pewnych cech w celu zarządzania pogrupowanymi urządzeniami jako pojedynczą jednostką w obrębie Kaspersky Security Center Linux.

Wszystkie zarządzane urządzenia w danej grupie administracyjnej są tak skonfigurowane, aby:

- Używać tych samych ustawień aplikacji (które można określić w zasadach grupy).
- Używaj wspólnego trybu działania dla wszystkich aplikacji poprzez tworzenie zadań grupowych z określonymi ustawieniami. Przykłady zadań grupowych obejmują tworzenie i instalowanie takich samych pakietów instalacyjnych, aktualizowanie baz danych i modułów aplikacji, skanowanie urządzenia na żądanie i włączanie ochrony w czasie rzeczywistym.

Zarządzane urządzenie może należeć tylko do jednej grupy administracyjnej.

Możesz tworzyć hierarchie o dowolnym poziomie zagnieżdżenia Serwerów administracyjnych i grup. Pojedynczy poziom hierarchii może zawierać podrzędne i wirtualne Serwery administracyjne, grupy i zarządzane urządzenia. Możesz przenosić urządzenia z jednej grupy do innej bez przenoszenia ich fizycznie. Na przykład, jeśli pozycja pracownika w firmie zmieni się z księgowego na dewelopera, możesz przenieść urządzenie tego pracownika z grupy administracyjnej Księgowi do grupy administracyjnej Deweloperzy. Następnie urządzenie automatycznie pobierze ustawienia aplikacji wymagane dla deweloperów.

Zarządzane urządzenie

Zarządzane urządzenie to urządzenie z systemem Linux, Windows lub macOS i zainstalowanym Agentem sieciowym. Możesz zarządzać takimi urządzeniami poprzez utworzenie zadań i zasad dla aplikacji zainstalowanych na tych urządzeniach. Możesz także otrzymywać raporty z zarządzanych urządzeń.

Możesz sprawić, że zarządzane urządzenie będzie działało jako punkt dystrybucji oraz jako brama połączenia.

Urządzenie może być zarządzane tylko przez jeden Serwer administracyjny. Liczba urządzeń, którymi można zarządzać przy użyciu jednego Serwera administracyjnego, zależy od konfiguracji urządzenia, na którym znajduje się Serwer administracyjny oraz od ograniczeń systemu DBMS.

Urządzenie nieprzypisane

Urządzenie nieprzypisane to urządzenie w sieci, które nie zostało uwzględnione w żadnej grupie administracyjnej. Na nieprzypisanych urządzeniach możesz wykonać różne działania, na przykład, przenieść je do grup administracyjnych lub zainstalować na nich aplikacje.

Jeśli nowe urządzenie zostanie wykryte w sieci, to urządzenie zostanie umieszczone w grupie administracyjnej **Urządzenia nieprzypisane**. Możesz skonfigurować reguły dla urządzeń, aby po wykryciu były przenoszone automatycznie do innych grup administracyjnych.

Stacja robocza administratora

Urządzenia, na których zainstalowany jest Kaspersky Security Center Web Console Server, nazywane są stacjami *roboczymi administratora*. Administratorzy mogą używać tych urządzeń do scentralizowanego zdalnego zarządzania aplikacjami Kaspersky zainstalowanymi na urządzeniach klienckich.

Liczba stacji roboczych administratora jest nieograniczona. Z każdej stacji roboczej administratora możesz jednocześnie zarządzać grupami administracyjnymi kilku Serwerów administracyjnych w sieci. Możesz połączyć stację roboczą administratora z Serwerem administracyjnym (fizycznym lub wirtualnym) znajdującym się na dowolnym poziomie hierarchii.

Możesz dodać stację roboczą administratora do grupy administracyjnej jako urządzenie klienckie.

W obrębie grup administracyjnych dowolnego Serwera administracyjnego to samo urządzenie może funkcjonować jako klient Serwera administracyjnego, Serwer administracyjny lub stacja robocza administratora.

Webowa wtyczka administracyjna

Specjalny składnik — *webowa wtyczka administracyjna* — jest używany do zdalnego administrowania oprogramowaniem Kaspersky przy użyciu Kaspersky Security Center Web Console. W dalszej części dokumentu webowa wtyczka zarządzająca jest zwana również *wtyczką zarządzającą*. Wtyczka zarządzająca to interfejs między Kaspersky Security Center Web Console a określoną aplikacją firmy Kaspersky. Korzystając z wtyczki zarządzającej, możesz skonfigurować zadania i zasady dla aplikacji.

Webową wtyczkę administracyjna można pobrać ze strony internetowej Kaspersky.

Wtyczka zarządzająca oferuje:

- Interfejs do tworzenia i edytowania zadań i ustawień aplikacji
- Interfejs do tworzenia i edytowania zasad i profili zasad do zdalnej i scentralizowanej konfiguracji aplikacji Kaspersky i urządzeń
- Przesyłanie zdarzeń wygenerowanych przez aplikację
- Funkcje Kaspersky Security Center Web Console do wyświetlania danych operacyjnych i zdarzeń aplikacji, a także statystyk przekazanych z urządzeń klienckich

Zasady

Zasada to zbiór ustawień aplikacji Kaspersky, które są stosowane do grupy administracyjnej i jej podgrup. Możesz zainstalować kilka aplikacji Kaspersky na urządzeniach należących do grupy administracyjnej. Kaspersky Security Center zapewnia jedną zasadę dla każdej aplikacji Kaspersky w grupie administracyjnej. Zasada ma jeden z następujących stanów:

Stan zasady

Stan	Opis
Aktywny	Bieżąca zasada, która jest stosowana do urządzenia. W każdej grupie administracyjnej dla aplikacji Kaspersky może być aktywna tylko jedna zasada. Urządzenia stosują wartości ustawień aktywnej zasady aplikacji Kaspersky.
Nieaktywna	Zasada, która nie jest obecnie stosowana do urządzenia.
Profil użytkownika mobilnego	Jeżeli ta opcja jest zaznaczona, zasada stanie się aktywna, gdy urządzenie znajdzie się poza siecią korporacyjną.

Zasady działają zgodnie z następującymi regułami:

- Dla jednej aplikacji można skonfigurować kilka zasad z różnymi wartościami.
- Tylko jedna zasada może być aktywna dla bieżącej aplikacji.
- Zasada może mieć zasady podrzędne.

Zazwyczaj można używać zasad w celu przygotowania się na sytuacje awaryjne, takie jak atak wirusa. Na przykład, jeśli wystąpi atak za pośrednictwem dysków flash, można aktywować zasadę blokującą dostęp do dysków flash. W takim przypadku bieżąca aktywna zasada automatycznie stanie się nieaktywna.

Aby zapobiec utrzymywaniu wielu zasad, na przykład, gdy przy różnych okazjach zakłada się zmianę tylko kilku ustawień, można użyć profili zasad.

Profil zasad to nazwany podzbiór wartości ustawień zasad, który zastępuje wartości ustawień zasady. Profil zasad wpływa na efektywne tworzenie ustawień na zarządzanym urządzeniu. *Obowiązujące ustawienia* to zbiory ustawień zasad, ustawień profilu zasad i lokalnych ustawień aplikacji, które są aktualnie zastosowane do urządzenia.

Profile zasad działają zgodnie z następującymi regułami:

- Profil zasad zaczyna obowiązywać, gdy wystąpi określony warunek aktywacji.
- Profile zasad zawierają wartości ustawień, które różnią się od ustawień zasad.
- Aktywacja profilu zasad zmienia obowiązujące ustawienia zarządzanego urządzenia.
- Zasada może zawierać maksymalnie 100 profili zasad.

Profile zasad

Czasami konieczne może być utworzenie kilku instancji jednej zasady dla różnych grup administracyjnych; możesz także zmodyfikować ustawienia tych zasad w sposób scentralizowany. Te instancje mogą różnić się jednym lub dwoma ustawieniami. Na przykład, wszyscy księgowi w firmie pracują pod kontrolą tego samej zasady—ale starsi księgowi mogą korzystać z dysków flash, a młodsi księgowi nie mają takich uprawnień. W tym przypadku, zastosowanie zasad do urządzeń tylko poprzez hierarchię grup administracyjnych może być niewygodne.

Aby uniknąć tworzenia kilku instancji jednej zasady, Kaspersky Security Center Linux umożliwia utworzenie *profili zasad*. Profile zasad są niezbędne, jeśli chcesz, żeby urządzenia w jednej grupie administracyjnej były uruchamiane z ustawieniami innych zasad.

Profil zasad jest to inaczej podzbiór ustawień zasady. Ten podzbiór jest stosowany na urządzeniach docelowych wraz z zasadą i uzupełnia ją zgodnie z określonym warunkiem zwanym *warunkiem aktywacji profilu*. Profile mogą zawierać tylko ustawienia różniące się od „podstawowej" zasady, która jest aktywna na zarządzanym urządzeniu. Aktywacja profilu zmodyfikuje ustawienia „podstawowych" zasad, które były wstępnie aktywne na urządzeniu. Zmodyfikowane ustawienia przyjmują wartości określone w profilu.

Zadania

Kaspersky Security Center Linux zarządza aplikacjami zabezpieczającymi Kaspersky, zainstalowanymi na urządzeniach poprzez tworzenie i uruchamianie *zadań*. Zadania są potrzebne do instalowania, uruchamiania i zatrzymywania działania aplikacji, skanowania plików, aktualizowania baz danych i modułów aplikacji, a także wykonywania innych działań na aplikacjach.

Zadania dla określonej aplikacji mogą być tworzone tylko wtedy, gdy zainstalowana jest wtyczka zarządzająca dla tej aplikacji.

Zadania mogą być wykonywane na Serwerze administracyjnym i na urządzeniach.

Na Serwerze administracyjnym wykonywane są następujące zadania:

- Automatyczne rozsyłanie raportów
- Pobieranie uaktualnień do repozytorium Serwera administracyjnego

- Tworzenie kopii zapasowych danych Serwera administracyjnego
- Obsługa baz danych

Na urządzeniach wykonywane są następujące typy zadań:

- *Zadania lokalne*—zadania wykonywane na określonym urządzeniu

  Zadania lokalne mogą zostać zmodyfikowane zarówno przez administratora przy użyciu narzędzi Kaspersky Security Center Web Console lub przez użytkownika zdalnego urządzenia (na przykład z poziomu interfejsu aplikacji zabezpieczającej). Jeśli zadanie lokalne zostało zmodyfikowane jednocześnie przez administratora i użytkownika zarządzanego urządzenia, zostaną zastosowane zmiany wprowadzone przez administratora, ponieważ mają wyższy priorytet.

- *Zadania grupowe*—zadania wykonywane na wszystkich urządzeniach określonej grupy

  Dopóki nie określono inaczej we właściwościach zadania, zadanie grupowe także wpływa na wszystkie podgrupy wybranej grupy. Zadanie grupowe także może wpływać (opcjonalnie) na urządzenia, które zostały podłączone do podrzędnych i wirtualnych Serwerów administracyjnych zainstalowanych w grupie lub w jej dowolnej podgrupie.

- *Zadania globalne*—zadania wykonywane na zbiorze urządzeń, niezależnie od tego, czy znajdują się w jakiejkolwiek grupie

Dla każdej aplikacji można utworzyć dowolną liczbę zadań grupowych, zadań globalnych lub zadań lokalnych.

Możesz wprowadzać zmiany w ustawieniach zadań, przeglądać postęp ich wykonywania, a także kopiować, eksportować, importować i usuwać zadania.

Zadanie jest uruchamiane na urządzeniu tylko wtedy, gdy uruchomiona jest aplikacja, dla której utworzono zadanie.

Wyniki zadań są zapisywane w dzienniku zdarzeń Syslog oraz w dzienniku zdarzeń Kaspersky Security Center Linux zarówno centralnie na Serwerze administracyjnym i lokalnie na każdym urządzeniu.

Nie używaj prywatnych danych w ustawieniach zadania. Na przykład, unikaj określania hasła administratora domeny.

Obszar zadania

Obszar zadania to zestaw urządzeń, na których wykonywane jest zadanie. Typy obszaru to:

- Dla *zadania lokalnego* obszarem jest samo urządzenie.
- Dla *zadania Serwera administracyjnego* obszarem jest Serwer administracyjny.
- Dla *zadania grupowego* obszarem jest lista urządzeń znajdujących się w grupie.

Podczas tworzenia *zadania globalnego* możesz użyć następujących metod do określenia jego obszaru:

- Ręcznie określ pewne urządzenia.

  Jako adresu urządzenia możesz użyć adresu IP (lub zakresu adresów IP) lub nazwy DNS. Możesz również wybrać urządzenia wykryte w sieci przez Serwer administracyjny.

- Zaimportuj listę urządzeń z pliku .txt zawierającego adresy dodawanych urządzeń (każdy adres powinien znajdować się w pojedynczej linii).

  Jeśli lista urządzeń jest importowana z pliku lub jest tworzona ręcznie, a urządzenia są identyfikowane po nazwie, lista może zawierać tylko urządzenia, o których informacje zostały już dodane do bazy danych Serwera administracyjnego. Co więcej, informacje musiały zostać wprowadzone, gdy te urządzenia były podłączone lub podczas wyszukiwania urządzeń.

- Utwórz wybór urządzeń.

  Obszar zadania zmienia się, gdy zmienia się zbiór urządzeń zawartych w wyborze. Wybór urządzeń można utworzyć w oparciu o atrybuty urządzeń, włączając w to oprogramowanie zainstalowane na urządzeniach, a także w oparciu o znaczniki przydzielone do urządzeń. Wybór urządzeń to najbardziej elastyczny sposób określania obszaru zadania.

  Zadania dla wyborów urządzeń są zawsze uruchamiane przez Serwer administracyjny zgodnie z terminarzem. Te zadania nie mogą zostać uruchomione na urządzeniach, które nie są połączone z Serwerem administracyjnym. Zadania, których obszar jest określony przy użyciu innych metod, są uruchamiane bezpośrednio na urządzeniach i dlatego nie zależą od połączenia urządzenia z Serwerem administracyjnym.

  Zadania dla wyborów urządzeń nie są uruchamiane zgodnie z czasem lokalnym urządzenia tylko z czasem lokalnym Serwera administracyjnego. Zadania, których obszar jest określony przy użyciu innych metod, są uruchamiane zgodnie z czasem lokalnym urządzenia.

Jak ustawienia lokalne aplikacji mają się do zasad

Za pomocą zasad możliwe jest ustawienie wspólnych wartości ustawień aplikacji dla wszystkich urządzeń należących do grupy.

Wartości ustawień określone w zasadzie mogą być zmieniane dla indywidualnych urządzeń znajdujących się w grupie przy użyciu lokalnych ustawień aplikacji. Możesz ustawić tylko te wartości ustawień, które zasada pozwala modyfikować, to znaczy odblokowanych ustawień.

Wartość ustawienia używana przez aplikację na urządzeniu klienckim jest wyznaczana przez pozycję zablokuj (🔒) dla tego ustawienia w zasadzie:

- Jeśli modyfikacja ustawienia jest zablokowana, wówczas ta sama wartość (określona w zasadzie) używana jest na wszystkich urządzeniach klienckich.

- Jeśli modyfikacja ustawienia jest odblokowana, wówczas na każdym urządzeniu klienckim aplikacja używa wartości lokalnej zamiast wartości określonej w zasadzie. W takiej sytuacji ustawienie może być zmieniane w lokalnych ustawieniach aplikacji.

Dlatego też, gdy zadanie jest uruchamiane na urządzeniu klienckim, aplikacja stosuje ustawienia określone na dwa różne sposoby:

- W ustawieniach zadania i lokalnych ustawieniach aplikacji, jeżeli modyfikowanie ustawienia nie jest zablokowane w zasadzie.

- W zasadzie grupy, jeżeli zablokowane jest modyfikowanie ustawienia.

Lokalne ustawienia aplikacji są zmieniane po pierwszym zastosowaniu zasady w zgodzie z jej ustawieniami.

Punkt dystrybucji

Punkt dystrybucji (wcześniej znany jako agent aktualizacji) to urządzenie z zainstalowanym Agentem sieciowym, które jest używane do rozsyłania uaktualnień, zdalnej instalacji aplikacji oraz gromadzenia informacji o urządzeniach w sieci.

Funkcje i przypadki użycia Agenta sieciowego zainstalowanego na urządzeniu pełniącym rolę punktu dystrybucji różnią się w zależności od systemu operacyjnego.

Punkt dystrybucji może wykonywać następujące funkcje:

- Rozsyłaj uaktualnienia i pakiety instalacyjne pobrane z Serwera administracyjnego na urządzenia klienckie w grupie (włączając w to taką metodę, jak multicasting z użyciem protokołu UDP). Uaktualnienia mogą być pobierane z Serwera administracyjnego lub z serwerów aktualizacji Kaspersky. W drugim przypadku należy utworzyć zadanie aktualizacji dla punktu dystrybucji.

  Punkty dystrybucji przyspieszają rozsyłanie uaktualnień i zwalniają zasoby Serwera administracyjnego.

- Dystrybuować zasady i zadania grupowe poprzez multiemisję z użyciem protokołu UDP.

- Pełnić funkcję bramy połączenia z Serwerem administracyjnym dla urządzeń w grupie administracyjnej.

  Jeśli nie można nawiązać bezpośredniego połączenia między zarządzanymi urządzeniami w grupie a Serwerem administracyjnym, punkt dystrybucji może zostać użyty jako brama połączenia z Serwerem administracyjnym dla tej grupy. W tej sytuacji, zarządzane urządzenia zostaną podłączone do bramy połączenia, która połączy się z Serwerem administracyjnym.

  Obecność punktu dystrybucji, który działa jako brama połączenia, nie blokuje opcji bezpośredniego połączenia pomiędzy zarządzanymi urządzeniami a Serwerem administracyjnym. Jeśli brama połączenia nie jest dostępna, ale bezpośrednie połączenie z Serwerem administracyjnym jest technicznie możliwe, zarządzane urządzenia zostaną połączone bezpośrednio z Serwerem administracyjnym.

- Przeszukiwać sieć w celu odnalezienia nowych urządzeń i zaktualizowania informacji o tych istniejących. Punkt dystrybucji może stosować te same metody wykrywania urządzeń co Serwer administracyjny.

- Wykonaj zdalną instalację aplikacji firmy Kaspersky i innych producentów oprogramowania, w tym instalację na urządzeniach klienckich bez Agenta sieciowego.

  Ta funkcja umożliwia zdalne przesłanie pakietów instalacyjnych Agenta sieciowego na urządzenia klienckie znajdujące się w sieciach, do których Serwer administracyjny nie ma bezpośredniego dostępu.

- Pełni funkcję serwera proxy uczestniczącego w Kaspersky Security Network (KSN).

  Możesz włączyć serwer KSN Proxy po stronie punktu dystrybucji, aby urządzenie pełniło rolę serwera proxy KSN. W tym przypadku usługa KSN proxy jest uruchomiona na urządzeniu.

Pliki są przesyłane z Serwera administracyjnego do punktu dystrybucji po protokole HTTP lub HTTPS (jeśli włączone jest połączenie SSL). W przeciwieństwie do SOAP, korzystanie z HTTP lub HTTPS zwiększa wydajność poprzez wyeliminowanie niezbędnego ruchu.

Urządzenia z zainstalowanym Agentem sieciowym mogą być wskazane do pełnienia roli punktów dystrybucji ręcznie (przez administratora) lub automatycznie (przez Serwer administracyjny). Pełna lista punktów dystrybucji dla określonych grup administracyjnych jest wyświetlana w raporcie na liście punktów dystrybucji.

Zakres punktu dystrybucji to grupa administracyjna, do której został przypisany przez administratora, a także jej podgrupy na wszystkich poziomach zagnieżdżenia. Jeśli w hierarchii grup administracyjnych przypisano kilka punktów dystrybucji, Agent sieciowy zarządzanego urządzenia nawiąże połączenie z najbliższym punktem dystrybucji w hierarchii.

Jeśli punkty dystrybucji są wskazywane automatycznie przez Serwer administracyjny, wskaże on je według domen rozgłoszeniowych, a nie według grup administracyjnych. Ma to miejsce wtedy, gdy znane są wszystkie domeny rozgłoszeniowe. Agent sieciowy wymienia wiadomości z innymi Agentami sieciowymi w tej samej podsieci, a następnie wysyła do Serwera administracyjnego informacje o sobie i innych Agentach sieciowych. Serwer administracyjny może użyć tych informacji do pogrupowania Agentów sieciowych według domen rozgłoszeniowych. Domeny rozgłoszeniowe są znane dla Serwera administracyjnego, gdy przeszuka on ponad 70% Agentów sieciowych w grupach administracyjnych. Serwer administracyjny wyszukuje domeny rozgłoszeniowe co dwie godziny. Po przypisaniu punktów dystrybucji według domen rozgłoszeniowych, nie mogą być one ponownie przypisane według grup administracyjnych.

Jeśli administrator ręcznie przypisuje punkty dystrybucji, można je przypisać do grup administracyjnych lub lokalizacji sieciowych.

Agenci sieciowi z aktywnym profilem połączenia nie uczestniczą w wykrywaniu domen rozgłoszeniowych.

Kaspersky Security Center Linux przypisuje każdemu Agentowi sieciowemu unikatowy adres IP multicastu, który różni się od każdego innego adresu. Pozwala to uniknąć przeciążenia sieci, które może mieć miejsce w wyniku nakładania się adresów IP. Adresy multicastowe IP, które zostały przydzielone w poprzednich wersjach aplikacji, nie zostaną zmienione.

Jeśli w jednym obszarze sieci lub jednej grupie administracyjnej przypisanych jest więcej niż dwa punkty dystrybucji, jeden z nich staje się aktywnym punktem dystrybucji, a pozostałe stają się rezerwowymi punktami dystrybucji. Aktywny punkt dystrybucji pobiera uaktualnienia i pakiety instalacyjne bezpośrednio z Serwera administracyjnego, natomiast rezerwowe punkty dystrybucji pobierają uaktualnienia tylko z aktywnego punktu dystrybucji. W tym przypadku pliki zostają raz pobrane z Serwera administracyjnego, a następnie zostają rozdystrybuowane pośród punktów dystrybucji. Jeśli z jakiegoś powodu aktywny punkt dystrybucji stanie się niedostępny, jeden z rezerwowych punktów dystrybucji stanie się aktywny. Serwer administracyjny automatycznie wskaże punkt dystrybucji jako rezerwowy.

Stan punktu dystrybucji (*Aktywny*/*Rezerwowy*) jest wyświetlany z polem do zaznaczenia w raporcie narzędzia klnagchk.

Punkt dystrybucji wymaga przynajmniej 4 GB wolnej przestrzeni na dysku. Jeśli przestrzeń na dysku punktu dystrybucji jest mniejsza niż 2 GB, Kaspersky Security Center Linux tworzy problem bezpieczeństwa z poziomem istotności *Ostrzeżenie*. Problem bezpieczeństwa zostanie opublikowany we właściwościach urządzenia, w sekcji **Incydenty związane z bezpieczeństwem**.

Uruchamianie zadań zdalnej instalacji na urządzeniu wskazanym jako punkt dystrybucji wymaga dodatkowej wolnej przestrzeni na dysku. Ilość wolnego miejsca na dysku musi przekraczać całkowity rozmiar wszystkich pakietów instalacyjnych, które zostaną użyte do instalacji.

Uruchamianie dowolnych zadań aktualizacji i naprawiania luk na urządzeniu wskazanym jako punkt dystrybucji wymaga dodatkowej wolnej przestrzeni na dysku. Ilość wolnego miejsca na dysku musi być równa podwojonej wartości całkowitego rozmiaru wszystkich poprawek przeznaczonych do zainstalowania.

Urządzenia pełniące rolę punktów dystrybucji muszą być chronione, włączając w to ochronę fizyczną, przed wszelkim nieautoryzowanym dostępem.

Brama połączenia

Brama połączenia to Agent sieciowy działający w trybie specjalnym. Brama połączenia akceptuje połączenia z innych Agentów sieciowych i tuneluje je przez Serwer administracyjny poprzez własne połączenie z serwerem. W przeciwieństwie do zwykłego Agenta sieciowego brama połączenia oczekuje na połączenia z Serwerem administracyjnym bardziej niż nawiązuje te połączenia z Serwerem administracyjnym.

Brama połączenia może komunikować się z maksymalnie 10 000 urządzeń.

Masz dwie możliwości korzystania z bram połączeń:

- Zalecamy zainstalowanie bramy połączenia w strefie zdemilitaryzowanej (DMZ). W przypadku innych Agentów sieciowych zainstalowanych na urządzeniach mobilnych, musisz specjalnie skonfigurować połączenie z Serwerem administracyjnym przez bramę połączenia.

  Brama połączenia w żaden sposób nie modyfikuje ani nie przetwarza danych przesyłanych od Agentów sieciowych do Serwera administracyjnego. Co więcej, nie zapisuje tych danych w żadnym buforze i dlatego nie może zaakceptować danych od Agenta sieciowego i później przesyłać ich na Serwer administracyjny. Jeśli Agent sieciowy próbuje nawiązać połączenie z Serwerem administracyjnym przez bramę połączenia, ale brama połączenia nie może połączyć się z Serwerem administracyjnym, Agent sieciowy postrzega to tak, jakby Serwer administracyjny był niedostępny. Wszystkie dane pozostają na Agencie sieciowym (nie w bramie połączenia).

  Brama połączenia nie może nawiązać połączenia z Serwerem administracyjnym przez inną bramę połączenia. Oznacza to, że Agent sieciowy nie może być jednocześnie bramą połączenia i używać bramy połączenia do łączenia się z Serwerem administracyjnym.

  Wszystkie bramy połączeń znajdują się na liście punktów dystrybucji we właściwościach Serwera administracyjnego.

- Możesz także używać bram połączeń w sieci. Na przykład, automatycznie przypisane punkty dystrybucji stają się również bramami połączeń w swoim własnym zakresie. Jednak w sieci wewnętrznej bramy połączeń nie zapewniają znaczących korzyści. Zmniejszają liczbę połączeń sieciowych odbieranych przez Serwer administracyjny, ale nie zmniejszają ilości przychodzących danych. Nawet bez bram połączeń wszystkie urządzenia mogą nadal łączyć się z Serwerem administracyjnym.

Wirtualne Serwery administracyjne

W oparciu o fizyczny Serwer administracyjny można utworzyć kilka wirtualnych Serwerów administracyjnych, które będą podobne do podrzędnych Serwerów administracyjnych. W przeciwieństwie do trybu poufnego dostępu, który jest oparty na listach kontroli dostępu (ACL), tryb wirtualnego Serwera administracyjnego jest bardziej funkcjonalny i zapewnia większy stopień izolacji. Jako dodatek do dedykowanej struktury grup administracyjnych dla przypisanych urządzeń z zasadami i zadaniami, każdy wirtualny Serwer administracyjny zawiera swoją grupę nieprzypisanych urządzeń, własne zestawy raportów, wybranych urządzeń i zdarzeń, pakietów instalacyjnych, reguł przenoszenia itd. Zasięg działania wirtualnego Serwera administracyjnego może być wykorzystany przez dostawców usług (xSP) do zwiększenia izolacji klientów, a także przez organizacje działające na szeroką skalę z zaawansowanym przepływem pracy i dużą liczbą administratorów.

Wirtualne Serwery administracyjne są bardzo podobne do podrzędnych Serwerów administracyjnych, jednakże posiadają pewne różnice:

- Wirtualny Serwer administracyjny nie posiada większości ustawień globalnych i swoich własnych portów TCP.

- Wirtualny Serwer administracyjny nie posiada podrzędnych Serwerów administracyjnych.

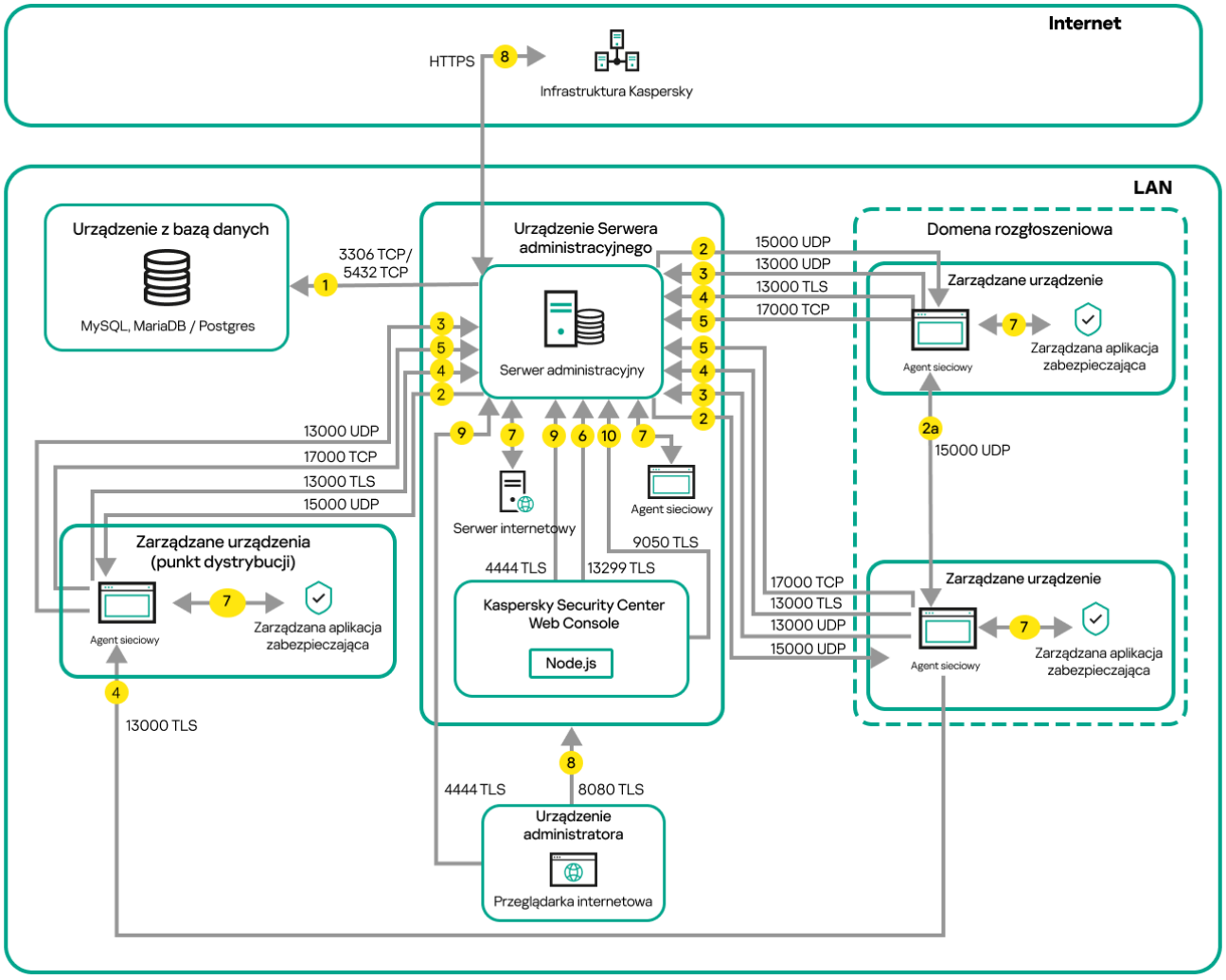
- Wirtualny Serwer administracyjny nie posiada innych wirtualnych Serwerów administracyjnych.
- Fizyczny Serwer administracyjny wyświetla urządzenia, grupy, zdarzenia i obiekty na zarządzanych urządzeniach (elementy w Kwarantannie, rejestrze aplikacji itd.) ze wszystkich swoich wirtualnych Serwerów administracyjnych.
- Wirtualny Serwer administracyjny może skanować sieć wyłącznie przy podłączonych punktach dystrybucji.

Schematy ruchu sieciowego danych i użycia portów

Ta sekcja zawiera schematy ruchu sieciowego danych między komponentami Kaspersky Security Center Linux, zarządzanymi aplikacjami zabezpieczającymi i serwerami zewnętrznymi w różnych konfiguracjach. Schematy są dostarczane z numerami portów, które muszą być dostępne na urządzeniach lokalnych.

Serwer administracyjny i zarządzane urządzenia w sieci LAN

Poniższy rysunek przedstawia ruch sieciowy danych, gdy Kaspersky Security Center jest zainstalowany tylko w sieci lokalnej (LAN).



Serwer administracyjny i zarządzane urządzenia w sieci lokalnej (LAN)

Rysunek przedstawia sposób, w jaki różne zarządzane urządzenia nawiązują połączenie z Serwerem administracyjnym na różne sposoby: bezpośrednio lub poprzez punkt dystrybucji. Punkty dystrybucji zmniejszają obciążenie na Serwerze administracyjnym podczas dystrybucji aktualizacji i optymalizowania ruchu sieciowego. Jednakże punkty dystrybucji są potrzebne tylko wtedy, gdy liczba zarządzanych urządzeń jest wystarczająco duża. Jeśli liczba zarządzanych urządzeń jest mała, wszystkie zarządzane urządzenia mogą pobierać uaktualnienia bezpośrednio z Serwera administracyjnego.

Strzałki wskazują inicjowanie ruchu sieciowego: każda strzałka wskazuje kierunek z urządzenia, które inicjuje połączenie, do urządzenia, które „odpowiada" na połączenie. Dostarczony jest numer portu oraz nazwa protokołu użytego do przesyłania danych. Każda strzałka posiada etykietę liczby, a szczegóły dotyczące odpowiedniego ruchu danych wyglądają następująco:

1. Serwer administracyjny wysyła dane do bazy danych. Jeśli instalujesz Serwer administracyjny i bazę danych na różnych urządzeniach, musisz udostępnić potrzebne porty na urządzeniu, na którym znajduje się baza danych (na przykład: port 3306 dla MySQL Server i MariaDB Server lub port 5432 dla PostgreSQL Server lub Postgres Pro Server). Odpowiednie informacje można znaleźć w dokumentacji do DBMS.

2. Żądania komunikacji od Serwera administracyjnego są przesyłane do wszystkich niemobilnych zarządzanych urządzeń poprzez port UDP o numerze 15000.

   Agenty sieciowe wysyłają żądania do siebie nawzajem w obrębie jednej domeny broadcastowej. Dane są następnie wysyłane do Serwera administracyjnego i są używane do określenia ograniczeń domeny broadcastowej i do automatycznego przydzielenia punktów dystrybucji (jeśli ta opcja jest włączona).

   Jeżeli Serwer administracyjny nie ma bezpośredniego dostępu do zarządzanych urządzeń, żądania komunikacji z Serwera administracyjnego nie są wysyłane bezpośrednio do tych urządzeń.

   2a. Agenci sieciowi na zarządzanych urządzeniach innych niż mobilne wymieniają dane o innych Agentach sieciowych w tej samej domenie rozgłoszeniowej (dane są następnie wysyłane do Serwera administracyjnego).

3. Informacje o zamknięciu zarządzanych urządzeń są przesyłane z Agenta sieciowego do Serwera administracyjnego poprzez port UDP o numerze 13000.

4. Serwer administracyjny odbiera połączenie od Agentów sieciowych i podrzędnych Serwerów administracyjnych poprzez port TLS o numerze 13000.

   Jeśli używałeś wcześniejszej wersji Kaspersky Security Center, Serwer administracyjny w Twojej sieci może odbierać połączenia od Agentów sieciowych poprzez port inny niż TLS o numerze 14000. Kaspersky Security Center obsługuje także połączenia Agentów sieciowych poprzez port 14000, chociaż zalecane jest korzystanie z portu TLS o numerze 13000.

5. Zarządzane urządzenia (za wyjątkiem urządzeń mobilnych) żądają aktywacji poprzez port TCP o numerze 17000. Nie jest to konieczne, jeśli urządzenie posiada własny dostęp do Internetu; w tym przypadku urządzenie wysyła dane do serwerów Kaspersky bezpośrednio przez Internet.

6. Kaspersky Security Center Web Console Server wysyła dane na Serwer administracyjny, który może być zainstalowany na tym samym lub innym urządzeniu, poprzez port TLS o numerze 13299.

   Komponent Menedżer tożsamości i dostępu (IAM) łączy się z Serwerem administracyjnym poprzez port TLS 13299.

7. Lokalny ruch sieciowy aplikacji na pojedynczym urządzeniu (na Serwerze administracyjnym lub na zarządzanym urządzeniu). Żadne porty zewnętrzne nie muszą być otwarte.

8. Dane z Serwera administracyjnego na serwery Kaspersky (takie jak dane KSN lub informacje o licencjach) oraz dane z serwerów Kaspersky na Serwer administracyjny (takie jak uaktualnienia aplikacji i aktualizacje antywirusowych baz danych) są przesyłane przy użyciu protokołu HTTPS.

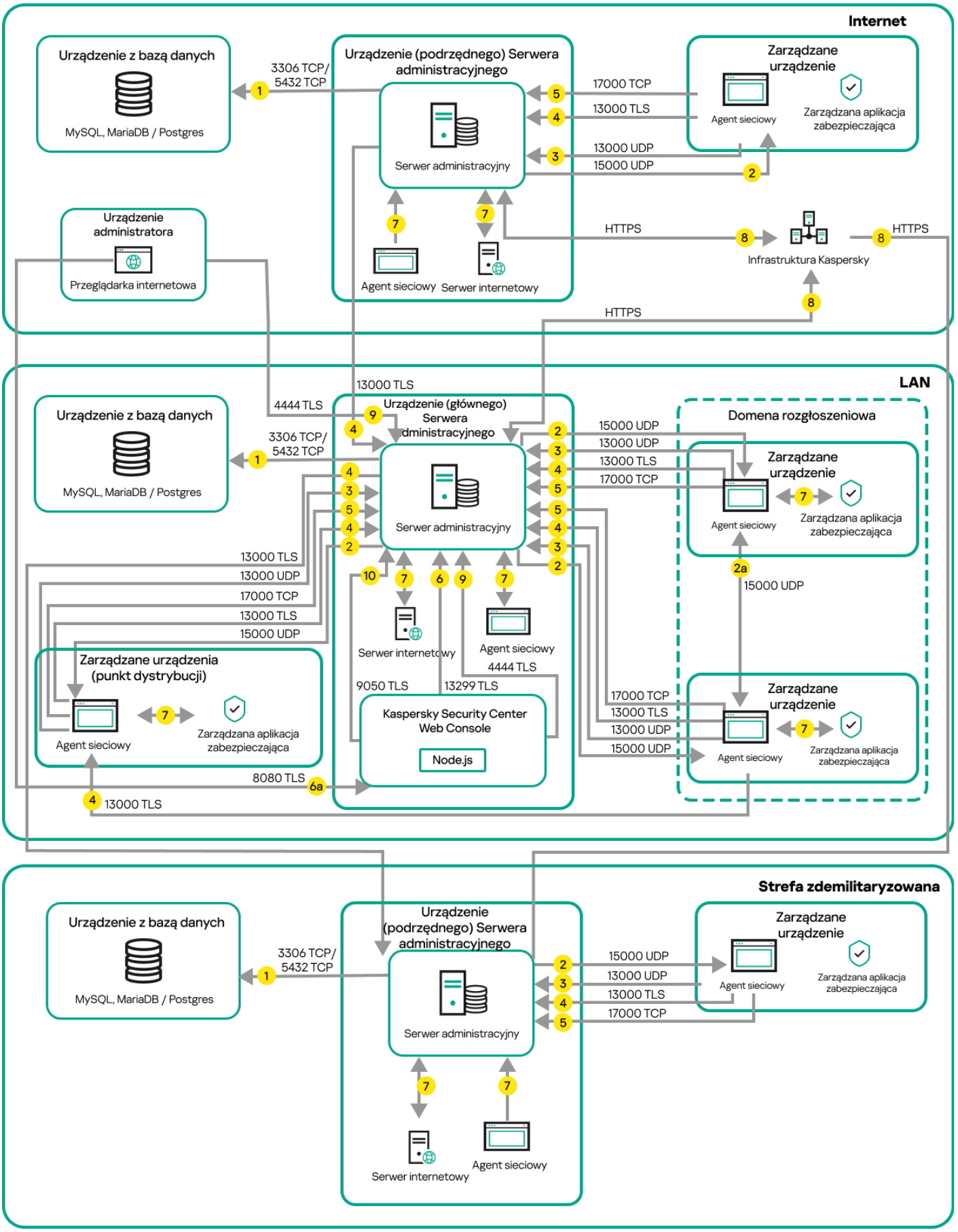
   Jeśli nie chcesz, żeby Twój Serwer administracyjny miał dostęp do internetu, musisz ręcznie zarządzać tymi danymi.

9. Kaspersky Security Center Web Console Server i przeglądarka (używana z Kaspersky Security Center Web Console) łączą się z Serwerem administracyjnym za pomocą protokołu uwierzytelniania OpenID Connect przez port TLS 4444.

10. Kaspersky Security Center Web Console Server nawiązuje połączenie z Serwerem administracyjnym poprzez port TLS 9050.

Główny Serwer administracyjny w sieci LAN i dwa podrzędne Serwery administracyjne

Poniższy rysunek przedstawia hierarchię Serwerów administracyjnych: główny Serwer administracyjny znajduje się w sieci lokalnej (LAN). Podrzędny Serwer administracyjny znajduje się w strefie zdemilitaryzowanej (DMZ); inny podrzędny Serwer administracyjny znajduje się w Internecie.



Hierarchia Serwerów administracyjnych: główny Serwer administracyjny i dwa podrzędne Serwery administracyjne

Strzałki wskazują inicjowanie ruchu sieciowego: każda strzałka wskazuje kierunek z urządzenia, które inicjuje połączenie, do urządzenia, które „odpowiada" na połączenie. Dostarczony jest numer portu oraz nazwa protokołu użytego do przesyłania danych. Każda strzałka posiada etykietę liczby, a szczegóły dotyczące odpowiedniego ruchu danych wyglądają następująco:

1. Serwer administracyjny wysyła dane do bazy danych. Jeśli instalujesz Serwer administracyjny i bazę danych na różnych urządzeniach, musisz udostępnić potrzebne porty na urządzeniu, na którym znajduje się baza danych (na przykład: port 3306 dla MySQL Server i MariaDB Server lub port 5432 dla PostgreSQL Server lub Postgres Pro Server). Odpowiednie informacje można znaleźć w dokumentacji do DBMS.

2. Żądania komunikacji od Serwera administracyjnego są przesyłane do wszystkich niemobilnych zarządzanych urządzeń poprzez port UDP o numerze 15000.

   Agenty sieciowe wysyłają żądania do siebie nawzajem w obrębie jednej domeny broadcastowej. Dane są następnie wysyłane do Serwera administracyjnego i są używane do określenia ograniczeń domeny broadcastowej i do automatycznego przydzielenia punktów dystrybucji (jeśli ta opcja jest włączona).

   Jeżeli Serwer administracyjny nie ma bezpośredniego dostępu do zarządzanych urządzeń, żądania komunikacji z Serwera administracyjnego nie są wysyłane bezpośrednio do tych urządzeń.

3. Informacje o zamknięciu zarządzanych urządzeń są przesyłane z Agenta sieciowego do Serwera administracyjnego poprzez port UDP o numerze 13000.

4. Serwer administracyjny odbiera połączenie od Agentów sieciowych i podrzędnych Serwerów administracyjnych poprzez port TLS o numerze 13000.

   Jeśli używałeś wcześniejszej wersji Kaspersky Security Center, Serwer administracyjny w Twojej sieci może odbierać połączenia od Agentów sieciowych poprzez port inny niż TLS o numerze 14000. Kaspersky Security Center Linux obsługuje także połączenia Agentów sieciowych poprzez port 14000, chociaż zalecane jest korzystanie z portu TLS o numerze 13000.

5. Zarządzane urządzenia (za wyjątkiem urządzeń mobilnych) żądają aktywacji poprzez port TCP o numerze 17000. Nie jest to konieczne, jeśli urządzenie posiada własny dostęp do Internetu; w tym przypadku urządzenie wysyła dane do serwerów Kaspersky bezpośrednio przez Internet.

6. Kaspersky Security Center Web Console Server wysyła dane na Serwer administracyjny, który może być zainstalowany na tym samym lub innym urządzeniu, poprzez port TLS o numerze 13299.

   Komponent Menedżer tożsamości i dostępu (IAM) łączy się z Serwerem administracyjnym poprzez port TLS 13299.

   6a. Dane z przeglądarki, która jest zainstalowana na oddzielnym urządzeniu administratora, są przesyłane do Kaspersky Security Center Web Console Server poprzez port TLS o numerze 8080. Kaspersky Security Center Web Console Server może zostać zainstalowany na Serwerze administracyjnym lub na innym urządzeniu.

7. Lokalny ruch sieciowy aplikacji na pojedynczym urządzeniu (na Serwerze administracyjnym lub na zarządzanym urządzeniu). Żadne porty zewnętrzne nie muszą być otwarte.

8. Dane z Serwera administracyjnego na serwery Kaspersky (takie jak dane KSN lub informacje o licencjach) oraz dane z serwerów Kaspersky na Serwer administracyjny (takie jak uaktualnienia aplikacji i aktualizacje antywirusowych baz danych) są przesyłane przy użyciu protokołu HTTPS.

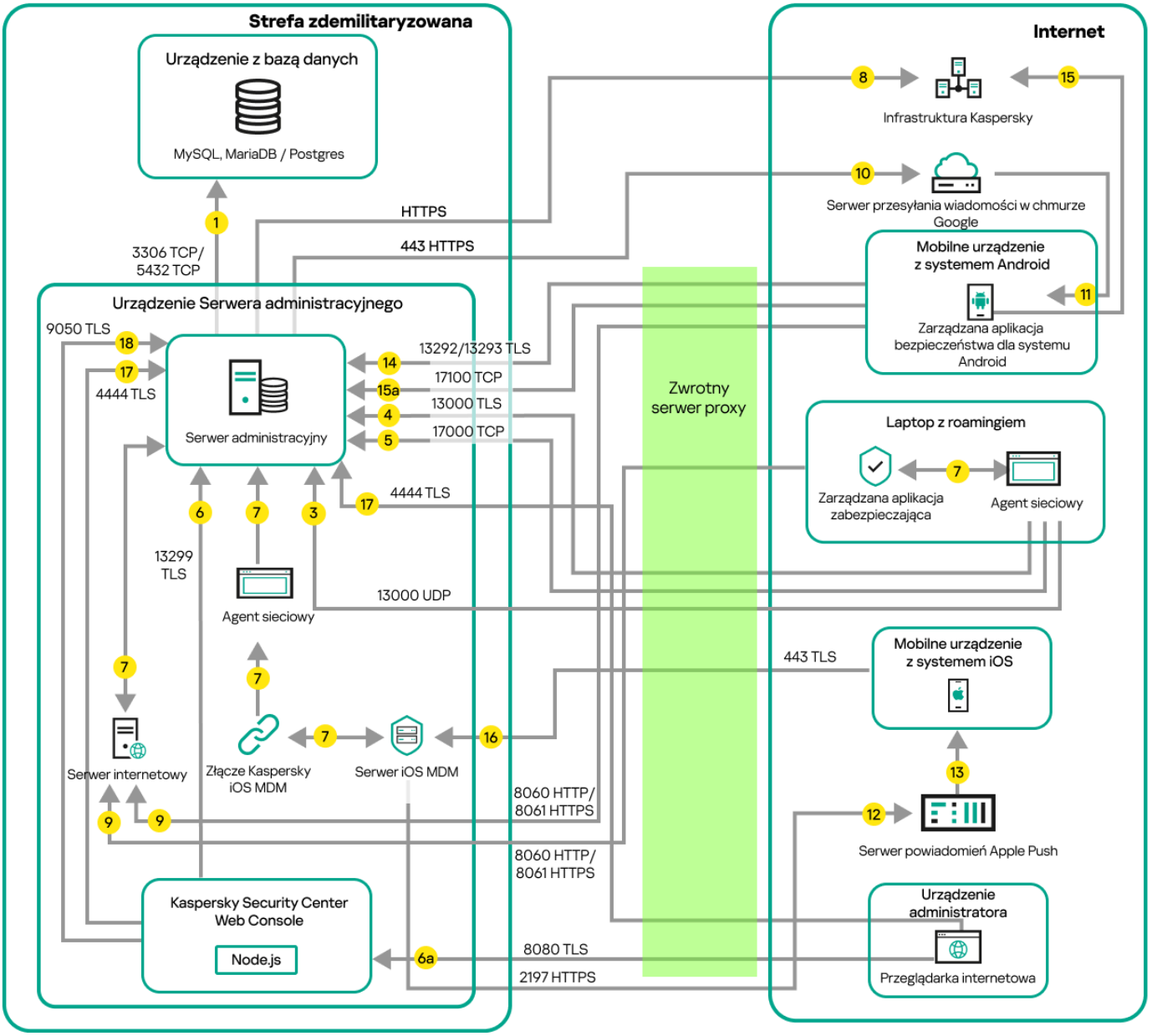
   Jeśli nie chcesz, żeby Twój Serwer administracyjny miał dostęp do internetu, musisz ręcznie zarządzać tymi danymi.

9. Kaspersky Security Center Web Console Server i przeglądarka (używana z Kaspersky Security Center Web Console) łączą się z Serwerem administracyjnym za pomocą protokołu uwierzytelniania OpenID Connect przez port TLS 4444.

10. Kaspersky Security Center Web Console Server nawiązuje połączenie z Serwerem administracyjnym poprzez port TLS 9050.

Serwer administracyjny w sieci LAN, zarządzane urządzenia w Internecie, odwrotny serwer proxy w użyciu

Poniższy rysunek przedstawia ruch sieciowy danych, gdy Serwer administracyjny jest w sieci lokalnej (LAN), a zarządzane urządzenia są w internecie. Na tym rysunku używany jest wybrany przez Ciebie odwrotny serwer proxy. Więcej informacji można znaleźć w dokumentacji aplikacji.



Serwer administracyjny w sieci lokalnej; zarządzane urządzenia nawiązują połączenie z Serwerem administracyjnym poprzez odwrotny serwer proxy

Ten schemat wdrażania jest zalecany, jeśli nie chcesz, żeby urządzenia mobilne nawiązywały połączenie bezpośrednio z Serwerem administracyjnym i nie chcesz przypisać bramy połączenia w DMZ.

Strzałki wskazują inicjowanie ruchu sieciowego: każda strzałka wskazuje kierunek z urządzenia, które inicjuje połączenie, do urządzenia, które „odpowiada" na połączenie. Dostarczony jest numer portu oraz nazwa protokołu użytego do przesyłania danych. Każda strzałka posiada etykietę liczby, a szczegóły dotyczące odpowiedniego ruchu danych wyglądają następująco:

1. Serwer administracyjny wysyła dane do bazy danych. Jeśli instalujesz Serwer administracyjny i bazę danych na różnych urządzeniach, musisz udostępnić potrzebne porty na urządzeniu, na którym znajduje się baza danych (na przykład: port 3306 dla MySQL Server i MariaDB Server lub port 5432 dla PostgreSQL Server lub Postgres Pro Server). Odpowiednie informacje można znaleźć w dokumentacji do DBMS.

2. Żądania komunikacji od Serwera administracyjnego są przesyłane do wszystkich niemobilnych zarządzanych urządzeń poprzez port UDP o numerze 15000.

   Agenty sieciowe wysyłają żądania do siebie nawzajem w obrębie jednej domeny broadcastowej. Dane są następnie wysyłane do Serwera administracyjnego i są używane do określenia ograniczeń domeny broadcastowej i do automatycznego przydzielenia punktów dystrybucji (jeśli ta opcja jest włączona).

   Jeżeli Serwer administracyjny nie ma bezpośredniego dostępu do zarządzanych urządzeń, żądania komunikacji z Serwera administracyjnego nie są wysyłane bezpośrednio do tych urządzeń.

3. Informacje o zamknięciu zarządzanych urządzeń są przesyłane z Agenta sieciowego do Serwera administracyjnego poprzez port UDP o numerze 13000.

4. Serwer administracyjny odbiera połączenie od Agentów sieciowych i podrzędnych Serwerów administracyjnych poprzez port TLS o numerze 13000.

   Jeśli używałeś wcześniejszej wersji Kaspersky Security Center, Serwer administracyjny w Twojej sieci może odbierać połączenia od Agentów sieciowych poprzez port inny niż TLS o numerze 14000. Kaspersky Security Center Linux obsługuje także połączenia Agentów sieciowych poprzez port 14000, chociaż zalecane jest korzystanie z portu TLS o numerze 13000.

5. Zarządzane urządzenia (za wyjątkiem urządzeń mobilnych) żądają aktywacji poprzez port TCP o numerze 17000. Nie jest to konieczne, jeśli urządzenie posiada własny dostęp do Internetu; w tym przypadku urządzenie wysyła dane do serwerów Kaspersky bezpośrednio przez Internet.

6. Kaspersky Security Center Web Console Server wysyła dane na Serwer administracyjny, który może być zainstalowany na tym samym lub innym urządzeniu, poprzez port TLS o numerze 13299.

   Komponent Menedżer tożsamości i dostępu (IAM) łączy się z Serwerem administracyjnym poprzez port TLS 13299.

   6a. Dane z przeglądarki, która jest zainstalowana na oddzielnym urządzeniu administratora, są przesyłane do Kaspersky Security Center Web Console Server poprzez port TLS o numerze 8080. Kaspersky Security Center Web Console Server może zostać zainstalowany na Serwerze administracyjnym lub na innym urządzeniu.

7. Lokalny ruch sieciowy aplikacji na pojedynczym urządzeniu (na Serwerze administracyjnym lub na zarządzanym urządzeniu). Żadne porty zewnętrzne nie muszą być otwarte.

8. Dane z Serwera administracyjnego na serwery Kaspersky (takie jak dane KSN lub informacje o licencjach) oraz dane z serwerów Kaspersky na Serwer administracyjny (takie jak uaktualnienia aplikacji i aktualizacje antywirusowych baz danych) są przesyłane przy użyciu protokołu HTTPS.

   Jeśli nie chcesz, żeby Twój Serwer administracyjny miał dostęp do internetu, musisz ręcznie zarządzać tymi danymi.

9. Żądania dla pakietów z zarządzanych urządzeń, w tym urządzeń mobilnych, są przesyłane do serwera WWW, który znajduje się na tym samym urządzeniu co Serwer administracyjny.

10. Tylko dla urządzeń mobilnych z systemem Android: dane z Serwera administracyjnego są przesyłane na serwery Google. To połączenie jest używane do informowania urządzeń mobilnych Android, że są niezbędne do nawiązania połączenia z Serwerem administracyjnym. Powiadomienia push są wysyłane na urządzenia mobilne.

11. Tylko dla urządzeń mobilnych z systemem Android: powiadomienia push z serwerów Google są wysyłane na urządzenie mobilne. To połączenie jest używane do informowania urządzeń mobilnych, że są niezbędne do nawiązania połączenia z Serwerem administracyjnym.

12. Tylko dla urządzeń mobilnych z systemem iOS: dane z serwera iOS MDM są przesyłane do serwerów Apple Push Notification. Powiadomienia push są wysyłane na urządzenia mobilne.

13. Tylko dla urządzeń mobilnych z systemem iOS: powiadomienia push z serwerów Apple są wysyłane na urządzenie mobilne. To połączenie jest używane do informowania urządzeń mobilnych iOS, że są niezbędne do nawiązania połączenia z serwerem iOS MDM.

14. Tylko dla urządzeń mobilnych: dane z zarządzanej aplikacji są przesyłane do Serwera administracyjnego (lub do bramy połączenia) poprzez port TLS o numerze 13292 / 13293—bezpośrednio lub poprzez odwrotny serwer proxy.

15. Tylko dla urządzeń mobilnych: dane z urządzenia mobilnego są przesyłane do infrastruktury Kaspersky.

    Jeśli urządzenie mobilne nie ma dostępu do Internetu, dane są przesyłane do Serwera administracyjnego poprzez port o numerze 17100, a Serwer administracyjny wysyła je do infrastruktury Kaspersky; jednakże ten scenariusz jest stosowany bardzo rzadko.

16. Tylko dla urządzeń mobilnych z systemem iOS: dane z urządzenia mobilnego są przesyłane za pośrednictwem portu TLS o numerze 443 na serwer iOS MDM, który znajduje się na tym samym urządzeniu co Serwer administracyjny, lub na bramie połączenia.

17. Kaspersky Security Center Web Console Server i przeglądarka (używana z Kaspersky Security Center Web Console) łączą się z Serwerem administracyjnym za pomocą protokołu uwierzytelniania OpenID Connect przez port TLS 4444.

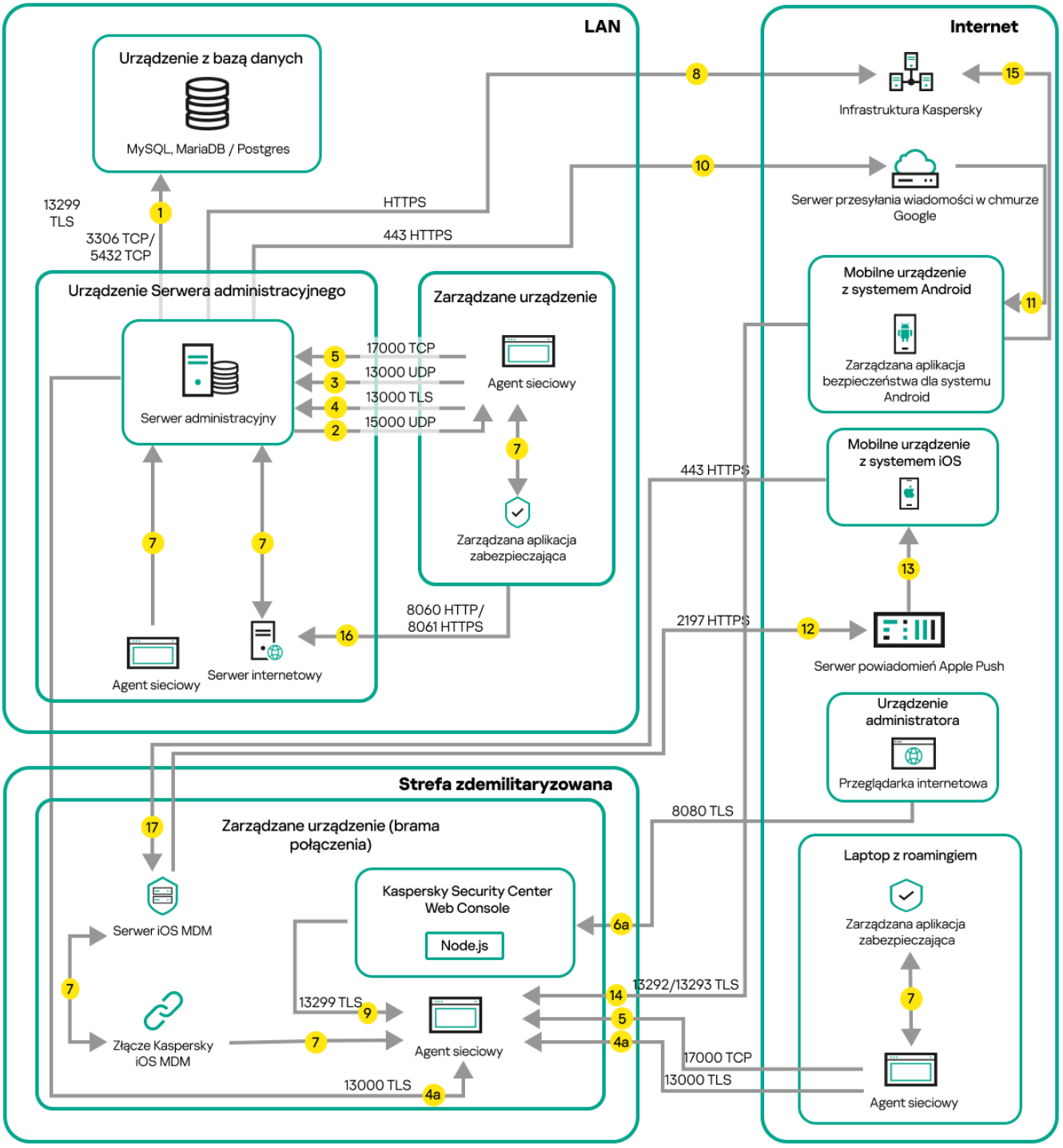
18. Kaspersky Security Center Web Console Server nawiązuje połączenie z Serwerem administracyjnym poprzez port TLS 9050.

Serwer administracyjny w sieci LAN, zarządzane urządzenia w internecie, brama połączenia w użyciu

Poniższy rysunek przedstawia ruch sieciowy danych, gdy Serwer administracyjny jest w sieci lokalnej (LAN), a zarządzane urządzenia są w internecie. Używana jest brama połączenia.

Ten schemat wdrażania jest zalecany, jeśli nie chcesz, żeby zarządzane urządzenia nawiązywały połączenie bezpośrednio z Serwerem administracyjnym i nie chcesz używać odwrotnego serwera proxy lub firmowej zapory sieciowej.

W tym schemacie wdrażania uwierzytelnianie domeny (pojedyncze logowanie) zapewniane przez Menedżera tożsamości i dostępu (IAM) nie jest obsługiwane.



Zarządzane urządzenia mobilne połączone z Serwerem administracyjnym poprzez bramę połączenia

Na tym rysunku zarządzane urządzenia są połączone z Serwerem administracyjnym poprzez bramę połączenia, która znajduje się w strefie DMZ. Nie jest używany odwrotny serwer proxy ani firmowa zapora sieciowa.

Strzałki wskazują inicjowanie ruchu sieciowego: każda strzałka wskazuje kierunek z urządzenia, które inicjuje połączenie, do urządzenia, które „odpowiada" na połączenie. Dostarczony jest numer portu oraz nazwa protokołu użytego do przesyłania danych. Każda strzałka posiada etykietę liczby, a szczegóły dotyczące odpowiedniego ruchu danych wyglądają następująco:

1. Serwer administracyjny wysyła dane do bazy danych. Jeśli instalujesz Serwer administracyjny i bazę danych na różnych urządzeniach, musisz udostępnić potrzebne porty na urządzeniu, na którym znajduje się baza danych (na przykład: port 3306 dla MySQL Server i MariaDB Server lub port 5432 dla PostgreSQL Server lub Postgres Pro Server). Odpowiednie informacje można znaleźć w dokumentacji do DBMS.

2. Żądania komunikacji od Serwera administracyjnego są przesyłane do wszystkich niemobilnych zarządzanych urządzeń poprzez port UDP o numerze 15000.

   Agenty sieciowe wysyłają żądania do siebie nawzajem w obrębie jednej domeny broadcastowej. Dane są następnie wysyłane do Serwera administracyjnego i są używane do określenia ograniczeń domeny broadcastowej i do automatycznego przydzielenia punktów dystrybucji (jeśli ta opcja jest włączona).

   Jeżeli Serwer administracyjny nie ma bezpośredniego dostępu do zarządzanych urządzeń, żądania komunikacji z Serwera administracyjnego nie są wysyłane bezpośrednio do tych urządzeń.

3. Informacje o zamknięciu zarządzanych urządzeń są przesyłane z Agenta sieciowego do Serwera administracyjnego poprzez port UDP o numerze 13000.

4. Serwer administracyjny odbiera połączenie od Agentów sieciowych i podrzędnych Serwerów administracyjnych poprzez port TLS o numerze 13000.

   Jeśli używałeś wcześniejszej wersji Kaspersky Security Center, Serwer administracyjny w Twojej sieci może odbierać połączenia od Agentów sieciowych poprzez port inny niż TLS o numerze 14000. Kaspersky Security Center Linux obsługuje także połączenia Agentów sieciowych poprzez port 14000, chociaż zalecane jest korzystanie z portu TLS o numerze 13000.

   4a. Brama połączenia w strefie DMZ odbiera również połączenie z Serwera administracyjnego przez port TLS 13000. Ponieważ brama połączenia w strefie DMZ nie obejmuje portów Serwera administracyjnego, Serwer administracyjny utworzy i zachowa ciągłe połączenie sygnałowe z bramą połączenia. Połączenie sygnałowe nie jest używane do przesyłania danych; jest używane tylko do wysyłania zaproszenia do interakcji z siecią. Jeśli brama połączenia musi nawiązać połączenie z Serwerem, poinformuje Serwer za pośrednictwem połączenia sygnałowego, a następnie Serwer utworzy wymagane połączenie do przesyłania danych.

   Urządzenia spoza biura nawiązują także połączenie z bramą połączenia za pośrednictwem portu TLS o numerze 13000.

5. Zarządzane urządzenia (za wyjątkiem urządzeń mobilnych) żądają aktywacji poprzez port TCP o numerze 17000. Nie jest to konieczne, jeśli urządzenie posiada własny dostęp do Internetu; w tym przypadku urządzenie wysyła dane do serwerów Kaspersky bezpośrednio przez Internet.

6. Kaspersky Security Center Web Console Server wysyła dane na Serwer administracyjny, który może być zainstalowany na tym samym lub innym urządzeniu, poprzez port TLS o numerze 13299.

   6a. Dane z przeglądarki, która jest zainstalowana na oddzielnym urządzeniu administratora, są przesyłane do Kaspersky Security Center Web Console Server poprzez port TLS o numerze 8080. Kaspersky Security Center Web Console Server może zostać zainstalowany na Serwerze administracyjnym lub na innym urządzeniu.

7. Lokalny ruch sieciowy aplikacji na pojedynczym urządzeniu (na Serwerze administracyjnym lub na zarządzanym urządzeniu). Żadne porty zewnętrzne nie muszą być otwarte.

8. Dane z Serwera administracyjnego na serwery Kaspersky (takie jak dane KSN lub informacje o licencjach) oraz dane z serwerów Kaspersky na Serwer administracyjny (takie jak uaktualnienia aplikacji i aktualizacje antywirusowych baz danych) są przesyłane przy użyciu protokołu HTTPS.

   Jeśli nie chcesz, żeby Twój Serwer administracyjny miał dostęp do internetu, musisz ręcznie zarządzać tymi danymi.

9. Żądania dla pakietów z zarządzanych urządzeń, w tym urządzeń mobilnych, są przesyłane do serwera WWW, który znajduje się na tym samym urządzeniu co Serwer administracyjny.

10. Tylko dla urządzeń mobilnych z systemem Android: dane z Serwera administracyjnego są przesyłane na serwery Google. To połączenie jest używane do informowania urządzeń mobilnych Android, że są niezbędne do nawiązania połączenia z Serwerem administracyjnym. Powiadomienia push są wysyłane na urządzenia mobilne.

11. Tylko dla urządzeń mobilnych z systemem Android: powiadomienia push z serwerów Google są wysyłane na urządzenie mobilne. To połączenie jest używane do informowania urządzeń mobilnych, że są niezbędne do nawiązania połączenia z Serwerem administracyjnym.

12. Tylko dla urządzeń mobilnych z systemem iOS: dane z serwera iOS MDM są przesyłane do serwerów Apple Push Notification. Powiadomienia push są wysyłane na urządzenia mobilne.

13. Tylko dla urządzeń mobilnych z systemem iOS: powiadomienia push z serwerów Apple są wysyłane na urządzenie mobilne. To połączenie jest używane do informowania urządzeń mobilnych iOS, że są niezbędne do nawiązania połączenia z serwerem iOS MDM.

14. Tylko dla urządzeń mobilnych: dane z zarządzanej aplikacji są przesyłane do Serwera administracyjnego (lub do bramy połączenia) poprzez port TLS o numerze 13292 / 13293—bezpośrednio lub poprzez odwrotny serwer proxy.

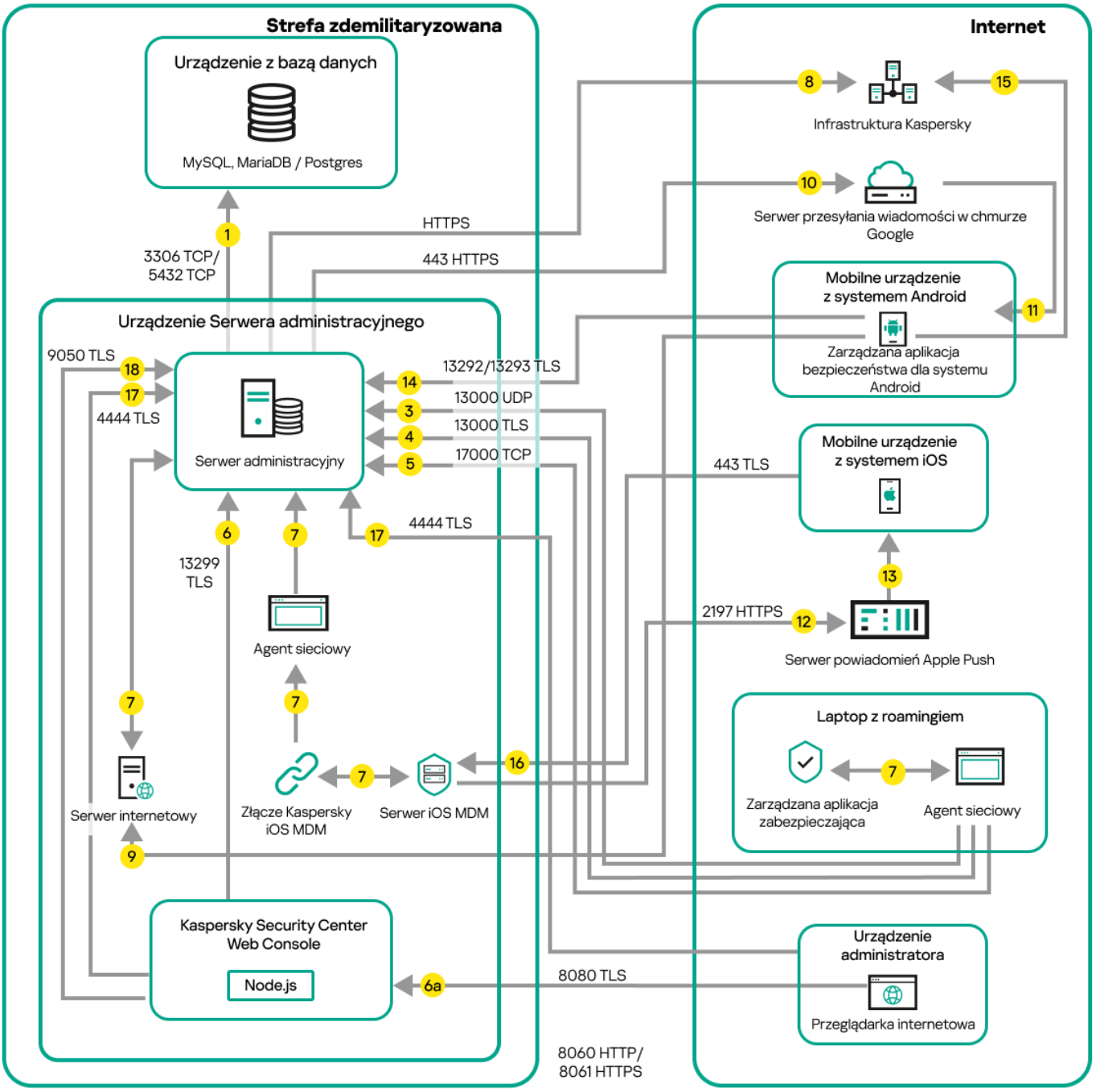
15. Tylko dla urządzeń mobilnych: dane z urządzenia mobilnego są przesyłane do infrastruktury Kaspersky.

    Jeśli urządzenie mobilne nie ma dostępu do Internetu, dane są przesyłane do Serwera administracyjnego poprzez port o numerze 17100, a Serwer administracyjny wysyła je do infrastruktury Kaspersky; jednakże ten scenariusz jest stosowany bardzo rzadko.

16. Tylko dla urządzeń mobilnych z systemem iOS: dane z urządzenia mobilnego są przesyłane za pośrednictwem portu TLS o numerze 443 na serwer iOS MDM, który znajduje się na tym samym urządzeniu co Serwer administracyjny, lub na bramie połączenia.

Serwer administracyjny w strefie DMZ, zarządzane urządzenia w Internecie

Poniższy rysunek przedstawia ruch sieciowy danych, gdy Serwer administracyjny jest w strefie zdemilitaryzowanej (DMZ), a zarządzane urządzenia są w Internecie.



Serwer administracyjny w strefie DMZ, zarządzane urządzenia mobilne w Internecie

Na tym rysunku brama połączenia nie jest używana: urządzenia mobilne nawiązują połączenie bezpośrednio z Serwerem administracyjnym.

Strzałki wskazują inicjowanie ruchu sieciowego: każda strzałka wskazuje kierunek z urządzenia, które inicjuje połączenie, do urządzenia, które „odpowiada" na połączenie. Dostarczony jest numer portu oraz nazwa protokołu użytego do przesyłania danych. Każda strzałka posiada etykietę liczby, a szczegóły dotyczące odpowiedniego ruchu danych wyglądają następująco:

1. Serwer administracyjny wysyła dane do bazy danych. Jeśli instalujesz Serwer administracyjny i bazę danych na różnych urządzeniach, musisz udostępnić potrzebne porty na urządzeniu, na którym znajduje się baza danych (na przykład: port 3306 dla MySQL Server i MariaDB Server lub port 5432 dla PostgreSQL Server lub Postgres Pro Server). Odpowiednie informacje można znaleźć w dokumentacji do DBMS.

2. Żądania komunikacji od Serwera administracyjnego są przesyłane do wszystkich niemobilnych zarządzanych urządzeń poprzez port UDP o numerze 15000.

   Agenty sieciowe wysyłają żądania do siebie nawzajem w obrębie jednej domeny broadcastowej. Dane są następnie wysyłane do Serwera administracyjnego i są używane do określenia ograniczeń domeny broadcastowej i do automatycznego przydzielenia punktów dystrybucji (jeśli ta opcja jest włączona).

   Jeżeli Serwer administracyjny nie ma bezpośredniego dostępu do zarządzanych urządzeń, żądania komunikacji z Serwera administracyjnego nie są wysyłane bezpośrednio do tych urządzeń.

3. Informacje o zamknięciu zarządzanych urządzeń są przesyłane z Agenta sieciowego do Serwera administracyjnego poprzez port UDP o numerze 13000.

4. Serwer administracyjny odbiera połączenie od Agentów sieciowych i podrzędnych Serwerów administracyjnych poprzez port TLS o numerze 13000.

   Jeśli używałeś wcześniejszej wersji Kaspersky Security Center, Serwer administracyjny w Twojej sieci może odbierać połączenia od Agentów sieciowych poprzez port inny niż TLS o numerze 14000. Kaspersky Security Center Linux obsługuje także połączenia Agentów sieciowych poprzez port 14000, chociaż zalecane jest korzystanie z portu TLS o numerze 13000.

5. Zarządzane urządzenia (za wyjątkiem urządzeń mobilnych) żądają aktywacji poprzez port TCP o numerze 17000. Nie jest to konieczne, jeśli urządzenie posiada własny dostęp do Internetu; w tym przypadku urządzenie wysyła dane do serwerów Kaspersky bezpośrednio przez Internet.

6. Kaspersky Security Center Web Console Server wysyła dane na Serwer administracyjny, który może być zainstalowany na tym samym lub innym urządzeniu, poprzez port TLS o numerze 13299.

   Komponent Menedżer tożsamości i dostępu (IAM) łączy się z Serwerem administracyjnym poprzez port TLS 13299.

   6a. Dane z przeglądarki, która jest zainstalowana na oddzielnym urządzeniu administratora, są przesyłane do Kaspersky Security Center Web Console Server poprzez port TLS o numerze 8080. Kaspersky Security Center Web Console Server może zostać zainstalowany na Serwerze administracyjnym lub na innym urządzeniu.

7. Lokalny ruch sieciowy aplikacji na pojedynczym urządzeniu (na Serwerze administracyjnym lub na zarządzanym urządzeniu). Żadne porty zewnętrzne nie muszą być otwarte.

8. Dane z Serwera administracyjnego na serwery Kaspersky (takie jak dane KSN lub informacje o licencjach) oraz dane z serwerów Kaspersky na Serwer administracyjny (takie jak uaktualnienia aplikacji i aktualizacje antywirusowych baz danych) są przesyłane przy użyciu protokołu HTTPS.

   Jeśli nie chcesz, żeby Twój Serwer administracyjny miał dostęp do internetu, musisz ręcznie zarządzać tymi danymi.

9. Żądania dla pakietów z zarządzanych urządzeń są przesyłane do serwera WWW, który znajduje się na tym samym urządzeniu co Serwer administracyjny.

10. Tylko dla urządzeń mobilnych z systemem Android: dane z Serwera administracyjnego są przesyłane na serwery Google. To połączenie jest używane do informowania urządzeń mobilnych Android, że są niezbędne do nawiązania połączenia z Serwerem administracyjnym. Powiadomienia push są wysyłane na urządzenia mobilne. Usługa FCM działa również na porcie HTTPS 443.

11. Tylko dla urządzeń mobilnych z systemem Android: powiadomienia push z serwerów Google są wysyłane na urządzenie mobilne. To połączenie jest używane do informowania urządzeń mobilnych, że są niezbędne do nawiązania połączenia z Serwerem administracyjnym.

12. Tylko dla urządzeń mobilnych z systemem iOS: dane z serwera iOS MDM są przesyłane do serwerów Apple Push Notification. Powiadomienia push są wysyłane na urządzenia mobilne.

13. Tylko dla urządzeń mobilnych z systemem iOS: powiadomienia push z serwerów Apple są wysyłane na urządzenie mobilne. To połączenie jest używane do informowania urządzeń mobilnych iOS, że są niezbędne do nawiązania połączenia z serwerem iOS MDM.

14. Tylko dla urządzeń mobilnych: dane z zarządzanej aplikacji są przesyłane do Serwera administracyjnego (lub do bramy połączenia) poprzez port TLS o numerze 13292 / 13293—bezpośrednio lub poprzez odwrotny serwer proxy.

15. Tylko dla urządzeń mobilnych: dane z urządzenia mobilnego są przesyłane do infrastruktury Kaspersky.

    Jeśli urządzenie mobilne nie ma dostępu do Internetu, dane są przesyłane do Serwera administracyjnego poprzez port o numerze 17100, a Serwer administracyjny wysyła je do infrastruktury Kaspersky; jednakże ten scenariusz jest stosowany bardzo rzadko.

16. Tylko dla urządzeń mobilnych z systemem iOS: dane z urządzenia mobilnego są przesyłane za pośrednictwem portu TLS o numerze 443 na serwer iOS MDM, który znajduje się na tym samym urządzeniu co Serwer administracyjny, lub na bramie połączenia.

17. Kaspersky Security Center Web Console Server i przeglądarka (używana z Kaspersky Security Center Web Console) łączą się z Serwerem administracyjnym za pomocą protokołu uwierzytelniania OpenID Connect przez port TLS 4444.

18. Kaspersky Security Center Web Console Server nawiązuje połączenie z Serwerem administracyjnym poprzez port TLS 9050.

Interakcja komponentów Kaspersky Security Center Linux i aplikacji zabezpieczających: więcej informacji

Ta sekcja opisuje schematy interakcji komponentów Kaspersky Security Center Linux z zarządzanymi aplikacjami zabezpieczającymi. Schematy zawierają numery portów, które muszą być dostępne, oraz nazwy procesów, które otwierają te porty.

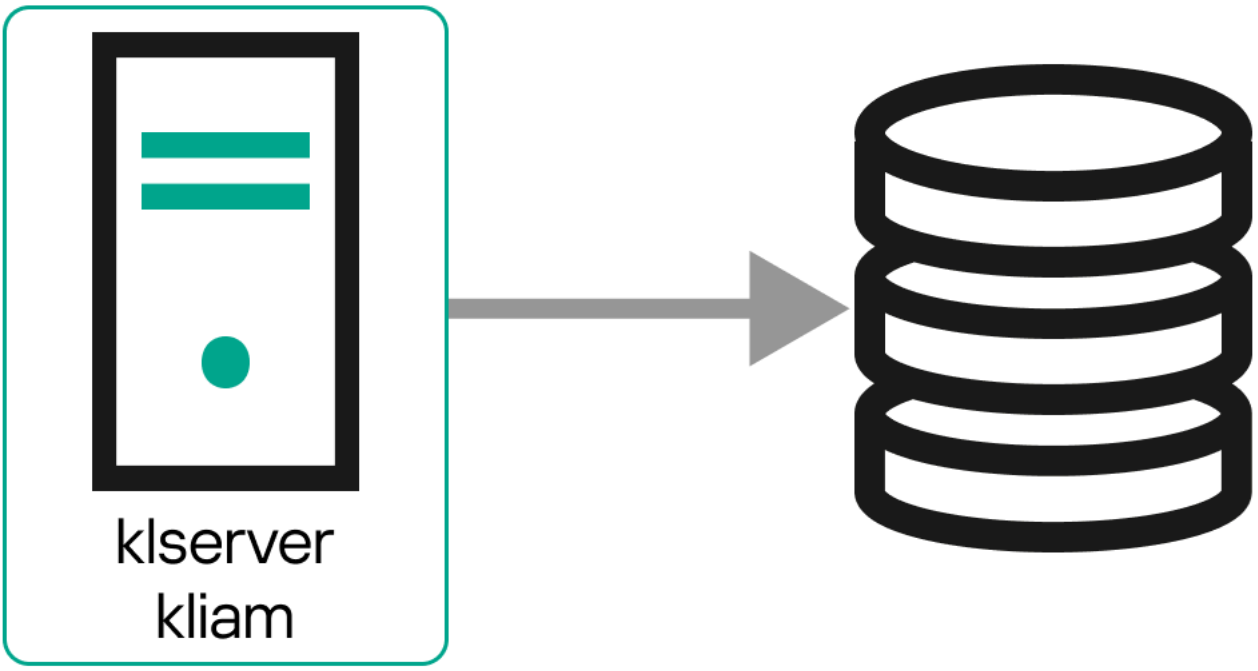
Konwencje stosowane w schematach interakcji

Poniższa tabela przedstawia konwencje stosowane w schematach.

Ikona	Znaczenie
	Serwer administracyjny
	Podrzędny Serwer administracyjny
	DBMS
	Urządzenie klienckie (na którym jest zainstalowany Agent sieciowy oraz aplikacja z rodziny Kaspersky Endpoint Security lub inna aplikacja zabezpieczająca, którą może zarządzać Kaspersky Security Center Linux)
	Brama połączenia
	Punkt dystrybucji
	Przeglądarka na urządzeniu użytkownika
klnagent	Proces uruchomiony na urządzeniu i otwierający port
13000 TLS	Port i jego numer
	Ruch TCP (kierunek strzałki przedstawia kierunek przepływu ruchu)
	Ruch UDP (kierunek strzałki przedstawia kierunek przepływu ruchu)
	Transport DBMS
	Granica strefy DMZ

Serwer administracyjny i DBMS

Dane Serwera administracyjnego i Menadżera tożsamości i dostępu (IAM) są przechowywane w oddzielnych bazach danych w ramach tego samego systemu DBMS.



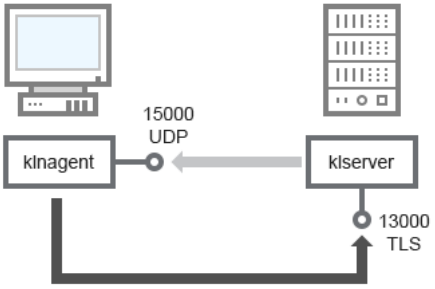
Serwer administracyjny, Menedżer tożsamości i dostępu oraz DBMS

Jeśli instalujesz Serwer administracyjny i bazę danych na różnych urządzeniach, musisz udostępnić potrzebne porty na urządzeniu, na którym znajduje się baza danych (na przykład: port 3306 dla MariaDB). Odpowiednie informacje można znaleźć w dokumentacji do DBMS.
Port służący do łączenia IAM z systemem DBMS jest określany przez użytkownika podczas instalacji Kaspersky Security Center Linux.

Serwer administracyjny nie usuwa automatycznie bazy danych Serwera administracyjnego ani bazy danych IAM podczas odinstalowywania lub przenoszenia serwera na inne urządzenie. W razie potrzeby należy usunąć bazy danych ręcznie.

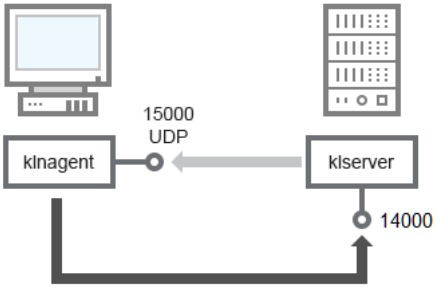
Serwer administracyjny i urządzenie klienckie: zarządzanie aplikacją zabezpieczająca

Serwer administracyjny odbiera połączenie od Agentów sieciowych za pośrednictwem portu TLS o numerze 13000 (patrz rysunek poniżej).



Serwer administracyjny i urządzenie klienckie: zarządzanie aplikacją zabezpieczająca, połączenie poprzez port 13000 (zalecane)

Jeśli używałeś wcześniejszej wersji Kaspersky Security Center Linux, Serwer administracyjny w Twojej sieci może odbierać połączenia od Agentów sieciowych poprzez port bez szyfrowania SSL o numerze 14000 (patrz rysunek poniżej). Kaspersky Security Center Linux obsługuje także połączenia Agentów sieciowych za pośrednictwem portu 14000, chociaż zalecane jest korzystanie z portu SSL o numerze 13000.



Serwer administracyjny i urządzenie klienckie: zarządzanie aplikacją zabezpieczająca, połączenie poprzez port 14000 (mniejsze bezpieczeństwo)

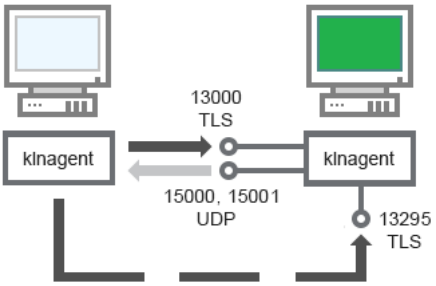
Wyjaśnienie schematów jest dostępne w tabeli poniżej.

Serwer administracyjny i urządzenie klienckie: zarządzanie aplikacją zabezpieczająca (ruch sieciowy)

Urządzenie	Numer portu	Nazwa procesu, który otwiera port	Protokół	Przeznaczenie portu
Agent sieciowy	15000	klnagent	UDP	Multiemisja dla Agentów sieciowych
Serwer administracyjny	13000	klserver	TCP (TLS)	Odbieranie połączeń od Agentów sieciowych
Serwer administracyjny	14000	klserver	TCP	Odbieranie połączeń od Agentów sieciowych

Aktualizowanie oprogramowania na urządzeniu klienckim poprzez punkt dystrybucji

Urządzenie klienckie nawiązuje połączenie z punktem dystrybucji poprzez port 13000, a jeśli używasz punktu dystrybucji jako serwera push, także poprzez port 13295; punkt dystrybucji wykonuje multiemisję do Agentów sieciowych poprzez port 15000 (patrz rysunek poniżej). Aktualizacje i pakiety instalacyjne są odbierane z punktu dystrybucji przez port 15001.



Aktualizowanie oprogramowania na urządzeniu klienckim poprzez punkt dystrybucji

Klasyfikacje schematu są dostępne w tabeli poniżej.

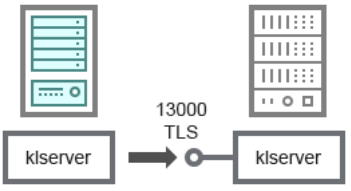
Aktualizowanie oprogramowania za pośrednictwem punktu dystrybucji (ruch sieciowy)

Urządzenie	Numer portu	Nazwa procesu, który otwiera port	Protokół	Przeznaczenie portu
Agent sieciowy	15000	klnagent	UDP	Multiemisja dla Agentów sieciowych
Agent sieciowy	15001	klnagent	UDP	Odbieranie aktualizacji i pakietów instalacyjnych z punktu dystrybucji
Punkt dystrybucji	13000	klnagent	TCP (TLS)	Odbieranie połączeń od Agentów sieciowych
Punkt dystrybucji	13295	klnagent	TCP (TLS)	Odbieranie połączeń z urządzeń klienckich (server push)

Hierarchia Serwerów administracyjnych: główny Serwer administracyjny i podrzędny Serwer administracyjny

Schemat (patrz rysunek poniżej) przedstawia korzystanie z portu 13000 do zapewnienia interakcji pomiędzy Serwerami administracyjnymi połączonymi w hierarchię.

Następnie, gdy Serwery administracyjne zostaną połączone w hierarchię, będziesz mógł zarządzać nimi przy użyciu konsoli Kaspersky Security Center Web Console połączonej z głównym Serwerem administracyjnym. Dlatego też, dostępność portu 13299 głównego Serwera administracyjnego jest niezbędnym wymaganiem.



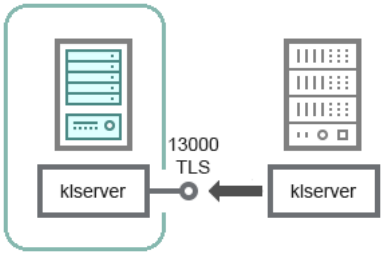
Hierarchia Serwerów administracyjnych: główny Serwer administracyjny i podrzędny Serwer administracyjny

Klasyfikacje schematu są dostępne w tabeli poniżej.

Hierarchia Serwerów administracyjnych (ruch sieciowy)

Urządzenie	Numer portu	Nazwa procesu, który otwiera port	Protokół	Przeznaczenie portu
Główny Serwer administracyjny	13000	klserver	TCP (TLS)	Odbieranie połączeń z podrzędnych Serwerów administracyjnych

Hierarchia Serwerów administracyjnych z podrzędnym Serwerem administracyjnym w strefie DMZ



Hierarchia Serwerów administracyjnych z podrzędnym Serwerem administracyjnym w strefie DMZ

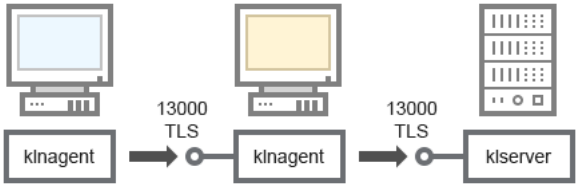
Schemat przedstawia hierarchię Serwerów administracyjnych, w której podrzędny Serwer administracyjny, znajdujący się w strefie DMZ, odbiera połączenie z głównego Serwera administracyjnego (patrz tabela poniżej dla wyjaśnienia schematu). Podczas łączenia dwóch Serwerów administracyjnych w hierarchię upewnij się, że port 13299 jest dostępny na obu Serwerach administracyjnych. Kaspersky Security Center Web Console nawiązuje połączenie z Serwerem administracyjnym poprzez port 13299.

Następnie, gdy Serwery administracyjne zostaną połączone w hierarchię, będziesz mógł zarządzać nimi przy użyciu konsoli Kaspersky Security Center Web Console połączonej z głównym Serwerem administracyjnym. Dlatego też, dostępność portu 13299 głównego Serwera administracyjnego jest niezbędnym wymaganiem.

Hierarchia Serwerów administracyjnych z podrzędnym Serwerem administracyjnym w strefie DMZ (ruch sieciowy)

Urządzenie	Numer portu	Nazwa procesu, który otwiera port	Protokół	Przeznaczenie portu
Podrzędny Serwer administracyjny	13000	klserver	TCP (TLS)	Odbieranie połączeń z głównego Serwera administracyjnego

Serwer administracyjny, brama połączenia w segmencie sieci i urządzenie klienckie



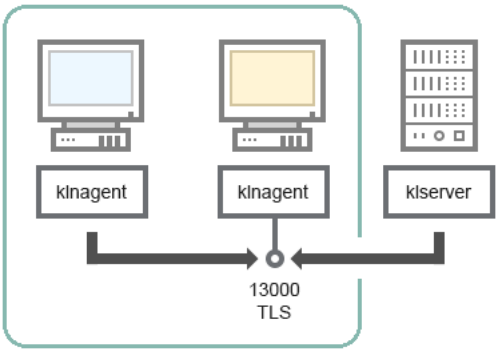
Serwer administracyjny, brama połączenia w segmencie sieci i urządzenie klienckie

Klasyfikacje schematu są dostępne w tabeli poniżej.

Serwer administracyjny, brama połączenia w segmencie sieci i urządzenie klienckie (ruch sieciowy)

Urządzenie	Numer portu	Nazwa procesu, który otwiera port	Protokół	Przeznaczenie portu
Serwer administracyjny	13000	klserver	TCP (TLS)	Odbieranie połączeń od Agentów sieciowych
Agent sieciowy	13000	klnagent	TCP (TLS)	Odbieranie połączeń od Agentów sieciowych

Serwer administracyjny i dwa urządzenia w strefie DMZ: brama połączenia i urządzenie klienckie



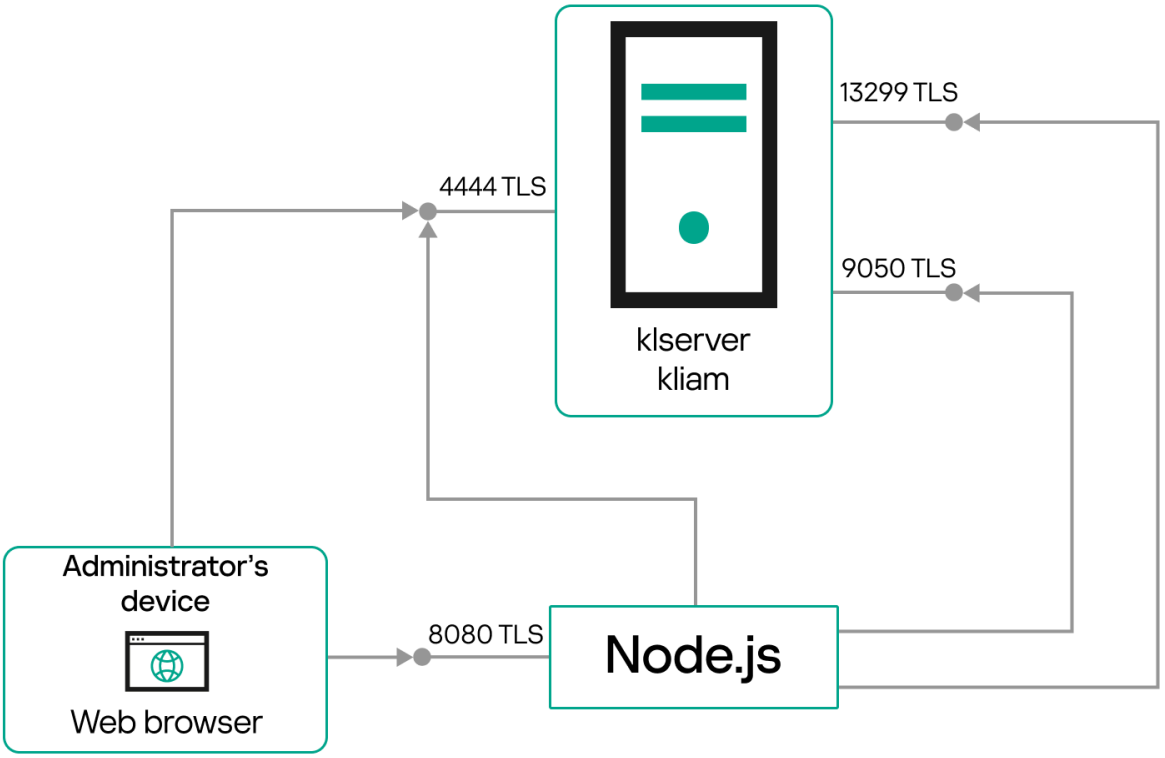
Serwer administracyjny z bramą połączenia i urządzeniem klienckim w strefie DMZ

Klasyfikacje schematu są dostępne w tabeli poniżej.

Serwer administracyjny z bramą połączenia w segmencie sieci i urządzenie klienckie (ruch sieciowy)

Urządzenie	Numer portu	Nazwa procesu, który otwiera port	Protokół	Przeznaczenie portu
Agent sieciowy	13000	klnagent	TCP (TLS)	Odbieranie połączeń od Agentów sieciowych

Serwer administracyjny i Kaspersky Security Center Web Console



Serwer administracyjny i Kaspersky Security Center Web Console

Klasyfikacje schematu są dostępne w tabeli poniżej.

Serwer administracyjny i Kaspersky Security Center Web Console (ruch sieciowy)

Urządzenie	Numer portu	Nazwa procesu, który otwiera port	Protokół	Przeznaczenie portu
Serwer administracyjny	13299	klserver	TCP (TLS)	Odbieranie połączeń z Kaspersky Security Center Web Console i Menedżera tożsamości i dostępu (IAM) do Serwera administracyjnego przez OpenAPI
Kaspersky Security Center Web Console Server lub Serwer administracyjny	8080	Node.js: Server-side JavaScript	TCP (TLS)	Odbieranie połączeń od Kaspersky Security Center Web Console
Serwer administracyjny	4444	kliam	TCP (TLS)	Odbieranie połączeń z Kaspersky Security Center Web Console Server i przeglądarki (używanej z Kaspersky Security Center Web Console) do Serwera administracyjnego z IAM przez protokół uwierzytelniania OpenID Connect
Serwer administracyjny	9050	kliam	TCP (TLS)	Odbieranie połączeń od Kaspersky Security Center Web Console do IAM

Konsola Kaspersky Security Center Web Console może zostać zainstalowana na Serwerze administracyjnym lub na innym urządzeniu.

Pierwsze kroki

Zgodnie ze scenariuszem, możesz przeprowadzić instalację Serwera administracyjnego Kaspersky Security Center Linux i konsoli Kaspersky Security Center Web Console, przeprowadzić wstępną konfigurację Serwera administracyjnego przy użyciu kreatora wstępnej konfiguracji, a także instalację aplikacji firmy Kaspersky na zarządzanych urządzeniach przy użyciu kreatora wdrażania ochrony.

Wymagania wstępne

Musisz posiadać klucz licencyjny (kod aktywacyjny) do Kaspersky Endpoint Security for Business lub klucze licencyjne (kody aktywacyjne) do aplikacji zabezpieczających Kaspersky.

Jeśli najpierw chcesz wypróbować Kaspersky Security Center Linux, możesz uzyskać bezpłatną, 30-dniową wersję testową na stronie internetowej Kaspersky.

Etapy

Główny scenariusz instalacji przebiega etapami:

1. **Wybieranie struktury ochrony organizacji**

   Zapoznaj się ze szczegółowymi informacjami dotyczącymi komponentów Kaspersky Security Center Linux. W oparciu o konfigurację sieci i przepustowość kanałów komunikacji, zdefiniuj liczbę używanych Serwerów administracyjnych oraz sposób ich dystrybucji pomiędzy biurami (jeśli pracujesz w sieci rozproszonej).

   Zdefiniuj, czy hierarchia Serwerów administracyjnych będzie używana w organizacji. W tym celu należy oszacować, czy jest to możliwe i korzystne, aby wszystkie urządzenia kliencie były zarządzane przez jeden Serwer administracyjny i czy konieczne jest tworzenie hierarchii Serwerów administracyjnych. Konieczne może być też utworzenie hierarchii Serwerów administracyjnych, która jest taka sama, jak struktura organizacyjna firmy, której sieć chcesz chronić.

2. **Przygotowanie do użycia certyfikatów niestandardowych**

   Jeśli infrastruktura kluczy publicznych (PKI) Twojej organizacji wymaga użycia certyfikatów niestandardowych opublikowanych przez określony Urząd certyfikacji (CA), przygotuj te certyfikaty i upewnij się, że spełniają wszystkie wymagania.

3. **Instalowanie systemu zarządzania bazą danych (DBMS)**

   Zainstaluj system DBMS, który będzie używany przez Kaspersky Security Center Linux lub użyj istniejącego systemu.

   Możesz wybrać jeden z obsługiwanych DBMS. Informacje o sposobie zainstalowania wybranego systemu DBMS znajdziesz w tym dokumencie.

   Jeśli dystrybucja Twojego systemu operacyjnego opartego na systemie Linux nie zawiera obsługiwanego systemu DBMS, możesz zainstalować system DBMS z repozytorium pakietów firmy trzeciej. Jeśli instalowanie dystrybucji z repozytoriów firm trzecich jest zabronione, możesz zainstalować DBMS na osobnym urządzeniu.

Jeśli zdecydujesz się zainstalować PostgreSQL lub Postgres Pro DBMS, upewnij się, że określone zostało hasło superużytkownika. Jeśli hasło nie zostanie określone, Serwer administracyjny może nie być w stanie połączyć się z bazą danych.

Jeśli instalujesz MariaDB, PostgreSQL lub Postgres Pro, użyj zalecanych ustawień, aby zapewnić prawidłowe działanie DBMS.

Jeśli chcesz zmienić typ systemu DBMS po instalacji, musisz ponownie zainstalować Kaspersky Security Center Linux. Możesz wyeksportować zadania i zasady, aby zaimportować je po ponownej instalacji. Zapoznaj się z następującymi artykułami: Eksportowanie zadania, Eksportowanie zasady.

4. **Konfigurowanie portów**

   Upewnij się, że wszystkie niezbędne porty są otwarte do interakcji pomiędzy komponentami zgodnie z wybrana strukturą bezpieczeństwa.

   Jeśli musisz zapewnić Serwerowi administracyjnemu dostęp do Internetu, skonfiguruj porty i określ ustawienia połączenia, w zależności od konfiguracji sieci.

5. **Instalowanie Kaspersky Security Center Linux**

   Wybierz urządzenie z systemem Linux, którego chcesz używać jako Serwera administracyjnego, upewnij się, że spełnia ono wymagania sprzętowe i programowe, a następnie zainstaluj na nim Kaspersky Security Center Linux. Wersja serwerowa Agenta sieciowego zostanie automatycznie zainstalowana na urządzeniu wraz z Serwerem administracyjnym.

6. **Instalacja programu Kaspersky Security Center Web Console i webowych wtyczek administracyjnych**

   Wybierz urządzenie Linux, którego zamierzasz używać jako stację roboczą administratora, upewnij się, że spełnia ono wymagania programowe i sprzętowe, a następnie zainstaluj na nim Kaspersky Security Center Web Console. Możesz zainstalować Kaspersky Security Center Web Console również na tym samym urządzeniu, na którym jest zainstalowany Serwer administracyjny, lub na innym.

   Pobierz webową wtyczkę administracyjną Kaspersky Endpoint Security for Linux a następnie zainstaluj go na tym samym urządzeniu, na którym zainstalowano Kaspersky Security Center Web Console.

7. **Instalowanie Kaspersky Endpoint Security for Linux i Agenta sieciowego na urządzeniu Serwera administracyjnego**

   Domyślnie aplikacja nie traktuje urządzenia Serwera administracyjnego jako urządzenia zarządzanego. Aby chronić Serwer administracyjny przed wirusami i innymi zagrożeniami oraz zarządzać urządzeniem jak każdym innym zarządzanym urządzeniem, zalecamy zainstalowanie Kaspersky Endpoint Security for Linux i Agenta sieciowego dla systemu Linux na urządzeniu Serwera administracyjnego. W takim przypadku Agent sieciowy dla systemu Linux jest instalowany i działa niezależnie od wersji serwerowej Agenta sieciowego zainstalowanego wraz z Serwerem administracyjnym.

8. **Przeprowadzanie wstępnej konfiguracji**

   Po zakończeniu instalacji Serwera administracyjnego, przy pierwszym połączeniu z Serwerem administracyjnym kreator wstępnej konfiguracji zostanie uruchomiony automatycznie. Przeprowadź wstępną konfigurację Serwera administracyjnego zgodnie z istniejącymi wymaganiami. Na etapie wstępnej konfiguracji kreator używa domyślnych ustawień do tworzenia zasad i zadań, które są niezbędne do wdrożenia ochrony. Jednakże ustawienia domyślne mogą być mniej niż optymalne dla potrzeb Twojej organizacji. Jeśli to konieczne, możesz edytować ustawienia zasad i zadań.

9. **Wyszukiwanie urządzeń w sieci**

   Odkryj urządzenia ręcznie. Kaspersky Security Center Linux pobiera adresy i nazwy wszystkich urządzeń wykrytych w sieci. Następnie możesz użyć Kaspersky Security Center Linux do zainstalowania aplikacji firmy Kaspersky i oprogramowania innych producentów na wykrytych urządzeniach. Kaspersky Security Center Linux regularnie uruchamia wyszukiwanie urządzeń, co oznacza, że jeśli nowe instancje pojawią się w sieci, zostaną wykryte automatycznie.

10. **Rozmieszczanie urządzeń w grupach administracyjnych**

    W niektórych przypadkach, wdrożenie ochrony na urządzeniach w sieci w najbardziej wygodny sposób może wymagać podzielenia całej puli urządzeń na grupy administracyjne, z uwzględnieniem struktury organizacji. Możesz utworzyć reguły przenoszenia urządzeń pomiędzy grupami lub możesz ręcznie przenieść urządzenia. Możesz przypisać zadania grupowe dla grup administracyjnych, zdefiniować obszar zasad oraz przypisać punkty dystrybucji.

    Upewnij się, że wszystkie zarządzane urządzenia zostały poprawnie przydzielone do odpowiednich grup administracyjnych i że w sieci nie ma żadnego nieprzypisanego urządzenia.

11. **Przypisywanie punktów dystrybucji**

    Punkty dystrybucji są przydzielane do grup administracyjnych automatycznie, ale możesz też przydzielić je ręcznie. Zalecane jest użycie punktów dystrybucji w sieciach dużej skali w celu zmniejszenia obciążenia na Serwerze administracyjnym, a także w sieciach, które posiadają strukturę rozproszoną, aby zapewnić Serwerowi administracyjnemu dostęp do urządzeń (lub grup urządzeń) komunikujących się przez kanały o niskiej przepustowości.

12. **Instalowanie Agenta sieciowego i aplikacji zabezpieczających na urządzeniach w sieci**

    Wdrożenie ochrony w sieci firmowej obejmuje instalację Agenta sieciowego i aplikacji zabezpieczających na urządzeniach, które zostały wykryte przez Serwer administracyjny podczas wykrywania urządzenia.

    Aby zdalnie zainstalować aplikacje, uruchom Kreator wdrażania ochrony.

    Aplikacje zabezpieczające chronią urządzenia przed wirusami i innymi programami stwarzającymi zagrożenie. Agent sieciowy zapewnienia komunikację pomiędzy urządzeniem a Serwerem administracyjnym. Domyślnie ustawienia Agenta sieciowego są konfigurowane automatycznie.

    Przed rozpoczęciem instalacji Agenta sieciowego i aplikacji zabezpieczających na urządzeniach w sieci, upewnij się, że te urządzenia są dostępne (włączone).

13. **Rozsyłanie kluczy licencyjnych na urządzenia klienckie**

    Roześlij klucze licencyjne na urządzenia klienckie, aby aktywować zarządzane aplikacje zabezpieczające na tych urządzeniach.

14. **Konfigurowanie zasad aplikacji Kaspersky**

    Aby zastosować różne ustawienia aplikacji na różnych urządzeniach, możesz użyć zarządzania ochroną skoncentrowaną na urządzeniu i/lub zarządzania ochroną skoncentrowaną na użytkowniku. Zarządzanie ochroną skoncentrowaną na urządzeniu może zostać zaimplementowane przy użyciu zasad i zadań. Możesz zastosować zadania tylko do tych urządzeń, które spełniają określone warunki. Aby ustawić warunki filtrowania urządzeń, użyj znaczników i wyborów urządzeń.

15. **Monitorowanie stanu ochrony sieci**

    Możesz monitorować swoją sieć przy użyciu widżetów na panelu nawigacyjnym, generować raporty z aplikacji Kaspersky, konfigurować i przeglądać wybory zdarzeń otrzymane z aplikacji na zarządzanych urządzeniach, a także przeglądać listy powiadomień.

Przewodnik po zwiększaniu odporności

Kaspersky Security Center Linux służy do scentralizowanego wykonywania podstawowych zadań dotyczących administracji i zarządzania w sieci firmy. Aplikacja zapewnia administratorowi dostęp do szczegółowych informacji o poziomie bezpieczeństwa sieci organizacji. Kaspersky Security Center Linux umożliwia skonfigurowanie wszystkich komponentów ochrony zbudowanych przy użyciu aplikacji Kaspersky.

Serwer administracyjny Kaspersky Security Center Linux ma pełny dostęp do zarządzania ochroną urządzeń klienckich i jest najważniejszym komponentem systemu bezpieczeństwa organizacji. Dlatego dla Serwera administracyjnego wymagane są zwiększone metody ochrony.

Przed rozpoczęciem konfiguracji utwórz kopię zapasową Serwera administracyjnego Kaspersky Security Center Linux za pomocą zadania Kopia zapasowa danych Serwera administracyjnego lub narzędzia klbackup i zapisz ją w bezpiecznym miejscu.

Przewodnik po zwiększaniu odporności opisuje zalecenia i funkcje konfigurowania Kaspersky Security Center Linux i jego komponentów, mające na celu zmniejszenie ryzyka związanego z jego włamaniem.

Przewodnik po zwiększaniu odporności zawiera następujące informacje:

- Wybór architektury Serwera administracyjnego
- Konfigurowanie bezpiecznego połączenia z Serwerem administracyjnym
- Konfigurowanie kont w celu uzyskania dostępu do Serwera administracyjnego
- Zarządzanie ochroną Serwera administracyjnego
- Zarządzanie ochroną urządzeń klienckich
- Konfigurowanie ochrony dla zarządzanych aplikacji
- Konserwacja Serwera administracyjnego
- Przesyłanie informacji do aplikacji firm trzecich
- Zalecenia dotyczące bezpieczeństwa systemów informatycznych innych firm

Lista kontrolna wzmocnienia zabezpieczeń

Wdrożenie Serwera administracyjnego

- Zainstaluj Serwer administracyjny na dedykowanym serwerze fizycznym lub wirtualnym.
- Nie używaj dedykowanego serwera do uruchamiania innych usług.

- Nie instaluj Serwera administracyjnego (zwanego dalej Serwerem) na:
  - Kontrolerze domeny
  - Serwerze terminalowym
  - Urządzeniu użytkownika

Bezpieczeństwo połączenia

- Skonfiguruj zaporę sieciową, aby ograniczyć dostęp do urządzenia Serwera na wszystkich portach i protokołach z wyjątkiem portów wymaganych przez Serwer. Zezwól na dostęp do urządzenia Serwera tylko z zaufanych urządzeń.
- Skonfiguruj listę dozwolonych adresów IP dla portów Serwera używanych do łączenia Kaspersky Security Center Web Console (zwanej również Web Console) z Serwerem.
- Skonfiguruj zaporę sieciową, aby zezwalała na dostęp do Serwera za pośrednictwem Web Console tylko z zaufanych urządzeń.
- Skonfiguruj protokół TLS w wersji 1.2 lub nowszej na Serwerze.
- Skonfiguruj zaporę sieciową, aby ograniczyć dostęp do urządzenia z zainstalowanym systemem DBMS Serwera.
- Skonfiguruj uwierzytelnianie SSL między Serwerem a systemem DBMS (MySQL lub PostgreSQL).

Konta i autoryzacja

- Skonfiguruj uwierzytelnianie dwuskładnikowe (TOTP, RFC 6238) w celu uzyskania dostępu do Serwera.
- Zdecydowanie nie zalecamy instalowania aplikacji uwierzytelniającej na tym samym urządzeniu, z którego nawiązywane jest połączenie z Serwerem poprzez Web Console.
- Zalecamy używanie uwierzytelniania wieloskładnikowego (MFA) do uwierzytelniania na urządzeniu Serwera przy użyciu tokena, inteligentnej karty lub innej metody.
- Utwórz dedykowaną grupę administracyjną i stwórz dla niej specjalną zasadę zabezpieczeń.
- Ogranicz liczbę użytkowników z rolą Administratora głównego.
- Skonfiguruj prawa dostępu do funkcji Serwera na podstawie ról użytkowników i grup.
- Zezwól na instalację zdalną aplikacji tylko dla oddzielnego konta użytkownika.
- Przeprowadzaj regularny audyt wszystkich użytkowników na Serwerze.

Zarządzanie ochroną Serwera administracyjnego

- Zainstaluj aplikację zabezpieczającą na urządzeniu Serwera:
  - Dla serwera fizycznego – Kaspersky Endpoint Security
  - Dla serwera wirtualnego – Kaspersky Security for Virtualization
- Utwórz i zastosuj osobną zasadę ochrony Serwera (inną niż zasada zabezpieczeń dla innych zarządzanych urządzeń).
- Utwórz i zastosuj osobne hasło do ochrony Serwera (inne niż hasło dla innych zarządzanych urządzeń).
- Włącz wszystkie dostępne moduły ochrony w aplikacji zabezpieczającej (informacje o zalecanych minimalnych ustawieniach zabezpieczeń wymaganych do pracy z Kaspersky Security Center Linux można znaleźć w Pomocy online programu Kaspersky Endpoint Security for Linux).

Konfigurowanie zasad i zadań dla zarządzanych aplikacji

- Utwórz i zastosuj zasady dla wszystkich zarządzanych urządzeń lub dla grupy zawierającej nowe zarządzane urządzenia dla następujących aplikacji:
  - Agent sieciowy
  - Kaspersky Endpoint Security for Windows/Linux/macOS
  - Kaspersky Endpoint Agent (lub inne aplikacje Kaspersky)
- Włącz ochronę hasłem przed wyłączeniem ochrony lub odinstalowaniem aplikacji Kaspersky.
- Zablokuj ustawienia zasad (zamknij „blokadę"), aby zapobiec ponownemu przypisaniu tych ustawień na zarządzanych urządzeniach.
- Utwórz zaplanowane zadanie pełnego skanowania wszystkich urządzeń.
- Włącz korzystanie z Kaspersky Security Network (KSN) i zaakceptuj najnowszą wersję Oświadczenia KSN.
- Skonfiguruj wykrywanie urządzeń i określ domyślną grupę administracyjną dla nowo wykrytych urządzeń.
- Zalecamy ograniczenie stosowania automatycznych reguł przenoszenia urządzeń między grupami administracyjnymi.
- Chroń punkty dystrybucji przed nieautoryzowanym dostępem.
- Unikaj automatycznego przypisywania punktów dystrybucji w małych sieciach lub sieciach o wysokim priorytecie.

Konserwacja Serwera administracyjnego

- Nie usuwaj ani nie wyłączaj następujących zadań:
  - Kopia zapasowa
  - Konserwacja Serwera administracyjnego
- Regularnie instaluj aktualizacje systemu operacyjnego i aktualizacje oprogramowania innych firm.

Transfer zdarzeń do systemów innych producentów

- Skonfiguruj monitorowanie i raportowanie zdarzeń bezpieczeństwa.
- Skonfiguruj eksportowania zdarzenia do systemu SIEM.
- Skonfiguruj powiadomienia Serwera dla:
  - Zdarzeń audytu
  - Zdarzenia krytyczne
  - Zdarzeń błędu i ostrzeżeń

Zalecenia dotyczące bezpieczeństwa systemów informatycznych innych firm

- Zastosuj zalecenia bezpieczeństwa CIS Benchmarks do używanych systemów operacyjnych, DBMS i hipernadzorców.
- W przypadku Astra Linux należy przestrzegać zaleceń dotyczących bezpieczeństwa zawartych w odpowiedniej wersji Red Book.
- W przypadku systemu RED OS należy przestrzegać zaleceń zawartych w oficjalnej dokumentacji systemu RED OS.

Wdrożenie Serwera administracyjnego

Architektura Serwera administracyjnego

Ogólnie rzecz biorąc, wybór scentralizowanej architektury zarządzania zależy od lokalizacji chronionych urządzeń, dostępu z sąsiednich sieci, schematów dostarczania aktualizacji baz danych i tak dalej.

Na początkowym etapie rozwoju architektury zalecamy zapoznanie się z komponentami Kaspersky Security Center Linux i ich wzajemną interakcją, a także ze schematami ruchu danych i wykorzystania portów.

Na podstawie tych informacji można utworzyć architekturę, która określa:

- Lokalizacja Serwera administracyjnego i połączenia sieciowe
- Organizacja obszarów roboczych administratora i metody łączenia się z Serwerem administracyjnym
- Metody wdrożenia agenta sieciowego i oprogramowania zabezpieczającego
- Korzystanie z punktów dystrybucji
- Korzystanie z wirtualnych Serwerów administracyjnych
- Użycie hierarchii Serwerów administracyjnych
- Schemat aktualizacji antywirusowej bazy danych
- Inne przepływy informacji

Wybieranie urządzenia do instalacji Serwera administracyjnego

Zalecamy zainstalowanie Serwera administracyjnego na serwerze dedykowanym w infrastrukturze organizacji. Jeśli na serwerze nie jest zainstalowane żadne inne oprogramowanie innych firm, możesz skonfigurować ustawienia bezpieczeństwa w oparciu o wymagania Kaspersky Security Center Linux, bez zależności od wymagań oprogramowania innych firm.

Możesz zainstalować Serwer administracyjny na serwerze fizycznym lub na serwerze wirtualnym. Prosimy upewnić się, że wybrane urządzenie spełnia wymagania sprzętowe i programowe.

Ograniczenie instalacji Serwera administracyjnego na kontrolerze domeny, serwerze terminali lub urządzeniu użytkownika

Zdecydowanie nie zalecamy instalowania Serwera administracyjnego na kontrolerze domeny, serwerze terminali lub urządzeniu użytkownika.

Zalecamy zapewnienie funkcjonalnej separacji kluczowych węzłów sieci. Takie podejście pozwala zachować funkcjonalność różnych systemów, gdy węzeł ulegnie awarii lub zostanie naruszony. Jednocześnie możesz tworzyć różne zasady zabezpieczeń dla każdego węzła.

Konta do instalowania i uruchamiania Serwera administracyjnego

Podczas instalacji Serwera administracyjnego konieczne jest utworzenie dwóch kont bez uprawnień. Usługi zawarte w Serwerze administracyjnym będą działać na tych kontach bez uprawnień. Przestrzegaj zasady najmniejszych uprawnień, gdy przyznajesz prawa i uprawnienia do kont. Unikaj dołączania niepotrzebnych kont do grupy „kladmins”.

Musisz także utworzyć wewnętrzne konto DBMS. Serwer administracyjny używa tego wewnętrznego konta DBMS do uzyskania dostępu do wybranego DBMS.

Zestaw wymaganych kont i ich uprawnienia zależą od wybranego typu DBMS oraz metody tworzenia bazy danych Serwera administracyjnego.

Bezpieczeństwo połączenia

Użycie TLS

Zalecamy zablokowanie niezabezpieczonych połączeń z Serwerem administracyjnym. Na przykład, możesz zabronić połączeń korzystających z HTTP w ustawieniach Serwera administracyjnego.

Należy pamiętać, że domyślnie kilka portów HTTP Serwera administracyjnego jest zamkniętych. Pozostały port jest używany przez serwer WWW Serwera administracyjnego (8060). Ten port może być ograniczony przez ustawienia zapory sieciowej urządzenia Serwera administracyjnego.

Ścisłe ustawienia TLS

Zalecamy korzystanie z protokołu TLS w wersji 1.2 lub nowszej oraz ograniczanie lub blokowanie niezabezpieczonych algorytmów szyfrowania.

Możesz skonfigurować protokoły szyfrowania (TLS) używane przez Serwer administracyjny. Należy pamiętać, że w momencie wydania wersji Serwera administracyjnego ustawienia protokołu szyfrowania są domyślnie skonfigurowane w celu zapewnienia bezpiecznego przesyłania danych.

Ograniczanie dostępu do bazy danych Serwera administracyjnego

Zalecamy ograniczenie dostępu do bazy danych Serwera administracyjnego. Na przykład, udzielasz dostępu tylko z urządzenia Serwera administracyjnego. Zmniejsza to prawdopodobieństwo naruszenia bezpieczeństwa bazy danych Serwera administracyjnego z powodu znanych luk w zabezpieczeniach.

Możesz skonfigurować parametry zgodnie z instrukcją obsługi używanej bazy danych, a także udostępnić zamknięte porty na zaporach ogniowych.

Interakcja bezpieczeństwa z zewnętrznym systemem DBMS

Jeżeli system DBMS jest instalowany na oddzielnym urządzeniu podczas instalacji Serwera administracyjnego (zewnętrzny system DBMS), zalecamy skonfigurowanie parametrów bezpiecznej interakcji i uwierzytelniania z tym systemem DBMS. Aby uzyskać więcej informacji na temat konfigurowania uwierzytelniania SSL, zobacz Uwierzytelnianie serwera PostgreSQL i Scenariusz: Uwierzytelnianie serwera MySQL.

Konfigurowanie listy zezwolonych adresów IP do łączenia się z Serwerem administracyjnym

Domyślnie użytkownicy Kaspersky Security Center Linux mogą logować się do Kaspersky Security Center Linux z dowolnego urządzenia, na którym zainstalowana jest Kaspersky Security Center Web Console lub aplikacje OpenAPI. Możesz skonfigurować serwer administracyjny tak, aby użytkownicy mogli łączyć się z nim tylko z urządzeń o dozwolonych adresach IP. W takim przypadku, jeśli intruz spróbuje nawiązać połączenie z Kaspersky Security Center Linux za pośrednictwem Kaspersky Security Center Web Console Server zainstalowanego na urządzeniu, które nie znajduje się na liście zezwolonych, nie będzie mógł zalogować się do Kaspersky Security Center Linux.

Konfigurowanie listy zezwolonych adresów IP do łączenia się z Kaspersky Security Center Web Console

Domyślnie użytkownicy Kaspersky Security Center Linux mogą łączyć się z Kaspersky Security Center Web Console z dowolnego urządzenia. Na urządzeniu z Kaspersky Security Center Web Console należy skonfigurować zaporę sieciową (wbudowaną w system operacyjny lub innej firmy), aby użytkownicy mogli łączyć się z Kaspersky Security Center Web Console wyłącznie z dozwolonych adresów IP.

Bezpieczeństwo połączenia z kontrolerem domeny podczas przeszukiwania

Aby przeszukać kontroler domeny, Serwer administracyjny lub punkt dystrybucji systemu Linux próbuje połączyć się z tą domeną przez protokół LDAPS. Domyślnie weryfikacja certyfikatu nie jest wymagana podczas łączenia. Aby wymusić weryfikację certyfikatu, należy ustawić flagę `KLNAG_LDAP_TLS_REQCERT` na 1. Można również określić niestandardową ścieżkę do urzędu certyfikacji (CA) w celu uzyskania dostępu do łańcucha certyfikatów, korzystając z flagi `KLNAG_LDAP_SSL_CACERT`.

Konta i uwierzytelnianie

Przed wykonaniem poniższych kroków utwórz kopię zapasową danych Serwera administracyjnego Kaspersky Security Center Linux przy użyciu zadania Kopia zapasowa danych Serwera administracyjnego lub narzędzia klbackup i zapisz ją w bezpiecznym miejscu.

Używanie uwierzytelniania dwuskładnikowego z Serwerem administracyjnym

Kaspersky Security Center Linux korzysta z uwierzytelniania dwuskładnikowego do logowania się do Kaspersky Security Center Web Console, w oparciu o standard RFC 6238 (TOTP: Algorytm czasowego hasła jednorazowego).

Za każdym razem, gdy logujesz się do Kaspersky Security Center Web Console, wprowadzasz swoją nazwę użytkownika, hasło i dodatkowy jednorazowy kod bezpieczeństwa. Aby otrzymać jednorazowy kod bezpieczeństwa, musisz zainstalować aplikację uwierzytelniającą na swoim komputerze lub urządzeniu mobilnym.

Istnieją zarówno programowe, jak i sprzętowe uwierzytelniacze (tokeny), które obsługują standard RFC 6238. Na przykład uwierzytelniacze oprogramowania obejmują Google Authenticator, Microsoft Authenticator, FreeOTP.

Zdecydowanie nie zalecamy instalowania aplikacji uwierzytelniającej na tym samym urządzeniu, z którego nawiązywane jest połączenie z Serwerem administracyjnym. Możesz zainstalować aplikację uwierzytelniającą na swoim urządzeniu mobilnym.

Używanie uwierzytelniania dwuskładnikowego dla systemu operacyjnego

Aby zapewnić kompleksową ochronę przy użyciu uwierzytelniania dwuskładnikowego, konieczne jest zabezpieczenie nie tylko Serwera administracyjnego, ale także urządzenia, na którym jest zainstalowany.

Podczas łączenia się z urządzeniem, na którym zainstalowany jest Serwer administracyjny (przez SSH, RDP lub inne protokoły), zalecamy korzystanie z uwierzytelniania wieloskładnikowego (MFA) z tokenem, kartą inteligentną lub inną metodą uwierzytelniania.

Ograniczenie możliwości zapisywania hasła administratora

Jeśli korzystasz z Kaspersky Security Center Web Console, nie zalecamy zapisywania hasła administratora w przeglądarce zainstalowanej na urządzeniu użytkownika.

Uwierzytelnianie wewnętrznego konta użytkownika

Domyślnie hasło do konta użytkownika wewnętrznego Serwera administracyjnego musi być zgodne z następującymi zasadami:

- Hasło musi zawierać od 8 do 256 znaków.
- Hasło musi zawierać znaki z przynajmniej trzech z poniższych grup:
  - Wielkie litery (A-Z)
  - Małe litery (a-z)
  - Cyfry (0-9)
  - Znaki specjalne (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)
- Hasło nie może zawierać spacji, znaków Unicode lub kombinacji znaków „.” i „@”, gdy „.” jest umieszczane przed „@”.

Domyślnie, maksymalna liczba dozwolonych prób wprowadzenia hasła to 10. Możesz zmienić liczby dozwolonych prób wprowadzenia hasła.

Użytkownik Kaspersky Security Center Linux może wprowadzić niepoprawne hasło ograniczoną liczbę razy. Po osiągnięciu limitu, konto użytkownika zostaje zablokowane na godzinę.

Konfigurowanie opcji zmiany hasła konta użytkownika wewnętrznego

Zalecamy skonfigurowanie następujących opcji w celu zmiany hasła konta użytkownika wewnętrznego:

- Okres rotacji hasła
- Konfigurowanie czasu wstępnego ostrzeżenia o konieczności zmiany hasła
- Wartość opcji **Użytkownik musi zmienić hasło przy pierwszym logowaniu**

Ochrona przed nieautoryzowaną modyfikacją

Zalecamy włączenie dodatkowej opcji chroniącej konto użytkownika wewnętrznego Serwera administracyjnego przed nieautoryzowaną modyfikacją. Tę ochronę należy skonfigurować osobno dla każdego użytkownika wewnętrznego.

Dedykowana grupa administracyjna dla Serwera administracyjnego

Zalecamy utworzenie dedykowanej grupy administracyjnej dla Serwera administracyjnego. Przyznaj tej grupie specjalne prawa dostępu i utwórz dla niej specjalną zasadę zabezpieczeń.

Aby uniknąć celowego obniżania poziomu bezpieczeństwa Serwera administracyjnego, zalecamy ograniczenie listy kont, które mogą zarządzać dedykowaną grupą administracyjną.

Ograniczanie przypisywania roli głównego administratora

Użytkownikowi utworzonemu przez narzędzie kladduser przypisywana jest rola głównego administratora na liście kontroli dostępu (ACL) Serwera administracyjnego lub wirtualnego Serwera administracyjnego. Zalecamy unikanie przypisywania roli głównego administratora dużej liczbie użytkowników.

Konfigurowanie praw dostępu do funkcji aplikacji

Zalecamy korzystanie z elastycznej konfiguracji praw dostępu do funkcji Kaspersky Security Center Linux dla każdego użytkownika lub grupy użytkowników.

Kontrola dostępu oparta na rolach umożliwia tworzenie standardowych ról użytkowników z predefiniowanym zestawem uprawnień i przypisywanie tych ról użytkownikom w zależności od ich zakresu obowiązków.

Główne zalety modelu kontroli dostępu opartego na rolach:

- Łatwość administracji
- Hierarchia ról
- Podejście w oparciu o najmniejsze uprawnienia
- Podział obowiązków

Możesz przypisywać wbudowane role do określonych pracowników na podstawie ich stanowisk lub tworzyć zupełnie nowe role.

Podczas konfigurowania ról zwróć uwagę na uprawnienia związane ze zmianą stanu ochrony urządzenia Serwera administracyjnego i zdalną instalacją oprogramowania firm trzecich:

- Zarządzanie grupami administracyjnymi.
- Operacje z Serwerem administracyjnym.
- Instalacja zdalna.
- Zmiana parametrów przechowywania zdarzeń i wysyłania powiadomień.

  To uprawnienie umożliwia ustawienie powiadomień uruchamiających skrypt lub moduł wykonywalny na urządzeniu Serwera administracyjnego po wystąpieniu zdarzenia.

Osobne konto do zdalnej instalacji aplikacji

Oprócz podstawowego zróżnicowania praw dostępu, zalecamy ograniczenie zdalnej instalacji aplikacji dla wszystkich kont (z wyjątkiem Głównego Administratora lub innego konta specjalistycznego).

Zalecamy korzystanie z osobnego konta do zdalnej instalacji aplikacji. Możesz przypisać rolę lub uprawnienia do osobnego konta.

Regularny audyt wszystkich użytkowników i działań użytkowników

Zalecamy przeprowadzanie regularnego audytu wszystkich użytkowników na urządzeniu Serwera administracyjnego. Pozwala to reagować na określone rodzaje zagrożeń bezpieczeństwa związanych z możliwym naruszeniem bezpieczeństwa urządzenia.

Można także śledzić działania użytkowników, takie jak łączenie się i rozłączanie z Serwerem administracyjnym, łączenie się z Serwerem administracyjnym z błędem, a także modyfikacje obiektów (w przypadku obiektów obsługujących zarządzanie wersjami).

Zarządzanie ochroną Serwera administracyjnego

Wybieranie oprogramowania zabezpieczającego Serwer administracyjny

W zależności od typu wdrożenia Serwera administracyjnego i ogólnej strategii ochrony wybierz aplikację, która ma chronić urządzenie Serwera administracyjnego.

Jeśli instalujesz Serwer administracyjny na dedykowanym urządzeniu, zalecamy wybranie aplikacji Kaspersky Endpoint Security w celu ochrony urządzenia Serwera administracyjnego. Pozwala to na zastosowanie wszystkich dostępnych technologii do ochrony urządzenia Serwera administracyjnego, w tym modułów analizy behawioralnej.

Jeżeli Serwer administracyjny jest zainstalowany na urządzeniu, które istnieje w infrastrukturze i było wcześniej używane do innych zadań, zalecamy rozważenie następującego oprogramowania zabezpieczającego:

- Kaspersky Industrial CyberSecurity for Nodes. Zalecamy zainstalowanie tej aplikacji na urządzeniach wchodzących w skład sieci przemysłowej. Kaspersky Industrial CyberSecurity for Nodes to aplikacja, która posiada certyfikaty kompatybilności z różnymi producentami oprogramowania przemysłowego.

- Zalecane produkty zabezpieczające. Jeśli Serwer administracyjny jest zainstalowany na urządzeniu z innym oprogramowaniem, zalecamy wzięcie pod uwagę zaleceń tego dostawcy oprogramowania dotyczących kompatybilności produktów zabezpieczających (mogą już istnieć zalecenia dotyczące wyboru rozwiązania zabezpieczającego i konieczne może być skonfigurowanie strefy zaufanej).

Tworzenie osobnej zasady zabezpieczeń dla aplikacji zabezpieczającej

Zalecamy utworzenie oddzielnej zasady zabezpieczeń dla aplikacji chroniącej urządzenie Serwera administracyjnego. Ta zasada musi różnić się od zasady zabezpieczeń dla urządzeń klienckich. Pozwala to na określenie najbardziej odpowiednich ustawień bezpieczeństwa dla Serwera administracyjnego, bez wpływu na poziom ochrony innych urządzeń.

Zalecamy podzielenie urządzeń na grupy, a następnie umieszczenie urządzenia Serwera administracyjnego w osobnej grupie, dla której można utworzyć specjalną zasadę zabezpieczeń.

Moduły ochrony

Jeśli nie ma specjalnych zaleceń od dostawcy oprogramowania innej firmy zainstalowanego na tym samym urządzeniu co Serwer administracyjny, zalecamy aktywację i skonfigurowanie wszystkich dostępnych modułów ochrony (po sprawdzeniu działania tych modułów ochrony przez określony czas).

Konfigurowanie zapory sieciowej urządzenia Serwera administracyjnego

Na urządzeniu Serwera administracyjnego zalecamy skonfigurowanie zapory sieciowej w celu ograniczenia liczby urządzeń, z których administratorzy mogą łączyć się z Serwerem administracyjnym poprzez konsolę Kaspersky Security Center Web Console.

Domyślnie Serwer administracyjny używa portu 13299 do odbierania połączeń z Kaspersky Security Center Web Console. Zalecamy ograniczenie liczby urządzeń, z których Serwer administracyjny może być zarządzany przy użyciu tego portu.

Zarządzanie ochroną urządzeń klienckich

Ograniczenie dodawania kluczy licencyjnych do pakietów instalacyjnych

Pakiety instalacyjne są przechowywane w folderze współdzielonym Serwera administracyjnego, w podfolderze Pakiety. Jeżeli dodasz klucz licencyjny do pakietu instalacyjnego, dostęp do klucza licencyjnego będą mogli uzyskać wszyscy użytkownicy posiadający uprawnienia do odczytu tego folderu (bezpośrednio lub poprzez serwer sieciowy osadzony w Serwerze administracyjnym).

Aby uniknąć naruszenia klucza licencyjnego, nie zalecamy dodawania kluczy licencyjnych do pakietów instalacyjnych.

Zalecamy korzystanie z automatycznej dystrybucji kluczy licencyjnych do zarządzanych urządzeń, wdrażanie za pomocą zadania Dodaj klucz licencyjny dla zarządzanej aplikacji oraz ręczne dodawanie kodu aktywacyjnego lub pliku klucza do urządzeń.

Automatyczne reguły przenoszenia urządzeń pomiędzy grupami administracyjnymi

Zalecamy ograniczenie stosowania automatycznych reguł przenoszenia urządzeń między grupami administracyjnymi.

Jeśli używasz automatycznych reguł przenoszenia urządzeń, może to prowadzić do propagowania zasad, które zapewniają przenoszonemu urządzeniu większe uprawnienia niż urządzenie przed przeniesieniem.

Ponadto przeniesienie urządzenia klienckiego do innej grupy administracyjnej może spowodować propagację ustawień zasad. Te ustawienia zasad mogą być niepożądane w przypadku dystrybucji do urządzeń gościa i niezaufanych.

To zalecenie nie dotyczy jednorazowego wstępnego przydziału urządzeń do grup administracyjnych.

Wymagania bezpieczeństwa dla punktów dystrybucji i bram połączeń

Urządzenia z zainstalowanym Agentem sieciowym mogą działać jako punkt dystrybucji i wykonywać następujące funkcje:

- Rozsyłaj aktualizacje i pakiety instalacyjne otrzymane z Serwera administracyjnego na urządzenia klienckie w grupie.
- Wykonaj zdalną instalację oprogramowania innych firm i aplikacji Kaspersky na urządzeniach klienckich.
- Przeszukiwać sieć w celu odnalezienia nowych urządzeń i zaktualizowania informacji o tych istniejących. Punkt dystrybucji może wykorzystywać te same metody wykrywania urządzeń, co Serwer administracyjny.

Umieszczanie punktów dystrybucji w sieci organizacji służących do:

- Zmniejszanie obciążenia na Serwerze administracyjnym
- Optymalizacja ruchu
- Zapewnienie Serwerowi administracyjnemu dostępu do urządzeń w trudno dostępnych częściach sieci

Biorąc pod uwagę dostępne możliwości, zalecamy zabezpieczenie urządzeń pełniących rolę punktów dystrybucji przed wszelkiego rodzaju nieautoryzowanym dostępem (w tym fizycznym).

Ograniczenie automatycznego przydzielania punktów dystrybucji

Aby uprościć administrację i zachować funkcjonalność sieci, zalecamy automatyczne przydzielanie punktów dystrybucji. Jednak w przypadku sieci przemysłowych i małych sieci zalecamy unikanie automatycznego przypisywania punktów dystrybucji, ponieważ na przykład prywatne informacje o kontach używanych do przesyłania zadań instalacji zdalnej mogą być przesyłane do punktów dystrybucji za pomocą systemu operacyjnego.

W przypadku sieci przemysłowych i małych sieci można ręcznie przypisać urządzenia, które będą działać jako punkty dystrybucji.

Możesz także przeglądać Raport z działalności punktów dystrybucji.

Wymagania bezpieczeństwa dla urządzeń użytkowników Kaspersky Security Center Linux

Urządzenia użytkowników Kaspersky Security Center Linux muszą spełniać specjalne wymagania bezpieczeństwa. Zalecamy zabezpieczenie tych urządzeń przed wszelkiego rodzaju nieautoryzowanym dostępem (również fizycznym).

Urządzenia użytkowników Kaspersky Security Center Linux obejmują:

- Urządzenia, z których użytkownicy Kaspersky Security Center Linux łączą się z Kaspersky Security Center Web Console za pomocą przeglądarki.
- Urządzenia, z których aplikacje, które komunikują się z Serwerem administracyjnym za pośrednictwem OpenAPI, są połączone z Kaspersky Security Center Linux.

Wymagania bezpieczeństwa dla urządzeń z zainstalowaną Kaspersky Security Center Web Console

Urządzenia z zainstalowaną Kaspersky Security Center Web Console służą do zarządzania systemem Kaspersky Security Center Linux, dlatego też muszą spełniać specjalne wymagania dotyczące bezpieczeństwa tych urządzeń. Zalecamy zabezpieczenie tych urządzeń przed wszelkiego rodzaju nieautoryzowanym dostępem (również fizycznym).

Konfigurowanie ochrony dla zarządzanych aplikacji

Zasady aplikacji zarządzanych

Zalecamy utworzenie zasady dla każdego typu używanej aplikacji i każdego komponentu Kaspersky Security Center Linux (Agent sieciowy, Kaspersky Endpoint Security for Windows, Kaspersky Endpoint Security for Linux, Kaspersky Endpoint Agent itp.). Ta zasada musi być zastosowana do wszystkich zarządzanych urządzeń (główna grupa administracyjna) lub do oddzielnej grupy, do której nowe zarządzane urządzenia są automatycznie przenoszone zgodnie ze skonfigurowanymi regułami przenoszenia.

Określenie hasła do wyłączenia ochrony i odinstalowania aplikacji

Zdecydowanie zalecamy włączenie ochrony hasłem, aby uniemożliwić intruzom wyłączenie lub odinstalowanie aplikacji zabezpieczających Kaspersky. Na platformach, na których obsługiwana jest ochrona hasłem, możesz ustawić hasło, na przykład, dla Kaspersky Endpoint Security, Agenta sieciowego i innych aplikacji Kaspersky. Po włączeniu ochrony hasłem zalecamy zablokowanie odpowiednich ustawień poprzez zamknięcie „kłódki".

Określanie hasła do ręcznego połączenia urządzenia klienckiego z Serwerem administracyjnym (narzędzie klmover)

Narzędzie klmover umożliwia ręczne podłączenie urządzenia klienckiego do Serwera administracyjnego. Narzędzie klmover znajduje się w folderze instalacyjnym Agenta sieciowego.

Aby uniemożliwić intruzom przeniesienie urządzeń poza Serwer administracyjny kontrolujący, zdecydowanie zalecamy włączenie ochrony hasłem podczas uruchamiania narzędzia klmover. Aby włączyć ochronę hasłem, wybierz opcję **Użyj hasła dezinstalacyjnego** w ustawieniach zasady Agenta sieciowego.

Narzędzie klmover wymaga uprawnień administratora lokalnego.

Jeśli zgubisz lub zapomnisz hasła do chronionego hasłem Agenta sieciowego zainstalowanego na urządzeniu, które nie jest już zarządzane przez Kaspersky Security Center Linux, nie będziesz mógł usunąć Agenta sieciowego przy użyciu narzędzia klmover ani wiersza poleceń. W takim przypadku należy ponownie zainstalować system operacyjny na urządzeniu z zainstalowanym Agentem sieciowym chronionym hasłem.

Włączenie opcji **Użyj hasła dezinstalacyjnego** na urządzeniach Windows umożliwia również ochronę hasłem narzędzia Cleaner (cleaner.exe).

Używanie Kaspersky Security Network

We wszystkich zasadach zarządzanych aplikacji oraz we właściwościach Serwera administracyjnego zalecamy włączenie korzystania z Kaspersky Security Network (KSN) i zaakceptowanie Oświadczenia KSN. Podczas aktualizacji lub aktualizacji Serwera administracyjnego możesz zaakceptować zaktualizowane Oświadczenie KSN. W niektórych przypadkach, gdy korzystanie z usług w chmurze jest zabronione przez prawo lub inne przepisy, możesz wyłączyć KSN.

Regularne skanowanie zarządzanych urządzeń

W przypadku wszystkich grup urządzeń zalecamy utworzenie zadania, które okresowo przeprowadza pełne skanowanie urządzeń.

Odkrywanie nowych urządzeń

Zalecamy odpowiednie skonfigurowanie ustawień wykrywania urządzeń: skonfiguruj integrację z kontrolerami domen, a także określ zakresy adresów IP do wykrywania nowych urządzeń.

Ze względów bezpieczeństwa możesz użyć domyślnej grupy administracyjnej, która obejmuje wszystkie nowe urządzenia oraz domyślne zasady mające wpływ na tę grupę.

Konserwacja Serwera administracyjnego

Tworzenie kopii zapasowych danych Serwera administracyjnego

Kopia zapasowa danych umożliwia przywrócenie danych Serwera administracyjnego bez utraty danych.

Domyślnie zadanie tworzenia kopii zapasowej danych jest tworzone automatycznie po instalacji Serwera administracyjnego i jest wykonywane okresowo, zapisując kopie zapasowe w odpowiednim katalogu.

Ustawienia zadania tworzenia kopii zapasowej danych można zmienić w następujący sposób:

- Częstotliwość tworzenia kopii zapasowych wzrasta
- Określono specjalny katalog do zapisywania kopii
- Zmieniono hasła do kopii zapasowych

Jeśli przechowujesz kopie zapasowe w specjalnym katalogu, innym niż katalog domyślny, zalecamy ograniczenie listy kontroli dostępu (ACL) do tego katalogu. Konta Serwera administracyjnego oraz konta bazy danych Serwera administracyjnego muszą mieć uprawnienia do zapisu dla tego katalogu.

Konserwacja Serwera administracyjnego

Konserwacja Serwera administracyjnego pozwala na zmniejszenie rozmiaru bazy danych oraz zwiększenie wydajności i ulepszenie działania aplikacji. Zalecamy przeprowadzanie konserwacji Serwera administracyjnego przynajmniej raz w tygodniu.

Konserwacja Serwera administracyjnego jest wykonywana przy pomocy dedykowanego zadania. Podczas konserwacji Serwera administracyjnego aplikacja wykonuje następujące działania:

- Reorganizuje indeksy w bazie danych
- Aktualizuje statystyki bazy danych
- Zmniejsza bazę danych (jeśli to konieczne)

Instalowanie aktualizacji systemu operacyjnego i aktualizacji oprogramowania innych firm

Zdecydowanie zalecamy regularne instalowanie aktualizacji oprogramowania dla systemu operacyjnego i oprogramowania innych firm na urządzeniu Serwera administracyjnego.

Urządzenia klienckie nie wymagają ciągłego połączenia z Serwerem administracyjnym, dlatego bezpieczne jest ponowne uruchomienie urządzenia Serwera administracyjnego po zainstalowaniu aktualizacji. Wszystkie zdarzenia zarejestrowane na urządzeniach klienckich podczas przestoju Serwera administracyjnego są do niego wysyłane po przywróceniu połączenia.

Transfer zdarzeń do systemów innych producentów

Monitorowanie i raportowanie

W celu szybkiego reagowania na problemy związane z bezpieczeństwem zalecamy skonfigurowanie funkcji monitorowania i raportowania.

Eksportowanie zdarzeń do systemów SIEM

W celu szybkiego wykrycia problemów związanych z bezpieczeństwem, zanim wystąpią poważne szkody, zalecamy wykorzystanie eksportu zdarzeń w systemie SIEM.

Powiadomienia e-mail o zdarzeniach audytu

Kaspersky Security Center Linux umożliwia otrzymywanie informacji o zdarzeniach występujących podczas działania Serwera administracyjnego i aplikacji firmy Kaspersky zainstalowanych na zarządzanych urządzeniach. W celu szybkiego reagowania na sytuacje awaryjne zalecamy skonfigurowanie Serwera administracyjnego do wysyłania powiadomień o zdarzeniach audytu, zdarzeniach krytycznych, zdarzeniach błędu i ostrzeżeniach, które publikuje.

Ponieważ zdarzenia te są zdarzeniami wewnątrzsystemowymi, można spodziewać się ich niewielkiej liczby, co ma zastosowanie w przypadku wysyłki.

Zalecenia dotyczące bezpieczeństwa systemów informatycznych innych firm

Zalecenia dotyczące bezpieczeństwa z CIS Benchmarks

W przypadku korzystania z wersji systemów operacyjnych, platform wirtualizacyjnych lub serwerów baz danych obsługiwanych przez Serwer administracyjny i Agenta sieciowego, zalecamy zastosowanie najlepszych praktyk bezpieczeństwa informacji z Centrum Bezpieczeństwa Internetowego (CIS), jeśli takie istnieją, w celu dostrojenia tych systemów informatycznych.

Centrum Bezpieczeństwa Internetu (CIS) jest organizacją non-profit zajmującą się poprawą bezpieczeństwa w dziedzinie technologii informatycznych. W szczególności CIS opracowuje i dystrybuuje standardy bezpieczeństwa, takie jak CIS Controls i CIS Benchmarks. Standardy te stanowią zbiór zaleceń i praktyk zapewniających bezpieczeństwo systemów informatycznych.

Portal CIS zawiera rekomendacje dla wersji następujących systemów informatycznych obsługiwanych przez Serwer administracyjny i Agenta sieciowego:

- Systemy operacyjne następujących rodzin:
  - Windows dla komputerów stacjonarnych
  - Windows dla serwerów
  - Debian
  - Ubuntu
  - CentOS

    - Oracle Linux
    - Red Hat Enterprise Linux
    - SUSE Linux Enterprise Server
    - macOS
- Platformy wirtualizacyjne VMware
- Serwery baz danych:
    - Microsoft SQL Server
    - MySQL
    - MariaDB
    - PostgreSQL

Zalecenia dotyczące bezpieczeństwa dla systemu operacyjnego Astra Linux

Korzystając z systemu operacyjnego Astra Linux należy przestrzegać zaleceń dotyczących bezpieczeństwa opisanych w czerwonej księdze dla odpowiedniej wersji Astra Linux.

Zalecenia dotyczące bezpieczeństwa dla systemu operacyjnego RED OS

Korzystając z systemu operacyjnego RED OS, należy stosować się do zaleceń dotyczących bezpieczeństwa z podręcznika administratora opisanych w oficjalnej dokumentacji RED OS.

Zalecenia dotyczące korzystania z aplikacji zabezpieczających Kaspersky

Korzystanie z hasła KLAdmin w Kaspersky Endpoint Security for Windows

Konto KLAdmin to konto administratora z nieograniczonym dostępem do programu Kaspersky Endpoint Security for Windows. Konto KLAdmin ma prawo do wykonywania wszelkich działań chronionych hasłem w programie Kaspersky Endpoint Security for Windows, w tym usunięcia aplikacji. Uprawnień konta KLAdmin nie można cofnąć. Możesz ustawić hasło do konta KLAdmin we właściwościach zasad Kaspersky Endpoint Security for Windows. Administrator Kaspersky Endpoint Security for Windows ponosi pełną odpowiedzialność za bezpieczne korzystanie z hasła do konta KLAdmin. Jeśli Twoja organizacja ma własną politykę dotyczącą haseł, postępuj zgodnie z instrukcjami zawartymi w tej polityce. Im dłuższe i bardziej złożone hasło, tym jest bardziej wiarygodne.

Nasze zalecenia dotyczące ochrony organizacji przed kradzieżą hasła KLAdmin są następujące:

- **Wymagania ogólne**

  Nie używaj nazwy konta ani części nazwy jako hasła.

- **Minimalne wymagania dotyczące długości hasła**

  Utwórz hasło składające się z co najmniej 10 znaków.

- **Wymagania dotyczące korzystania z wielu rodzajów znaków**

  Ustaw złożone hasło, które będzie zawierać znaki z różnych kategorii: małe i wielkie litery, cyfry oraz znaki specjalne.

- **Wymagania dotyczące wygaśnięcia hasła**

  Ustaw minimalny okres ważności hasła wynoszący 90 dni. Nowe hasło nie może być takie samo jak jakiekolwiek hasło z 24 ostatnio użytych haseł.

Scenariusz: uwierzytelnianie serwera MySQL

Zalecamy użycie certyfikatu TLS do uwierzytelnienia serwera MySQL. Możesz użyć certyfikatu z zaufanego urzędu certyfikacji lub certyfikatu z podpisem własnym.

Serwer administracyjny obsługuje zarówno jednokierunkowe, jak i dwukierunkowe uwierzytelnianie SSL dla MySQL.

Włącz jednokierunkowe uwierzytelnianie SSL

Wykonaj poniższe kroki, aby skonfigurować jednokierunkowe uwierzytelnianie SSL dla MySQL:

1. **Wygeneruj certyfikat TLS z podpisem własnym dla serwera MySQL**

   Uruchom następujące polecenie:

   ```
   openssl genrsa 1024 > ca-key.pem
   ```

   ```
   openssl req -new -x509 -nodes -days 365 -key ca-key.pem -config myssl.cnf > ca-cert.pem
   ```

   ```
   openssl req -newkey rsa:1024 -days 365 -nodes -keyout server-key.pem -config myssl.cnf
   > server-req.pem
   ```

   ```
   openssl x09 -req -in server-req.pem -days 365 -CA ca-cert.pem -CAkey ca-key.pem -
   set_serial 01 > server-cert.pem
   ```

2. **Utwórz plik flagi serwera**

   Użyj narzędzia klscflag, aby utworzyć flagę serwera KLSRV_MYSQL_OPT_SSL_CA i jako jej wartość określ ścieżkę do certyfikatu. Narzędzie klscflag znajduje się w katalogu, w którym zainstalowany jest serwer administracyjny. Domyślna ścieżka instalacji to /opt/kaspersky/ksc64/sbin.

   ```
   klscflag -fset -pv klserver -n KLSRV_MYSQL_OPT_SSL_CA -v < ścieżka do ca-cert.pem> -t d
   ```

3. **Skonfiguruj bazę danych**

   Określ certyfikaty w pliku my.cnf. Otwórz plik my.cnf w edytorze tekstu i dodaj następujące wiersze do sekcji [mysqld]:

```
[mysqld]
ssl-ca=".../mysqlcerts/ca-cert.pem"
ssl-cert=".../mysqlcerts/server-cert.pem"
ssl-key=".../mysqlcerts/server-key.pem"
```

Włącz dwukierunkowe uwierzytelnianie SSL

Wykonaj poniższe kroki, aby skonfigurować dwukierunkowe uwierzytelnianie SSL dla MySQL:

1. **Utwórz pliki flag serwera**

   Użyj narzędzia klscflag, aby utworzyć flagi serwera i jako ich wartości określ ścieżkę do plików certyfikatów:

   ```
   klscflag -fset -pv klserver -n KLSRV_MYSQL_OPT_SSL_CA -v <ścieżka do ca-cert.pem> -t s
   klscflag -fset -pv klserver -n KLSRV_MYSQL_OPT_SSL_CERT -v <ścieżka do server-cert.pem> -t s
   klscflag -fset -pv klserver -n KLSRV_MYSQL_OPT_SSL_KEY -v <ścieżka do server-key.pem> -t s
   ```

   Narzędzie klscflag znajduje się w katalogu, w którym zainstalowany jest serwer administracyjny. Domyślna ścieżka instalacji to /opt/kaspersky/ksc64/sbin.

2. **Określ hasło (opcjonalnie)**

   Jeśli plik server-key.pem wymaga hasła, utwórz flagę KLSRV_MARIADB_OPT_TLS_PASPHRASE i podaj hasło jako jego wartość:

   ```
   klscflag -fset -pv klserver -n KLSRV_MARIADB_OPT_TLS_PASPHRASE -v <hasło> -t s
   ```

3. **Skonfiguruj bazę danych**

   Określ certyfikaty w pliku my.cnf. Otwórz plik my.cnf w edytorze tekstu i dodaj następujące wiersze do sekcji [mysqld]:

   ```
   [mysqld]
   ssl-ca=".../mysqlcerts/ca-cert.pem"
   ssl-cert=".../mysqlcerts/server-cert.pem"
   ssl-key=".../mysqlcerts/server-key.pem"
   ```

Scenariusz: uwierzytelnianie serwera PostgreSQL

Zalecamy użycie certyfikatu TLS do uwierzytelnienia serwera PostgreSQL. Możesz użyć certyfikatu z zaufanego urzędu certyfikacji lub certyfikatu z podpisem własnym.

Serwer administracyjny obsługuje zarówno jednokierunkowe, jak i dwukierunkowe uwierzytelnianie SSL dla PostgreSQL.

Uwierzytelnianie serwera PostgreSQL odbywa się etapami:

1. **Wygeneruj certyfikat dla serwera PostgreSQL**

Uruchom następujące polecenia:

```
openssl req -new -x509 -days 365 -nodes -text -out psql.crt -keyout psql.key -subj "/CN=psql"
```

```
chmod og-rwx psql.key
```

2. **Wygeneruj certyfikat dla Serwera administracyjnego**

   Uruchom następujące polecenia. Wartość CN powinna odpowiadać nazwie użytkownika, który łączy się z PostgreSQL w imieniu Serwera administracyjnego. Domyślnie nazwa użytkownika jest ustawiona na postgres.

   ```
   openssl req -new -x509 -days 365 -nodes -text -out postgres.crt -keyout postgres.key -subj "/CN=postgres"
   ```

   ```
   chmod og-rwx postgres.key
   ```

3. **Skonfiguruj uwierzytelnianie certyfikatu klienta**

   Zmodyfikuj plik pg_hba.conf w następujący sposób:

   ```
   hostssl mydb myuser 192.168.1.0/16 scram-sha-256
   ```

   Upewnij się, że plik pg_hba.conf nie zawiera rekordu rozpoczynającego się od `host`.

4. **Określ certyfikat PostgreSQL**

   Jednokierunkowe uwierzytelnianie SSL

   Zmodyfikuj plik postgresql.conf w następujący sposób (podaj poprawną ścieżkę do plików .crt i .key):

   ```
   listen_addresses ='localhost, server-ip'
   ssl = on
   ssl_cert_file = '<psql.crt>'
   ssl_key_file = '<psql.key>'
   ```

   Dwukierunkowe uwierzytelnianie SSL

   Zmodyfikuj plik postgresql.conf w następujący sposób (podaj poprawną ścieżkę do plików .crt i .key):

   ```
   listen_addresses ='localhost, server-ip'
   ssl = on
   ssl_ca_file = '<postgres.crt>'
   ssl_cert_file = '<psql.crt>'
   ssl_key_file = '<psql.key>'
   ```

5. **Uruchom ponownie demona PostgreSQL**

   Uruchom następujące polecenie:

   ```
   systemctl restart postgresql-14.service
   ```

6. **Określ flagę serwera dla Serwera administracyjnego**

   Jednokierunkowe uwierzytelnianie SSL

   Użyj narzędzia klscflag, aby utworzyć flagę serwera KLSRV_POSTGRES_OPT_SSL_CA i jako jej wartość określ ścieżkę do certyfikatu.

   Uruchom wiersz poleceń, a następnie zmień bieżący katalog na katalog z narzędziem klscflag. Narzędzie klscflag znajduje się w katalogu, w którym zainstalowany jest serwer administracyjny. Domyślna ścieżka instalacji to /opt/kaspersky/ksc64/sbin.

Uruchom następujące polecenie:

```
klscflag -fset -pv klserver -n KLSRV_POSTGRES_OPT_SSL_CA -v <ścieżka do psql.crt> -t
s
```

Dwukierunkowe uwierzytelnianie SSL

Użyj narzędzia klscflag, aby utworzyć flagi serwera i jako ich wartości określ ścieżkę do plików certyfikatów.

Uruchom wiersz poleceń, a następnie zmień bieżący katalog na katalog z narzędziem klscflag. Narzędzie klscflag znajduje się w katalogu, w którym zainstalowany jest serwer administracyjny. Domyślna ścieżka instalacji to /opt/kaspersky/ksc64/sbin.

Uruchom następujące polecenia:

```
klscflag -fset -pv klserver -n KLSRV_POSTGRES_OPT_SSL_CA -v <ścieżka do psql.crt> -
t s
```

```
klscflag -fset -pv klserver -n KLSRV_POSTGRES_OPT_SSL_CERT -v <ścieżka do
postgres.crt> -t s
```

```
klscflag -fset -pv klserver -n KLSRV_POSTGRES_OPT_SSL_KEY -v <ścieżka do
postgres.key> -t s
```

Jeśli `postgres.key` wymaga hasła, utwórz flagę KLSRV_POSTGRES_OPT_TLS_PASPHRASE i podaj hasło jako jego wartość:

```
klscflag -fset -pv klserver -n KLSRV_POSTGRES_OPT_TLS_PASPHRASE -v <hasło> -t s
```

7. **Uruchom ponownie usługę Serwera administracyjnego**

Przygotowanie do wdrożenia

W tej sekcji opisano, jak wybrać opcję wdrożenia Kaspersky Security Center Linux, konfigurację Kaspersky Security Center Linux oraz system DBMS zgodnie z potrzebami Twojej organizacji.

Istnieje kilka opcji wdrożenia komponentów Kaspersky Security Center Linux w sieci organizacji, w zależności od następujących kryteriów:

- Całkowitą liczbę urządzeń
- Jednostki (biura lokalne, oddziały), które są oddalone geograficznie lub pod względem organizacyjnym
- Oddalone od siebie sieci połączone wąskimi kanałami
- Potrzeba uzyskania dostępu do Serwera administracyjnego przez Internet

Jeden Serwer administracyjny może obsługiwać maksymalnie 50 000 urządzeń (z PostgreSQL lub Postgres Pro jako DBMS). Jeśli całkowita liczba urządzeń w sieci organizacji przekroczy 50 000, wówczas w tej sieci należy zainstalować kilka Serwerów administracyjnych i połączyć je w hierarchię w celu uproszczenia scentralizowanego zarządzania.

Jeśli organizacja zawiera znaczną liczbę zdalnych biur lokalnych (oddziałów), z których każdy posiada swojego administratora, znacznym ułatwieniem będzie zainstalowanie Serwera administracyjnego w każdym z tych biur. W przeciwnym razie biura te należy postrzegać jako odizolowane sieci komunikujące się przez wąskie kanały; patrz artykuł „Standardowa konfiguracja: Duże oddziały posiadające swoich własnych administratorów”.

Podczas korzystania z oddalonych od siebie sieci połączonych wąskimi kanałami, ruch sieciowy można zmniejszyć, wskazując kilku Agentów sieciowych jako punkty dystrybucji (zapoznaj się z tabelą zawierającą wyliczenie liczby punktów dystrybucji). W tym przypadku wszystkie urządzenia w oddalonej sieci pobierają uaktualnienia z tych lokalnych centrów aktualizacji. Punkty dystrybucji mogą pobrać aktualizacje zarówno z Serwera administracyjnego (domyślny scenariusz) oraz z serwerów Kaspersky dostępnych w Internecie (patrz artykuł „Standardowa konfiguracja: Wiele małych, zdalnych biur").

Sekcja „Standardowa konfiguracja Kaspersky Security Center Linux" zawiera szczegółowy opis standardowej konfiguracji Kaspersky Security Center Linux. Podczas planowania instalacji wybierz najodpowiedniejszą konfigurację, mając na uwadze strukturę organizacji.

Na etapie planowania wdrożenia należy rozważyć przydzielenie do Serwera administracyjnego specjalnego certyfikatu X.509. Przydzielenie certyfikatu X.509 do Serwera administracyjnego może być przydatne między innymi do:

- Sprawdzania ruchu SSL poprzez kończenie żądań SSL na serwerze proxy lub do korzystania ze zwrotnego serwera proxy
- Integracji z infrastrukturą kluczy publicznych (PKI) organizacji
- Określenia wymaganych wartości w polach certyfikatu
- Zapewnienia wymaganej siły szyfrowania certyfikatu

Wybieranie konfiguracji Kaspersky Security Center Linux

Ta sekcja opisuje standardowe konfiguracje używane podczas wdrażania komponentów Kaspersky Security Center Linux w sieci organizacji:

- Jedno biuro
- Kilka dużych oddziałów, które są oddalone geograficznie od siebie i posiadają swoich własnych administratorów
- Wiele małych biur, które są oddalone geograficznie od siebie

Standardowa konfiguracja: Jedno biuro

W sieci organizacji można zainstalować jeden lub kilka Serwerów administracyjnych. Liczba Serwerów administracyjnych może zostać wybrana w oparciu o dostępny sprzęt lub całkowitą liczbę zarządzanych urządzeń.

Jeden Serwer administracyjny może obsługiwać maksymalnie 50 000 urządzeń (z PostgreSQL lub Postgres Pro jako DBMS). Rozważyć możliwość zwiększenia liczby zarządzanych urządzeń w najbliższej przyszłości: wygodniejsze może być podłączenie do jednego Serwera administracyjnego mniejszej liczby urządzeń.

Serwery administracyjne mogą być instalowane w sieci wewnętrznej lub w strefie DMZ, w zależności od tego, czy wymagany jest dostęp do Serwera administracyjnego przez Internet.

Jeśli jest używanych kilka Serwerów, zalecane jest połączenie ich w hierarchię. Korzystanie z hierarchii Serwerów administracyjnych pozwala uniknąć mieszania zasad i zadań oraz zarządzać całym zbiorem zarządzanych urządzeń tak, jakby były zarządzane przez jeden Serwer administracyjny (czyli wyszukiwać urządzenia, tworzyć wybory urządzeń oraz generować raporty).

Standardowa konfiguracja: Duże oddziały posiadające swoich administratorów

Jeśli organizacja posiada kilka dużych oddziałów, które są oddalone geograficznie od siebie, należy uwzględnić opcję wdrożenia Serwerów administracyjnych w każdym z biur. W jednym biurze można wdrożyć jeden lub kilka Serwerów administracyjnych, w zależności od liczby urządzeń klienckich i dostępnego sprzętu. W tym przypadku, dla każdego z biur można przeprowadzić „Standardową konfigurację: Jedno biuro". Aby ułatwić zarządzanie, zalecane jest połączenie wszystkich Serwerów administracyjnych w hierarchię (najlepiej wielopoziomową).

Jeśli niektórzy pracownicy przemieszczają się między biurami ze swoimi urządzeniami (laptopami), utwórz profile połączenia Agenta sieciowego w zasadzie Agenta sieciowego.

Standardowa konfiguracja: Małe zdalne biura

Ta standardowa konfiguracja została utworzona z myślą o głównej siedzibie i wielu małych zdalnych biurach, które mogą kontaktować się z główną siedzibą za pośrednictwem Internetu. Każde z tych zdalnych biur może znajdować się poza NAT (Network Address Translation - translacja adresów sieciowych), czyli nie można nawiązać połączenia między dwoma zdalnymi biurami, gdyż są odizolowane.

W głównej siedzibie należy zainstalować Serwer administracyjny, natomiast we wszystkich pozostałych biurach należy przydzielić jeden lub kilka punktów dystrybucji. Jeśli biura są połączone przez internet, przydatne może być utworzenie zadania *Pobierz uaktualnienia do repozytoriów punktów dystrybucji* dla punktów dystrybucji, aby mogły one pobierać uaktualnienia bezpośrednio z serwerów Kaspersky, folderu lokalnego lub sieciowego, a nie z Serwera administracyjnego.

Jeśli niektóre urządzenia w zdalnym biurze nie mają bezpośredniego dostępu do Serwera administracyjnego (na przykład, dostęp do Serwera administracyjnego jest możliwy przez Internet, ale niektóre urządzenia nie mają dostępu do Internetu), punkty dystrybucji muszą zostać przełączone do trybu bramy połączenia. W tym przypadku Agenty sieciowe na urządzeniach w zdalnym biurze zostaną połączone, w celu dalszej synchronizacji, z Serwerem administracyjnym, ale poprzez bramę, a nie bezpośrednio.

Ponieważ Serwer administracyjny najprawdopodobniej nie będzie mógł przeszukać sieci zdalnego biura, zalecane jest przekazanie tej funkcji punktowi dystrybucji.

Serwer administracyjny nie będzie mógł wysyłać powiadomień poprzez port UDP o numerze 15000 na zarządzane urządzenia znajdujące się poza NAT w zdalnym biurze. Aby rozwiązać ten problem, we właściwościach urządzeń pełniących rolę punktów dystrybucji możesz włączyć tryb stałego połączenia z Serwerem administracyjnym (pole **Nie odłączaj od Serwera administracyjnego**). Ten tryb jest dostępny, jeśli całkowita liczba punktów dystrybucji nie przekracza 300. Aby zapewnić ciągłą łączność między zarządzanym urządzeniem a Serwerem administracyjnym, należy używać serwerów push. Szczegółowe informacje można znaleźć w następującym artykule: Włączanie serwera push.

Wybieranie struktury ochrony firmy

Wybór struktury ochrony organizacji jest definiowany przez następujące czynniki:

- Topologię sieci firmy.
- Strukturę organizacyjną.

- Liczbę pracowników zajmujących się ochroną sieci, a także zakres ich obowiązków.
- Zasoby sprzętu, które mogą zostać przydzielone dla komponentów do zarządzania ochroną.
- Przepustowość kanałów komunikacji, które mogą zostać przydzielone w celu utrzymania działania składników ochrony w sieci organizacji.
- Ograniczenia czasu wykonywania krytycznych działań administracyjnych w sieci firmowej. Na krytyczne działania administracyjne składają się, na przykład, dystrybucja uaktualnień antywirusowych baz danych i modyfikacja zasad dla urządzeń klienckich.

Podczas wybierania struktury ochrony zalecamy najpierw określić dostępną sieć i zasoby sprzętu, które będą wykorzystane do działania scentralizowanego systemu ochrony.

W celu przeprowadzenia analizy infrastruktury sprzętu i sieci zalecane jest wykonanie następujących czynności:

1. Określenie następujących ustawień sieci, w obrębie której zostanie zainstalowana ochrona:
   - Liczba segmentów sieci.
   - Prędkość komunikacji przez kanały komunikacyjne pomiędzy pojedynczymi segmentami sieci.
   - Liczba zarządzanych urządzeń w każdym segmencie sieci.
   - Przepustowość każdego kanału komunikacji, który może zostać przydzielony w celu utrzymania działania ochrony.
2. Określenie maksymalnego dozwolonego czasu na wykonanie kluczowych działań administracyjnych dla wszystkich zarządzanych urządzeń.
3. Przeanalizuj informacje z kroków 1 i 2, a także dane z testów obciążeniowych systemu administracyjnego. Opierając się na wynikach analizy, odpowiedz na następujące pytania:
   - Czy jest możliwa obsługa wszystkich klientów przy pomocy pojedynczego Serwera administracyjnego, czy też niezbędna jest hierarchia Serwerów administracyjnych?
   - Jaka konfiguracja sprzętowa Serwerów administracyjnych jest potrzebna do zajmowania się wszystkimi klientami w przedziale czasu określonym w punkcie 2?
   - Czy konieczne jest użycie punktów dystrybucji do zmniejszenia obciążenia kanałów komunikacji?

Po uzyskaniu odpowiedzi na powyższe pytania, możesz stworzyć zestaw dozwolonych struktur ochrony organizacji.

W sieci firmowej można użyć jednej z poniższych standardowych struktur ochrony:

- Jeden Serwer administracyjny. Wszystkie urządzenia klienckie są połączone z jednym Serwerem administracyjnym. Serwer administracyjny działa jako punkt dystrybucji.
- Jeden Serwer administracyjny z punktami dystrybucji. Wszystkie urządzenia klienckie są połączone z jednym Serwerem administracyjnym. Niektóre urządzenia klienckie w sieci działają jako punkty dystrybucji.

- Hierarchia Serwerów administracyjnych. Dla każdego segmentu sieci przydzielony jest pojedynczy Serwer administracyjny, który staje się częścią ogólnej hierarchii Serwerów administracyjnych. Główny Serwer administracyjny działa jako punkt dystrybucji.

- Hierarchia Serwerów administracyjnych z punktami dystrybucji. Dla każdego segmentu sieci przydzielony jest pojedynczy Serwer administracyjny, który staje się częścią ogólnej hierarchii Serwerów administracyjnych. Niektóre urządzenia klienckie w sieci działają jako punkty dystrybucji.

Typowe schematy wdrażania systemu ochrony

Ta sekcja opisuje standardowe schematy wdrażania systemu ochrony w sieci firmowej, korzystając z Kaspersky Security Center.

System musi być chroniony przed wszelkimi rodzajami nieautoryzowanego dostępu. Przed zainstalowaniem aplikacji na urządzeniu i fizyczną ochroną Serwerów administracyjnych i punktów dystrybucji zalecamy zainstalowanie wszystkich dostępnych aktualizacji zabezpieczeń dla systemu operacyjnego.

Możesz użyć Kaspersky Security Center do wdrożenia systemu ochrony w sieci korporacyjnej, wykorzystując następujące schematy:

- Wdrażanie systemu ochrony poprzez Kaspersky Security Center Web Console.

  Aplikacje Kaspersky są instalowane automatycznie na urządzeniach klienckich, które łączą się automatycznie z Serwerem administracyjnym poprzez Kaspersky Security Center.

- Ręczna instalacja systemu ochrony przy pomocy autonomicznych pakietów instalacyjnych wygenerowanych przez Kaspersky Security Center.

  Instalacja aplikacji Kaspersky na urządzeniach klienckich i stacji roboczej administratora jest wykonywana ręcznie; ustawienia połączenia urządzeń klienckich z Serwerem administracyjnym są określane podczas instalacji Agenta sieciowego.

  Ta metoda wdrożenia jest zalecana w sytuacjach, gdy zdalna instalacja nie jest możliwa.

Kaspersky Security Center nie obsługuje wdrożenia przy użyciu zasad grupy Microsoft Active Directory®.

Wybieranie systemu zarządzania bazą danych

Poniższa tabela zawiera listę prawidłowych opcji DBMS, a także zalecenia i ograniczenia dotyczące ich używania.

Zalecenia i ograniczenia dotyczące DBMS

DBMS	Zalecenia i ograniczenia
MySQL (zobacz obsługiwane wersje)	Użyj tego DBMS, jeśli zamierzasz uruchomić pojedynczy Serwer administracyjny dla mniej niż 20 000 urządzeń.
MariaDB (zobacz obsługiwane wersje)	Użyj tego DBMS, jeśli zamierzasz uruchomić pojedynczy Serwer administracyjny dla mniej niż 20 000 urządzeń.

PostgreSQL, Postgres Pro (zobacz obsługiwane wersje)	Użyj tego DBMS, jeśli zamierzasz uruchomić pojedynczy Serwer administracyjny dla mniej niż 50 000 urządzeń.
Tantor (zobacz obsługiwane wersje)	Użyj tego DBMS, jeśli zamierzasz uruchomić pojedynczy Serwer administracyjny dla mniej niż 50 000 urządzeń. System DBMS Tantor jest obsługiwany tylko w Astra Linux Special Edition RUSB.10015-01 (aktualizacja operacyjna 1.8).

Informacje o sposobie zainstalowania wybranego systemu DBMS znajdziesz w tym dokumencie.

Zaleca się wyłączenie zadania Inwentaryzacja oprogramowania i wyłączenie (w ustawieniach zasad Kaspersky Endpoint Security) powiadomień Serwera administracyjnego o uruchomionych aplikacjach.

Jeśli zdecydujesz się zainstalować PostgreSQL lub Postgres Pro DBMS, upewnij się, że określone zostało hasło superużytkownika. Jeśli hasło nie zostanie określone, Serwer administracyjny może nie być w stanie połączyć się z bazą danych.

Jeśli instalujesz MySQL, MariaDB, PostgreSQL lub Postgres Pro, użyj zalecanych ustawień, aby zapewnić prawidłowe działanie DBMS.

Jeśli używasz systemu PostgreSQL, MariaDB lub MySQL DBMS, karta **Zdarzenia** może wyświetlać niekompletną listę zdarzeń dla wybranego urządzenia klienckiego. Dzieje się tak, gdy system DBMS przechowuje bardzo dużą liczbę zdarzeń. Liczbę wyświetlanych zdarzeń można zwiększyć, wykonując jedną z następujących czynności:

- Usuwanie niepotrzebnych zdarzeń.
- Skrócenie okresu przechowywania niepotrzebnych zdarzeń.

Aby zobaczyć pełną listę zdarzeń zarejestrowanych na Serwerze administracyjnym dla danego urządzenia, należy użyć opcji Raporty.

Umożliwianie uzyskania dostępu do Serwera administracyjnego przez internet

Wykonanie następujących czynności wymaga dostępu do Serwera administracyjnego przez Internet:

- Regularne aktualizowanie baz danych, modułów oprogramowania i aplikacji Kaspersky
- Aktualizowanie oprogramowania firm trzecich

  Domyślnie połączenie internetowe w przypadku Serwera administracyjnego nie jest wymagane w celu instalowania aktualizacji oprogramowania firmy Microsoft na zarządzanych urządzeniach. Na przykład zarządzane urządzenia mogą pobierać aktualizacje oprogramowania firmy Microsoft bezpośrednio z serwerów Microsoft Update lub z systemu Windows Server z programem Microsoft Windows Server Update Services (WSUS) wdrożonymi w sieci organizacji. Serwer administracyjny musi być połączony z Internetem w następujących przypadkach:

  - Używanie Serwera administracyjnego jako serwera WSUS
  - Instalowanie aktualizacji oprogramowania firm trzecich innego niż oprogramowanie firmy Microsoft

- Eliminowanie luk w oprogramowaniu innych firm

  Połączenie internetowe w przypadku Serwera administracyjnego jest wymagane, aby można było wykonywać następujące zadania:

  - Sporządzanie listy zalecanych poprawek dla luk w oprogramowaniu firmy Microsoft. Lista jest tworzona i regularnie aktualizowana przez specjalistów z Kaspersky.
  - Naprawianie luk w oprogramowaniu firm trzecich innym niż oprogramowanie firmy Microsoft.
- Zarządzanie urządzeniami (laptopami) użytkowników mobilnych
- Zarządzanie urządzeniami w zdalnych biurach
- Komunikowanie się z głównym lub podrzędnym Serwerem administracyjnym w zdalnych biurach
- Zarządzanie urządzeniami mobilnymi

Ta sekcja opisuje podstawowe sposoby zapewnienia dostępu do Serwera administracyjnego poprzez Internet. W każdym przypadku skupiającym się na zapewnieniu Serwerowi administracyjnemu dostępu do Internetu może być wymagany dedykowany certyfikat dla Serwera administracyjnego.

Dostęp do internetu: Serwer administracyjny w sieci lokalnej

Jeśli Serwer administracyjny znajduje się w wewnętrznej sieci organizacji, możesz udostępnić port TCP o numerze 13000 Serwera administracyjnego z zewnątrz za pomocą przekierowania portów.

Dostęp do internetu: Serwer administracyjny w strefie DMZ

Jeśli Serwer administracyjny znajduje się w DMZ sieci organizacji, nie ma on dostępu do wewnętrznej sieci organizacji. Dlatego też występują następujące ograniczenia:

- Serwer administracyjny nie może wykryć nowych urządzeń.
- Serwer administracyjny nie może wykonać wstępnego wdrożenia Agenta sieciowego przy użyciu wymuszonej instalacji na urządzeniach w wewnętrznej sieci organizacji.

  Dotyczy to tylko wstępnej instalacji Agenta sieciowego. Jednakże jakiekolwiek późniejsze uaktualnienia Agenta sieciowego lub instalacja aplikacji zabezpieczającej mogą zostać wykonane przez Serwer administracyjny.

Należy pamiętać, że Kaspersky Security Center Linux nie obsługuje wdrożenia przy użyciu zasad grupy systemu Microsoft Windows.

Możesz skorzystać z punktów dystrybucji zlokalizowanych w sieci organizacji. Aby przeprowadzić wstępne wdrożenie na urządzeniach bez Agenta sieciowego, w pierwszej kolejności zainstaluj Agenta sieciowego na jednym z urządzeń, a następnie przypisz mu stan punktu dystrybucji. W rezultacie, wstępna instalacja Agenta sieciowego na pozostałych urządzeniach zostanie przeprowadzona przez Serwer administracyjny poprzez ten punkt dystrybucji.

Aby zapewnić pomyślne wysyłanie powiadomień przez port UDP o numerze 15000 na zarządzane urządzenia znajdujące się w wewnętrznej sieci organizacji, musisz wypełnić całą swoją sieć punktami dystrybucji. We właściwościach przypisanych punktów dystrybucji zaznacz pole **Nie odłączaj od Serwera administracyjnego**. Serwer administracyjny nawiąże stale połączenie z punktami dystrybucji, które będą mogły wysyłać powiadomienia poprzez port UDP o numerze 15000 na urządzenia, które znajdują się w wewnętrznej sieci organizacji (to może być.sieć IPv4 lub IPv6).

Instalacja

Ta sekcja opisuje instalację Kaspersky Security Center Linux i Kaspersky Security Center Web Console.

Konfigurowanie serwera MariaDB x64 do pracy z Kaspersky Security Center Linux

Aby pomyślnie skonfigurować serwer MariaDB x64 do pracy z Kaspersky Security Center, należy użyć domyślnych parametrów serwera, z wyjątkiem parametrów serwera określonych w tym artykule.

Zalecane ustawienia dla pliku my.cnf

Więcej szczegółów na temat konfiguracji DBMS znajdziesz także w procedurze konfiguracji konta. Aby uzyskać informacje na temat instalacji DBMS, zapoznaj się z procedurą instalacji DBMS.

W celu skonfigurowania pliku my.cnf:

1. Otwórz plik my.cnf w dowolnym edytorze tekstu.

2. Wprowadź następujące wiersze do sekcji [mysqld] pliku my.cnf:
```
sort_buffer_size=10M
join_buffer_size=100M
join_buffer_space_limit=300M
join_cache_level=8
tmp_table_size=512M
max_heap_table_size=512M
key_buffer_size=200M
innodb_buffer_pool_size=< rzeczywista wartość nie może być niższa niż 80%
oczekiwanego rozmiaru bazy danych KAV >
innodb_thread_concurrency=20
innodb_flush_log_at_trx_commit=0
innodb_lock_wait_timeout=300
max_allowed_packet=32M
max_connections=151
max_prepared_stmt_count=12800
table_open_cache=60000
table_open_cache_instances=4
table_definition_cache=60000
sql_mode="STRICT_TRANS_TABLES,NO_AUTO_CREATE_USER,NO_ENGINE_SUBSTITUTION"
```

Wartość `innodb_buffer_pool_size` nie może być mniejsza niż 80 procent oczekiwanego rozmiaru bazy danych KAV. Należy pamiętać, że określona pamięć jest przydzielana podczas uruchamiania serwera. Jeśli rozmiar bazy danych jest mniejszy niż określony rozmiar bufora, przydzielana jest tylko wymagana pamięć. Jeśli używasz MariaDB w wersji 10.4.3 lub starszej, rzeczywisty rozmiar przydzielonej pamięci jest o około 10 procent większy niż określony rozmiar bufora.

Zalecane jest użycie wartości parametru `innodb_flush_log_at_trx_commit=0`, ponieważ wartości „1" lub „2" negatywnie wpływają na prędkość działania MariaDB. Upewnij się, że parametr `innodb_file_per_table` jest ustawiony na `1`.

W przypadku MariaDB 10.1 dodatkowo wprowadź następujące wiersze w sekcji [mysqld]:

```
innodb_file_format='Barracuda'
innodb_default_row_format=dynamic
innodb_large_prefix=1
```

W przypadku MariaDB 10.6 dodatkowo wprowadź następujące wiersze w sekcji [mysqld]:

```
optimizer_prune_level=0
optimizer_search_depth=8
```

Domyślnie dodatki optymalizujące `join_cache_incremental`, `join_cache_hashed`, `join_cache_bka` są włączone. Jeśli te dodatki nie są włączone, musisz je włączyć.

W celu sprawdzenia, czy dodatki optymalizujące są włączone:

1. W konsoli klienta MariaDB wykonaj polecenie:

   ```
   SELECT @@optimizer_switch;
   ```

2. Upewnij się, że jego dane wyjściowe zawierają następujące wiersze:

   ```
   join_cache_incremental=on
   join_cache_hashed=on
   join_cache_bka=on
   ```

   Jeśli te wiersze są obecne i mają wartości `on`, to dodatki optymalizujące są włączone.

   Jeśli tych wierszy brakuje lub mają one wartości `off`, musisz wykonać następujące czynności:

   a. Otwórz plik my.cnf w dowolnym edytorze tekstu.

   b. Dodaj do pliku my.cnf następujące wiersze:

   ```
   optimizer_switch='join_cache_incremental=on'
   optimizer_switch='join_cache_hashed=on'
   optimizer_switch='join_cache_bka=on'
   ```

Dodatki `join_cache_incremental`, `join_cache_hash` i `join_cache_bka` są włączone.

Zwiększ domyślny limit plików, które można otworzyć (deskryptory plików) dla usługi systemd MariaDB, aby zapewnić stabilność pod obciążeniem.

Aby zwiększyć limit deskryptorów plików:

1. Wykonaj następujące polecenia:

   ```
   sudo systemctl edit mariadb.service
   ```

2. Określ limit deskryptorów plików w parametrze `LimitNOFILE` sekcji `[Service]`:

   ```
   LimitNOFILE=1048576
   ```

3. Uruchom następujące polecenie, aby upewnić się, że parametry zostały określone poprawnie:

   ```
   sudo systemd-analyze verify mariadb.service
   ```

4. Uruchom następujące polecenie, aby ponownie załadować proces systemowy:

   ```
   sudo systemctl daemon-reload
   ```

5. Uruchom następujące polecenie, aby ponownie uruchomić usługę MariaDB:

   ```
   sudo systemctl restart mariadb.service
   ```

   Limit deskryptorów plików został zwiększony.

Konfigurowanie serwera PostgreSQL lub Postgres Pro do pracy z Kaspersky Security Center Linux

Aby pomyślnie skonfigurować serwer PostgreSQL lub Postgres Pro do pracy z Kaspersky Security Center Linux, należy użyć domyślnych parametrów serwera, z wyjątkiem parametrów serwera określonych w tym artykule.

Kaspersky Security Center Linux obsługuje DBMS PostgreSQL i Postgres Pro. Jeśli używasz jednego z tych systemów DBMS, rozważ skonfigurowanie parametrów serwera DBMS w celu optymalizacji pracy DBMS z Kaspersky Security Center Linux.

Domyślna ścieżka do pliku konfiguracyjnego to: `/etc/postgresql/< WERSJA >/main/postgresql.conf`

W systemie operacyjnym Linux ALT domyślna ścieżka to `/var/lib/pgsql/data/postgresql.conf`

Zalecane parametry w przypadku PostgreSQL i Postgres Pro:

- `max_connections = 151`

  Jeśli używasz klastra Postgres DBMS, określ parametr `max_connections` dla wszystkich serwerów DBMS, a także w konfiguracji klastra.

- `shared_buffers =` N

  N = 25% szacowanego rozmiaru pamięci RAM dla systemu DBMS. Jeśli system DBMS jest zainstalowany na urządzeniu obok Serwera administracyjnego, obliczenia powinny być oparte na pamięci RAM przydzielonej dla systemu DBMS, a nie na całkowitej pamięci RAM urządzenia.

  Jeśli pamięć RAM to mniej niż 1 GB, pozostaw wartość domyślną.

- `temp_buffers = 24MB`

- `work_mem = 16MB`

- `maintenance_work_mem = 128MB`

- `max_stack_depth =` maksymalny rozmiar stosu (wykonaj polecenie „`ulimit -s`”, aby uzyskać tę wartość w KB) minus margines bezpieczeństwa 1 MB

- `max_parallel_workers_per_gather = 0`

- `standard_conforming_strings =` on

Jeśli używasz Postgres Pro 15.7 lub Postgres Pro 15.7.1, wyłącz parametr `enable_compound_index_stats`:

```
enable_compound_index_stats = off
```

Po zaktualizowaniu pliku konfiguracyjnego ponownie załaduj konfigurację lub uruchom ponownie serwer DBMS.

Aby uzyskać szczegółowe informacje na temat parametrów serwerów PostgreSQL i Postgres Pro oraz sposobu określania parametrów, zapoznaj się z odpowiednią dokumentacją DBMS.

Zapoznaj się z następującym artykułem, aby uzyskać szczegółowe informacje na temat tworzenia i konfigurowania kont dla PostgreSQL i Postgres Pro: Konfigurowanie kont do pracy z PostgreSQL i Postgres Pro.

Szczegółowe informacje na temat konfiguracji klastra DBMS o wysokiej dostępności można znaleźć w następującym artykule: Przygotowanie klastra DBMS o wysokiej dostępności do pracy z Kaspersky Security Center Linux.

Konfigurowanie serwera MySQL x64 do pracy z Kaspersky Security Center Linux

Aby pomyślnie skonfigurować serwer MySQL x64 do pracy z Kaspersky Security Center, należy użyć domyślnych parametrów serwera, z wyjątkiem parametrów serwera określonych w tym artykule.

Jeśli używasz serwera MySQL dla Kaspersky Security Center, włącz obsługę InnoDB i pamięci MEMORY oraz kodowania UTF-8 i UCS-2.

Zalecane ustawienia dla pliku my.cnf

Więcej szczegółów na temat konfiguracji DBMS znajdziesz także w procedurze konfiguracji konta. Aby uzyskać informacje na temat instalacji DBMS, zapoznaj się z procedurą instalacji DBMS.

W celu skonfigurowania pliku my.cnf:

1. Otwórz plik my.cnf w dowolnym edytorze tekstu.

2. Dodaj następujące wiersze do sekcji `[mysqld]` pliku my.cnf:
```
sort_buffer_size=10M
join_buffer_size=20M
tmp_table_size=600M
max_heap_table_size=600M
key_buffer_size=200M
innodb_buffer_pool_size=< rzeczywista wartość nie może być niższa niż 80%
oczekiwanego rozmiaru bazy danych KAV >
innodb_thread_concurrency=20
innodb_flush_log_at_trx_commit=0 (w większości przypadków, serwer używa niewielkich
transakcji)
innodb_lock_wait_timeout=300
max_allowed_packet=32M
max_connections=151
```

```
max_prepared_stmt_count=12800
table_open_cache=60000
table_open_cache_instances=4
table_definition_cache=60000
```

Należy pamiętać, że określona w wartości `innodb_buffer_pool_size` pamięć jest przydzielana podczas uruchamiania serwera. Jeśli rozmiar bazy danych jest mniejszy niż określony rozmiar bufora, przydzielana jest tylko wymagana pamięć. Rzeczywisty rozmiar przydzielonej pamięci jest o około 10 procent większy niż określony rozmiar bufora. Więcej informacji można znaleźć w dokumentacji MySQL.

Zalecane jest użycie wartości parametru `innodb_flush_log_at_trx_commit = 0`, ponieważ wartości „1" lub „2" negatywnie wpływają na prędkość działania MySQL. Upewnij się, że parametr `innodb_file_per_table` jest ustawiony na `1`.

Przygotowanie klastra DBMS o wysokiej dostępności do pracy z Kaspersky Security Center Linux

Kaspersky Security Center Linux obsługuje następujące klastry o wysokiej dostępności:

- Platform V Pangolin
- Wbudowany klaster o wysokiej dostępności Postgres Pro
- Patroni (z opcjonalnym modułem równoważenia obciążenia HAProxy)

Typ replikacji musi być ustawiony na synchroniczny.

Jeśli używasz szablonu Patroni w wersji 3.3.1 lub starszej dla PostgreSQL, upewnij się, że parametr `synchronous_standby_names` jest zastosowany poprawnie. Aby sprawdzić, czy replikacja synchroniczna jest używana, uruchom następujące zapytanie na węźle głównym:

```
SELECT application_name, client_addr, client_hostname, client_port, sync_state
FROM pg_stat_replication;
```

Jeśli kolumna `sync_state` dla dowolnego węzła wyświetla wartości inne niż `sync` lub `potential` klaster korzysta z replikacji asynchronicznej, która nie jest obsługiwana. Aby rozwiązać ten problem, wykonaj jedną z następujących czynności:

- Zaktualizuj Patroni do wersji 3.3.2 lub nowszej.
- W pliku konfiguracyjnym Patroni znajdź podsekcję `dcs` sekcji `bootstrap` i ustaw parametr `synchronous_mode` na `true`:

  `bootstrap:`

  `dcs:`

  `<...>`

  `synchronous_mode: true`

Minimalna zalecana konfiguracja klastra DBMS o wysokiej dostępności musi obejmować co najmniej trzy węzły.

Aby przygotować klaster DBMS o wysokiej dostępności do pracy z Kaspersky Security Center Linux:

1. Konfigurowanie serwera PostgreSQL lub Postgres Pro do pracy z Kaspersky Security Center Linux.

2. Jeśli chcesz, aby Serwer administracyjny automatycznie wykrywał adresy węzłów klastra, tak żebyś musiał określić tylko nazwę DNS lub adres IP głównego węzła lub węzła repliki podczas instalacji, wykonaj następujące kroki:

   a. Zmodyfikuj plik konfiguracyjny /etc/pangolin-manager/postgres.yml (jeśli używasz Platform V Pangolin) lub /etc/postgresql/<WERSJA>/main/postgresql.conf (jeśli używasz wbudowanego klastra o wysokiej dostępności Postgres Pro) na wszystkich węzłach klastra DBMS o wysokiej dostępności poprzez dodanie następującego wiersza w sekcji `postgresql`:

   `log_hostname=1`

   W przypadku innych parametrów pliku konfiguracyjnego możesz użyć zalecanych wartości parametrów dla PostgreSQL i Postgres Pro.

   b. Po edycji pliku konfiguracyjnego uruchom ponownie usługę klastra DBMS na wszystkich węzłach klastra DBMS o wysokiej dostępności.

   c. Upewnij się, że użytkownik bazy danych ma uprawnienia `pg_read_all_stats`. Możesz przyznać takie uprawnienie uruchamiając następujące polecenie:

   `GRANT pg_read_all_stats TO "%1";`

   Gdzie `%1` to nazwa użytkownika bazy danych.

   Nazwa użytkownika jest określana w trakcie instalacji Serwera administracyjnego w parametrze `KLSRV_UNATT_DBMS_LOGIN`.

   d. Skonfiguruj moduł równoważenia obciążenia dla bazy danych IAM. Zapoznaj się z dokumentacją wybranego modułu równoważenia obciążenia.

Klaster DBMS o wysokiej dostępności jest gotowy do pracy z Kaspersky Security Center Linux.

Instalowanie Kaspersky Security Center Linux

Ta procedura opisuje sposób instalacji Kaspersky Security Center Linux.

Przed instalacją wykonaj następujące czynności:

- Skonfiguruj system DBMS do pracy z Kaspersky Security Center Linux. Możesz wybrać dowolny obsługiwany system DBMS. Informacje o sposobie zainstalowania wybranego systemu DBMS znajdziesz w tym dokumencie.

  Jeśli dystrybucja Twojego systemu operacyjnego opartego na systemie Linux nie zawiera obsługiwanego systemu DBMS, możesz zainstalować system DBMS z repozytorium pakietów firmy trzeciej.

  Po zainstalowaniu systemu DBMS postępuj zgodnie z odpowiednimi instrukcjami:

  - Konfigurowanie serwera PostgreSQL lub Postgres Pro do pracy z Kaspersky Security Center Linux

    Konfiguracja konta DBMS do pracy z PostgreSQL i Postgres Pro

    Jeśli chcesz, aby Serwer administracyjny automatycznie wykrywał adresy węzłów klastra, tak aby podczas instalacji wystarczyło określić nazwę DNS lub adres IP węzła podstawowego lub węzła repliki, upewnij się, że wykonano krok 2 instrukcji w następującym artykule: Przygotowanie klastra DBMS o wysokiej dostępności do pracy z Kaspersky Security Center Linux.

- Konfigurowanie serwera MariaDB x64 do pracy z Kaspersky Security Center Linux

  Konfiguracja konta DBMS do pracy z MySQL i MariaDB

- Konfigurowanie serwera MySQL x64 do pracy z Kaspersky Security Center Linux

  Konfiguracja konta DBMS do pracy z MySQL i MariaDB

- Upewnij się, że na urządzeniu, na którym chcesz zainstalować Kaspersky Security Center Linux, działa jedna z obsługiwanych dystrybucji systemu Linux.

  Jeżeli używasz systemu operacyjnego RED OS 7.3.4 lub nowszego albo MSVSPHERE 9.2 lub nowszego, zainstaluj pakiet libxcrypt-compat, aby zapewnić prawidłowe działanie Serwera administracyjnego.

- Upewnij się, że serwer DNS jest dostępny w sieci.

- Pobierz plik instalacyjny ze strony Kaspersky. Wybierz plik instalacyjny odpowiadający dystrybucji Linux zainstalowanej na Twoim urządzeniu — ksc64_<version_number>_amd64.deb or ksc64-<version_number>.x86_64.rpm.

Aby zainstalować Kaspersky Security Center Linux, uruchom polecenia podane w poniższej instrukcji na koncie z uprawnieniami root.

W celu zainstalowania Kaspersky Security Center Linux:

1. Utwórz grupę 'kladmins' i nieuprzywilejowane konta 'ksc' i 'ksciam'. Konto musi należeć do grupy 'kladmins'. Aby to zrobić, kolejno uruchom następujące polecenia:

   `adduser ksc`

   `groupadd kladmins`

   `gpasswd -a ksc kladmins`

   `usermod -g kladmins ksc`

   `adduser ksciam`

   `gpasswd -a ksciam kladmins`

   `usermod -g kladmins ksciam`

2. Na DBMS utwórz bazę danych dla IAM. Nazwa bazy danych musi być inna niż baza danych, którą zainstalowałeś, aby działać z Kaspersky Security Center Linux. Serwer administracyjny nie usuwa bazy danych IAM automatycznie podczas odinstalowywania lub przenoszenia serwera na inne urządzenie, należy usunąć bazę danych ręcznie.

   - W przypadku PostgreSQL uruchom następujące polecenie:

     ```
     sudo -i -u postgres psql -U postgres -c "CREATE DATABASE <iam_db_name>;"
     ```

   - W przypadku MariaDB uruchom następujące polecenie:

     ```
     sudo mysql -u root -p -e "CREATE DATABASE <iam_db_name>;"
     ```

3. Jeśli używasz klastra DBMS o wysokiej dostępności, wykonaj następujące kroki:

   a. Udziel użytkownikowi „ksc” uprawnienia `pg_read_all_stats`:

   ```
   GRANT pg_read_all_stats TO "ksc";
   ```

   b. Zmodyfikuj plik konfiguracyjny /etc/pangolin-manager/postgres.yml (jeśli używasz Platform V Pangolin) lub /etc/postgresql/main/postgresql.conf (jeśli używasz wbudowanego klastra wysokiej dostępności Postgres Pro) na wszystkich węzłach klastra DBMS o wysokiej dostępności. Dodaj następujący wiersz do sekcji `postgresql`, jeśli podczas łączenia klastra z Kaspersky Security Center Linux chcesz określić tylko nazwę DNS lub adres IP węzła głównego albo węzła repliki:

   ```
   log_hostname: '1'
   ```

   c. Po edycji pliku konfiguracyjnego /etc/pangolin-manager/postgres.yml uruchom ponownie usługę klastra DBMS na wszystkich węzłach klastra DBMS o wysokiej dostępności (z wyłączeniem węzła arbitra) w następujący sposób:

   ```
   systemctl restart pangolin-manager.service
   ```

   lub

   ```
   systemctl restart postgresql-<version>
   ```

4. W razie potrzeby zwiększ domyślny limit plików, które można otworzyć (deskryptory plików) dla kont używanych w ramach usług Serwera administracyjnego. Aby to zrobić, otwórz plik /etc/security/limits.conf i określ miękkie i twarde ograniczenia deskryptorów plików w następujący sposób:

   ```
   ksc  soft  nofile  <max_number_of_opened_files>
   ```

   ```
   ksc  hard  nofile  <max_number_of_opened_files>
   ```

   Domyślnie limity deskryptorów plików są określane podczas instalacji. Miękki limit plików wynosi 32 768 plików, twardy limit plików wynosi 131 072 plików.

5. Uruchom instalację Kaspersky Security Center Linux. W zależności od dystrybucji Linux uruchom jedno z następujących poleceń:

   ```
   sudo apt-get install /<path>/ksc64_<version_number>_amd64.deb
   ```

   ```
   sudo yum install /<path>/ksc64-<version_number>.x86_64.rpm
   ```

6. Uruchom konfigurację Kaspersky Security Center Linux:

   ```
   /opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl
   ```

7. Przeczytaj Umowę Licencyjną Użytkownika Końcowego (EULA) i Politykę prywatności. Tekst jest wyświetlany w oknie wiersza poleceń. Naciśnij spację, aby wyświetlić następny segment tekstu. Następnie po wyświetleniu monitu wprowadź następujące wartości:

   a. Wpisz `y`, jeśli rozumiesz i akceptujesz warunki Umowy licencyjnej użytkownika końcowego. Wpisz `n`, jeśli nie akceptujesz warunków Umowy licencyjnej użytkownika końcowego. Aby korzystać z Kaspersky Security Center Linux, musisz zaakceptować warunki Umowy licencyjnej użytkownika końcowego.

   b. Wpisz `y`, jeśli rozumiesz i akceptujesz warunki Polityki Prywatności oraz zgadzasz się, że Twoje dane będą przetwarzane i przekazywane (w tym do krajów trzecich) zgodnie z Polityką Prywatności. Wpisz `n`, jeśli nie akceptujesz warunków Polityki Prywatności. Aby korzystać z Kaspersky Security Center Linux, musisz zaakceptować warunki Polityki prywatności.

8. Po wyświetleniu monitu wprowadź następujące ustawienia:

   a. Wybierz **Standardowy** jako tryb instalacji Serwera administracyjnego.

   b. Wprowadź nazwę DNS Serwera administracyjnego lub statyczny adres IP. Ten adres będzie używany przez inne urządzenia w celu łączenia się z Serwerem administracyjnym.

   c. Wprowadź numer portu SSL Serwera administracyjnego. Domyślnie wykorzystywany jest port 13000.

   d. Oceń przybliżoną liczbę urządzeń, którymi zamierzasz zarządzać:

      - Jeśli masz od 1 do 100 zarządzanych urządzeń, wpisz 1.
      - Jeśli masz od 101 do 1000 zarządzanych urządzeń, wpisz 2.
      - Jeśli masz więcej niż 1000 zarządzanych urządzeń, wpisz 3.

      To ustawienie służy do automatycznego losowego opóźnienia uruchamiania zadań w celu optymalizacji obciążenia sieci. Poniższa tabela przedstawia przedział czasu, w którym obliczane jest opóźnienie:

      - 1 do 100 zarządzanych urządzeń, wartość 1. Opóźnienie nie jest używane.
      - 101 do 1000 zarządzanych urządzeń, wartość 2. Opóźnienie wynosi 5 minut.
      - Ponad 1000 zarządzanych urządzeń, wartość 3. Opóźnienie wynosi 10 minut.

   e. Wprowadź nazwę grupy zabezpieczeń dla usług. Domyślnie używana jest grupa `kladmins`.

   f. Wprowadź nazwę konta, aby uruchomić usługę Serwera administracyjnego. Konto musi należeć do wprowadzonej grupy zabezpieczeń. Domyślnie używane jest konto „`ksc`”.

   g. Wprowadź nazwę konta, aby uruchomić inne usługi. Konto musi należeć do wprowadzonej grupy zabezpieczeń. Domyślnie używane jest konto „`ksc`”.

   h. Wybierz DBMS, który zainstalowałeś do pracy z Kaspersky Security Center Linux:

      - Jeśli zainstalowałeś MySQL lub MariaDB, wpisz 1.
      - Jeśli zainstalowałeś PostgreSQL lub Postgres Pro, wpisz 2.

   i. Wprowadź nazwę DNS lub adres IP urządzenia, na którym zainstalowany jest system DBMS Serwera administracyjnego. Domyślnie 127.0.0.1 dla lokalnej instalacji sytemu DBMS.

Aby użyć klastra trybu failover o wysokiej dostępności, wykonaj jedną z następujących czynności:

- Wprowadź nazwy DNS lub adresy IP i porty wszystkich węzłów w następującym formacie:

  ```
  <fqdn1>:<port>,<fqdn2>:<port>,<...><fqdnX>:<port>;
  ```

- Określ tylko nazwę DNS lub adres IP węzła głównego lub węzła repliki.

j. Wprowadź numer portu bazy danych. Ten port jest używany do komunikacji z Serwerem administracyjnym. Ten krok zostanie pominięty, jeśli wprowadzono nazwy DNS lub adresy IP i porty wszystkich węzłów klastra o wysokiej dostępności w kroku 8.h.

   Domyślnie używane są następujące porty:

   - Port `3306` dla MySQL lub MariaDB
   - Port `5432` dla PostgreSQL lub Postgres Pro

k. Wprowadź nazwę bazy danych.

l. Wprowadź login konta administratora bazy danych, którego używasz do uzyskiwania dostępu do bazy danych.

m. Wprowadź hasło konta administratora bazy danych, którego używasz do uzyskiwania dostępu do bazy danych.

n. Jeśli zainstalowano PostgreSQL lub Postgres Pro, można określić schemat bazy danych, który będzie używany przez Serwer administracyjny. W tym celu określ nazwę schematu.

   > W nazwie schematu rozróżniana jest wielkość liter: należy używać wyłącznie małych liter.

   Jeśli nie chcesz używać schematu niestandardowego, naciśnij klawisz ENTER. Zostanie użyty schemat domyślny.

o. Wprowadź nazwę DNS serwera FQDN. Jeśli nie określisz tej zmiennej, używana jest nazwa DNS urządzenia z zainstalowanym Serwerem administracyjnym.

   Musisz określić nazwę DNS Serwera administracyjnego, którą wprowadziłeś w kroku 8a.

p. Wprowadź nazwę konta, aby uruchomić usługę IAM. Konto musi należeć do wprowadzonej grupy zabezpieczeń. Domyślnie używane jest konto ksciam.

q. Wybierz DBMS, który zainstalowałeś do pracy z usługą IAM:

   - Jeśli zainstalowałeś MySQL lub MariaDB, wpisz 1.
   - Jeśli zainstalowałeś PostgreSQL lub Postgres Pro, wpisz 2.

r. Wprowadź adres IAM DBMS, który ma być używany przez usługę IAM.

Aby użyć klastra o wysokiej dostępności, wykonaj jedną z następujących czynności:

- Wprowadź nazwy DNS lub adresy IP i porty wszystkich węzłów w następującym formacie:

  ```
  <fqdn1>:<port>,<fqdn2>:<port>,<...><fqdnX>:<port>;
  ```

- Określ tylko nazwę DNS lub adres IP modułu równoważenia obciążenia.

s. Wprowadź numer portu IAM DBMS. Ten port jest używany do komunikacji z usługą IAM. Ten krok zostanie pominięty, jeśli w kroku 8.p wprowadzono nazwy DNS lub adresy IP i porty wszystkich węzłów klastra o wysokiej dostępności.

   Domyślnie używane są następujące porty:

   - Port 3306 dla MySQL lub MariaDB
   - Port 5432 dla PostgreSQL lub Postgres Pro

t. Wprowadź nazwę bazy danych IAM, która ma być używana przez usługę IAM. Nazwa bazy danych używanej przez usługę IAM powinna być inna niż nazwa bazy danych używanej przez Serwer administracyjny.

u. Wprowadź login konta bazy danych, którego używasz do uzyskiwania dostępu do bazy danych IAM.

v. Wprowadź hasło konta bazy danych, którego używasz do uzyskiwania dostępu do bazy danych IAM.

   Poczekaj, aż usługi zostaną dodane i uruchomione automatycznie:

   - `klnagent_srv`
   - `kladminserver_srv`
   - `klactprx_srv`
   - `klwebsrv_srv`
   - `kliam_srv`

w. Jeśli zainstalowano PostgreSQL lub Postgres Pro, można określić schemat bazy danych, który ma być używany przez IAM. Aby to zrobić, podaj nazwę schematu.

   Jeśli nie chcesz używać schematu niestandardowego, naciśnij klawisz ENTER, a zostanie użyty schemat publiczny.

   > W nazwie schematu rozróżniana jest wielkość liter: należy używać wyłącznie małych liter.
   > Nie podawaj zastrzeżonych nazw schematów IAM: client, iam, ksc, locker, pat, scope, voltron.

x. Utwórz konto, które będzie działać jako administrator Serwera administracyjnego. Wprowadź nazwę użytkownika i hasło.

Hasło musi być zgodne z następującymi regułami:

- Hasło użytkownika nie może mieć mniej niż 8 ani więcej niż 256 znaków.
- Hasło musi zawierać znaki z przynajmniej trzech z poniższych grup:
  - Wielkie litery (A-Z)
  - Małe litery (a-z)
  - Cyfry (0-9)
  - Znaki specjalne (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)

Jeśli pominiesz ten krok, możesz później użyć następującego polecenia, aby utworzyć nowego użytkownika:

```
/opt/kaspersky/ksc64/sbin/kladduser -n kscadmin -p <password>
```

Użytkownik zostanie dodany i zainstalowany Kaspersky Security Center Linux.

Instalacja Agenta sieciowego

Aby zarządzać urządzeniem Serwera administracyjnego jak każdym innym zarządzanym urządzeniem, zainstaluj Agenta sieciowego dla systemu Linux na urządzeniu Serwera administracyjnego. W takim przypadku Agent sieciowy dla systemu Linux jest instalowany i działa niezależnie od wersji serwerowej Agenta sieciowego zainstalowanego wraz z Serwerem administracyjnym.

Weryfikacja usługi

Użyj następujących poleceń, aby sprawdzić, czy usługa jest uruchomiona:

- `systemctl status klnagent_srv.service`
- `systemctl status kladminserver_srv.service`
- `systemctl status klactprx_srv.service`
- `systemctl status klwebsrv_srv.service`
- `systemctl status kliam_srv.service`

Instalowanie Kaspersky Security Center Linux w trybie cichym

Możesz zainstalować Kaspersky Security Center Linux na urządzeniach z systemem Linux, używając pliku odpowiedzi do uruchomienia instalacji w trybie cichym, czyli bez udziału użytkownika. Plik odpowiedzi zawiera niestandardowy zestaw parametrów instalacji: zmienne i odpowiadające im wartości.

Przed instalacją:

- Skonfiguruj system DBMS do pracy z Kaspersky Security Center Linux. Możesz wybrać dowolny obsługiwany system DBMS. Informacje o sposobie zainstalowania wybranego systemu DBMS znajdziesz w tym dokumencie.

  Jeśli dystrybucja Twojego systemu operacyjnego opartego na systemie Linux nie zawiera obsługiwanego systemu DBMS, możesz zainstalować system DBMS z repozytorium pakietów firmy trzeciej.

  Po zainstalowaniu systemu DBMS postępuj zgodnie z odpowiednimi instrukcjami:

  - Konfigurowanie serwera PostgreSQL lub Postgres Pro do pracy z Kaspersky Security Center Linux

    Konfiguracja konta DBMS do pracy z PostgreSQL i Postgres Pro

    Jeśli chcesz, aby Serwer administracyjny automatycznie wykrywał adresy węzłów klastra, tak aby podczas instalacji wystarczyło określić nazwę DNS lub adres IP węzła podstawowego lub węzła repliki, upewnij się, że wykonano krok 2 instrukcji w następującym artykule: Przygotowanie klastra DBMS o wysokiej dostępności do pracy z Kaspersky Security Center Linux.

  - Konfigurowanie serwera MariaDB x64 do pracy z Kaspersky Security Center Linux

    Konfiguracja konta DBMS do pracy z MySQL i MariaDB

  - Konfigurowanie serwera MySQL x64 do pracy z Kaspersky Security Center Linux

    Konfiguracja konta DBMS do pracy z MySQL i MariaDB

- Upewnij się, że na urządzeniu z zainstalowanym systemem DBMS nie ma kont użytkowników DBMS o następujących nazwach:

  - client
  - iam
  - ksc
  - locker
  - pat
  - scope
  - voltron

- Upewnij się, że na urządzeniu, na którym chcesz zainstalować Kaspersky Security Center Linux, działa jedna z obsługiwanych dystrybucji systemu Linux.

  > Jeżeli używasz systemu operacyjnego RED OS 7.3.4 lub nowszego albo MSVSPHERE 9.2 lub nowszego, zainstaluj pakiet libxcrypt-compat, aby zapewnić prawidłowe działanie Serwera administracyjnego.

- Pobierz plik instalacyjny ze strony Kaspersky. Wybierz plik instalacyjny odpowiadający dystrybucji Linux zainstalowanej na Twoim urządzeniu — ksc64_[numer_wersji]_amd64.deb lub ksc64-[numer_wersji].x86_64.rpm.

W celu zainstalowania Kaspersky Security Center Linux w trybie cichym:

1. Przeczytaj Umowę licencyjną użytkownika końcowego. Wykonaj poniższe kroki tylko wtedy, gdy rozumiesz i akceptujesz warunki Umowy licencyjnej użytkownika końcowego.

2. Utwórz grupę 'kladmins' i nieuprzywilejowane konto 'ksc', które musi należeć do grupy 'kladmins' Aby to zrobić, uruchom kolejno następujące polecenia na koncie z uprawnieniami roota:

   `adduser ksc`

   `groupadd kladmins`

   `gpasswd -a ksc kladmins`

   `usermod -g kladmins ksc`

   `adduser ksciam`

   `gpasswd -a ksciam kladmins`

   `usermod -g kladmins ksciam`

3. Na DBMS utwórz bazę danych dla IAM. Nazwa bazy danych musi być inna niż baza danych, którą zainstalowałeś, aby działać z Kaspersky Security Center Linux. Serwer administracyjny nie usuwa bazy danych IAM automatycznie podczas odinstalowywania lub przenoszenia serwera na inne urządzenie, należy usunąć bazę danych ręcznie.

   - W przypadku PostgreSQL uruchom następujące polecenie:

     ```
     sudo -i -u postgres psql -U postgres -c "CREATE DATABASE <iam_db_name>;"
     ```

   - W przypadku MariaDB uruchom następujące polecenie:

     ```
     sudo mysql -u root -p -e "CREATE DATABASE <iam_db_name>;"
     ```

4. Utwórz plik odpowiedzi (w formacie TXT) i dodaj do pliku odpowiedzi listę zmiennych w formacie `VARIABLE_NAME=variable_value`, każdą w osobnym wierszu. Plik odpowiedzi powinien zawierać zmienne wymienione w poniższej tabeli.

5. Ustaw wartość zmiennej środowiskowej `KLAUTOANSWERS` w środowisku root lub środowisku użytkownika zawierającej pełną nazwę pliku odpowiedzi wraz ze ścieżką, na przykład za pomocą następującego polecenia:

   `export KLAUTOANSWERS=/tmp/ksc_install/answers.txt`

6. Uruchom instalację Kaspersky Security Center Linux w trybie cichym — w zależności od używanej dystrybucji Linuksa uruchom jedno z następujących poleceń:

   W środowisku root:

```
apt-get install /<path>/ksc64_[version_number]_amd64.deb -y
```

```
yum install /<path>/ksc64-[version_number].x86_64.rpm -y
```

   W środowisku użytkownika:

```
sudo -E apt-get install /<path>/ksc64_[version_number]_amd64.deb -y
```

```
sudo -E yum install /<path>/ksc64-[version_number].x86_64.rpm -y
```

7. Utwórz użytkownika do pracy z Kaspersky Security Center Web Console. Aby to zrobić, uruchom następujące polecenie na koncie z uprawnieniami roota:

   `/opt/kaspersky/ksc64/sbin/kladduser -n kscadmin -p <password>`, gdzie hasło musi zawierać co najmniej 8 znaków.

8. Zainstaluj Kaspersky Security Center Web Console.

Zmienne pliku odpowiedzi użyte jako parametry instalacji Kaspersky Security Center Linux w trybie cichym

Nazwa zmiennej	Wymagane	Opis	Możliwe wartości
EULA_ACCEPTED	Tak	Ten parametr potwierdza, że w pełni przeczytano, zrozumiano i zaakceptowano warunki Umowy licencyjnej użytkownika końcowego.	1
PP_ACCEPTED	Tak	Potwierdza, że rozumiesz i akceptujesz warunki Polityki prywatności.	1
KLSRV_UNATT_SERVERADDRESS	Tak	Wprowadź nazwę DNS Serwera administracyjnego lub statyczny adres IP.	Nazwa DNS lub adres IP
KLSRV_UNATT_PORT_SRV	Nie	Wprowadź numer portu Serwera administracyjnego. Wartość domyślna to 14000.	Numer portu
KLSRV_UNATT_PORT_SRV_SSL	Nie	Wprowadź numer portu SSL Serwera administracyjnego. Wartość domyślna to 13000.	Numer portu
KLSRV_UNATT_PORT_KLOAPI	Nie	Numer portu do pracy z OpenAPI. Ten port służy również do odbierania połączeń z Kaspersky Security Center Web Console. Opcjonalne, wartość domyślna to 13299.	Numer portu
KLSRV_UNATT_PORT_GUI	Nie	Numer portu do pracy z narzędziem klakaut. Opcja, wartość domyślna to 13291. Narzędzie klakaut i jego system pomocy znajdują się w folderze instalacyjnym Kaspersky Security Center Linux. Ten port jest domyślnie zamknięty. Jeśli chcesz użyć narzędzia klakaut w celu zautomatyzowania działania Kaspersky Security Center Linux, otwórz port 13291 przy użyciu narzędzia klscflag.	Numer portu

`KLSRV_UNATT_NETRANGETYPE`	Nie	Oceń przybliżoną liczbę urządzeń, którymi zamierzasz zarządzać. To ustawienie służy do optymalizacji obciążenia sieci. Opcja, wartość domyślna to 1.	`1` dla 1 do 100 zarządzanych urządzeń. `2` dla 101 do 1000 zarządzanych urządzeń. `3` dla ponad 1000 zarządzanych urządzeń.

`KLSRV_UNATT_DBMS_TYPE`	Tak	Typ systemu zarządzania bazą danych: MySQL (MariaDB) lub Postgres.	`mysql`
			lub
			`postgres`

`KLSRV_UNATT_DBMS_INSTANCE`	Tak	Adres IP serwera bazy danych. Aby użyć wbudowanego klastra o wysokiej dostępności PostgreSQL, Postgres Pro lub klastra Platform V Pangolin DBMS, wprowadź nazwy DNS lub adresy IP i porty wszystkich węzłów w następującym formacie: `<fqdn1>:<port>,<fqdn2>:<port>,<...> <fqdnX>:<port>;` Alternatywnie, jeśli chcesz użyć klastra Platform V Pangolin DBMS, możesz podczas określania adresu DBMS określić tylko nazwę DNS lub adres IP węzła głównego, albo węzła repliki.	Adres IP

`KLSRV_UNATT_DBMS_PORT`	Tak	Port serwera bazy danych. Domyślna wartość dla MySQL (MariaDB) to 3306; domyślna wartość dla Postgres to 5432.	`3306`
			lub
			`5432`

`KLSRV_UNATT_DB_NAME`	Tak	Nazwa bazy danych. Nazwa bazy danych musi być inna niż nazwa bazy danych IAM określona w zmiennej `KLSRV_UNATT_DB_IAM_NAME`.	`kav`
`KLSRV_UNATT_DBMS_LOGIN`	Tak	Nazwa użytkownika, który ma dostęp do bazy danych.	
`KLSRV_UNATT_DBMS_PASSWORD`	Tak	Hasło użytkownika, który ma dostęp do bazy danych.	
`KLSRV_UNATT_DBMS_SCHEMA`	Nie	Niestandardowy schemat DBMS. Jeżeli nie określisz niestandardowego schematu, Serwer administracyjny użyje schematu domyślnego. W nazwie schematu rozróżniana jest wielkość liter: należy używać wyłącznie małych liter. Niestandardowy schemat można określić tylko wtedy, gdy jako system DBMS używany jest PostgreSQL lub Postgres Pro. W przeciwnym razie zmienna jest ignorowana.	`database_schema`
`KLSRV_UNATT_IAM_ADDRESS`	Tak	Przeglądarki użytkowników zostaną przekierowane na ten adres przez OpenIDConnect. Wprowadź nazwę DNS serwera FQDN. Musisz użyć nazwy DNS Serwera administracyjnego określonej w parametrze `KLSRV_UNATT_SERVERADDRESS`.	FQDN
`KLSRV_UNATT_KLIAMUSER`	Tak	Nazwa konta do uruchomienia usługi IAM. Konto musi należeć do grupy zabezpieczeń określonej w zmiennej `KLSRV_UNATT_KLADMINSGROUP`.	ksciam

`KLSRV_UNATT_DBMS_IAM_TYPE`	Tak	Typ systemu zarządzania bazą danych IAM: MySQL (MariaDB) lub Postgres.	`mysql`
			lub
			`postgres`

KLSRV_UNATT_DBMS_IAM_INSTANCE	Tak	Adres serwera bazy danych IAM. Aby użyć wbudowanego klastra o wysokiej dostępności PostgreSQL, Postgres Pro lub klastra Platform V Pangolin DBMS, wprowadź nazwy DNS lub adresy IP i porty wszystkich węzłów w następującym formacie: `<fqdn1>:<port>,<fqdn2>:<port>,<...> <fqdnX>:<port>;` Alternatywnie, jeśli chcesz użyć klastra Platform V Pangolin DBMS, możesz podczas określania adresu DBMS określić tylko nazwę DNS lub adres IP węzła głównego, albo węzła repliki.	Adres IP
KLSRV_UNATT_DBMS_IAM_PORT	Tak	Port serwera bazy danych IAM. Domyślna wartość dla MySQL (MariaDB) to 3306; domyślna wartość dla Postgres to 5432.	3306 lub 5432
KLSRV_UNATT_DBMS_IAM_LOGIN	Tak	Nazwa użytkownika, który ma dostęp do bazy danych IAM. Jeśli typem bazy danych IAM jest MySQL (MariaDB) i ma ona oba poniższe ustawienia: • `gtid_mode=ON` • `gtid_purged=ON|AUTO` upewnij się, że określony użytkownik ma jedno z następujących uprawnień DBMS: • `RELOAD` • `FLUSH_TABLES`	
KLSRV_UNATT_DBMS_IAM_PASSWORD	Tak	Hasło użytkownika, który ma dostęp do bazy danych IAM.	
KLSRV_UNATT_DBMS_IAM_SCHEMA	Nie	Niestandardowy schemat DBMS. Jeśli nie określisz niestandardowego schematu, IAM użyje schematu publicznego. Niestandardowy schemat można określić tylko wtedy, gdy jako system DBMS używany jest PostgreSQL lub Postgres Pro. W przeciwnym razie zmienna jest ignorowana. W nazwie schematu rozróżniana jest wielkość liter: należy używać wyłącznie małych liter. Nie określaj zarezerwowanych nazw schematów iam: `client, iam, ksc, locker, pat, scope, voltron`.	`database_schema`
KLSRV_UNATT_DB_IAM_NAME	Tak	Nazwa bazy danych IAM. Nazwa bazy danych IAM musi być inna niż nazwa bazy danych określona w zmiennej `KLSRV_UNATT_DB_NAME`. Określ ręcznie utworzoną pustą bazę danych.	`iamdb`
KLSRV_UNATT_KLADMINSGROUP	Tak	Wprowadź nazwę grupy zabezpieczeń dla usług.	`kladmins`
KLSRV_UNATT_KLSRVUSER	Tak	Nazwa konta do uruchomienia usługi Serwera administracyjnego. Konto musi należeć do grupy zabezpieczeń określonej w zmiennej `KLSRV_UNATT_KLADMINSGROUP`.	`ksc`
KLSRV_UNATT_KLSVCUSER	Tak	Nazwa konta do uruchomienia innych usług. Konto musi należeć do grupy zabezpieczeń określonej w zmiennej `KLSRV_UNATT_KLADMINSGROUP`.	`ksc`
Jeśli Serwer administracyjny ma zostać wdrożony jako klaster pracy awaryjnej Kaspersky Security Center Linux, plik odpowiedzi musi zawierać następujące dodatkowe zmienne:			

`KLFOC_UNATT_EXT_RESOURCE_MANAGEMENT`	Nie	Konfiguracja klastra trybu failover. Jeśli parametr zostanie pominięty w pliku odpowiedzi, używana jest wartość domyślna.
		Możliwe wartości:
		`0` — Klaster trybu failover, którego węzły znajdują się w jednym centrum danych (wartość domyślna).
		`2` — Geograficznie rozproszony klaster trybu failover, którego węzły znajdują się w różnych centrach danych.
			`0`
			lub
			`2`

`KLFOC_UNATT_NODE`	Tak	Numer węzła (1 lub 2).	`1`
			lub
			`2`

`KLFOC_UNATT_STATE_SHARE_MOUNT_PATH`	Tak	Punkt podłączenia dzielenia stanu.	
`KLFOC_UNATT_DATA_SHARE_MOUNT_PATH`	Tak	Punkt podłączenia dzielenia danych.	

`KLFOC_UNATT_CONN_MODE`	Tak	Tryb łączności klastra pracy awaryjnej.	`VirtualAdapter`
			lub
			`ExternalLoadBalancer`

W przypadku, gdy zmienna `KLFOC_UNATT_CONN_MODE` ma wartość `VirtualAdapter`, plik odpowiedzi musi zawierać następujące zmienne dodatkowe:			
`KLFOC_UNATT_CONN_MODE_VA_NAME`	Tak	Nazwa wirtualnej karty sieciowej.	
`KLFOC_UNATT_CONN_MODE_VA_IPV4`	Jedna z tych zmiennych jest wymagana	Adres IP wirtualnej karty sieciowej.	Adres IP
`KLFOC_UNATT_CONN_MODE_VA_IPV6`		Adres IPv6 wirtualnej karty sieciowej.	Adres IPv6

Instalowanie Kaspersky Security Center Linux na Astra Linux w trybie zamkniętego środowiska oprogramowania

Ta sekcja opisuje sposób instalacji Kaspersky Security Center Linux w systemie operacyjnym Astra Linux Special Edition.

Przed instalacją:

- Zainstaluj system DBMS.
- Pobierz klucz aplikacji kaspersky_astra_pub_key.gpg.
- Pobierz plik instalacyjny ksc64_[numer_wersji]_amd64.deb ze strony internetowej Kaspersky.

Na koncie z uprawnieniami administratora uruchom polecenia podane w tej instrukcji z zachowaniem wysokiej integralności i zerowej poufności.

W celu zainstalowania Kaspersky Security Center Linux w systemie operacyjnym Astra Linux Special Edition (aktualizacja operacyjna 1.7.2) i Astra Linux Special Edition (aktualizacja operacyjna 1.6):

1. Otwórz plik `/etc/digsig/digsig_initramfs.conf` a następnie określ następujące ustawienie:

   ```
   DIGSIG_ELF_MODE=1
   ```

2. W wierszu polecenia uruchom następujące polecenie, aby zainstalować pakiet zgodności:

   ```
   apt install astra-digsig-oldkeys
   ```

3. Utwórz katalog dla klucza aplikacji:

   ```
   mkdir -p /etc/digsig/keys/legacy/kaspersky/
   ```

4. Umieść klucz aplikacji w katalogu utworzonym w poprzednim kroku:

   ```
   cp kaspersky_astra_pub_key.gpg /etc/digsig/keys/legacy/kaspersky/
   ```

5. Zaktualizuj początkowy obraz systemu plików RAM dla wszystkich jąder systemu:

   ```
   update-initramfs -u -k all
   ```

   Uruchom ponownie system.

6. Utwórz grupę 'kladmins' i nieuprzywilejowane konta 'ksc' i 'ksciam'. Konto musi należeć do grupy 'kladmins'. Aby to zrobić, kolejno uruchom następujące polecenia:

   ```
   # adduser ksc
   # groupadd kladmins
   # gpasswd -a ksc kladmins
   # usermod -g kladmins ksc
   # adduser ksciam
   # gpasswd -a ksciam kladmins
   # usermod -g kladmins ksciam
   ```

7. Uruchom instalację Kaspersky Security Center Linux:

   ```
   # apt install /<path>/ksc64_[numer_wersji]_amd64.deb
   ```

8. Uruchom konfigurację Kaspersky Security Center Linux:

   ```
   # /opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl
   ```

9. Przeczytaj Umowę Licencyjną Użytkownika Końcowego (EULA) i Politykę prywatności. Tekst jest wyświetlany w oknie wiersza poleceń. Naciśnij spację, aby wyświetlić następny segment tekstu. Po wyświetleniu monitu wprowadź następujące ustawienia:

   a. Wpisz `y`, jeśli rozumiesz i akceptujesz warunki Umowy licencyjnej użytkownika końcowego. Wpisz `n`, jeśli nie akceptujesz warunków Umowy licencyjnej użytkownika końcowego. Aby korzystać z Kaspersky Security Center Linux, musisz zaakceptować warunki Umowy licencyjnej użytkownika końcowego.

   b. Wpisz `y`, jeśli rozumiesz i akceptujesz warunki Polityki Prywatności oraz zgadzasz się, że Twoje dane będą przetwarzane i przekazywane (w tym do krajów trzecich) zgodnie z Polityką Prywatności. Wpisz `n`, jeśli nie akceptujesz warunków Polityki Prywatności. Aby korzystać z Kaspersky Security Center Linux, musisz zaakceptować warunki Polityki prywatności.

10. Po wyświetleniu monitu wprowadź następujące ustawienia:

    a. Wprowadź nazwę DNS Serwera administracyjnego lub statyczny adres IP.

    b. Wprowadź numer portu Serwera administracyjnego. Domyślnie wykorzystywany jest port 14000.

    c. Wprowadź numer portu SSL Serwera administracyjnego. Domyślnie wykorzystywany jest port 13000.

    d. Oceń przybliżoną liczbę urządzeń, którymi zamierzasz zarządzać:

       - Jeśli masz od 1 do 100 zarządzanych urządzeń, wpisz 1.
       - Jeśli masz od 101 do 1000 zarządzanych urządzeń, wpisz 2.
       - Jeśli masz więcej niż 1000 zarządzanych urządzeń, wpisz 3.

To ustawienie służy do automatycznego losowego opóźnienia uruchamiania zadań w celu optymalizacji obciążenia sieci. Poniższa tabela przedstawia przedział czasu, w którym obliczane jest opóźnienie:

- 1 do 100 zarządzanych urządzeń, wartość 1. Opóźnienie nie jest używane.
- 101 do 1000 zarządzanych urządzeń, wartość 2. Opóźnienie wynosi 5 minut.
- Ponad 1000 zarządzanych urządzeń, wartość 3. Opóźnienie wynosi 10 minut.

e. Wprowadź nazwę grupy zabezpieczeń dla usług. Domyślnie używana jest grupa „kladmins".

f. Wprowadź nazwę konta, aby uruchomić usługę Serwera administracyjnego. Konto musi należeć do wprowadzonej grupy zabezpieczeń. Domyślnie używane jest konto „ksc".

g. Wprowadź nazwę konta, aby uruchomić inne usługi. Konto musi należeć do wprowadzonej grupy zabezpieczeń. Domyślnie używane jest konto „ksc".

h. Wybierz DBMS, który zainstalowałeś do pracy z Kaspersky Security Center Linux:

- Jeśli zainstalowałeś MySQL lub MariaDB, wpisz 1.
- Jeśli zainstalowałeś PostgreSQL lub Postgres Pro, wpisz 2.

i. Wprowadź adres IP urządzenia, na którym zainstalowana jest baza danych.

j. Wprowadź numer portu bazy danych. Ten port jest używany do komunikacji z Serwerem administracyjnym. Domyślnie używane są następujące porty:

- Port 3306 dla MySQL lub MariaDB.
- Port 5432 dla PostgreSQL lub Postgres Pro.

k. Wprowadź nazwę bazy danych.

l. Wprowadź login konta administratora bazy danych, którego używasz do uzyskiwania dostępu do bazy danych.

m. Wprowadź hasło konta administratora bazy danych, którego używasz do uzyskiwania dostępu do bazy danych.

n. Wprowadź nazwę FQDN serwera IAM.

Należy określić nazwę DNS Serwera administracyjnego wprowadzoną w kroku 10a.

o. Wprowadź nazwę konta, aby uruchomić usługę kliam. Konto musi należeć do wprowadzonej grupy zabezpieczeń.

p. Wybierz DBMS, który zainstalowałeś do pracy z usługą IAM:

- Jeśli zainstalowałeś MySQL lub MariaDB, wpisz 1.
- Jeśli zainstalowałeś PostgreSQL lub Postgres Pro, wpisz 2.

q. Wprowadź adres DBMS, który ma być używany przez usługę IAM.

r. Wprowadź numer portu bazy danych. Ten port jest używany do komunikacji z usługą IAM. Domyślnie używane są następujące porty:

- Port 3306 dla MySQL lub MariaDB.
- Port 5432 dla PostgreSQL lub Postgres Pro.

s. Wprowadź nazwę bazy danych, która ma być używana przez usługę IAM. Nazwa bazy danych używanej przez usługę IAM powinna być inna niż nazwa bazy danych używanej przez Serwer administracyjny.

t. Wprowadź login konta głównego bazy danych, którego używasz do uzyskiwania dostępu do bazy danych IAM.

u. Wprowadź hasło konta głównego bazy danych, którego używasz do uzyskiwania dostępu do bazy danych IAM.

Poczekaj, aż usługi zostaną dodane i uruchomione automatycznie:

- `klnagent_srv`
- `kladminserver_srv`
- `klactprx_srv`
- `klwebsrv_srv`
- `kliam_srv`

v. Utwórz konto, które będzie działać jako administrator Serwera administracyjnego. Wprowadź nazwę użytkownika i hasło.

Hasło musi być zgodne z następującymi regułami:

- Hasło użytkownika musi mieć co najmniej 8, a maksymalnie 256 znaków.
- Hasło musi zawierać znaki z przynajmniej trzech z poniższych grup:
  - Wielkie litery (A-Z)
  - Małe litery (a-z)
  - Cyfry (0-9)
  - Znaki specjalne (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)

Kaspersky Security Center Linux zostanie zainstalowany, a użytkownik zostanie dodany.

Weryfikacja usługi

Użyj następujących poleceń, aby sprawdzić, czy usługa jest uruchomiona:

- `# systemctl status klnagent_srv.service`
- `# systemctl status kladminserver_srv.service`

- `# systemctl status klactprx_srv.service`
- `# systemctl status klwebsrv_srv.service`
- `# systemctl status kliam_srv.service`

Instalowanie Kaspersky Security Center Web Console

W tej sekcji opisano sposób osobnego instalowania Kaspersky Security Center Web Console Server (zwanego również Kaspersky Security Center Web Console) na urządzeniach działających pod kontrolą systemu operacyjnego Linux. Przed instalacją musisz zainstalować system DBMS i Serwerem administracyjnym Kaspersky Security Center Linux.

> Jeśli instalujesz Kaspersky Security Center Web Console na Astra Linux w trybie zamkniętego środowiska oprogramowania, postępuj zgodnie z instrukcjami określonymi dla Astra Linux.

Użyj jednego z następujących plików instalacyjnych, które odpowiadają dystrybucji Linux zainstalowanej na Twoim urządzeniu:

- Dla Debian — ksc-web-console-<build number>.x86_64.deb
- Dla systemów operacyjnych opartych na RPM — ksc-web-console-<build number>.x86_64.rpm

Plik instalacyjny można pobrać ze strony internetowej Kaspersky.

W celu zainstalowania Kaspersky Security Center Web Console:

1. Upewnij się, że na urządzeniu, na którym chcesz zainstalować Kaspersky Security Center Web Console, działa jedna z obsługiwanych dystrybucji systemu Linux.
2. Przeczytaj Umowę licencyjną Użytkownika Końcowego (EULA). Jeśli pakiet dystrybucyjny Kaspersky Security Center Linux nie zawiera pliku TXT z treścią Umowy licencyjnej użytkownika końcowego, możesz pobrać ten plik ze strony internetowej Kaspersky. Jeśli nie akceptujesz warunków Umowy licencyjnej, nie instaluj aplikacji.
3. Utwórz plik odpowiedzi, który zawiera parametry połączenia Kaspersky Security Center Web Console z Serwerem administracyjnym: `/etc/ksc-web-console-setup.json`.

   Przykład pliku odpowiedzi zawierającego minimalny zestaw parametrów

Zestaw parametrów pliku odpowiedzi zależy od wersji Serwera administracyjnego, z którym łączy się Kaspersky Security Center Web Console:

- Serwer administracyjny w wersji 16 lub nowszej

  Przykład pliku odpowiedzi z minimalnym zestawem parametrów do logowania się do Serwera administracyjnego w wersji 16 lub nowszej:

```
{
    "address": "ksc-web-console.example.com",
    "port": 8080,
    "trusted":  {
        "Administration Server v16": {
            "iamHost": "ksc16.example.com",
            "iamOAuthPort": 4444,
            "iamProxyPort": 9050,
            "iamCertPath": "/var/opt/kaspersky/klnagent_srv/iam/main_certificate.pem",
            "iamPATPath": "/var/opt/kaspersky/klnagent_srv/iam/initial_token.txt",
            "kscPort": 13299,
            "kscCertPath": "/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer"
        }
    },
    "certDomain":"ksc-web-console.example.com",
    "acceptEula": true
}
```

- Serwer administracyjny w wersji 15.4 lub starszej

  Przykład pliku odpowiedzi z minimalnym zestawem parametrów do logowania się do Serwera administracyjnego w wersji 15.4 lub starszej:

```
{
    "address": "ksc-web-console.example.com",
    "port": 8080,
    "trusted":  {
         "Administration Server v15.4": {
             "kscHost": "ksc.example.com",
             "kscPort": 13299,
             "kscCertPath": "/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer"
         }
    },
    "certDomain":"ksc-web-console.example.com",
    "acceptEula": true
}
```

Możesz zainstalować Kaspersky Security Center Web Console na tym samym urządzeniu, na którym jest zainstalowany Serwer administracyjny, lub na innym. Jeżeli Kaspersky Security Center Web Console jest zainstalowana na innym urządzeniu, adres Kaspersky Security Center Web Console (określony przez `address`) i adres Serwera administracyjnego (określony przez `iamHost` lub `kscHost`) różnią się. Jeśli Kaspersky Security Center Web Console jest zainstalowana na tym samym urządzeniu co Serwer administracyjny, parametry te mają takie same wartości.

Wartość `iamHost` musi być zgodna z adresem IAM określonym podczas instalacji Serwera administracyjnego. Aby uzyskać określony adres IAM, uruchom następujące polecenie na urządzeniu z zainstalowanym Serwerem administracyjnym:

```
grep "iam_address:" /var/opt/kaspersky/klnagent_srv/iam/iam_config.yaml
```

Szczegółowe informacje można znaleźć w artykule: Parametry instalacji Kaspersky Security Center Web Console.

Do listy zaufanych serwerów można dodać wiele Serwerów administracyjnych o różnych wersjach. W takim przypadku serwery mogą używać różnych metod uwierzytelniania.

Zalecamy określenie numerów portów powyżej 1024. Jeśli chcesz, aby Kaspersky Security Center Web Console działał na portach poniżej 1024, po instalacji musisz upewnić się, że masz narzędzie setcap, a następnie uruchom następujące polecenie:

```
sudo setcap 'cap_net_bind_service=+ep' /var/opt/kaspersky/ksc-web-console/node
```

Jeśli nie masz narzędzia setcap, możesz je zainstalować. **Kliknij ten link, aby wyświetlić polecenia**.

W przypadku systemów operacyjnych Debian i Ubuntu uruchom jedno z następujących poleceń:

- `sudo apt-get install libcap2-bin`
- `sudo apt install libcap2-bin`

W przypadku SUSE Linux Enterprise Server i Red Hat Enterprise Linux uruchom polecenie:

- `sudo zypper install libcap-progs`

Podczas instalacji konsoli Kaspersky Security Center Web Console w systemie operacyjnym Linux ALT, musisz określić numer portu inny niż 8080, ponieważ port 8080 jest używany przez system operacyjny.

Kaspersky Security Center Web Console nie można zaktualizować przy użyciu tego samego pliku instalacyjnego .rpm. Jeśli chcesz zmienić ustawienia w pliku odpowiedzi i użyć tego pliku do ponownego zainstalowania aplikacji, w pierwszej kolejności musisz usunąć aplikację, a następnie zainstalować ją ponownie z nowym plikiem odpowiedzi.

4. Z poziomu konta z uprawnieniami administratora użyj wiersza polecenia, aby uruchomić plik instalacji z rozszerzeniem .deb lub .rpm, w zależności od posiadanej dystrybucji systemu Linux.

   - W celu zainstalowania lub uaktualnienia Kaspersky Security Center Web Console z pliku .deb uruchom następujące polecenie:
     ```
     sudo apt-get install ksc-web-console-<numer kompilacji>.x86_64.deb
     ```
   - W celu zainstalowania Kaspersky Security Center Web Console z pliku .rpm uruchom jedno z następujących poleceń:
     ```
     sudo yum install ksc-web-console-<numer kompilacji>.x86_64.rpm
     ```
     lub
     ```
     sudo alien -i ksc-web-console-<numer kompilacji>.x86_64.rpm
     ```
   - W celu przeprowadzenia aktualizacji z poprzedniej wersji Kaspersky Security Center Web Console, uruchom jedno z następujących poleceń:
     - W przypadku urządzeń z systemem operacyjnym opartym na RPM:
       ```
       sudo yum install ksc-web-console-<numer kompilacji>.x86_64.rpm
       ```
     - Dla urządzeń z systemem operacyjnym opartym na systemie Debian:
       ```
       sudo apt-get install ksc-web-console-<numer kompilacji>.x86_64.deb
       ```

   Rozpocznie się wypakowywanie pliku instalacji. Zaczekaj na zakończenie instalacji. Kaspersky Security Center Web Console jest instalowany w następującym katalogu: /var/opt/kaspersky/ksc-web-console.

5. Uruchom ponownie wszystkie usługi Kaspersky Security Center Web Console, uruchamiając następujące polecenie:
   ```
   sudo systemctl restart KSC*
   ```

Po zakończeniu instalacji możesz użyć przeglądarki internetowej do otwarcia i zalogowania się do Kaspersky Security Center Web Console.

Jeśli certyfikat wspólny Serwera administracyjnego zostanie zastąpiony innym certyfikatem z kopii zapasowej lub zastąpiony za pomocą narzędzia klsetsrvcert należy usunąć i ponownie zainstalować Kaspersky Security Center Web Console. W przeciwnym razie logowanie do Web Console będzie ograniczone.
Jeśli po ponownej instalacji nie możesz zalogować się do Web Console, sprawdź konfigurację Serwera IAM.

Parametry instalacji Kaspersky Security Center Web Console

Aby zainstalować Kaspersky Security Center Web Console Server na urządzeniach działających pod kontrolą systemu Linux, musisz utworzyć plik odpowiedzi — plik .json, który zawiera parametry połączenia Kaspersky Security Center Web Console z Serwerem administracyjnym. Nadaj plikowi nazwę ksc-web-console-setup.json i umieść go w następującym katalogu: /etc/ksc-web-console-setup.json.

Zestaw parametrów pliku odpowiedzi zależy od wersji Serwera administracyjnego, z którym łączy się Kaspersky Security Center Web Console.

- Serwer administracyjny w wersji 16 lub nowszej

  Wersja 16 Serwera administracyjnego lub nowsza obejmuje usługę Menedżera tożsamości i dostępu (IAM) zapewniającą uwierzytelnianie domeny za pomocą pojedynczego logowania (SSO) w Kaspersky Security Center Web Console. Aby Kaspersky Security Center Web Console mogła połączyć się z Serwerem administracyjnym, plik odpowiedzi musi zawierać parametry interakcji z komponentem IAM, nawet jeśli nie korzystasz z pojedynczego logowania (Single Sign-On).

  Przykład pliku odpowiedzi dla instalacji Web Console, która połączy się z Serwerem administracyjnym w wersji 16 lub nowszej. W tym przykładzie Web Console i Serwer administracyjny są zainstalowane na różnych urządzeniach:

```
{
    "address": "ksc-web-console.example.com",
    "port": 8080,
    "defaultLangId": 1049,
    "enableLog": true,
    "trusted":  {
        "Administration Server v16": {
    "iamHost": "ksc16.example.com",
    "iamOAuthPort": 4444,
    "iamProxyPort": 9050,
    "iamCertPath": "/var/opt/kaspersky/klnagent_srv/iam/main_certificate.pem",
    "iamPATPath": "/var/opt/kaspersky/klnagent_srv/iam/initial_token.txt",
    "kscPort": 13299,
    "kscCertPath": "/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer"
        }
    },
    "acceptEula": true,
    "certPath": "/root/server.crt",
    "keyPath": "/root/key-without-passphrase.pem",
    "webConsoleAccount": "Group1:User1",
    "managementServiceAccount": "Group1:User2",
    "serviceWebConsoleAccount": "Group1:User3",
    "pluginAccount": "Group1:User4",
    "natsMessageQueueAccount": "Group1:User6"
}
```

- Serwer administracyjny w wersji 15.4 lub starszej

  Serwer administracyjny w wersji 15.4 lub starszej obsługuje uwierzytelnianie poprzez określenie nazwy i hasła użytkownika wewnętrznego lub użytkownika domeny.

Przykład pliku odpowiedzi do instalacji Web Console, która połączy się z Serwerem administracyjnym w wersji 15.4 lub starszej:

```
{
    "address": "ksc-web-console.example.com",
    "port": 8080,
    "defaultLangId": 1049,
    "enableLog": true,
    "trusted":  {
        "Administration Server v15.4": {
    "kscHost": "ksc.example.com",
    "kscPort": 13299,
    "kscCertPath": "/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer"
        }
    },
    "acceptEula": true,
    "certPath": "/root/server.crt",
    "keyPath": "/root/key-without-passphrase.pem",
    "webConsoleAccount": "Group1:User1",
    "managementServiceAccount": "Group1:User2",
    "serviceWebConsoleAccount": "Group1:User3",
    "pluginAccount": "Group1:User4",
    "natsMessageQueueAccount": "Group1:User6"
}
```

Parametry `webConsoleAccount`, `managementServiceAccount`, `serviceWebConsoleAccount`, `pluginAccount, natsMessageQueueAccount`, `certPath` i `keyPath` są opcjonalne. Można je pominąć w pliku odpowiedzi.

Jeśli chcesz użyć niestandardowego certyfikatu, podaj parametry `certPath` i `keyPath`. Jeśli nie podasz parametrów lub podasz tylko jeden, przeglądarka internetowa będzie stale informować, że połączenie nie jest prywatne.

Ze względów bezpieczeństwa śr nie zalecamy określania parametrów `webConsoleAccount`, `managementServiceAccount`, `serviceWebConsoleAccount`, `pluginAccount` i `natsMessageQueueAccount`.
Jeśli zdecydujesz się określić te parametry, upewnij się, że niestandardowe konta użytkowników należą do tej samej grupy zabezpieczeń. Jeśli te parametry nie zostaną określone, instalator Kaspersky Security Center Web Console utworzy domyślną grupę zabezpieczeń, a następnie utworzy w tej grupie konta użytkowników o domyślnych nazwach.
Parametrów `webConsoleAccount`, `managementServiceAccount`, `serviceWebConsoleAccount`, `pluginAccount` i `natsMessageQueueAccount` nie wolno używać niezależnie od siebie: należy określić wartości wszystkich tych parametrów albo nie określać żadnego z nich.

Możesz zainstalować Kaspersky Security Center Web Console na tym samym urządzeniu, na którym jest zainstalowany Serwer administracyjny, lub na innym. Jeżeli Kaspersky Security Center Web Console jest zainstalowana na innym urządzeniu, adres Kaspersky Security Center Web Console (określony przez `address`) i adres Serwera administracyjnego (określony przez `iamHost` lub `kscHost`) różnią się. Jeśli Kaspersky Security Center Web Console jest zainstalowana na tym samym urządzeniu co Serwer administracyjny, parametry te mają takie same wartości.

Ta wartość `iamHost` musi być zgodna z adresem IAM określonym podczas instalacji Serwera administracyjnego. Aby uzyskać określony adres IAM, uruchom następujące polecenie na hoście Serwera administracyjnego:

```
grep "iam_address:" /var/opt/kaspersky/klnagent_srv/iam/iam_config.yaml
```

Zalecamy określenie numerów portów powyżej 1024. Jeśli chcesz, aby Kaspersky Security Center Web Console działała na portach poniżej 1024, po instalacji musisz uruchomić następujące polecenie:

```
sudo setcap 'cap_net_bind_service=+ep' /var/opt/kaspersky/ksc-web-console/node
```

Jeśli nie masz narzędzia setcap, możesz je zainstalować. **Kliknij ten link, aby wyświetlić polecenia**.

W przypadku systemów operacyjnych Debian i Ubuntu uruchom jedno z następujących poleceń:

- `sudo apt-get install libcap2-bin`
- `sudo apt install libcap2-bin`

W przypadku SUSE Linux Enterprise Server i Red Hat Enterprise Linux uruchom polecenie:

- `sudo zypper install libcap-progs`

Podczas instalacji konsoli Kaspersky Security Center Web Console w systemie operacyjnym Linux ALT, musisz określić numer portu inny niż 8080, ponieważ port 8080 jest używany przez system operacyjny.

Poniższa tabela opisuje parametry, które mogą zostać określone w pliku odpowiedzi.

Parametry instalacji Kaspersky Security Center Web Console na urządzeniach działających pod kontrolą systemu Linux

Parametr	Opis	Dostępne wartości
`address`	Adres urządzenia (FQDN lub nazwa hosta), na którym zainstalowano Kaspersky Security Center Web Console (wymagane). Jeśli instalujesz Kaspersky Security Center Web Console na Kaspersky Security Center Server, użyj adresu, który podałeś podczas instalacji Kaspersky Security Center Linux. Jeśli instalujesz Kaspersky Security Center Web Console na urządzeniu zewnętrznym, określ zewnętrzny adres urządzenia (FQDN lub nazwę hosta), który będzie używany przez przeglądarkę internetową do łączenia się z Kaspersky Security Center Web Console Server.	Wartość wiersza. Przykład: `"ksc.example.com"`
`port`	Port używany przez Kaspersky Security Center Web Console do odbierania połączeń z przeglądarek internetowych (wymagany).	Wartość numeryczna. Zalecana wartość wynosi 8080 (z wyjątkie operacyjnego Linux ALT).
`defaultLangId`	Język interfejsu użytkownika (domyślnie, `1033`). W razie konieczności możesz zmienić język interfejsu Kaspersky Security Center Web Console.	Kod numeryczny języka: • Niemiecki: `1031` • Angielski: `1033` • Hiszpański: `1034` • Hiszpański (Meksyk): `2058` • Francuski: `1036` • włoski: `1040` • Japoński: `1041` • Kazachstański: `1087` • Polski: `1045` • Portugalski (Brazylia): `1046` • Rosyjski: `1049` • Turecki: `1055` • Chiński uproszczony: `2052` • Chiński tradycyjny: `1028` Jeśli nie określono wartości, używany jest (en-US).
`enableLog`	Czy włączyć rejestrowania śledzenia Kaspersky Security Center Web Console? Zalecamy zmianę domyślnej wartości parametru wyłącznie na prośbę specjalisty pomocy technicznej Kaspersky.	Wartość zerojedynkowa: • `true` — Rejestrowanie jest włączone • `false` — Rejestrowanie jest wyłączo domyślnie).

Parametr	Opis	Dostępne wartości

`trusted`	Lista adresów zaufanych Serwerów administracyjnych, z którymi może połączyć się Kaspersky Security Center Web Console. Do listy zaufanych serwerów można dodać wiele Serwerów administracyjnych o różnych wersjach.
	
	Serwer administracyjny w wersji 16 lub nowszej:
	
	• Nazwa Serwera administracyjnego, która jest wyświetlana w oknie logowania.
	• `iamHost` to adres (FQDN lub nazwa hosta) Serwera administracyjnego, który zawiera komponent IAM (począwszy od Kaspersky Security Center Linux wersja 16) i z którym łączy się Kaspersky Security Center Web Console.
	Ta wartość `iamHost` musi być zgodna z adresem IAM określonym podczas instalacji Serwera administracyjnego. Aby uzyskać określony adres IAM, uruchom następujące polecenie na hoście Serwera administracyjnego:
	`grep "iam_address:" /var/opt/kaspersky/klnagent_srv/iam/iam_config.yaml`
	• `iamOAuthPort` to port używany do wymiany tokenów uwierzytelniania przez protokół uwierzytelniania OpenID Connect (wartość domyślna to 4444). Ten port jest używany zarówno do komunikacji między Kaspersky Security Center Web Console Server a Serwerem administracyjnym, jak i między przeglądarką (używaną z Kaspersky Security Center Web Console) a Serwerem administracyjnym.
	• `iamProxyPort` to port, który jest używany przez Kaspersky Security Center Web Console Server do nawiązywania połączenia z Serwerem administracyjnym (domyślnie jest to port 9050).
	• `iamCertPath` to ścieżka do certyfikatu IAM. Certyfikat IAM jest tworzony automatycznie przy pierwszym uruchomieniu Serwera administracyjnego. Plik certyfikatu jest przechowywany na urządzeniu, na którym zainstalowany jest Serwer administracyjny. Domyślna ścieżka do certyfikatu: /var/opt/kaspersky/klnagent_srv/iam/main_certificate.pem. Certyfikat IAM z podpisem własnym jest automatycznie rotowany.
	• `iamPATPath` to ścieżka do tokena używanego do rejestracji Kaspersky Security Center Web Console jako klienta OAuth w IAM. Ten plik jest generowany automatycznie podczas pierwszego uruchomienia Serwera administracyjnego. Plik certyfikatu jest przechowywany na urządzeniu, na którym zainstalowany jest Serwer administracyjny. Domyślna ścieżka do tokena: /var/opt/kaspersky/klnagent_srv/iam/initial_token.txt. Token jest ważny bezterminowo i nie wymaga rotacji.
	• `kscPort` to port używany do łączenia Kaspersky Security Center Web Console z Serwerem administracyjnym przez OpenAPI (domyślna wartość to 13299).
	• `kscCertPath` to ścieżka do certyfikatu Serwera administracyjnego. Plik certyfikatu jest przechowywany na urządzeniu, na którym zainstalowany jest Serwer administracyjny. Domyślna ścieżka do pliku certyfikatu to: /var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer.
		Sekcja pliku JSON w następującym forma
		
		`"trusted": {`
		`"Administration Server v16": {`
		`"iamHost": "ksc-iam.example.com",`
		`"iamOAuthPort": 4444,`
		`"iamProxyPort": 9050,`
		`"iamCertPath": "/var/opt/kaspersky/klnagent_srv/iam/main_c`
		`"iamPATPath": "/var/opt/kaspersky/klnagent_srv/iam/initia`
		`"kscPort": 13299,`
		`"kscCertPath": "/var/opt/kaspersky/klnagent_srv/1093/cert/`
		`},`
		`"Administration Server v15.4": {`
		`"kscHost": "ksc.example.com",`
		`"kscPort": 13299,`
		`"kscCertPath": "/var/opt/kaspersky/klnagent_srv/1093/cert/`
		`}`
		`}`
		
		Możesz określić dowolne nazwy Serwerów administracyjnych zamiast `Administrat` `v16` i `Administration Server v15.4`.

Parametr	Opis	Dostępne wartości
	Serwer administracyjny w wersji 15.4 lub starszej: • Nazwa Serwera administracyjnego, która jest wyświetlana w oknie logowania. • `kscHost` to adres (FQDN lub nazwa hosta) Serwera administracyjnego, z którym łączy się Kaspersky Security Center Web Console. • `kscPort` to port OpenAPI, który jest używany przez Kaspersky Security Center Web Console Server do nawiązywania połączenia z Serwerem administracyjnym (domyślnie jest to port 13299). • `kscCertPath` to ścieżka do certyfikatu Serwera administracyjnego. Plik certyfikatu jest przechowywany na urządzeniu, na którym zainstalowany jest Serwer administracyjny. Domyślna ścieżka do pliku certyfikatu to: /var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer. Podczas instalacji Kaspersky Security Center Web Console na innym urządzeniu niż urządzenie z zainstalowanym Serwerem administracyjnym należy skopiować plik certyfikatu Serwera administracyjnego (określony parametrem `kscCertPath`), plik certyfikatu IAM (określony parametrem `iamCertPath`) oraz plik tokena (określony parametrem `iamPATPath`) z urządzenia z zainstalowanym Serwerem administracyjnym na urządzenie docelowe. Określ ścieżkę lokalną do certyfikatu w pliku odpowiedzi instalatora Web Console.	
`acceptEula`	Czy chcesz zaakceptować warunki Umowy licencyjnej użytkownika końcowego (EULA). Plik zawierający warunki Umowy licencyjnej użytkownika końcowego jest pobierany wraz z plikiem instalacyjnym.	Wartość zerojedynkowa: • `true` — Potwierdzam, że w pełni prze am), rozumiem i akceptuję warunki nir licencyjnej użytkownika końcowego. • `false` — Nie akceptuję postanowień Umowy licencyjnej (wybrana domyśln Jeśli nie zostanie określona żadna wartoś Kaspersky Security Center Web Console Umowę licencyjną użytkownika końcoweg zgadzasz się zaakceptować warunki Umov użytkownika końcowego.
`certDomain`	Jeśli chcesz wygenerować nowy certyfikat z podpisem własnym, użyj tego parametru, aby określić nazwę FQDN służącą do łączenia przeglądarki internetowej z Kaspersky Security Center Web Console.	Wartość wiersza.
`certPath`	Użyj tego parametru, aby określić ścieżkę do niestandardowego certyfikatu Kaspersky Security Center Web Console, który jest zaufany w Twojej infrastrukturze i spełnia wymagania dotyczące niestandardowych certyfikatów. Można określić tylko jeden klucz prywatny (`keyPath`) dla jednego certyfikatu lub łańcucha certyfikatów.	Wartość wiersza. Zaszyfrowane certyfikaty nie są obsługiw Kaspersky Security Center Web Console Na urządzeniu, na którym ma zostać zains Kaspersky Security Center Web Console do pliku certyfikatu w formacie PEM. Przykład: `/root/server.crt`
`keyPath`	Użyj parametru, aby określić ścieżkę do klucza prywatnego skojarzonego z niestandardowym certyfikatem Kaspersky Security Center Web Console określonym w parametrze `certPath`.	Wartość wiersza. Plik z kluczem prywatnym nie może być p szyfrowaniu. Na urządzeniu, na którym ma zostać zains Kaspersky Security Center Web Console do pliku klucza w formacie PEM. Przykład: `/root/key-without-passph`
`webConsoleAccount`	Nazwa konta, z poziomu którego uruchamiana jest usługa Kaspersky Security Center Web Console.	Wartość wiersza w następującym formac `grupy >:< nazwę użytkownika >"`. Przykład: `"Group1:User1"`. Jeśli nie określono żadnej wartości, instala Security Center Web Console utworzy n domyślnej nazwie `user_management_%u`

Parametr	Opis	Dostępne wartości
`managementServiceAccount`	Nazwa konta uprzywilejowanego, z poziomu którego uruchamiana jest Usługa zarządzania Kaspersky Security Center Web Console.	Wartość wiersza w następującym formac `grupy >:< nazwę użytkownika >"`. Przykład: `"Group1:User2"`. Jeśli nie określono żadnej wartości, instala Security Center Web Console utworzy n domyślnej nazwie `user_nodejs_%uid%`.
`serviceWebConsoleAccount`	Nazwa konta, z poziomu którego uruchamiana jest usługa Kaspersky Security Center Web Console.	Wartość wiersza w następującym formac `grupy >:< nazwę użytkownika >"`. Przykład: `"Group1:User3"`. Jeśli nie określono żadnej wartości, instala Security Center Web Console utworzy n domyślnej nazwie `user_svc_nodejs_%u`
`pluginAccount`	Nazwa konta, na którym działa usługa wtyczki produktu Kaspersky Security Center.	Wartość wiersza w następującym formac `grupy >:< nazwę użytkownika >"`. Przykład: `"Group1:User4"`. Jeśli nie określono żadnej wartości, instala Security Center Web Console utworzy n domyślnej nazwie `user_web_plugin_%u`
`natsMessageQueueAccount`	Nazwa konta, z poziomu którego uruchamiana jest usługa Kaspersky Security Center Web Console NATS.	Wartość wiersza w następującym formac `grupy >:< nazwę użytkownika >"`. Przykład: `"Group1:User6"`. Jeśli nie określono żadnej wartości, instala Security Center Web Console utworzy n domyślnej nazwie `user_message_queue`

Instalowanie Kaspersky Security Center Web Console na Astra Linux w trybie zamkniętego środowiska oprogramowania

W tej sekcji opisano sposób instalowania Kaspersky Security Center Web Console Server (zwanego również Kaspersky Security Center Web Console) w systemie operacyjnym Astra Linux Special Edition. Przed instalacją musisz zainstalować system DBMS i Serwerem administracyjnym Kaspersky Security Center Linux.

W celu zainstalowania Kaspersky Security Center Web Console:

1. Upewnij się, że na urządzeniu, na którym chcesz zainstalować Kaspersky Security Center Web Console, działa jedna z obsługiwanych dystrybucji systemu Linux.

2. Przeczytaj Umowę licencyjną Użytkownika Końcowego (EULA). Jeśli pakiet dystrybucyjny Kaspersky Security Center Linux nie zawiera pliku TXT z treścią Umowy licencyjnej użytkownika końcowego, możesz pobrać ten plik ze strony internetowej Kaspersky. Jeśli nie akceptujesz warunków Umowy licencyjnej, nie instaluj aplikacji.

3. Utwórz plik odpowiedzi, który zawiera parametry połączenia Kaspersky Security Center Web Console z Serwerem administracyjnym: `/etc/ksc-web-console-setup.json`.

   Przykład pliku odpowiedzi zawierającego minimalny zestaw parametrów

Zestaw parametrów pliku odpowiedzi zależy od wersji Serwera administracyjnego, z którym łączy się Kaspersky Security Center Web Console:

- Serwer administracyjny w wersji 16 lub nowszej

  Przykład pliku odpowiedzi z minimalnym zestawem parametrów do logowania się do Serwera administracyjnego w wersji 16 lub nowszej:

```
{
    "address": "ksc-web-console.example.com",
    "port": 8080,
    "trusted":  {
        "Administration Server v16": {
            "iamHost": "ksc16.example.com",
            "iamOAuthPort": 4444,
            "iamProxyPort": 9050,
            "iamCertPath": "/var/opt/kaspersky/klnagent_srv/iam/main_certificate.pem",
            "iamPATPath": "/var/opt/kaspersky/klnagent_srv/iam/initial_token.txt",
            "kscPort": 13299,
            "kscCertPath": "/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer"
        }
    },
    "certDomain":"ksc-web-console.example.com",
    "acceptEula": true
}
```

- Serwer administracyjny w wersji 15.4 lub starszej

  Przykład pliku odpowiedzi z minimalnym zestawem parametrów do logowania się do Serwera administracyjnego w wersji 15.4 lub starszej:

```
{
    "address": "ksc-web-console.example.com",
    "port": 8080,
    "trusted":  {
         "Administration Server v15.4": {
             "kscHost": "ksc.example.com",
             "kscPort": 13299,
             "kscCertPath": "/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer"
         }
    },
    "certDomain":"ksc-web-console.example.com",
    "acceptEula": true
}
```

Możesz zainstalować Kaspersky Security Center Web Console na tym samym urządzeniu, na którym jest zainstalowany Serwer administracyjny, lub na innym. Jeżeli Kaspersky Security Center Web Console jest zainstalowana na innym urządzeniu, adres Kaspersky Security Center Web Console (określony przez `address`) i adres Serwera administracyjnego (określony przez `iamHost` lub `kscHost`) różnią się. Jeśli Kaspersky Security Center Web Console jest zainstalowana na tym samym urządzeniu co Serwer administracyjny, parametry te mają takie same wartości.

Wartość `iamHost` musi być zgodna z adresem IAM określonym podczas instalacji Serwera administracyjnego. Aby uzyskać określony adres IAM, uruchom następujące polecenie na urządzeniu z zainstalowanym Serwerem administracyjnym:

```
grep "iam_address:" /var/opt/kaspersky/klnagent_srv/iam/iam_config.yaml
```

Szczegółowe informacje można znaleźć w artykule: Parametry instalacji Kaspersky Security Center Web Console.

Do listy zaufanych serwerów można dodać wiele Serwerów administracyjnych o różnych wersjach. W takim przypadku serwery mogą używać różnych metod uwierzytelniania.

4. Otwórz plik `/etc/digsig/digsig_initramfs.conf` a następnie określ następujące ustawienie:

```
DIGSIG_ELF_MODE=1
```

5. W wierszu polecenia uruchom następujące polecenie, aby zainstalować pakiet zgodności:

```
apt install astra-digsig-oldkeys
```

6. Utwórz katalog dla klucza aplikacji:

```
mkdir -p /etc/digsig/keys/legacy/kaspersky/
```

7. Umieść klucz aplikacji `/opt/kaspersky/ksc64/share/kaspersky_astra_pub_key.gpg` w katalogu utworzonym w poprzednim kroku:

```
cp kaspersky_astra_pub_key.gpg /etc/digsig/keys/legacy/kaspersky/
```

Jeśli pakiet dystrybucyjny Kaspersky Security Center Linux nie zawiera klucza aplikacji kaspersky_astra_pub_key.gpg, możesz go pobrać, klikając łącze: https://media.kaspersky.com/utilities/CorporateUtilities/kaspersky_astra_pub_key.gpg.

8. Zaktualizuj dyski RAM:

```
update-initramfs -u -k all
```

Uruchom ponownie system.

9. Na koncie z uprawnieniami administratora użyj wiersza poleceń, aby uruchomić plik instalacyjny. Plik konfiguracyjny można pobrać ze strony internetowej Kaspersky.

   - W celu zainstalowania lub uaktualnienia Kaspersky Security Center Web Console uruchom następujące polecenie:

     ```
     sudo apt-get install ksc-web-console-<numer_kompilacji>.x86_64.deb
     ```

   - W celu przeprowadzenia aktualizacji z poprzedniej wersji Kaspersky Security Center Web Console, uruchom następujące polecenie:

     ```
     sudo apt-get install ksc-web-console-<numer_kompilacji>.x86_64.deb
     ```

   Rozpocznie się wypakowywanie pliku instalacji. Zaczekaj na zakończenie instalacji. Kaspersky Security Center Web Console jest instalowany w następującym katalogu: `/var/opt/kaspersky/ksc-web-console`.

10. Uruchom ponownie wszystkie usługi Kaspersky Security Center Web Console, uruchamiając następujące polecenie:

```
sudo systemctl restart KSC*
```

Po zakończeniu instalacji możesz użyć przeglądarki internetowej do otwarcia i zalogowania się do Kaspersky Security Center Web Console.

Instalowanie Kaspersky Security Center Linux za pomocą skryptu

Skrypt `ksc_fast_install.py` umożliwia wdrożenie Kaspersky Security Center Linux i przeprowadzenie wstępnej konfiguracji jego komponentów: Serwera administracyjnego i Web Console, w tym systemu DBMS i wymaganych pakietów pomocniczych.

Skrypt odczytuje parametry z pliku parametrów. Używane są wartości domyślne parametrów. W razie potrzeby możesz zmienić wartości.

Jak działa skrypt?

Podczas działania skrypt:

- Sprawdza, czy spełnione są następujące warunki:
  - Masz uprawnienia wymagane do uruchomienia skryptu.
  - Skrypt jest zgodny z systemem operacyjnym i systemem DBMS.
  - Umowy licencyjne użytkownika końcowego i Polityka prywatności zostały zaakceptowane.

    Jeśli nie zaakceptujesz ich w pliku parametrów, po uruchomieniu skryptu pojawi się monit o ich zaakceptowanie.
  - Wymagania sprzętowe dla Serwera administracyjnego i Web Console.

    Wymagania określono w Poradniku dotyczącym rozmiarów.
- Instaluje DBMS (jeśli nie jest jeszcze zainstalowany) i konfiguruje jego parametry
- Tworzy bazy danych Kaspersky Security Center i konfiguruje poświadczenia systemu operacyjnego
- Instaluje Serwer administracyjny i Web Console
- Udostępnia login i hasło umożliwiające zalogowanie się do Web Console.

  Przed zamknięciem terminala wiersza poleceń zapisz poświadczenia w dowolny wygodny sposób. Jeśli utracisz poświadczenia, musisz dodać nowe konto użytkownika, uruchamiając polecenie:
  `` `/opt/kaspersky/ksc64/sbin/kladduser -n <użytkownik>` ``

Jeśli co najmniej jeden warunek nie zostanie spełniony lub wystąpi błąd, działanie skryptu zostanie przerwane i wyświetli się odpowiednie powiadomienie.

Skrypt nie obejmuje działań związanych ze zwiększaniem odporności systemu. Aby zmniejszyć ryzyko naruszenia bezpieczeństwa Kaspersky Security Center, uwzględnij zalecenia zawarte w Przewodniku po zwiększaniu odporności.
Metodę instalacji opartą na skrypcie można stosować do wdrażania Kaspersky Security Center Linux w wersji 16.3 lub nowszej na urządzeniu, na którym nie zainstalowano jeszcze Kaspersky Security Center Linux.
Do uruchomienia skryptu wymagany jest Python 3.6 lub nowszy.

Wdrożenie jest możliwe tylko wtedy, gdy na bieżącym urządzeniu nie zainstalowano Kaspersky Security Center Linux.

Skryptu nie można użyć do uaktualnienia Kaspersky Security Center Linux do nowej wersji ani w przypadku wdrożenia klastra pracy awaryjnej Kaspersky Security Center Linux.

Skrypt `ksc_fast_install.py` obsługuje instalację Kaspersky Security Center Linux w wersjach systemów operacyjnych z systemami DBMS opisanymi w tabeli.

Wersja systemu operacyjnego	DBMS
Ubuntu Server 26.04 LTS	PostgreSQL 18
RED OS 8	PostgreSQL 16
Astra Linux Special Edition RUSB.10015-01 (wersja 1.8.5)	PostgreSQL 15
CentOS Stream 10	PostgreSQL 18

Skrypt nie obsługuje niestandardowego schematu bazy danych.

Jak przeprowadzić wdrożenie za pomocą skryptu?

Wymagania wstępne

Przed uruchomieniem skryptu wykonaj następujące czynności:

- Zaktualizuj system operacyjny, wykonując jedno z poleceń: `dnf update` lub `apt update`
- Uzyskaj uprawnienia superużytkownika, wykonując polecenie: `sudo -i`
- Zezwól na uruchamianie skryptu, wykonując polecenie: `chmod +x ./ksc_fast_install.py`
- Upewnij się, że repozytorium systemu operacyjnego zawiera obsługiwany system DBMS, wykonując polecenie: `sudo apt policy postgresql`

Aby wdrożyć Kaspersky Security Center Linux przez uruchomienie skryptu:

1. Z witryny Kaspersky pobierz następujące elementy:
   - Pakiety dystrybucyjne .deb lub .rpm dla Serwera administracyjnego i Web Console.
   - Archiwum „Skrypt instalacyjny KSC”.

     Podczas korzystania ze skryptu wybierz pakiety dystrybucyjne Serwera administracyjnego i Web Console zgodne z menedżerem pakietów systemu operacyjnego.

Archiwum zawiera następujące pliki:

- Plik skryptu `ksc_fast_install.py`.
- Plik parametrów.

  Domyślna nazwa pliku to `params.txt`. Jeśli chcesz zmienić nazwę pliku, upewnij się, że podczas uruchamiania skryptu w terminalu wiersza poleceń podano nową nazwę za pomocą parametru `--params`.
- Plik z Umową licencyjną użytkownika końcowego i Polityką prywatności dla Serwera administracyjnego.
- Plik z Umową licencyjną użytkownika końcowego dla Kaspersky Security Center Web Console.
- Pliki z sumami skrótów Umów licencyjnych użytkownika końcowego.

2. Umieść wszystkie pobrane pliki w tym samym katalogu lokalnym.
3. W razie potrzeby skonfiguruj plik parametrów.

   Kliknij tutaj, aby wyświetlić przykład pliku parametrów z opisem jego parametrów

```
# Required parameters:

#klfi_server_eula_accepted=N

#klfi_nwc_eula_accepted=N

#klfi_pp_accepted=N

# Optional parameters:

#klfi_klserver_db=KAV

#klfi_klserver_dbuser=klserver

#klfi_klserver_address=

#klfi_kliam_db=KAV_IAM

#klfi_kliam_dbuser=kliam

#klfi_kliam_address=

#klfi_sys_group_kladmin=kladmins

#klfi_sys_user_klserver=klsrvuser

#klfi_sys_user_kliam=kliamuser

#klfi_sys_user_svc=klsvcuser

#klfi_nwc_port=8080

#klfi_display_name=

#klfi_netsize=M
```

Parametry `klfi_server_eula_accepted=N`, `klfi_nwc_eula_accepted=N` i `klfi_pp_accepted=N` są obowiązkowe i zawsze znajdują się w pliku parametrów. Pozostałe parametry są opcjonalne.

Parametry obowiązkowe:

- Jeśli zmienisz wartość domyślną bez odkomentowania wiersza, zostanie wyświetlony monit o zaakceptowanie Umowy licencyjnej użytkownika końcowego i Polityki prywatności.
- Jeśli określisz wartość inną niż `Y` lub `N`, zostanie wyświetlony monit o zaakceptowanie Umowy licencyjnej użytkownika końcowego i Polityki prywatności, niezależnie od tego, czy wiersz został odkomentowany.
- Jeśli odkomentujesz wiersz bez zmiany domyślnej wartości `N`, skrypt nie będzie działać.
- Jeśli odkomentujesz wiersz i ustawisz wartość `Y`, skrypt nie wyświetli monitu.

Parametr i jego wartość domyślna	Opis parametru i inne możliwe wartości (jeśli istnieją)
`klfi_server_eula_accepted=N`	Umowa licencyjna użytkownika końcowego dla Serwera administracyjnego. Możliwe wartości: • `Y` – zaakceptowano Umowę licencyjną użytkownika końcowego. • `N` – nie zaakceptowano Umowy licencyjnej użytkownika końcowego.
`klfi_nwc_eula_accepted=N`	Umowa licencyjna użytkownika końcowego dla Kaspersky Security Center Web Console. Możliwe wartości: • `Y` – zaakceptowano Umowę licencyjną użytkownika końcowego. • `N` – nie zaakceptowano Umowy licencyjnej użytkownika końcowego.
`klfi_pp_accepted=N`	Polityka prywatności. Możliwe wartości: • `Y` – zaakceptowano Politykę prywatności. • `N` – nie zaakceptowano Polityki prywatności.
`klfi_klserver_db=KAV`	Nazwa bazy danych Serwera administracyjnego. Nazwa musi być inna niż nazwa bazy danych IAM określona w parametrze `klfi_kliam_db`.
`klfi_kliam_db=KAV_IAM`	Nazwa bazy danych IAM. Nazwa musi być inna niż nazwa bazy danych Serwera administracyjnego określona w parametrze `klfi_klserver_db`.
`klfi_klserver_dbuser=klserver`	Nazwa użytkownika bazy danych Serwera administracyjnego.
`klfi_kliam_dbuser=kliam`	Nazwa użytkownika bazy danych IAM.
`klfi_klserver_address=FQDN`	Nazwa FQDN Serwera administracyjnego lub nazwa bieżącego urządzenia. Jeśli wartość parametru nie zostanie określona, skrypt automatycznie określi FQDN lub nazwę urządzenia, na którym uruchamiany jest skrypt. Jeśli skrypt nie zdoła określić tych wartości, instalacja zakończy się błędem.
`klfi_kliam_address=FQDN`	Nazwa FQDN serwera IAM lub nazwa bieżącego urządzenia. Jeśli wartość parametru nie zostanie określona, skrypt automatycznie określi FQDN lub nazwę urządzenia, na którym uruchamiany jest skrypt. Jeśli skrypt nie zdoła określić tych wartości, instalacja zakończy się błędem.
`klfi_sys_group_kladmin=kladmins`	Wprowadź nazwę grupy zabezpieczeń dla usług.
`klfi_sys_user_klserver=klsrvuser`	Nazwa konta do uruchomienia usługi Serwera administracyjnego.
`klfi_sys_user_kliam=kliamuser`	Nazwa konta do uruchomienia usługi IAM.
`klfi_sys_user_svc=klsvcuser`	Nazwa konta do uruchomienia innych usług.
`klfi_nwc_port=8080`	Port do połączenia z Kaspersky Security Center Web Console.
`klfi_display_name=FQDN`	Nazwa Serwera administracyjnego, która jest wyświetlana w oknie logowania.

`klfi_netsize=M`	Oceń przybliżoną liczbę urządzeń, którymi zamierzasz zarządzać.
	Każde oszacowanie uwzględnia zasoby wymagane do uruchomienia aplikacji firmy Kaspersky. Obliczenia obejmują jednoczesne działanie Serwera administracyjnego, Agenta sieciowego, Kaspersky Security Center Web Console oraz Kaspersky Endpoint Security for Linux na jednym urządzeniu.
	
	Miejsce na kopie zapasowe Serwera administracyjnego nie zostało uwzględnione w tych obliczeniach. Użyj zewnętrznego zasobu plikowego jako punktu montowania, aby przechowywać kopie zapasowe na oddzielnym urządzeniu, lub zwiększ ilość dostępnego miejsca na dysku, uwzględniając miejsce potrzebne na kopie zapasowe.
	
	Śr zalecamy zapewnienie dodatkowych 4–6 GB pamięci RAM i 20 GB wolnego miejsca na dysku na potrzeby instalacji systemu operacyjnego.
	
	Szacunkowe wymagania dotyczące zasobów sprzętowych w zależności od rozmiaru sieci:
	• `S` – od 1 do 1000 zarządzanych urządzeń.
	  • Procesor – 8 rdzeni
	  • Pamięć RAM – 16 GB
	  • Dostępne miejsce na dysku dla katalogu `/var` – 70 GB, co najmniej 300 IOPS
	• `M` – od 1001 do 10000 zarządzanych urządzeń.
	  • Procesor – 12 rdzeni
	  • Pamięć RAM – 24 GB
	  • Dostępne miejsce na dysku dla katalogu `/var` – 340 GB, co najmniej 300 IOPS
	• `L` – od 10001 do 30000 zarządzanych urządzeń.
	  • Procesor – 20 rdzeni
	  • Pamięć RAM – 40 GB
	  • Dostępne miejsce na dysku dla katalogu `/var` – 490 GB, co najmniej 300 IOPS
	• `XL` – od 30001 do 50000 zarządzanych urządzeń.
	  • Procesor – 28 rdzeni
	  • Pamięć RAM – 54 GB
	  • Dostępne miejsce na dysku dla katalogu `/var` – 640 GB, co najmniej 300 IOPS

Wiersze pliku parametrów są zakomentowane. Jeśli chcesz skonfigurować wartości, usuń symbol # na początku wiersza, który chcesz odkomentować.

Parametry `klfi_server_eula_accepted`, `klfi_nwc_eula_accepted` i `klfi_pp_accepted` są obowiązkowe, a ich wartość domyślna to `N`. Jeśli uruchomisz skrypt bez zmiany tych wartości w pliku parametrów, zostanie wyświetlony monit o zaakceptowanie Umowy licencyjnej użytkownika końcowego i Polityki prywatności.

4. Uruchom skrypt.

Po wykonaniu skryptu zostanie wyświetlone powiadomienie o pomyślnym wdrożeniu komponentów Kaspersky Security Center Linux, a także login i hasło umożliwiające zalogowanie się do Web Console.

Jeśli warunki instalacji przy użyciu skryptu nie zostaną spełnione, w pliku parametrów zostaną określone nieznane parametry lub parametr zostanie powtórzony wiele razy, skrypt zwróci błąd i zostanie wyświetlone odpowiednie powiadomienie.

Jeśli podczas etapu wykrywania zasobów skrypt błędnie wykryje niewystarczającą ilość pamięci RAM, wyłącz dynamiczne użycie pamięci RAM na czas instalacji.

Jeśli podczas instalacji komponentów Kaspersky Security Center Linux lub systemu DBMS wystąpi błąd, skrypt wycofuje zmiany, a następnie kończy działanie.

Wycofanie nieudanej instalacji

Jeśli podczas instalacji komponentów Kaspersky Security Center Linux lub systemu DBMS wystąpi błąd, skrypt automatycznie wykona wycofanie zmian. Komponent lub system DBMS zainstalowany przed wystąpieniem błędu zostanie usunięty.

Uaktualnienie pakietów systemu operacyjnego i instalacja pakietów pomocniczych nie są wycofywane.

Jeśli ręcznie przerwiesz działanie skryptu, pomyślnie ukończone kroki nie zostaną wycofane. W razie potrzeby możesz ponownie uruchomić skrypt, a instalacja zostanie wznowiona od kroku, w którym została przerwana.

Aby wznowić instalację, uruchom skrypt w terminalu wiersza poleceń z parametrem `rollback`: `python3 ksc_fast_install.py rollback`

Wdrażanie klastra trybu failover Kaspersky Security Center Linux

Klaster trybu failover Kaspersky Security Center Linux zapewnia wysoką dostępność Kaspersky Security Center Linux i minimalizuje czas przestoju Serwera administracyjnego w przypadku awarii. Klaster trybu failover opiera się na dwóch identycznych instancjach Kaspersky Security Center Linux, zainstalowanych na dwóch komputerach. Jedna z instancji pracuje jako węzeł aktywny, a druga jako węzeł pasywny. Węzeł aktywny zarządza ochroną urządzeń klienckich, natomiast węzeł pasywny jest przygotowany do przejęcia wszystkich funkcji węzła aktywnego w przypadku awarii węzła aktywnego. Gdy wystąpi awaria, węzeł pasywny staje się aktywny, a węzeł aktywny staje się pasywny.

Klaster trybu failover Kaspersky Security Center Linux obsługuje dwie konfiguracje:

- Klaster trybu failover, którego węzły znajdują się w jednym centrum danych.
- Geograficznie rozproszony klaster trybu failover, którego węzły znajdują się w różnych centrach danych.

W klastrze pracy awaryjnej Kaspersky Security Center Linux, wszystkie usługi Kaspersky Security Center Linux są zarządzane automatycznie. Nie próbuj ponownie uruchamiać usług ręcznie.

Użyj funkcji syslog w celu rozwiązywania problemów.

Warunki przełączenia

Klaster trybu failover przełącza zarządzanie ochroną urządzeń klienckich z węzła aktywnego na pasywny, jeśli na węźle aktywnym wystąpi dowolne z następujących zdarzeń:

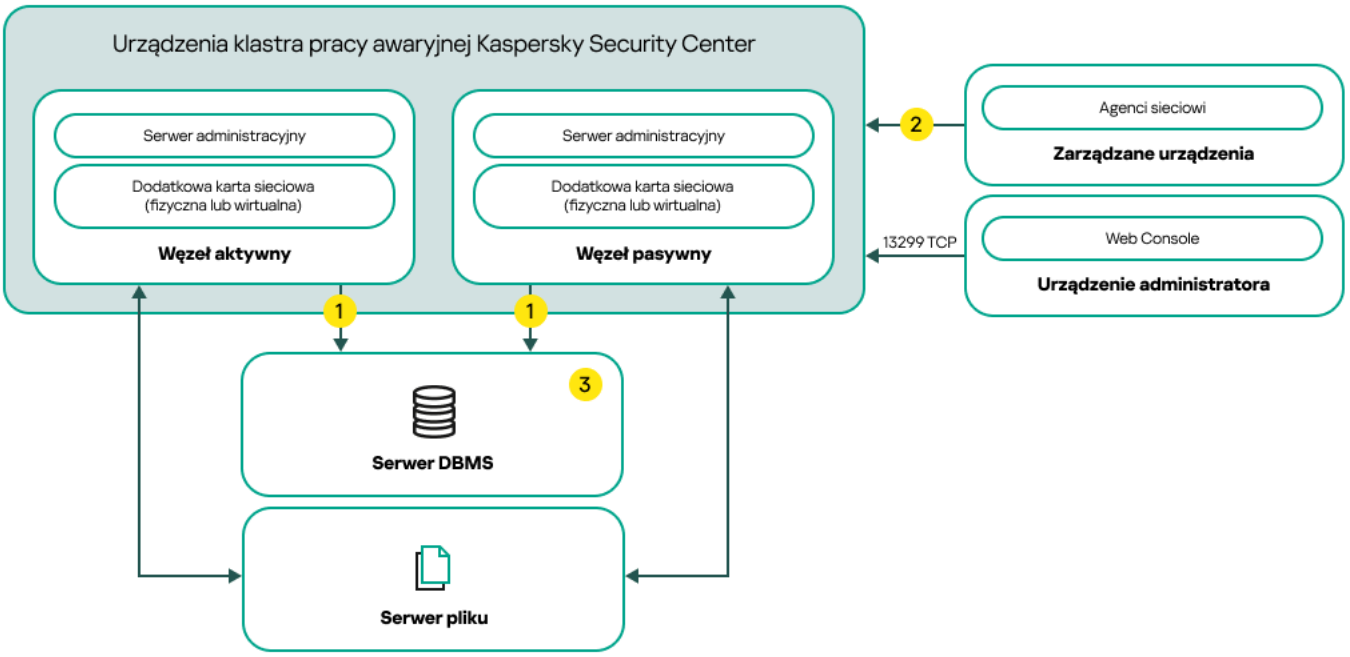
- Węzeł aktywny jest uszkodzony z powodu awarii oprogramowania lub sprzętu.
- Węzeł aktywny został tymczasowo zatrzymany na działania konserwacyjne.
- Przynajmniej jedna z usług (lub procesów) Kaspersky Security Center Linux uległa awarii lub została przypadkowo zamknięta przez użytkownika. Usługi Kaspersky Security Center Linux to: klnagent_klfoc, kladminserver_klfoc, klactprx_klfoc, klwebsrv_klfoc.
- Połączenie sieciowe między aktywnym węzłem a magazynem na serwerze plików zostało przerwane lub zakończone (dotyczy tylko klastra znajdującego się w jednym centrum danych).

Klaster pracy awaryjnej Kaspersky Security Center Linux. Schematy wdrażania

Możesz wybrać jeden z następujących schematów wdrożenia klastra trybu failover Kaspersky Security Center Linux:

- Klaster trybu failover Kaspersky Security Center Linux wdrożony w jednym centrum danych:
  - Schemat wykorzystujący dodatkową kartę sieciową i system DBMS zainstalowany na dedykowanym urządzeniu.
  - Schemat wykorzystujący zewnętrzny moduł równoważenia obciążenia i system DBMS zainstalowany na dedykowanym urządzeniu.
- Geograficznie rozproszony klaster trybu failover Kaspersky Security Center Linux wdrożony w wielu centrach danych.

Schemat wykorzystujący dodatkową kartę sieciową i system DBMS zainstalowany na dedykowanym urządzeniu



Schemat wykorzystujący dodatkową kartę sieciową i system DBMS zainstalowany na dedykowanym urządzeniu

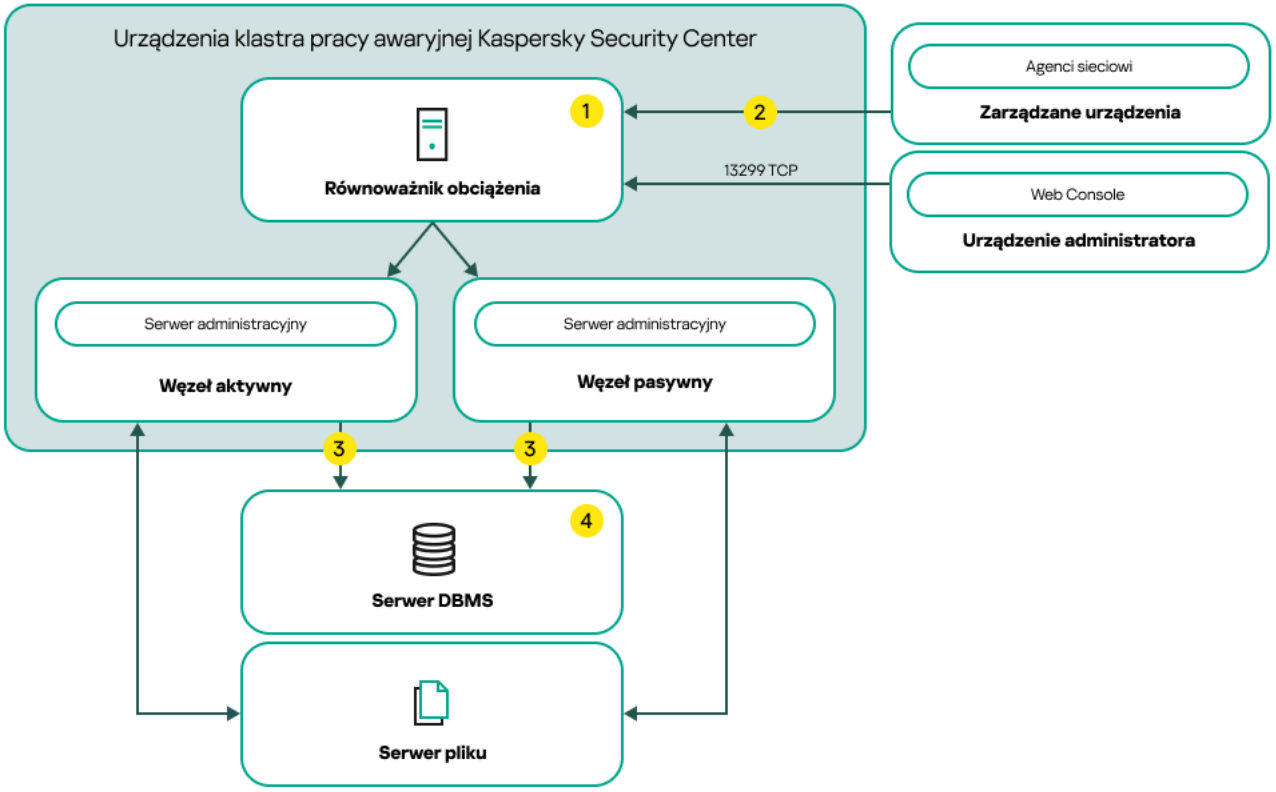
Legenda schematu:

1 Serwer administracyjny wysyła dane do bazy danych. Otwórz odpowiednie porty na urządzeniu, na którym znajduje się baza danych, na przykład port 3306 dla serwera MySQL lub port 5432 dla PostgreSQL lub Postgres Pro. Odpowiednie informacje można znaleźć w dokumentacji do DBMS.

2 Aby połączyć się z zarządzanymi urządzeniami, na urządzeniach z Serwerem administracyjnym otwórz następujące porty: TCP 13000, UDP 13000 i TCP 17000.

3 Urządzenie z systemem zarządzania bazami danych (DBMS). Jeśli używasz MariaBD Galera Cluster jako DBMS, dedykowane urządzenie do tego celu nie jest wymagane. Zainstaluj klaster MariaDB Galera Cluster na każdym z węzłów.

Schemat wykorzystujący zewnętrzny moduł równoważenia obciążenia i system DBMS zainstalowany na dedykowanym urządzeniu



Schemat wykorzystujący zewnętrzny moduł równoważenia obciążenia i system DBMS zainstalowany na dedykowanym urządzeniu

Legenda schematu:

1 Na serwerze równoważenia obciążenia otwórz wszystkie porty Serwera administracyjnego: TCP 13000, UDP 13000, TCP 13299 i TCP 17000.

> Jeśli chcesz wykorzystać narzędzie klakaut do automatyzacji, musisz także otworzyć port TCP 13291.

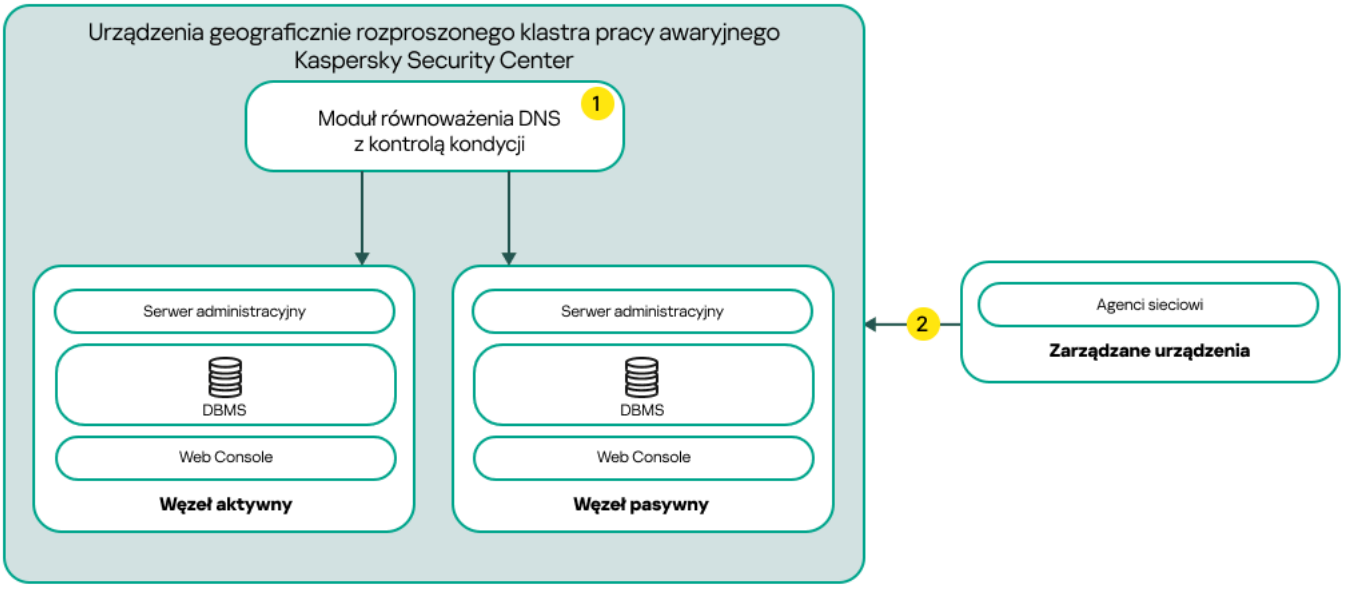
2 Aby połączyć się z zarządzanymi urządzeniami, na urządzeniach z Serwerem administracyjnym otwórz następujące porty: TCP 13000, UDP 13000 i TCP 17000.

3 Serwer administracyjny wysyła dane do bazy danych. Otwórz odpowiednie porty na urządzeniu, na którym znajduje się baza danych, na przykład port 3306 dla serwera MySQL lub port 5432 dla PostgreSQL lub Postgres Pro. Odpowiednie informacje można znaleźć w dokumentacji do DBMS.

4 Urządzenie z systemem zarządzania bazami danych (DBMS). Jeśli używasz MariaBD Galera Cluster jako DBMS, dedykowane urządzenie do tego celu nie jest wymagane. Zainstaluj klaster MariaDB Galera Cluster na każdym z węzłów.

Geograficznie rozproszony klaster trybu failover Kaspersky Security Center Linux

Ten schemat wdrożenia pozwala zapewnić wysoką dostępność wszystkich komponentów. W tym schemacie Serwer Administracyjny, system DBMS i Kaspersky Security Center Web Console są zainstalowane na obu węzłach klastra.



Schemat wdrażania geograficznie rozproszonego klastra trybu failover Kaspersky Security Center Linux

1 Moduł równoważenia DNS z kontrolą kondycji musi zostać wdrożony po Twojej stronie przed instalacją geograficznie rozproszonego klastra trybu failover Kaspersky Security Center Linux.

Moduł równoważenia obciążenia DNS okresowo sprawdza stan węzłów klastra. Podczas uzyskiwania ułatwień dostępu do klastra za pomocą nazwy domeny DNS moduł równoważenia obciążenia DNS zawsze zwraca adres IP aktywnego węzła.

2 Aby połączyć się z zarządzanymi urządzeniami, na urządzeniach z Serwerem administracyjnym otwórz następujące porty: TCP 13000, UDP 13000 i TCP 17000.

Klaster pracy awaryjnej Kaspersky Security Center Linux

W tej sekcji znajdują się ogólne informacje o klastrze trybu failover Kaspersky Security Center Linux wdrożonym w pojedynczym centrum danych, a także instrukcje dotyczące przygotowania i wdrożenia klastra trybu failover Kaspersky Security Center Linux w Twojej sieci.

Scenariusz: Wdrażanie klastra trybu failover Kaspersky Security Center Linux

Klaster trybu failover Kaspersky Security Center Linux zapewnia wysoką dostępność Kaspersky Security Center Linux i minimalizuje czas przestoju Serwera administracyjnego w przypadku awarii. Klaster trybu failover opiera się na dwóch identycznych instancjach Kaspersky Security Center Linux, zainstalowanych na dwóch komputerach. Jedna z instancji pracuje jako węzeł aktywny, a druga jako węzeł pasywny. Węzeł aktywny zarządza ochroną urządzeń klienckich, natomiast węzeł pasywny jest przygotowany do przejęcia wszystkich funkcji węzła aktywnego w przypadku awarii węzła aktywnego. Gdy wystąpi awaria, węzeł pasywny staje się aktywny, a węzeł aktywny staje się pasywny.

Wdrożenie aplikacji firmy Kaspersky odbywa się w krokach:

> Zaleca się przestrzeganie kolejności etapów opisanych w tym scenariuszu.

1. **Sprawdzanie wymagań sprzętowych**

   Upewnij się, że posiadasz sprzęt spełniający wymagania dla klastra trybu failover.

2. **Wybór schematu wdrażania**

   Wybierz schemat wdrażania. Ma to wpływ na kolejne etapy wdrażania.

3. **Przygotowanie kont użytkownika dla usług Kaspersky Security Center Linux**

   Wykonaj następujące czynności na węźle aktywnym, węźle pasywnym i serwerze plików:

   1. Utwórz grupę `kladmins`. Uruchom następujące polecenia:

      `sudo groupadd kladmins`

      `sudo groupmod -g <nowy_GID> kladmins`

      Upewnij się, że grupa ma ten sam GID na wszystkich trzech urządzeniach. Uruchom następujące polecenie:

      `getent group kladmins`

      Jeśli GID nie pasuje, możesz użyć następującego polecenia, aby określić GID:

      `sudo groupmod -g <nowy_GID> kladmins`

   2. Utwórz konto użytkownika `ksc`. Przypisz konta użytkowników do grupy `kladmins`. Uruchom następujące polecenia:

      `sudo adduser ksc`

      `sudo usermod -u <nowy_UID> ksc`

      `sudo gpasswd -a ksc kladmins`

      `sudo usermod -g kladmins ksc`

      Upewnij się, że konto użytkownika ma ten sam UID na wszystkich trzech urządzeniach. Uruchom następujące polecenie:

      `getent passwd ksc`

      Jeśli UID nie pasuje, możesz użyć następującego polecenia, aby określić UID:

      `sudo usermod -u <nowy_UID> ksc`

3. Utwórz konto użytkownika `rightless`. Przypisz konta użytkowników do grupy `kladmins`. Uruchom następujące polecenia:

   `sudo adduser rightless`

   `sudo usermod -u <nowy_UID> rightless`

   `sudo gpasswd -a rightless kladmins`

   `sudo usermod -g kladmins rightless`

   Upewnij się, że konto użytkownika ma ten sam UID na wszystkich trzech urządzeniach. Uruchom następujące polecenie:

   `getent passwd rightless`

   Jeśli UID nie pasuje, możesz użyć następującego polecenia, aby określić UID:

   `sudo usermod -u <nowy_UID> rightless`

4. Utwórz konto użytkownika `ksciam`. Przypisz konta użytkowników do grupy `kladmins`. Uruchom następujące polecenia:

   `sudo adduser ksciam`

   `sudo usermod -u <nowy_UID> ksciam`

   `sudo gpasswd -a ksciam kladmins`

   `sudo usermod -g kladmins ksciam`

   Upewnij się, że konto użytkownika ma ten sam UID na wszystkich trzech urządzeniach. Uruchom następujące polecenie:

   `getent passwd ksciam`

   Jeśli UID nie pasuje, możesz użyć następującego polecenia, aby określić UID:

   `sudo usermod -u <nowy_UID> ksciam`

5. W razie potrzeby zwiększ domyślny limit plików, które można otworzyć (deskryptory plików) dla kont używanych w ramach usług Kaspersky Security Center Linux. Aby to zrobić, otwórz plik /etc/security/limits.conf i określ miękkie i twarde ograniczenia deskryptorów plików w następujący sposób:

   `ksc soft nofile <maksymalna_liczba_otwartych_plików>`

   `ksc hard nofile <maksymalna_liczba_otwartych_plików>`

   Domyślnie limity deskryptorów plików są określane podczas instalacji. Miękki limit plików wynosi 32 768 plików, twardy limit plików wynosi 131 072 plików.

4 Przygotowanie serwera plików

Przygotuj serwer plików do pracy jako komponent klastra trybu failover Kaspersky Security Center Linux. Upewnij się, że serwer plików spełnia wymagania sprzętowe i programowe, utwórz dwa foldery współdzielone dla danych Kaspersky Security Center Linux i skonfiguruj uprawnienia dostępu do folderów współdzielonych.

Instrukcje: Przygotowanie serwera plików dla klastra trybu failover Kaspersky Security Center Linux

5 Instalacja systemu DBMS

Skonfiguruj system DBMS do pracy z Kaspersky Security Center Linux. Możesz wybrać dowolny obsługiwany system DBMS. Informacje o sposobie zainstalowania wybranego systemu DBMS znajdziesz w tym dokumencie.

Jeśli dystrybucja Twojego systemu operacyjnego opartego na systemie Linux nie zawiera obsługiwanego systemu DBMS, możesz zainstalować system DBMS z repozytorium pakietów firmy trzeciej.

Po zainstalowaniu systemu DBMS postępuj zgodnie z odpowiednimi instrukcjami:

- Konfigurowanie serwera PostgreSQL lub Postgres Pro do pracy z Kaspersky Security Center Linux
- Konfigurowanie serwera MariaDB x64 do pracy z Kaspersky Security Center Linux

Ręcznie utwórz pustą bazę danych dla IAM. Serwer administracyjny nie usuwa bazy danych automatycznie podczas odinstalowywania lub przenoszenia serwera na inne urządzenie, należy usunąć bazę danych ręcznie.

- W przypadku PostgreSQL uruchom następujące polecenie:

  `sudo -i -u postgres psql -U postgres -c "CREATE DATABASE <iam_db_name>;"`

- W przypadku MariaDB uruchom następujące polecenie:

  `sudo mysql -u root -p -e "CREATE DATABASE <iam_db_name>;"`

Na urządzeniu z zainstalowanym systemem DBMS skonfiguruj połączenie z urządzeniami, które będą działać jako węzły aktywne i pasywne.

6. **Przygotowanie węzłów aktywnych i pasywnych**

   Przygotuj dwa urządzenia z identycznym sprzętem i oprogramowaniem do pracy jako węzły aktywne i pasywne.

   Instrukcje: Przygotowywanie węzłów dla klastra trybu failover Kaspersky Security Center Linux

7. **Instalacja Kaspersky Security Center Linux**

   Zainstaluj Kaspersky Security Center Linux w klastrze trybu failover na obu węzłach.

   Najpierw musisz zainstalować Kaspersky Security Center Linux na urządzeniu, które ma być pełnić funkcję węzła aktywnego, a następnie zainstalować go na węźle pasywnym.

   Instrukcje: Instalowanie Kaspersky Security Center Linux na węzłach klastra trybu failover Kaspersky Security Center Linux

8. **Instalacja Kaspersky Security Center Web Console**

   Zainstaluj Kaspersky Security Center Web Console na oddzielnym urządzeniu, które nie jest węzłem klastra.

   Określ klaster trybu failover jako adres Serwera administracyjnego w pliku odpowiedzi.

   Certyfikat Serwera administracyjnego znajduje się w następującej ścieżce: /mnt/KlFocDataShare_klfoc/1093/cert/klserver.cer

   Skopiuj plik certyfikatu na urządzenie, na którym instalowana jest Kaspersky Security Center Web Console. Określ ścieżkę lokalną do certyfikatu w pliku odpowiedzi.

9. **Testowanie klastra trybu failover**

   Sprawdź, czy poprawnie skonfigurowano klaster trybu failover i czy działa poprawnie. Na przykład, możesz uruchomić następujące polecenie, aby zainicjować przełączenie na węzeł pasywny:

   `/opt/kaspersky/ksc64/sbin/klfoc -failover --stp klfoc`

   Użyj poniższego polecenia, aby sprawdzić, czy usługa zarządzania klastrem trybu failover jest `Active: active (running)` na obu węzłach:

   `systemctl status klfocsvc_klfoc`

Użyj poniższych poleceń, aby sprawdzić, czy inne usługi klastra trybu failover są `Active: active (running)` na węźle aktywnym. Na węźle pasywnym te usługi klastra trybu failover muszą być `Active: inactive (dead)` lub `Active: failed (Result: signal)`.

- `systemctl status klnagent_klfoc`
- `systemctl status kladminserver_klfoc`
- `systemctl status klactprx_klfoc`
- `systemctl status klwebsrv_klfoc`

Wdrożony zostaje klaster trybu failover Kaspersky Security Center Linux.

Klaster pracy awaryjnej Kaspersky Security Center Linux. Wymagania sprzętowe i programowe

Zalecamy zainstalowanie Kaspersky Endpoint Security for Linux na węzłach aktywnym i pasywnym, na urządzeniu z systemem DBMS oraz na serwerze plików. W przypadku instalacji jednoczesnej klastra pracy awaryjnej Kaspersky Security Center Linux i Kaspersky Endpoint Security for Linux należy zwiększyć wymagania dotyczące węzłów i serwera plików o 1,5 GB pamięci RAM oraz 15% zasobów procesora, a także zapewnić minimum 300 IOPS.

W celu zainstalowania klastra trybu failover Kaspersky Security Center Linux musisz mieć następujący sprzęt:

- Dwa urządzenia z identycznym sprzętem i oprogramowaniem. Te urządzenia będą działać jako węzły aktywne i pasywne.

  Minimalna konfiguracja węzłów aktywnych i pasywnych

Sprzęt	Wartość
Procesor	2 rdzenie, 2500 MHz
Pamięć RAM	6 GB
Przestrzeń dyskowa	10 GB, 150 IOPS lub więcej
Kontroler interfejsu sieciowego	1 Gb/s

- Serwer plików obsługujący protokół CIFS/SMB w wersji 2.0 lub nowszej. Musisz zapewnić dedykowane urządzenie, które będzie działać jako serwer plików.

  Konfiguracja serwera plików

Sprzęt	Wartość
Procesor	16 rdzeni, 2500 MHz
Pamięć RAM	32 GB
Przestrzeń dyskowa	500 GB, 500 IOPS lub więcej
Kontroler interfejsu sieciowego	10 Gb/s

  Upewnij się, że zapewniłeś wysoką przepustowość sieci między serwerem plików a aktywnymi i pasywnymi węzłami.

- Urządzenie z systemem zarządzania bazami danych (DBMS). Jeśli używasz MariaBD Galera Cluster jako DBMS, dedykowane urządzenie do tego celu nie jest wymagane.

Przygotowywanie serwera plików dla klastra trybu failover Kaspersky Security Center Linux

Serwer plików działa jako wymagany składnik klastra trybu failover Kaspersky Security Center Linux.

W celu przygotowania serwera plików:

1. Upewnij się, że serwer plików spełnia wymagania sprzętowe i programowe.

2. Zainstaluj i skonfiguruj serwer NFS:

   - Dostęp do serwera plików musi być włączony dla obu węzłów w ustawieniach serwera NFS.

   - Protokół NFS musi mieć wersję 4.0 lub 4.1.

   - Minimalne wymagania dla jądra Linux:

     - 3.19.0-25, jeśli używasz NFS 4.0

     - 4.4.0-176, jeśli używasz NFS 4.1

   W zależności od dystrybucji systemu Linux zainstaluj pakiet nfs-utils lub pakiet nfs-kernel-server, uruchamiając odpowiednie polecenie:

   ```
   sudo yum install nfs-utils
   sudo apt install nfs-kernel-server
   ```

3. Na serwerze plików utwórz dwa foldery i udostępnij je przy użyciu systemu plików NFS. Jeden z nich służy do przechowywania informacji o klastrze trybu failover. Drugi służy do przechowywania danych i ustawień Kaspersky Security Center Linux. Ścieżki do folderów współdzielonych określisz podczas konfigurowania instalacji Kaspersky Security Center Linux.

   Upewnij się, że poniższe foldery nie istnieją:

   - `/mnt/KlFocStateShare`

   - `/mnt/KlFocDataShare_klfoc`

   Jeśli któryś z tych folderów istnieje, usuń go rekursywnie.

   Uruchom następujące polecenia:

   ```
   sudo mkdir -p /mnt/KlFocStateShare
   sudo mkdir -p /mnt/KlFocDataShare_klfoc
   sudo chown ksc:kladmins /mnt/KlFocStateShare
   sudo chown ksc:kladmins /mnt/KlFocDataShare_klfoc
   sudo chmod -R 770 /mnt/KlFocStateShare /mnt/KlFocDataShare_klfoc
   sudo sh -c "echo /mnt/KlFocStateShare *\(rw,sync,no_subtree_check,no_root_squash\) >>
   /etc/exports"
   sudo sh -c "echo /mnt/KlFocDataShare_klfoc *\
   (rw,sync,no_subtree_check,no_root_squash\) >> /etc/exports"
   sudo exportfs -a
   sudo systemctl start rpcbind
   sudo systemctl start nfs-server
   ```

Włącz autostart, uruchamiając następujące polecenie:

```
sudo systemctl enable rpcbind
```

Możesz określić niestandardowe foldery, ale zalecamy korzystanie z sugerowanych nazw folderów dla wygody podczas korzystania z Pomocy online.

4. Uruchom ponownie serwer plików.

Serwer plików jest przygotowany. Aby zainstalować klaster trybu failover Kaspersky Security Center Linux, postępuj zgodnie z dalszymi instrukcjami w tym scenariuszu.

Przygotowywanie węzłów dla klastra trybu failover Kaspersky Security Center Linux

Przed kontynuowaniem upewnij się, że wykonałeś poprzednie kroki w Scenariuszu: Wdrażanie klastra trybu failover Kaspersky.

Przygotuj dwa urządzenia do pracy jako węzły aktywne i pasywne dla klastra pracy awaryjnej Kaspersky Security Center Linux.

Konfiguracja wspólnych folderów

Aby skonfigurować wspólne foldery:

1. W zależności od dystrybucji systemu Linux zainstaluj pakiet nfs-utils lub pakiet nfs-kernel-server na każdym węźle, uruchamiając odpowiednie polecenie:

   ```
   yum install nfs-utils
   ```

   ```
   apt install nfs-kernel-server
   ```

2. Utwórz punkty montowania, uruchamiając następujące polecenia:

   ```
   mkdir -p /mnt/KlFocStateShare
   ```

   ```
   mkdir -p /mnt/KlFocDataShare_klfoc
   ```

3. Dopasuj punkty montowania i foldery współdzielone:

   ```
   sudo sh -c "echo <serwer plików>:/mnt/KlFocStateShare /mnt/KlFocStateShare nfs vers=4,soft,timeo=50,retrans=2,auto,user,rw 0 0 >> /etc/fstab"
   ```

   ```
   sudo sh -c "echo <serwer plików>:/mnt/KlFocDataShare_klfoc /mnt/KlFocDataShare_klfoc nfs vers=4,noauto,user,rw,exec 0 0 >> /etc/fstab"
   ```

   Tutaj `{serwer plików}` jest nazwą FQDN serwera plików z folderami współdzielonymi.

4. Zamontuj foldery współdzielone, uruchamiając następujące polecenia:

   ```
   mount /mnt/KlFocStateShare
   ```

   ```
   mount /mnt/KlFocDataShare_klfoc
   ```

5. Upewnij się, że uprawnienia dostępu do folderów udostępnionych należą do ksc:kladmins.

   Uruchom następujące polecenie:

   ```
   ls -la /mnt/
   ```

Konfiguracja kart sieciowych

Dodatkowa karta sieciowa może być fizyczna lub wirtualna. Jeśli wybrałeś schemat wdrażania z dodatkową kartą sieciową, wykonaj odpowiednią procedurę na obu węzłach:

- Użyj wirtualnej dodatkowej karty sieciowej opartej na fizycznej karcie sieciowej (technologia MACVLAN):

  1. Zainstaluj pakiet iputils-arping. W zależności od dystrybucji Linux uruchom jedno z następujących poleceń:

     - `yum install iputils`

     lub

     - `apt install iputils-arping`

  2. Aby upewnić się, że NetworkManager jest używany do zarządzania fizyczną kartą sieciową, uruchom następujące polecenie:

     `nmcli device status`

     Jeśli dane wyjściowe polecenia pokazują, że fizyczna karta sieciowa nie jest zarządzana, skonfiguruj NetworkManager do zarządzania fizyczną kartą sieciową. Dokładne kroki konfiguracji zależą od Twojej dystrybucji systemu Linux.

  3. Aby zidentyfikować interfejsy, należy użyć następującego polecenia:

     `ip a`

  4. Aby utworzyć profil konfiguracyjny, uruchom następujące polecenie:

     `nmcli connection add type macvlan dev <interfejs fizyczny> mode bridge ifname <interfejs wirtualny> ipv4.addresses <maska adresu> ipv4.method manual autoconnect no`

- Użyj fizycznej dodatkowej karty sieciowej lub utwórz wirtualne urządzenie TAP za pomocą hiperwizora. W tym scenariuszu wyłącz oprogramowanie NetworkManager.

  1. Podłącz dodatkową kartę sieciową do węzła.

  2. Zainstaluj pakiet iputils-arping. W zależności od dystrybucji Linux uruchom jedno z następujących poleceń:

     - `yum install iputils`

     lub

     - `apt install iputils-arping`

  3. Aby usunąć połączenie NetworkManager dla interfejsu docelowego, uruchom następujące polecenie:

     `nmcli con del <nazwa połączenia>`

     Aby sprawdzić połączenia z interfejsem docelowym, uruchom następujące polecenie:

     `nmcli con show`

  4. Edytuj plik NetworkManager.conf. Znajdź sekcję pliku klucza i przypisz interfejs docelowy do parametru `unmanaged-devices`:

     `[keyfile]`

     `unmanaged-devices=interface-name:<nazwa interfejsu>`

5. Uruchom ponownie NetworkManager:

   `systemctl reload NetworkManager`

   Aby upewnić się, że interfejs docelowy nie jest już zarządzany, uruchom następujące polecenie:

   `nmcli dev status`

Konfiguracja modułu równoważenia obciążenia

Jeśli wybrano schemat wdrożenia z modułem równoważenia obciążenia, postępuj zgodnie z poniższymi instrukcjami, aby go skonfigurować.

Aby skonfigurować moduł równoważenia obciążenia:

1. Przygotuj dedykowane urządzenie z systemem Linux z zainstalowanym serwerem nginx lub innym modułem równoważenia obciążenia.

2. Skonfiguruj moduł równoważenia obciążenia. Ustaw węzeł aktywny jako serwer główny, a węzeł pasywny jako serwer zapasowy.

3. Na serwerze nginx otwórz wszystkie porty Serwera administracyjnego zgodnie z następującym artykułem: Porty używane przez Kaspersky Security Center Linux.

Aby zainstalować klaster trybu failover Kaspersky Security Center Linux, postępuj zgodnie z dalszymi instrukcjami scenariusza.

> Dostępność węzłów klastra trybu failover powinna być określona przez dostępność głównych portów połączeń z Serwerem administracyjnym. Węzeł pasywny nie akceptuje żadnych połączeń zewnętrznych, dopóki nie nastąpi przełączenie.

Instalowanie Kaspersky Security Center Linux na węzłach klastra trybu failover Kaspersky Security Center Linux

Przed kontynuowaniem upewnij się, że wykonałeś poprzednie kroki w Scenariuszu: Wdrażanie klastra trybu failover Kaspersky.

Ta procedura opisuje sposób instalacji Kaspersky Security Center Linux na węzłach klastra failover Kaspersky Security Center Linux. Kaspersky Security Center Linux jest instalowany na obu węzłach klastra trybu failover Kaspersky Security Center Linux oddzielnie. W pierwszej kolejności instalujesz aplikację na węźle aktywnym, a następnie na węźle pasywnym. Podczas instalacji wybierasz, który węzeł będzie aktywny, a który będzie pasywny.

W zależności od dystrybucji Linux zainstalowanej na urządzeniu, należy użyć jednego z następujących plików instalacyjnych:

- ksc64_[numer_wersji]_amd64.deb

- ksc64-[numer_wersji].x86_64.rpm

Plik instalacyjny można pobrać ze strony internetowej Kaspersky.

Jeśli używasz RED OS w wersji 7.3.4 lub nowszej albo MSVSPHERE w wersji 9.2 lub nowszej, zainstaluj pakiet libxcrypt-compat na obu węzłach.

Instalacja na aktywnym węźle

W celu zainstalowania Kaspersky Security Center Linux na aktywnym węźle:

1. Upewnij się, że na urządzeniu, na którym chcesz zainstalować Kaspersky Security Center Linux, działa jedna z obsługiwanych dystrybucji systemu Linux.

2. Jeśli używasz dodatkowej karty sieciowej, wprowadź jej nazwę, gdy zostaniesz o to poproszony. Aby wyświetlić wszystkie interfejsy sieciowe, możesz wprowadzić następujące polecenie:

   ```
   ip addr
   ```

3. Uruchom instalację Kaspersky Security Center Linux. W zależności od dystrybucji Linux uruchom jedno z następujących poleceń:

   - `sudo apt-get install /<path>/ksc64_<numer_wersji>_amd64.deb`

   - `sudo yum install /<path>/ksc64-<numer_wersji>.x86_64.rpm`

4. Uruchom konfigurację Kaspersky Security Center Linux:

   ```
   /opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl
   ```

5. Przeczytaj Umowę Licencyjną Użytkownika Końcowego (EULA) i Politykę prywatności. Tekst jest wyświetlany w oknie wiersza poleceń. Naciśnij spację, aby wyświetlić następny segment tekstu. Następnie po wyświetleniu monitu wprowadź następujące wartości:

   a. Wpisz `y`, jeśli rozumiesz i akceptujesz warunki Umowy licencyjnej użytkownika końcowego. Wpisz `n`, jeśli nie akceptujesz warunków Umowy licencyjnej użytkownika końcowego. Aby korzystać z Kaspersky Security Center Linux, musisz zaakceptować warunki Umowy licencyjnej użytkownika końcowego.

   b. Wpisz `y`, jeśli rozumiesz i akceptujesz warunki Polityki Prywatności oraz zgadzasz się, że Twoje dane będą przetwarzane i przekazywane (w tym do krajów trzecich) zgodnie z Polityką Prywatności. Wpisz `n`, jeśli nie akceptujesz warunków Polityki Prywatności. Aby korzystać z Kaspersky Security Center Linux, musisz zaakceptować warunki Polityki prywatności.

6. Wybierz **Podstawowy węzeł klastra** jako tryb instalacji Serwera administracyjnego.

7. Po wyświetleniu monitu określ następujące ustawienia:

   a. Wprowadź ścieżkę lokalną do punktu podłączenia dzielenia stanu: `/mnt/KlFocStateShare`

   b. Wprowadź ścieżkę lokalną do punktu podłączenia dzielenia danych: `/mnt/KlFocDataShare_klfoc`

   c. Wybierz tryb łączności klastra pracy awaryjnej: za pośrednictwem wirtualnej karty sieciowej lub zewnętrznego modułu równoważenia obciążenia.

   d. Jeśli używasz dodatkowej karty sieciowej, wprowadź jej nazwę.

   e. Wprowadź adres FQDN/IP dodatkowej karty sieciowej lub adres FQDN/IP zewnętrznego modułu równoważenia obciążenia.

   f. Wprowadź numer portu SSL Serwera administracyjnego. Domyślnie wykorzystywany jest port 13000.

g. Oceń przybliżoną liczbę urządzeń, którymi zamierzasz zarządzać:

- Jeśli masz od 1 do 100 zarządzanych urządzeń, wpisz 1.
- Jeśli masz od 101 do 1000 zarządzanych urządzeń, wpisz 2.
- Jeśli masz więcej niż 1000 zarządzanych urządzeń, wpisz 3.

To ustawienie służy do automatycznego losowego opóźnienia uruchamiania zadań w celu optymalizacji obciążenia sieci. Poniższa tabela przedstawia przedział czasu, w którym obliczane jest opóźnienie:

- 1 do 100 zarządzanych urządzeń, wartość 1. Opóźnienie nie jest używane.
- 101 do 1000 zarządzanych urządzeń, wartość 2. Opóźnienie wynosi 5 minut.
- Ponad 1000 zarządzanych urządzeń, wartość 3. Opóźnienie wynosi 10 minut.

h. Wprowadź nazwę grupy zabezpieczeń dla usług. Domyślnie używana jest grupa kladmins.

i. Wprowadź nazwę konta, aby uruchomić usługę Serwera administracyjnego. Konto musi należeć do wprowadzonej grupy zabezpieczeń. Domyślnie używane jest konto „ksc".

j. Wprowadź nazwę konta, aby uruchomić inne usługi. Konto musi należeć do wprowadzonej grupy zabezpieczeń. Domyślnie używane jest konto „ksc".

k. Wybierz DBMS, który zainstalowałeś do pracy z Kaspersky Security Center Linux:

- Jeśli zainstalowałeś MySQL lub MariaDB, wpisz 1.
- Jeśli zainstalowałeś PostgreSQL lub Postgres Pro, wpisz 2.

l. Wprowadź nazwę DNS lub adres IP urządzenia, na którym zainstalowana jest baza danych.

m. Wprowadź numer portu bazy danych. Ten port jest używany do komunikacji z Serwerem administracyjnym. Domyślnie używane są następujące porty:

- Port 3306 dla MySQL lub MariaDB
- Port 5432 dla PostgreSQL lub Postgres Pro

n. Wprowadź nazwę bazy danych.

o. Wprowadź login konta administratora bazy danych, którego używasz do uzyskiwania dostępu do bazy danych.

p. Wprowadź hasło konta administratora bazy danych, którego używasz do uzyskiwania dostępu do bazy danych.

q. Wprowadź nazwę DNS serwera FQDN.

Należy określić nazwę DNS Serwera administracyjnego wprowadzoną w kroku 7e.

r. Wprowadź nazwę konta, aby uruchomić usługę IAM. Konto musi należeć do wprowadzonej grupy zabezpieczeń. Domyślnie używane jest konto ksciam.

s. Wybierz DBMS, który zainstalowałeś do pracy z usługą IAM:

- Jeśli zainstalowałeś MySQL lub MariaDB, wpisz 1.
- Jeśli zainstalowałeś PostgreSQL lub Postgres Pro, wpisz 2.

t. Wprowadź adres IAM DBMS, który ma być używany przez usługę IAM.

u. Wprowadź numer portu IAM DBMS. Ten port jest używany do komunikacji z usługą IAM. Domyślnie używane są następujące porty:

- Port 3306 dla MySQL lub MariaDB
- Port 5432 dla PostgreSQL lub Postgres Pro

v. Wprowadź nazwę bazy danych IAM, która ma być używana przez usługę IAM. Nazwa bazy danych używanej przez usługę IAM powinna być inna niż nazwa bazy danych używanej przez Serwer administracyjny.

w. Wprowadź login konta bazy danych, którego używasz do uzyskiwania dostępu do bazy danych IAM.

x. Wprowadź hasło konta bazy danych, którego używasz do uzyskiwania dostępu do bazy danych IAM.

8. Poczekaj, aż usługi zostaną dodane i uruchomione automatycznie:

- klfocsvc_klfoc
- kladminserver_klfoc
- klwebsrv_klfoc
- klactprx_klfoc
- klnagent_klfoc
- kliam_klfoc

9. Utwórz konto, które będzie działać jako administrator Serwera administracyjnego. Wprowadź nazwę użytkownika i hasło. Hasło użytkownika nie może mieć mniej niż 8 ani więcej niż 256 znaków.

   Jeśli pominiesz ten krok, możesz utworzyć konto później, uruchamiając następujące polecenie:

   ```
   /opt/kaspersky/ksc64/sbin/kladduser -n kscadmin -p <hasło>
   ```

Użytkownik zostanie dodany, a Kaspersky Security Center Linux zostanie zainstalowany na węźle podstawowym.

Instalacja na węźle dodatkowym (pasywnym)

W celu zainstalowania Kaspersky Security Center Linux na węźle dodatkowym:

1. Upewnij się, że na urządzeniu, na którym chcesz zainstalować Kaspersky Security Center Linux, działa jedna z obsługiwanych dystrybucji systemu Linux.

2. Uruchom instalację Kaspersky Security Center Linux. W zależności od dystrybucji Linux uruchom jedno z następujących poleceń:

   - `sudo apt-get install /<path>/ksc64_<numer_wersji>_amd64.deb`

   - `sudo yum install /<path>/ksc64-<numer_wersji>.x86_64.rpm`

3. Uruchom konfigurację Kaspersky Security Center Linux:

   `/opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl`

4. Przeczytaj Umowę Licencyjną Użytkownika Końcowego (EULA) i Politykę prywatności. Tekst jest wyświetlany w oknie wiersza poleceń. Naciśnij spację, aby wyświetlić następny segment tekstu. Następnie po wyświetleniu monitu wprowadź następujące wartości:

   a. Wpisz `y`, jeśli rozumiesz i akceptujesz warunki Umowy licencyjnej użytkownika końcowego. Wpisz `n`, jeśli nie akceptujesz warunków Umowy licencyjnej użytkownika końcowego. Aby korzystać z Kaspersky Security Center Linux, musisz zaakceptować warunki Umowy licencyjnej użytkownika końcowego.

   b. Wpisz `y`, jeśli rozumiesz i akceptujesz warunki Polityki Prywatności oraz zgadzasz się, że Twoje dane będą przetwarzane i przekazywane (w tym do krajów trzecich) zgodnie z Polityką Prywatności. Wpisz `n`, jeśli nie akceptujesz warunków Polityki Prywatności. Aby korzystać z Kaspersky Security Center Linux, musisz zaakceptować warunki Polityki prywatności.

5. Wybierz **Dodatkowy węzeł klastra** jako tryb instalacji Serwera administracyjnego.

6. Po wyświetleniu monitu wprowadź ścieżkę lokalną do punktu montowania dzielenia stanu:
   `/mnt/KlFocStateShare`

Kaspersky Security Center Linux jest zainstalowany na aktywnym węźle.

Weryfikacja usługi

Użyj następującego polecenia, aby sprawdzić, czy usługa zarządzania klastrem trybu failover jest `Active: active (running)`:

```
systemctl status klfocsvc_klfoc
```

Użyj następujących poleceń, aby sprawdzić, czy inne usługi klastra trybu failover są `Active: inactive (dead)`:

- `systemctl status klnagent_klfoc`

- `systemctl status kladminserver_klfoc`

- `systemctl status klactprx_klfoc`

- `systemctl status klwebsrv_klfoc`
- `systemctl status kliam_klfoc`

Teraz możesz przetestować klaster trybu failover Kaspersky Security Center Linux, aby upewnić się, że został poprawnie skonfigurowany i działa poprawnie.

Ręczne uruchamianie i zatrzymywanie węzłów klastra

Konieczne może być zatrzymanie całego klastra trybu failover Kaspersky Security Center Linux lub tymczasowe odłączenie jednego z węzłów klastra w celu konserwacji. W takim przypadku postępuj zgodnie z instrukcjami w tej sekcji. Nie próbuj uruchamiać ani zatrzymywać usług lub procesów związanych z klastrem trybu failover za pomocą innych środków. To może spowodować utratę danych.

Uruchamianie i zatrzymywanie całego klastra trybu failover w celu konserwacji

W celu uruchomienia lub zatrzymania całego klastra trybu failover:

Na aktywnym węźle uruchom jedno z następujących poleceń:

- Aby zatrzymać klaster, uruchom: `/opt/kaspersky/ksc64/sbin/klfoc -stopcluster --stp klfoc`
- Aby uruchomić klaster, uruchom: `/opt/kaspersky/ksc64/sbin/klfoc -startcluster --stp klfoc`

Klaster trybu failover jest uruchamiany lub zatrzymywany w zależności od uruchomionego polecenia.

Utrzymywanie jednego z węzłów

W celu utrzymania jednego z węzłów:

1. W węźle aktywnym zatrzymaj klaster trybu failover, używając polecenia `klfoc -stopcluster --stp klfoc`.
2. W węźle, którym chcesz zarządzać, przejdź do /opt/kaspersky/ksc64/sbin.
3. Otwórz wiersz poleceń, a następnie odłącz węzeł od klastra, uruchamiając polecenie `detach_node.sh`.
4. W węźle aktywnym uruchom klaster trybu failover za pomocą polecenia `klfoc -startcluster --stp klfoc`.
5. Wykonaj działania konserwacyjne.
6. W węźle aktywnym zatrzymaj klaster trybu failover, używając polecenia `klfoc -stopcluster --stp klfoc`.
7. W utrzymywanym węźle przejdź do /opt/kaspersky/ksc64/sbin.
8. Otwórz wiersz poleceń, a następnie dołącz węzeł do klastra, uruchamiając polecenie `attach_node.sh`.
9. W węźle aktywnym uruchom klaster trybu failover za pomocą polecenia `klfoc -startcluster --stp klfoc`.
10. Aby upewnić się, że bieżący węzeł jest aktywny, uruchom następujące polecenia, aby sprawdzić, czy usługi są uruchomione:

`systemctl status klnagent_klfoc.service`

`systemctl status kladminserver_klfoc.service`

`systemctl status klactprx_klfoc.service`

`systemctl status klwebsrv_klfoc.service`

`systemctl status kliam_klfoc.service`

Te usługi są uruchamiane na węźle aktywnym, a nie na węźle pasywnym.

Węzeł jest utrzymywany i dołączany do klastra trybu failover.

Ponowna instalacja węzła klastra trybu failover

Aby ponownie zainstalować węzeł klastra trybu failover:

1. Utwórz kopię zapasową Serwera administracyjnego.
2. Przełącz węzeł aktywny w tryb konserwacji.
3. Aby zachować bieżący system operacyjny, wykonaj następujące czynności.

   Jeśli chcesz wymienić urządzenie lub system operacyjny, pomiń ten krok.

   a. Aby zatrzymać klaster trybu failover, uruchom następujące polecenie:

   `klfoc -stopcluster --stp klfoc`

   b. Aby wymusić zatrzymanie usług klastra trybu failover, uruchom następujące polecenia:

   `sudo systemctl stop klfocsvc_klfoc`

   `systemctl status kl*klfoc*`

   c. Aby odmontować katalogi klastra trybu failover, uruchom następujące polecenia:

   `sudo umount /mnt/KlFocDataShare_klfoc`

   `sudo umount /mnt/KlFocStateShare`

   d. Aby odinstalować Kaspersky Security Center Linux, uruchom jedno z poniższych poleceń w zależności od dystrybucji Linux:

   - `sudo dpkg --remove ksc64`

   lub

   - `sudo yum remove ksc64`

   e. Wykonaj wszystkie kroki z następujących instrukcji dla węzła pasywnego:

   1. Przygotowywanie węzłów dla klastra trybu failover Kaspersky Security Center Linux.
   2. Instalowanie Kaspersky Security Center Linux na węzłach klastra trybu failover Kaspersky Security Center Linux.

4. Wyjdź z trybu konserwacji. Kontynuuj od kroku 6 (zatrzymanie klastra trybu failover) instrukcji Ręczne uruchamianie i zatrzymywanie węzłów klastra.

Instalowanie Kaspersky Security Center Web Console połączonej z Serwerem administracyjnym zainstalowanym na węzłach klastra przełączania awaryjnego Kaspersky Security Center Linux

Ta sekcja opisuje sposób instalacji Serwera Kaspersky Security Center Web Console Server (zwanego dalej również Kaspersky Security Center Web Console), który łączy się z Serwerem administracyjnym zainstalowanym na węzłach klastra pracy awaryjnej Kaspersky Security Center Linux. Przed zainstalowaniem Kaspersky Security Center Web Console zainstaluj system DBMS i serwer administracyjny Kaspersky Security Center Linux na węzłach klastra trybu failover Kaspersky Security Center Linux.

> Kaspersky Security Center Web Console nie obsługuje instalacji na węzłach klastra. Zalecamy zainstalowanie Kaspersky Security Center Web Console na osobnym serwerze.

Instalowanie Kaspersky Security Center Web Console łączącej się z Serwerem administracyjnym zainstalowanym na węzłach klastra przełączania awaryjnego Kaspersky Security Center Linux:

1. Wykonaj krok 1 i krok 2 instalacji Kaspersky Security Center Web Console.

2. W kroku 3 w pliku odpowiedzi określ parametr `trusted` instalacji, aby umożliwić Kaspersky Security Center Web Console nawiązanie połączenia z klastrem trybu failover Kaspersky Security Center Linux.

   Składniki parametru `trusted` **instalacji**

   Jeśli łączysz się z klastrem trybu failover Kaspersky Security Center Linux za pomocą uwierzytelniania domeny z funkcją SSO, określ parametr zaufany instalacji w następujący sposób: Jeśli łączysz Kaspersky Security Center Web Console z Serwerem administracyjnym w wersji 16 lub nowszej, zostanie użyte uwierzytelnianie domeny z funkcją pojedynczego logowania (SSO) zapewniane przez usługę Menedżera tożsamości i dostępu (IAM). W takim przypadku określ parametr `trusted` instalacji w następujący sposób:

   ```
   "trusted":  {
     "<Nazwa Serwera administracyjnego>": {
       "iamHost": "ksc-iam.example.com",
       "iamOAuthPort": 4444,
       "iamProxyPort": 9050,
       "iamCertPath": "<udostepniony folder danych>/iam/main_certificate.pem",
       "iamPATPath": "<udostepniony folder danych>/iam/initial_token.txt",
       "kscPort": 13299,
       "kscCertPath": "<udostepniony folder danych>/1093/cert/klserver.cer"
     }
   }
   ```

   gdzie:

   - `<Nazwa Serwera administracyjnego>` to nazwa klastra trybu failover Kaspersky Security Center Linux, która będzie wyświetlana w oknie logowania Kaspersky Security Center Web Console.

   - `iamHost` to adres urządzenia, na którym zainstalowane są Serwer administracyjny i IAM. Jeśli utworzyłeś dodatkową kartę sieciową podczas przygotowywania węzłów klastra, użyj FQDN, nazwy hosta lub adresu IP karty jako adresu klastra trybu failover Kaspersky Security Center Linux. W przeciwnym razie określ FQDN lub nazwę hosta modułu równoważenia obciążenia innej firmy, którego używasz.

     Ta wartość `iamHost` musi być zgodna z adresem IAM określonym podczas instalacji Serwera administracyjnego. Aby uzyskać określony adres IAM, uruchom następujące polecenie na hoście Serwera administracyjnego:

     ```
     grep "iam_address:" /var/opt/kaspersky/klnagent_srv/iam/iam_config.yaml
     ```

- `iamOAuthPort` to port używany do wymiany tokenów uwierzytelniania przez protokół uwierzytelniania OpenID Connect (wartość domyślna to 4444). Ten port jest używany zarówno do komunikacji między Kaspersky Security Center Web Console Server a Serwerem administracyjnym, jak i między przeglądarką (używaną z Kaspersky Security Center Web Console) a Serwerem administracyjnym.

- `iamProxyPort` to port, który jest używany przez Kaspersky Security Center Web Console Server do nawiązywania połączenia z Serwerem administracyjnym (domyślnie jest to port 9050).

- `iamCertPath` to ścieżka do certyfikatu IAM. Certyfikat IAM jest tworzony automatycznie przy pierwszym uruchomieniu Serwera administracyjnego. Plik certyfikatu jest przechowywany na urządzeniu, na którym zainstalowany jest Serwer administracyjny. Domyślna ścieżka do certyfikatu: `< udostępniony folder danych >/iam/main_certificate.pem`. Certyfikat Serwera administracyjnego znajduje się we współdzielonym magazynie danych klastra trybu failover Kaspersky Security Center Linux. Certyfikat IAM z podpisem własnym jest automatycznie rotowany.

- `iamPATPath` to ścieżka do tokena używanego do rejestracji Kaspersky Security Center Web Console jako klienta OAuth w IAM. Ten plik jest generowany podczas pierwszego uruchomienia Serwera administracyjnego. Plik certyfikatu jest przechowywany na urządzeniu, na którym zainstalowany jest Serwer administracyjny. Domyślna ścieżka do tokena: <udostępniony folder danych>/iam/initial_token.txt. Token znajduje się we współdzielonym magazynie danych klastra trybu failover Kaspersky Security Center Linux. Token jest ważny bezterminowo i nie wymaga rotacji.

- `kscPort` to port OpenAPI, którego Kaspersky Security Center Web Console używa do łączenia się z Serwerem administracyjnym (wartość domyślna to 13299).

- `kscCertPath` to certyfikat Serwera administracyjnego, który znajduje się we współdzielonym magazynie danych klastra trybu failover Kaspersky Security Center Linux. Domyślna ścieżka do pliku certyfikatu to: `< udostępniony folder danych >\1093\cert\klserver.cer`.

  Skopiuj plik certyfikatu Serwera administracyjnego (określony przez `kscCertPath`), plik certyfikatu IAM (określony przez `iamCertPath`) i plik tokena (określony przez `iamPATPath`) z współdzielonego magazynu danych na urządzenie, na którym instalujesz Kaspersky Security Center Web Console. Określ lokalną ścieżkę do certyfikatu Serwera administracyjnego.

Jeśli łączysz Kaspersky Security Center Web Console z Serwerem administracyjnym w wersji 15.4 lub starszej, zostanie użyte uwierzytelnianie poprzez określenie nazwy i hasła użytkownika domeny lub użytkownika wewnętrznego. W takim przypadku określ parametr zaufany instalacji w następujący sposób:

```
"trusted":  {
  "<Nazwa Serwera administracyjnego>": {
    "kscHost": "ksc.example.com",
    "kscPort": 13299,
    "kscCertPath": "<udostepniony folder danych>/1093/cert/klserver.cer"
  }
}
```

gdzie:

- `< Nazwa Serwera administracyjnego >` to nazwa klastra trybu failover Kaspersky Security Center Linux, która będzie wyświetlana w oknie logowania Kaspersky Security Center Web Console.

- `kscHost` to adres Serwera administracyjnego (FQDN lub nazwa hosta). Jeśli utworzyłeś dodatkową kartę sieciową podczas przygotowywania węzłów klastra, użyj adresu karty jako adresu klastra trybu failover Kaspersky Security Center Linux. W przeciwnym razie określ adres modułu równoważenia obciążenia innej firmy, którego używasz.

- `kscPort` to port OpenAPI, którego Kaspersky Security Center Web Console używa do łączenia się z Serwerem administracyjnym (wartość domyślna to 13299).

- `kscCertPath` to certyfikat Serwera administracyjnego, który znajduje się we współdzielonym magazynie danych klastra trybu failover Kaspersky Security Center Linux. Domyślna ścieżka do pliku certyfikatu to: `<udostępniony folder danych>\1093\cert\klserver.cer`. Skopiuj plik certyfikatu ze współdzielonego magazynu danych na urządzenie, na którym instalujesz Kaspersky Security Center Web Console. Określ lokalną ścieżkę do certyfikatu Serwera administracyjnego.

3. Kontynuuj standardową instalację Kaspersky Security Center Web Console.

Po zakończeniu instalacji możesz użyć przeglądarki internetowej do otwarcia i zalogowania się do Kaspersky Security Center Web Console.

Geograficznie rozproszony klaster trybu failover Kaspersky Security Center Linux

Ta sekcja zawiera ogólne informacje o geograficznie rozproszonym klastrze trybu failover Kaspersky Security Center Linux, a także instrukcje dotyczące przygotowywania i wdrażania geograficznie rozproszonego klastra trybu failover w sieci dla następujących konfiguracji:

- Węzły klastra z system Ubuntu i PostgreSQL DBMS

- Węzły klastra z systemem SberLinux i Platform V Pangolin DBMS

Geograficznie rozproszony klaster z systemem Ubuntu i PostgreSQL DBMS

Postępując zgodnie z tym scenariuszem, możesz przygotować infrastrukturę i wdrożyć geograficznie rozproszony klaster trybu failover Kaspersky Security Center Linux.

Wymagania wstępne

- Wdróż moduł równoważenia DNS o wysokiej dostępności z kontrolą kondycji.

- Upewnij się, że aktywne i pasywne węzły klastra to dwa urządzenia o identycznej konfiguracji sprzętu i oprogramowania.

  - Wymagania sprzętowe:

    - CPU — 16 rdzenie, 2500 MHz

    - Pamięć RAM — 32 GB

    - Miejsce na dysku — 500 GB z 300 IOPS lub więcej

    - Kontroler interfejsu sieciowego — 1 Gbps

- Wymagania programowe:
  - System operacyjny: Ubuntu Server 24.04 LTS (Noble Numbat) 64-bitowy
  - DBMS: PostgreSQL 17 64-bitowy

Etapy

Klaster trybu failover Kaspersky Security Center Linux wdrożony w pojedynczym centrum danych nie może zostać uaktualniony do geograficznie rozproszonego klastra trybu failover.

Wdrażanie geograficznie rozproszonego klastra trybu failover Kaspersky Security Center Linux przebiega etapami:

1. **Przygotowanie systemu plików węzłów klastra trybu failover**

   Przygotuj system plików na obu węzłach klastra. Przygotowanie obejmuje utworzenie woluminów logicznych LVM i skonfigurowanie katalogów jako punktów montowania.

2. **Konfigurowanie zreplikowanego systemu plików klastra**

   Zainstaluj narzędzia DRBD i skonfiguruj zasoby DRBD do replikacji danych między węzłami klastra trybu failover. Następnie utwórz zreplikowany system plików na aktywnym węźle klastra.

3. **Instalowanie i konfigurowanie Corosync i Pacemaker na węzłach klastra trybu failover**

   Zainstaluj Corosync i Pacemaker, aby zapewnić komunikację klastra i zarządzanie zasobami na potrzeby wysokiej dostępności.

4. **Instalowanie i konfigurowanie PostgreSQL DBMS**

   Zainstaluj i skonfiguruj PostgreSQL na węzłach klastra.

5. **Instalowanie Kaspersky Security Center Linux na węzłach klastra trybu failover**

   Zainstaluj Kaspersky Security Center Linux na węzłach klastra, a następnie skonfiguruj szyfrowanie między węzłami klastra.

6. **Instalowanie Kaspersky Security Center Web Console na węzłach klastra trybu failover**

   Zainstaluj Kaspersky Security Center Web Console na obu węzłach klastra trybu failover, aby zapewnić wysoką dostępność.

Przygotowanie system plików węzłów klastra

Pierwszym krokiem w przygotowaniu do wdrożenia geograficznie rozproszonego klastra trybu failover Kaspersky Security Center Linux jest skonfigurowanie systemu plików na obu węzłach klastra. Przygotowanie obejmuje utworzenie woluminów logicznych LVM i skonfigurowanie katalogów jako punktów montowania. Wykonaj poniższą procedurę na obu węzłach klastra.

Aby przygotować system plików węzłów klastra:

1. Utwórz wolumin logiczny LVM dla danych i bazy danych Serwera administracyjnego:

```
lvcreate -L <volume size> -n klfocdata <volume group name>
```

Utwórz oddzielny wolumin logiczny LVM do przechowywania pliku odpowiedzi:

```
lvcreate -L <volume size> -n klfocstate <volume group name>
```

gdzie:

- `volume group name` jest nazwą grupy woluminów używaną przez LVM.
- `klfocdata` i `klfocstate` to nazwy woluminów logicznych. Te woluminy logiczne są tworzone w obrębie tej grupy woluminów.

  Zalecamy używanie tych nazw woluminów dla zachowania spójności, chociaż w razie potrzeby można określić nazwy niestandardowe.
- `volume size` rozmiar woluminu. Zalecamy przydzielenie co najmniej 500 GB na dane i bazy danych Serwera administracyjnego. Wolumin do przechowywania pliku odpowiedzi wymaga niewielkiej ilości miejsca.

2. Utwórz katalogi, które będą używane jako punkty montowania dla woluminów logicznych.

   - Dla danych i bazy danych Serwera administracyjnego:

     ```
     mkdir -p /mnt/KlFocDataShare_klfoc
     ```

   - Dla pliku odpowiedzi:

     ```
     mkdir -p /mnt/KlFocStateShare_klfoc
     ```

Zalecamy użycie katalogów `/mnt/KlFocDataShare_klfoc` i `/mnt/KlFocStateShare_klfoc`, aby zapewnić spójność, choć w razie potrzeby można określić niestandardowe nazwy.

System plików węzłów klastra jest przygotowany. Następnie należy skonfigurować zreplikowany system plików klastra.

Konfigurowanie zreplikowanego systemu plików klastra

Instalowanie i konfigurowanie DRBD

DRBD to oprogramowanie firm trzecich służące do replikacji danych (w szczególności woluminów danych i punktów montowania przygotowanych w poprzednim kroku).

Po przygotowaniu systemu plików węzłów klastra należy zainstalować narzędzia DRBD i skonfigurować zasoby DRBD do replikacji danych między węzłami klastra. Wykonaj poniższą procedurę na obu węzłach klastra.

Aby zainstalować i skonfigurować DRBD na węzłach klastra:

1. Zainstaluj narzędzia DRBD:

   ```
   apt update
   apt install -y drbd-utils
   ```

   Zalecamy korzystanie z DRBD w wersji 9.2.6 lub nowszej, ponieważ zapewnia ona wbudowane szyfrowanie ruchu.

   Ruch DRBD można również szyfrować za pomocą własnego rozwiązania VPN.

2. Utwórz pliki konfiguracyjne zasobów DRBD dla każdego woluminu logicznego utworzonego podczas przygotowywania systemu plików (`klfocdata` i `klfocstate`).

   Wszystkie pliki konfiguracyjne muszą być umieszczone w `/etc/drbd.d/`.

   - Zasób `klfocdata` (Dane i bazy danych Serwera administracyjnego)

     Użyj replikacji asynchronicznej (protokół A) dla zasobu klfocdata. Skonfiguruj wszystkie pozostałe parametry zgodnie ze swoim środowiskiem.

     Przykład pliku konfiguracyjnego

```
resource klfocdata {
    protocol A;
    net {
        after-sb-0pri    discard-least-changes;
        after-sb-1pri    call-pri-lost-after-sb;
        after-sb-2pri    call-pri-lost-after-sb;
    }
    syncer {
        rate 110M;
    }
    # Hostname of the active node
    on db1 {
        device    /dev/drbd0;
        disk      /dev/<volume group name>/klfocdata;
        address   <disk IP address>;
        meta-disk internal;
    }
    # Hostname of the passive node
    on db2 {
        device    /dev/drbd0;
        disk      /dev/<volume group name>/klfocdata;
        address   <disk IP address>;
        meta-disk internal;
    }
}
```

   - Zasób `klfocstate` (plik odpowiedzi)

     Użyj replikacji synchronicznej (protokół C), aby utworzyć zasób klfocstate. Skonfiguruj wszystkie pozostałe parametry zgodnie ze swoim środowiskiem.

     Przykład pliku konfiguracyjnego

```
resource klfocstate {
    protocol C;
    net {
        after-sb-0pri    discard-least-changes;
        after-sb-1pri    call-pri-lost-after-sb;
        after-sb-2pri    call-pri-lost-after-sb;
    }
    syncer {
        rate 110M;
    }
    # Hostname of the active node
    on db1 {
        device    /dev/drbd2;
        disk      /dev/<volume group name>/klfocstate;
        address   <disk IP address>;
        meta-disk internal;
    }
    # Hostname of the passive node
    on db2 {
        device    /dev/drbd2;
        disk      /dev/<volume group name>/klfocstate;
        address   <disk IP address>;
        meta-disk internal;
    }
}
```

3. Zainicjuj metadane DRBD dla obu zasobów:

```
drbdadm create-md klfocdata
drbdadm create-md klfocstate
```

4. Uruchom DRBD dla wszystkich skonfigurowanych zasobów:

```
drbdadm up all
```

DRBD jest zainstalowany i skonfigurowany na obu węzłach klastra.

Utwórz zreplikowany system plików na aktywnym węźle klastra

Po zainstalowaniu i skonfigurowaniu DRBD na obu węzłach klastra utwórz zreplikowany system plików na aktywnym węźle klastra. Wykonaj poniższą procedurę na aktywnym węźle klastra.

Aby utworzyć zreplikowany system plików na aktywnym węźle klastra:

1. Awansuj oba zasoby DRBD do roli głównej:

```
drbdadm primary --force klfocdata
drbdadm primary --force klfocstate
```

2. Sformatuj urządzenia DRBD, aby przygotować zreplikowane woluminy do użycia na węzłach klastra:

```
mkfs.ext4 /dev/drbd0
mkfs.ext4 /dev/drbd2
```

3. Skonfiguruj parametry systemu plików:

```
tune2fs -m 0 /dev/drbd0
tune2fs -m 0 /dev/drbd2
```

4. Zamontuj urządzenia DRBD w utworzonych wcześniej katalogach:

```
mount -o noatime /dev/drbd0 /mnt/KlFocDataShare_klfoc
mount -o noatime /dev/drbd2 /mnt/KlFocStateShare_klfoc
```

Jeśli usługa multipathd jest zainstalowana, należy ją skonfigurować tak, aby ignorowała urządzenia `/dev/drbd*` na obu węzłach klastra.

5. Sprawdź status replikacji:

```
drbdadm status
```

Wyjście prawidłowej konfiguracji systemu plików:

```
klfocdata role:Secondary
disk:UpToDate open:no
db2 role:Primary tls:yes
peer-disk:UpToDate

klfocstate role:Secondary
disk:UpToDate open:no
db2 role:Primary tls:yes
peer-disk:UpToDate
```

Zreplikowany system plików na aktywnym węźle klastra jest skonfigurowany. Następnie musisz zainstalować i skonfigurować Corosync i Pacemaker na węzłach klastra.

Instalowanie i konfigurowanie Corosync i Pacemaker na węzłach klastra

Corosync i Pacemaker zapewniają komunikację klastra i zarządzanie zasobami w celu zapewnienia wysokiej dostępności. Zapewniają automatyczne przenoszenie usług do sprawnego węzła w przypadku awarii, minimalizując przestoje.

Aby zainstalować i skonfigurować Corosync i Pacemaker na węzłach klastra:

1. Na obu węzłach klastra zainstaluj wymagane pakiety:

```
sudo apt install pacemaker -y
sudo apt install crmsh -y
sudo apt install resource-agent-extra -y
```

2. Skonfiguruj Corosync i Pacemaker na obu węzłach klastra zgodnie z oficjalną dokumentacją. Obejmuje to włączenie automatycznego uruchamiania, generowanie i dystrybucję klucza uwierzytelniającego oraz konfigurowanie uprawnień dostępu do pliku klucza uwierzytelniającego.

   Aby mieć pewność, że ustawienia są prawidłowe, uruchom następujące polecenie na jednym z węzłów klastra:

```
crm status
```

   Oczekiwany wynik powinien pokazywać status klastra i listę wszystkich aktywnych węzłów, potwierdzając, że Corosync działa prawidłowo i że komunikacja między węzłami działa.

3. Na obu węzłach klastra skonfiguruj podstawowe ustawienia klastra Pacemaker:

```
crm configure property stonith-enabled="false"
crm configure property symmetric-cluster="false"
crm configure rsc_defaults resource-stickiness="110"
crm configure rsc_defaults migration-threshold=3
crm configure property no-quorum-policy=ignore
```

4. Na obu węzłach klastra wyłącz uruchamianie skryptów, które będą zarządzane przez Corosync:

```
systemctl disable drbd.service
```

5. Na jednym z węzłów klastra utwórz zasoby oparte na DRBD w Pacemaker.

- Zasób DRBD dla klfocdata

  a. Utwórz zasób klastra dla woluminu DRBD `klfocdata`, umożliwiając klastrowi automatyczne zarządzanie swoim stanem i monitorowanie jego kondycji:

  ```
  crm configure primitive drbd_klfocdata ocf:linbit:drbd params drbd_resource="klfocdata" \
  op monitor interval="60s" op start interval="0" timeout="240s" op stop interval="0" \
  timeout="240s" op monitor role=Master interval="10s" op monitor role=Slave interval="30s"
  ```

  b. Utwórz zasób zarządzany przez klaster `ms_drbd_klfocdata` na podstawie utworzonego zasobu `drbd_klfocdata`:

  ```
  crm configure ms ms_drbd_klfocdata drbd_klfocdata meta master-max="1" master-node-max="1" \
  clone-max="2" clone-node-max="1" notify="true"
  ```

  c. Utwórz punkt montowania dla woluminu DRBD `fs_klfocdata`, określając urządzenie, katalog docelowy, typ systemu plików i opcje montowania:

  ```
  crm configure primitive fs_klfocdata ocf:heartbeat:Filesystem params device="/dev/drbd0" \
  directory="/mnt/KlFocDataShare_klfoc" fstype="ext4" options="data=journal"
  ```

- Zasób DRBD dla klfocstate

  a. Utwórz zasób klastra dla woluminu DRBD `klfocstate`, umożliwiając klastrowi automatyczne zarządzanie swoim stanem i monitorowanie jego kondycji:

  ```
  crm configure primitive drbd_klfocstate ocf:linbit:drbd params drbd_resource="klfocstate" \
  op monitor interval="60s" op start interval="0" timeout="240s" op stop interval="0" \
  timeout="240s" op monitor role=Master interval="10s" op monitor role=Slave interval="30s"
  ```

  b. Utwórz zasób zarządzany przez klaster ms_drbd_klfocstate na podstawie utworzonego zasobu `drbd_klfocstate`:

  ```
  crm configure ms ms_drbd_klfocstate drbd_klfocstate meta master-max="1" master-node-max="1" \
  clone-max="2" clone-node-max="1" notify="true"
  ```

  c. Utwórz punkt montowania dla woluminu DRBD `fs_klfocstate`, określając urządzenie, katalog docelowy, typ systemu plików i opcje montowania:

  ```
  crm configure primitive fs_klfocstate ocf:heartbeat:Filesystem params device="/dev/drbd2" \
  directory="/mnt/KlFocStateShare_klfoc" fstype="ext4" options="noatime"
  ```

6. Na obu węzłach klastra wyłącz automatyczne uruchamianie usługi DRBD:

```
systemctl disable drbd.service
```

Corosync i Pacemaker zostały zainstalowane i skonfigurowane na węzłach klastra. Następnie należy zainstalować system DBMS i utworzyć bazę danych Serwera administracyjnego oraz bazę danych IAM.

Instalowanie i konfigurowanie PostgreSQL DBMS

Po zainstalowaniu i skonfigurowaniu Corosync i Pacemaker na węzłach klastra należy zainstalować system DBMS na obu węzłach klastra.

Instalowanie i konfigurowanie systemu DBMS:

1. Na obu węzłach klastra zainstaluj PostgreSQL 17 x64 lub nowszy.

   Informacje o sposobie zainstalowania PostgreSQL znajdziesz w tym dokumencie.

2. Upewnij się, że węzły klastra z zainstalowanym systemem DBMS nie mają kont użytkowników DBMS o następujących nazwach:

   - client
   - iam
   - ksc
   - locker
   - pat
   - scope
   - voltron

3. Na obu węzłach klastra zatrzymaj system DBMS, a następnie wyłącz automatyczne uruchamianie usługi DBMS:

```
sudo systemctl stop postgresql
sudo systemctl disable postgresql
```

4. Na aktywnym węźle klastra skopiuj katalog DBMS do katalogu `/mnt/KlFocDataShare_klfoc/dbms`:

```
rsync -av /var/lib/postgresql/17/main/ /mnt/KlFocDataShare_klfoc/dbms
mv /var/lib/postgresql/17/main /var/lib/postgresql/17/main.bk
```

5. Na aktywnym węźle klastra skopiuj pliki konfiguracyjne PostgreSQL do katalogu `/mnt/KlFocDataShare_klfoc/dbms`:

```
sudo cp /etc/postgresql/17/main/pg_hba.conf /mnt/KlFocDataShare_klfoc/dbms
sudo cp /etc/postgresql/17/main/pg_ident.conf /mnt/KlFocDataShare_klfoc/dbms
```

6. Na obu węzłach klastra otwórz plik konfiguracyjny `/etc/postgresql/17/main/postgresql.conf`, a następnie ustaw katalog `/mnt/KlFocDataShare_klfoc/dbms` jako katalog danych bazy danych.

   Określ również ścieżki do plików konfiguracyjnych (`/mnt/KlFocDataShare_klfoc/dbms/pg_hba.conf` i `/mnt/KlFocDataShare_klfoc/dbms/pg_ident.conf`) i usuń parametr `include_dir`:

```
data_directory = '/mnt/KlFocDataShare_klfoc/dbms'
hba_file = '/mnt/KlFocDataShare_klfoc/dbms/pg_hba.conf'
ident_file = '/mnt/KlFocDataShare_klfoc/dbms/pg_ident.conf'
listen_addresses = '*'
```

7. W pliku konfiguracyjnym `/etc/postgresql/17/main/postgresql.conf`, dostosuj konfigurację systemu DBMS do wymagań Kaspersky Security Center Linux.

8. Utwórz i skonfiguruj konta do pracy z PostgreSQL.

9. Utwórz zasób usługi PostgreSQL:

```
crm configure primitive klfocsvc_dbms ocf:heartbeat:pgsql \
params pgctl="/usr/lib/postgresql/17/bin/pg_ctl" \
psql="/usr/bin/psql" \
pgdata="/mnt/KlFocDataShare_klfoc/dbms" \
config="/etc/postgresql/17/main/postgresql.conf" \
socketdir="/var/run/postgresql" \
op start timeout=60s \
op stop timeout=60s \
op monitor interval=30s timeout=60s
```

10. Dodaj zasób PostgreSQL do grupy klastrów `group_klfoc`:

```
crm configure edit klfoc_group
```

11. Dodaj nazwę zasobu PostgreSQL `klfocsvc_dbms` na końcu listy, na przykład:

```
group klfoc_group {
...
klfocsvc_dbms
}
```

12. Na aktywnym węźle klastra, na serwerze DBMS, utwórz bazę danych dla IAM. Nazwa bazy danych musi być inna niż baza danych, którą zainstalowałeś, aby pracować z Kaspersky Security Center Linux. Serwer administracyjny nie usuwa bazy danych IAM automatycznie podczas odinstalowywania lub przenoszenia serwera na inne urządzenie, należy usunąć bazę danych ręcznie:

```
sudo -i -u postgres psql -U postgres -c "CREATE DATABASE <iam_db_name>;"
```

System DBMS został zainstalowany i skonfigurowany. Baza danych Serwera administracyjnego i baza danych IAM zostały utworzone. Następnie należy zainstalować Kaspersky Security Center Linux na węzłach klastra.

Instalowanie Kaspersky Security Center Linux na geograficznie rozproszonych węzłach klastra trybu failover

Kaspersky Security Center Linux jest instalowany na geograficznie rozproszonych węzłach klastra trybu failover przy użyciu pliku odpowiedzi w trybie cichym, czyli bez udziału użytkownika. Plik odpowiedzi zawiera niestandardowy zestaw parametrów instalacji: zmienne i odpowiadające im wartości.

Wymagania wstępne:

- Wykonaj wszystkie kroki przygotowawcze:
  - Przygotowanie system plików węzłów klastra
  - Konfigurowanie zreplikowanego systemu plików klastra
  - Instalowanie i konfigurowanie Corosync i Pacemaker na węzłach klastra
  - Instalowanie i konfigurowanie PostgreSQL DBMS

- Upewnij się, że węzły klastra działają na Ubuntu Server 24.04 LTS (Noble Numbat) x64.
- Pobierz plik instalacyjny `ksc64_[version_number]_amd64.deb` ze strony internetowej Kaspersky.

Instalacja na aktywnym węźle

W celu zainstalowania Kaspersky Security Center Linux na aktywnym węźle w trybie cichym:

1. Przeczytaj Umowę licencyjną użytkownika końcowego. Wykonaj poniższe kroki tylko wtedy, gdy rozumiesz i akceptujesz warunki Umowy licencyjnej użytkownika końcowego.
2. Utwórz grupę `kladmins` i nieuprzywilejowane konta `ksc` oraz `ksciam`, które muszą należeć do grupy `kladmins`. Aby to zrobić, uruchom kolejno następujące polecenia na koncie z uprawnieniami roota:

```
adduser ksc
groupadd kladmins
gpasswd -a ksc kladmins
usermod -g kladmins ksc
adduser ksciam
gpasswd -a ksciam kladmins
usermod -g kladmins ksciam
```

3. W katalogu `/mnt/KlFocDataShare_klfoc/` utwórz katalog dla plików Kaspersky Security Center Linux:

```
mkdir /mnt/KlFocDataShare_klfoc/ksc/
```

4. Utwórz plik odpowiedzi (w formacie TXT) i dodaj do pliku odpowiedzi listę zmiennych w formacie VARIABLE_NAME=variable_value, każdą w osobnym wierszu.

   Na liście parametrów używanych do instalacji Kaspersky Security Center Linux w trybie cichym określ następujące parametry wymagane dla wdrożenia geograficznie rozproszonego klastra:

   - `KLFOC_UNATT_EXT_RESOURCE_MANAGEMENT=2`

     Ustaw wartość `2`, aby wdrożyć geograficznie rozproszony klaster.

   - `KLSRV_UNATT_SERVERADDRESS=<DNS balancer address>` i `KLSRV_UNATT_IAM_ADDRESS=<DNS balancer address>`

     Moduł równoważenia DNS z kontrolą kondycji musi być już wdrożony. Wartości tych parametrów muszą być identyczne i ustawione na nazwę FQDN modułu równoważenia DNS.

5. Ustaw wartość zmiennej środowiskowej `KLAUTOANSWERS` w środowisku root lub środowisku użytkownika zawierającej pełną nazwę pliku odpowiedzi wraz ze ścieżką, na przykład za pomocą następującego polecenia:

```
export KLAUTOANSWERS=/tmp/ksc_install/answers.txt
```

6. Uruchom instalację Kaspersky Security Center Linux w trybie cichym, uruchamiając następujące polecenia:

   - W środowisku root:

```
apt-get install /<path>/ksc64_[version_number]_amd64.deb -y
```

- W środowisku użytkownika:

```
sudo -E apt-get install /<path>/ksc64_[version_number]_amd64.deb -y
```

7. Wyłącz automatyczne uruchamianie usługi klfocsvc_klfoc.service:

```
systemctl disable klfocsvc_klfoc.service
```

8. Po zainstalowaniu Kaspersky Security Center Linux zatrzymaj aktywny węzeł klastra.

9. Przenieś wszystkie zasoby klastra na węzeł pasywny.

   Możesz użyć polecenia `crm node standby` (i przywróć go za pomocą `crm node online`).

Instalacja na węźle pasywnym

W celu zainstalowania Kaspersky Security Center Linux na węźle pasywnym:

1. Uruchom instalację Kaspersky Security Center Linux:

```
sudo apt-get install /<path>/ksc64_<version_number>_amd64.deb
```

2. Uruchom konfigurację Kaspersky Security Center Linux:

```
/opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl
```

3. Przeczytaj Umowę Licencyjną Użytkownika Końcowego (EULA) i Politykę prywatności. Tekst jest wyświetlany w oknie wiersza poleceń. Naciśnij spację, aby wyświetlić następny segment tekstu. Następnie po wyświetleniu monitu wprowadź następujące wartości:

   - Wpisz `y`, jeśli rozumiesz i akceptujesz warunki Umowy licencyjnej użytkownika końcowego. Wpisz `n`, jeśli nie akceptujesz warunków Umowy licencyjnej użytkownika końcowego. Aby korzystać z Kaspersky Security Center Linux, musisz zaakceptować warunki Umowy licencyjnej użytkownika końcowego.

   - Wpisz `y`, jeśli rozumiesz i akceptujesz warunki Polityki Prywatności oraz zgadzasz się, że Twoje dane będą przetwarzane i przekazywane (w tym do krajów trzecich) zgodnie z Polityką Prywatności. Wpisz n, jeśli nie akceptujesz warunków Polityki Prywatności. Aby korzystać z Kaspersky Security Center Linux, musisz zaakceptować warunki Polityki prywatności.

4. Wybierz węzeł pasywny klastra jako tryb instalacji Serwera administracyjnego.

5. Po wyświetleniu monitu wprowadź ścieżkę lokalną do punktu montowania dzielenia stanu: `/mnt/KlFocStateShare_klfoc`.

6. Wyłącz automatyczne uruchamianie usługi klfocsvc_klfoc.service:

```
systemctl disable klfocsvc_klfoc.service
```

7. Utwórz zasób usługi `klfocsvc_klfoc`:

```
crm configure primitive klfocsvc_klfoc systemd:klfocsvc_klfoc \
op start timeout="900s" interval="0" \
op stop timeout="900s" interval="0" \
op monitor interval="30s" timeout="90s"
```

8. Dodaj zasób `klfocsvc_klfoc` do grupy `group_klfoc`:

```
crm configure edit klfoc_group
```

9. Dołącz `klfocsvc_klfoc` na końcu wiersza grupy, na przykład:

```
group klfoc_group {
...
klfocsvc_klfoc
}
```

10. Sprawdź, czy wszystkie zasoby są w stanie uruchomienia na aktywnym węźle.

```
crm status
```

Konfigurowanie szyfrowania między węzłami klastra

Aby skonfigurować szyfrowanie między węzłami klastra,

Jeśli zainstalowano DRBD w wersji 9.2.6 lub nowszej podczas konfigurowania zreplikowanego systemu plików klastra, skonfiguruj szyfrowanie między węzłami klastra zgodnie z oficjalną dokumentacją DRBD.

Alternatywnie, możesz zastosować szyfrowanie ruchu między węzłami klastra, używając własnego rozwiązania VPN.

Geograficznie rozproszony klaster trybu failover Kaspersky Security Center Linux został zainstalowany. Następnie musisz zainstalować Kaspersky Security Center Web Console na obu węzłach klastra.

Geograficznie rozproszony klaster z systemem SberLinux i Platform V Pangolin DBMS

Postępując zgodnie z tym scenariuszem, możesz przygotować infrastrukturę i wdrożyć geograficznie rozproszony klaster trybu failover Kaspersky Security Center Linux.

Wymagania wstępne

- Wdróż moduł równoważenia DNS o wysokiej dostępności z kontrolą kondycji.
- Upewnij się, że aktywne i pasywne węzły klastra to dwa urządzenia o identycznej konfiguracji sprzętu i oprogramowania.
  - Wymagania sprzętowe:
    - CPU — 16 rdzenie, 2500 MHz
    - Pamięć RAM — 32 GB
    - Miejsce na dysku — 500 GB z 300 IOPS lub więcej
    - Kontroler interfejsu sieciowego — 1 Gbps
  - Wymagania programowe:
    - System operacyjny: Platform V SberLinux OS Server (SLO) 9.5.1 64-bitowy
    - DBMS: Platform V Pangolin 6.5.1 64-bitowy

Etapy

Klaster trybu failover Kaspersky Security Center Linux wdrożony w pojedynczym centrum danych nie może zostać uaktualniony do geograficznie rozproszonego klastra trybu failover.

Wdrażanie geograficznie rozproszonego klastra trybu failover Kaspersky Security Center Linux przebiega etapami:

1. **Przygotowanie systemu plików węzłów klastra trybu failover**

   Przygotuj system plików na obu węzłach klastra. Przygotowanie obejmuje utworzenie woluminów logicznych LVM i skonfigurowanie katalogów jako punktów montowania.

2. **Konfigurowanie zreplikowanego systemu plików klastra**

   Zainstaluj narzędzia DRBD i skonfiguruj zasoby DRBD do replikacji danych między węzłami klastra trybu failover. Następnie utwórz zreplikowany system plików na aktywnym węźle klastra.

3. **Instalowanie i konfigurowanie Corosync i Pacemaker na węzłach klastra trybu failover**

   Zainstaluj Corosync i Pacemaker, aby zapewnić komunikację klastra i zarządzanie zasobami na potrzeby wysokiej dostępności.

4. **Instalowanie i konfigurowanie Platform V Pangolin DBMS**

   Zainstaluj i skonfiguruj Platform V Pangolin na węzłach klastra.

5. **Instalowanie Kaspersky Security Center Linux na węzłach klastra trybu failover**

   Zainstaluj Kaspersky Security Center Linux na węzłach klastra, a następnie skonfiguruj szyfrowanie między węzłami klastra.

6. **Instalowanie Kaspersky Security Center Web Console na węzłach klastra trybu failover**

   Zainstaluj Kaspersky Security Center Web Console na obu węzłach klastra trybu failover, aby zapewnić wysoką dostępność.

Przygotowanie system plików węzłów klastra

Pierwszym krokiem w przygotowaniu do wdrożenia geograficznie rozproszonego klastra trybu failover Kaspersky Security Center Linux jest skonfigurowanie systemu plików na obu węzłach klastra. Przygotowanie obejmuje utworzenie woluminów logicznych LVM i skonfigurowanie katalogów jako punktów montowania. Wykonaj poniższą procedurę na obu węzłach klastra.

Aby przygotować system plików węzłów klastra:

1. Utwórz wolumin logiczny LVM dla danych i bazy danych Serwera administracyjnego:

   ```
   lvcreate -L <volume size> -n klfocdata <volume group name>
   ```

   Utwórz oddzielny wolumin logiczny LVM do przechowywania pliku odpowiedzi:

   ```
   lvcreate -L <volume size> -n klfocstate <volume group name>
   ```

   gdzie:

   - `volume group name` jest nazwą grupy woluminów używaną przez LVM.
   - `klfocdata` i `klfocstate` to nazwy woluminów logicznych. Te woluminy logiczne są tworzone w obrębie tej grupy woluminów.

     Zalecamy używanie tych nazw woluminów dla zachowania spójności, chociaż w razie potrzeby można określić nazwy niestandardowe.
   - `volume size` rozmiar woluminu. Zalecamy przydzielenie co najmniej 500 GB na dane i bazy danych Serwera administracyjnego. Wolumin do przechowywania pliku odpowiedzi wymaga niewielkiej ilości miejsca.

2. Utwórz katalogi, które będą używane jako punkty montowania dla woluminów logicznych.

   - Dla danych i bazy danych Serwera administracyjnego:

     ```
     mkdir -p /mnt/KlFocDataShare_klfoc
     ```

   - Dla pliku odpowiedzi:

     ```
     mkdir -p /mnt/KlFocStateShare_klfoc
     ```

   Zalecamy użycie katalogów `/mnt/KlFocDataShare_klfoc` i `/mnt/KlFocStateShare_klfoc`, aby zapewnić spójność, choć w razie potrzeby można określić niestandardowe nazwy.

System plików węzłów klastra jest przygotowany. Następnie należy skonfigurować zreplikowany system plików klastra.

Konfigurowanie zreplikowanego systemu plików klastra

Instalowanie i konfigurowanie DRBD

DRBD to oprogramowanie firm trzecich służące do replikacji danych (w szczególności woluminów danych i punktów montowania przygotowanych w poprzednim kroku).

Po przygotowaniu systemu plików węzłów klastra należy zainstalować narzędzia DRBD i skonfigurować zasoby DRBD do replikacji danych między węzłami klastra. Wykonaj poniższą procedurę na obu węzłach klastra.

Aby zainstalować i skonfigurować DRBD na węzłach klastra:

1. Zainstaluj narzędzia DRBD w następujący sposób:

   a. Włącz repozytoria EPEL i ELRepo na obu węzłach:

   ```
   dnf install https://dl.fedoraproject.org/pub/epel/epel-release-latest-9.noarch.rpm
   dnf install https://www.elrepo.org/elrepo-release-9.el9.elrepo.noarch.rpm
   ```

   b. Wyświetl wszystkie dostępne wersje pakietu kmod-drbd9x i przefiltruj listę pakietów utworzoną dla platformy el9_6 (na przykład użyto Platform V SberLinux OS Server (SLO) 9.6):

   ```
   dnf search --showduplicates kmod-drbd9x | grep el9_6
   ```

   c. Zainstaluj najnowszą dostępną wersję z listy na obu węzłach. Przykład dla Platform V SberLinux OS Server (SLO) 9.6:

   ```
   dnf install kmod-drbd9x-9.2.14-1.el9_6.elrepo.x86_64
   dnf install drbd drbd-utils drbd-udev drbd-pacemaker drbd-selinux
   modprobe drbd
   ```

   Jeśli w przyszłości pojawi się nowsza wersja, zastąp odpowiednio ciąg wersji.

   Zalecamy korzystanie z DRBD w wersji 9.2.6 lub nowszej, ponieważ zapewnia ona wbudowane szyfrowanie ruchu.

   Ruch DRBD można również szyfrować za pomocą własnego rozwiązania VPN.

2. Utwórz pliki konfiguracyjne zasobów DRBD dla każdego woluminu logicznego utworzonego podczas przygotowywania systemu plików (`klfocdata` i `klfocstate`).

   Wszystkie pliki konfiguracyjne muszą być umieszczone w `/etc/drbd.d/`.

   - Zasób `klfocdata` (Dane i bazy danych Serwera administracyjnego)

     Użyj replikacji asynchronicznej (protokół A) dla zasobu klfocdata. Skonfiguruj wszystkie pozostałe parametry zgodnie ze swoim środowiskiem.

     Przykład pliku konfiguracyjnego

     ```
     resource klfocdata {
         protocol A;
         net {
             after-sb-0pri    discard-least-changes;
             after-sb-1pri    call-pri-lost-after-sb;
             after-sb-2pri    call-pri-lost-after-sb;
         }
         syncer {
             rate 110M;
         }
         # Hostname of the active node
         on db1 {
             device    /dev/drbd0;
             disk      /dev/<volume group name>/klfocdata;
     ```

```
        address   <disk IP address>;
        meta-disk internal;
    }
    # Hostname of the passive node
    on db2 {
        device    /dev/drbd0;
        disk      /dev/<volume group name>/klfocdata;
        address   <disk IP address>;
        meta-disk internal;
    }
}
```

- Zasób `klfocstate` (plik odpowiedzi)

  Użyj replikacji synchronicznej (protokół C), aby utworzyć zasób klfocstate. Skonfiguruj wszystkie pozostałe parametry zgodnie ze swoim środowiskiem.

  Przykład pliku konfiguracyjnego

```
resource klfocstate {
    protocol C;
    net {
        after-sb-0pri    discard-least-changes;
        after-sb-1pri    call-pri-lost-after-sb;
        after-sb-2pri    call-pri-lost-after-sb;
    }
    syncer {
        rate 110M;
    }
    # Hostname of the active node
    on db1 {
        device    /dev/drbd2;
        disk      /dev/<volume group name>/klfocstate;
        address   <disk IP address>;
        meta-disk internal;
    }
    # Hostname of the passive node
    on db2 {
        device    /dev/drbd2;
        disk      /dev/<volume group name>/klfocstate;
        address   <disk IP address>;
        meta-disk internal;
    }
}
```

3. Zainicjuj metadane DRBD dla obu zasobów:

```
drbdadm create-md klfocdata
drbdadm create-md klfocstate
```

4. Uruchom DRBD dla wszystkich skonfigurowanych zasobów:

```
drbdadm up all
```

DRBD jest zainstalowany i skonfigurowany na obu węzłach klastra.

Utwórz zreplikowany system plików na aktywnym węźle klastra

Po zainstalowaniu i skonfigurowaniu DRBD na obu węzłach klastra utwórz zreplikowany system plików na aktywnym węźle klastra. Wykonaj poniższą procedurę na aktywnym węźle klastra.

Aby utworzyć zreplikowany system plików na aktywnym węźle klastra:

1. Awansuj oba zasoby DRBD do roli głównej:

```
drbdadm primary --force klfocdata
drbdadm primary --force klfocstate
```

2. Sformatuj urządzenia DRBD, aby przygotować zreplikowane woluminy do użycia na węzłach klastra:

```
mkfs.ext4 /dev/drbd0
mkfs.ext4 /dev/drbd2
```

3. Skonfiguruj parametry systemu plików:

```
tune2fs -m 0 /dev/drbd0
tune2fs -m 0 /dev/drbd2
```

4. Zamontuj urządzenia DRBD w utworzonych wcześniej katalogach:

```
mount -o noatime /dev/drbd0 /mnt/KlFocDataShare_klfoc
mount -o noatime /dev/drbd2 /mnt/KlFocStateShare_klfoc
```

   Jeśli usługa multipathd jest zainstalowana, należy ją skonfigurować tak, aby ignorowała urządzenia `/dev/drbd*` na obu węzłach klastra.

5. Sprawdź status replikacji:

```
drbdadm status
```

   Wyjście prawidłowej konfiguracji systemu plików:

```
klfocdata role:Secondary
disk:UpToDate open:no
db2 role:Primary tls:yes
peer-disk:UpToDate

klfocstate role:Secondary
disk:UpToDate open:no
db2 role:Primary tls:yes
peer-disk:UpToDate
```

Zreplikowany system plików na aktywnym węźle klastra jest skonfigurowany. Następnie musisz zainstalować i skonfigurować Corosync i Pacemaker na węzłach klastra.

Instalowanie i konfigurowanie Corosync i Pacemaker na węzłach klastra

Corosync i Pacemaker zapewniają komunikację klastra i zarządzanie zasobami w celu zapewnienia wysokiej dostępności. Zapewniają automatyczne przenoszenie usług do sprawnego węzła w przypadku awarii, minimalizując przestoje.

Aby zainstalować i skonfigurować Corosync i Pacemaker na węzłach klastra:

1. Na obu węzłach klastra zainstaluj wymagane pakiety:

```
dnf install pcs
dnf install drbd-pacemaker
```

2. Skonfiguruj Corosync i Pacemaker na obu węzłach klastra zgodnie z oficjalną dokumentacją. Obejmuje to włączenie automatycznego uruchamiania, generowanie i dystrybucję klucza uwierzytelniającego oraz konfigurowanie uprawnień dostępu do pliku klucza uwierzytelniającego.

   Aby mieć pewność, że ustawienia są prawidłowe, uruchom następujące polecenie na jednym z węzłów klastra:

```
crm status
```

   Oczekiwany wynik powinien pokazywać status klastra i listę wszystkich aktywnych węzłów, potwierdzając, że Corosync działa prawidłowo i że komunikacja między węzłami działa.

3. Na obu węzłach klastra skonfiguruj podstawowe ustawienia klastra Pacemaker:

```
pcs property set stonith-enabled=false
pcs property set symmetric-cluster=false
pcs resource defaults resource-stickiness=110
pcs resource defaults migration-threshold=3
pcs property set no-quorum-policy=ignore
```

4. Na obu węzłach klastra wyłącz uruchamianie skryptów, które będą zarządzane przez Corosync:

```
systemctl disable drbd.service
```

5. Na jednym z węzłów klastra utwórz zasoby oparte na DRBD w Pacemaker.

   - Zasób DRBD dla klfocdata

     a. Utwórz zasób klastra dla woluminu DRBD `klfocdata`, umożliwiając klastrowi automatyczne zarządzanie swoim stanem i monitorowanie jego kondycji:

```
pcs resource create drbd_klfocdata ocf:linbit:drbd \
drbd_resource="klfocdata" \
op monitor interval=60s \
op start interval=0 timeout=240s \
op stop interval=0 timeout=240s \
op monitor role=Master interval=10s \
op monitor role=Slave interval=30s \
```

     b. Utwórz zasób zarządzany przez klaster `ms_drbd_klfocdata` na podstawie utworzonego zasobu `drbd_klfocdata`:

```
pcs resource clone drbd_klfocdata promotable=true
master-max=1
clone-max=2
clone-node-max=1 notify=true
```

c. Utwórz punkt montowania dla woluminu DRBD `fs_klfocdata`, określając urządzenie, katalog docelowy, typ systemu plików i opcje montowania:

```
pcs resource create fs_klfocdata ocf:heartbeat:Filesystem \
device="/dev/drbd0" \
directory="/mnt/KlFocDataShare_klfoc" \
fstype="ext4" \
options="data=journal"
```

- Zasób DRBD dla klfocstate

a. Utwórz zasób klastra dla woluminu DRBD `klfocstate`, umożliwiając klastrowi automatyczne zarządzanie swoim stanem i monitorowanie jego kondycji:

```
pcs resource create drbd_klfocstate ocf:linbit:drbd \
drbd_resource=klfocstate \
op monitor interval=60s \
op start interval=0 timeout=240s \
op stop interval=0 timeout=240s \
op monitor role=Promoted interval=10s \
op monitor role=Unpromoted interval=30s \
```

b. Utwórz zasób zarządzany przez klaster ms_drbd_klfocstate na podstawie utworzonego zasobu `drbd_klfocstate`:

```
pcs resource clone drbd_klfocstate promotable=true \
master-max=1 \
clone-max=2 \
clone-node-max=1 \
notify=true
```

c. Utwórz punkt montowania dla woluminu DRBD `fs_klfocstate`, określając urządzenie, katalog docelowy, typ systemu plików i opcje montowania:

```
pcs resource create fs_klfocstate ocf:heartbeat:Filesystem \
device="/dev/drbd2" \
directory="/mnt/KlFocStateShare_klfoc" \
fstype="ext4" \
options="noatime"
```

6. Na obu węzłach klastra wyłącz automatyczne uruchamianie usługi DRBD:

```
systemctl disable drbd.service
```

Corosync i Pacemaker zostały zainstalowane i skonfigurowane na węzłach klastra. Następnie należy zainstalować system DBMS i utworzyć bazę danych Serwera administracyjnego oraz bazę danych IAM.

Instalowanie i konfigurowanie Platform V Pangolin DBMS

Po zainstalowaniu i skonfigurowaniu Corosync i Pacemaker na węzłach klastra należy zainstalować system DBMS na obu węzłach klastra.

Instalowanie i konfigurowanie systemu DBMS:

1. Na obu węzłach klastra zainstaluj Platform V Pangolin 6.5.1 x64 lub nowszy.

   Informacje o sposobie zainstalowania Platform V Pangolin znajdziesz w tym dokumencie.

2. Upewnij się, że węzły klastra z zainstalowanym systemem DBMS nie mają kont użytkowników DBMS o następujących nazwach:

   - client
   - iam
   - ksc
   - locker
   - pat
   - scope
   - voltron

3. Na aktywnym węźle klastra skopiuj katalog DBMS do katalogu `/mnt/KlFocDataShare_klfoc/dbms`:

```
sudo rsync -av  /pgdata/06/data/ /mnt/KlFocDataShare_klfoc/dbms
sudo mv /pgdata/06/data/ /pgdata/06/data.bk/
```

4. Na obu węzłach klastra otwórz plik konfiguracyjny `/mnt/KlFocDataShare_klfoc/dbms/postgresql.conf`, a następnie ustaw katalog `/mnt/KlFocDataShare_klfoc/dbms` jako katalog danych bazy danych.

   Określ również ścieżki do plików konfiguracyjnych (`/mnt/KlFocDataShare_klfoc/dbms/pg_hba.conf` i `/mnt/KlFocDataShare_klfoc/dbms/pg_ident.conf`) i usuń parametr `include_dir`:

```
data_directory = '/mnt/KlFocDataShare_klfoc/dbms'
hba_file = '/mnt/KlFocDataShare_klfoc/dbms/pg_hba.conf'
ident_file = '/mnt/KlFocDataShare_klfoc/dbms/pg_ident.conf'
listen_addresses = '*'
```

5. W pliku konfiguracyjnym `/mnt/KlFocDataShare_klfoc/dbms/postgresql.conf` dostosuj konfigurację systemu DBMS do wymagań Kaspersky Security Center Linux.

6. Utwórz i skonfiguruj konta do pracy z PostgreSQL.

7. Utwórz zasób usługi DBMS:

```
pcs resource create klfocsvc_dbms pgsql \
pgctl="/usr/pangolin-6.5/bin/pg_ctl"  psql="/usr/bin/psql" pgdata="/mnt/KlFocDataShare_klfoc/dbms"
config="/mnt/KlFocDataShare_klfoc/dbms/postgresql.conf" socketdir="/tmp" \
op start timeout=60s interval=0s \
op stop timeout=60s interval=0s \
op monitor interval=30s timeout=60s \
op promote timeout=120s interval=0s \
op demote timeout=120s interval=0s \
meta target-role=Started
```

8. Na obu węzłach klastra wyłącz automatyczne uruchamianie usługi DBMS:

```
sudo systemctl disable pangolin.service
```

9. Dodaj zasób DBMS `klfocsvc_dbms` do grupy klastra `group_klfoc`:

```
pcs resource group add group_klfoc klfocsvc_dbms
```

10. Dodaj nazwę zasobu DBMS `klfocsvc_dbms` na końcu listy, na przykład:

```
group klfoc_group {
...
klfocsvc_dbms
}
```

11. Na aktywnym węźle klastra, na serwerze DBMS, utwórz bazę danych dla IAM. Nazwa bazy danych musi być inna niż baza danych, którą zainstalowałeś, aby pracować z Kaspersky Security Center Linux. Serwer administracyjny nie usuwa bazy danych IAM automatycznie podczas odinstalowywania lub przenoszenia serwera na inne urządzenie, należy usunąć bazę danych ręcznie:

```
sudo -i -u postgres psql -U postgres -c "CREATE DATABASE <iam_db_name>;"
```

System DBMS został zainstalowany i skonfigurowany. Baza danych Serwera administracyjnego i baza danych IAM zostały utworzone. Następnie należy zainstalować Kaspersky Security Center Linux na węzłach klastra.

Instalowanie Kaspersky Security Center Linux na geograficznie rozproszonych węzłach klastra trybu failover

Kaspersky Security Center Linux jest instalowany na geograficznie rozproszonych węzłach klastra trybu failover przy użyciu pliku odpowiedzi w trybie cichym, czyli bez udziału użytkownika. Plik odpowiedzi zawiera niestandardowy zestaw parametrów instalacji: zmienne i odpowiadające im wartości.

Wymagania wstępne:

- Wykonaj wszystkie kroki przygotowawcze:
  - Przygotowanie system plików węzłów klastra
  - Konfigurowanie zreplikowanego systemu plików klastra
  - Instalowanie i konfigurowanie Corosync i Pacemaker na węzłach klastra
  - Instalowanie i konfigurowanie Platform V Pangolin DBMS
- Upewnij się, że węzły klastra działają na Platform V SberLinux OS Server (SLO) 9.5.1 x64.
- Pobierz plik instalacyjny `ksc64_[version_number]_amd64.deb` ze strony internetowej Kaspersky.

Instalacja na aktywnym węźle

W celu zainstalowania Kaspersky Security Center Linux na aktywnym węźle w trybie cichym:

1. Przeczytaj Umowę licencyjną użytkownika końcowego. Wykonaj poniższe kroki tylko wtedy, gdy rozumiesz i akceptujesz warunki Umowy licencyjnej użytkownika końcowego.

2. Utwórz grupę `kladmins` i nieuprzywilejowane konta `ksc` oraz `ksciam`, które muszą należeć do grupy `kladmins`. Aby to zrobić, uruchom kolejno następujące polecenia na koncie z uprawnieniami roota:

```
adduser ksc
groupadd kladmins
gpasswd -a ksc kladmins
usermod -g kladmins ksc
adduser ksciam
gpasswd -a ksciam kladmins
usermod -g kladmins ksciam
```

3. W katalogu `/mnt/KlFocDataShare_klfoc/` utwórz katalog dla plików Kaspersky Security Center Linux:

```
mkdir /mnt/KlFocDataShare_klfoc/ksc/
```

4. Utwórz plik odpowiedzi (w formacie TXT) i dodaj do pliku odpowiedzi listę zmiennych w formacie VARIABLE_NAME=variable_value, każdą w osobnym wierszu.

   Na liście parametrów używanych do instalacji Kaspersky Security Center Linux w trybie cichym określ następujące parametry wymagane dla wdrożenia geograficznie rozproszonego klastra:

   - `KLFOC_UNATT_EXT_RESOURCE_MANAGEMENT=2`

     Ustaw wartość `2`, aby wdrożyć geograficznie rozproszony klaster.

   - `KLSRV_UNATT_SERVERADDRESS=<DNS balancer address>` i `KLSRV_UNATT_IAM_ADDRESS=<DNS balancer address>`

     Moduł równoważenia DNS z kontrolą kondycji musi być już wdrożony. Wartości tych parametrów muszą być identyczne i ustawione na nazwę FQDN modułu równoważenia DNS.

5. Ustaw wartość zmiennej środowiskowej `KLAUTOANSWERS` w środowisku root lub środowisku użytkownika zawierającej pełną nazwę pliku odpowiedzi wraz ze ścieżką, na przykład za pomocą następującego polecenia:

```
export KLAUTOANSWERS=/tmp/ksc_install/answers.txt
```

6. Uruchom instalację Kaspersky Security Center Linux w trybie cichym, uruchamiając następujące polecenia:

   - W środowisku root:

```
apt-get install /<path>/ksc64_[version_number]_amd64.deb -y
```

   - W środowisku użytkownika:

```
sudo -E apt-get install /<path>/ksc64_[version_number]_amd64.deb -y
```

7. Wyłącz automatyczne uruchamianie usługi klfocsvc_klfoc.service:

```
systemctl disable klfocsvc_klfoc.service
```

8. Po zainstalowaniu Kaspersky Security Center Linux zatrzymaj aktywny węzeł klastra.

9. Przenieś wszystkie zasoby klastra na węzeł pasywny.

   Możesz użyć polecenia `pcs node standby` (i przywrócić za pomocą `pcs node online`).

Instalacja na węźle pasywnym

W celu zainstalowania Kaspersky Security Center Linux na węźle pasywnym:

1. Uruchom instalację Kaspersky Security Center Linux:

```
sudo apt-get install /<path>/ksc64_<version_number>_amd64.deb
```

2. Uruchom konfigurację Kaspersky Security Center Linux:

```
/opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl
```

3. Przeczytaj Umowę Licencyjną Użytkownika Końcowego (EULA) i Politykę prywatności. Tekst jest wyświetlany w oknie wiersza poleceń. Naciśnij spację, aby wyświetlić następny segment tekstu. Następnie po wyświetleniu monitu wprowadź następujące wartości:

   - Wpisz `y`, jeśli rozumiesz i akceptujesz warunki Umowy licencyjnej użytkownika końcowego. Wpisz `n`, jeśli nie akceptujesz warunków Umowy licencyjnej użytkownika końcowego. Aby korzystać z Kaspersky Security Center Linux, musisz zaakceptować warunki Umowy licencyjnej użytkownika końcowego.

   - Wpisz `y`, jeśli rozumiesz i akceptujesz warunki Polityki Prywatności oraz zgadzasz się, że Twoje dane będą przetwarzane i przekazywane (w tym do krajów trzecich) zgodnie z Polityką Prywatności. Wpisz n, jeśli nie akceptujesz warunków Polityki Prywatności. Aby korzystać z Kaspersky Security Center Linux, musisz zaakceptować warunki Polityki prywatności.

4. Wybierz węzeł pasywny klastra jako tryb instalacji Serwera administracyjnego.

5. Po wyświetleniu monitu wprowadź ścieżkę lokalną do punktu montowania dzielenia stanu: `/mnt/KlFocStateShare_klfoc`.

6. Wyłącz automatyczne uruchamianie usługi klfocsvc_klfoc.service:

```
systemctl disable klfocsvc_klfoc.service
```

7. Utwórz zasób usługi `klfocsvc_klfoc`:

```
crm configure primitive klfocsvc_klfoc systemd:klfocsvc_klfoc \
op start timeout="900s" interval="0" \
op stop timeout="900s" interval="0" \
op monitor interval="30s" timeout="90s"
```

8. Dodaj zasób `klfocsvc_klfoc` do grupy `group_klfoc`:

```
pcs resource group add group_klfoc klfocsvc_klfoc
```

9. Dołącz `klfocsvc_klfoc` na końcu wiersza grupy, na przykład:

```
group klfoc_group {
...
klfocsvc_klfoc
}
```

10. Sprawdź, czy wszystkie zasoby są w stanie uruchomienia na aktywnym węźle.

```
pcs status
```

Konfigurowanie szyfrowania między węzłami klastra

Aby skonfigurować szyfrowanie między węzłami klastra,

Jeśli zainstalowano DRBD w wersji 9.2.6 lub nowszej podczas konfigurowania zreplikowanego systemu plików klastra, skonfiguruj szyfrowanie między węzłami klastra zgodnie z oficjalną dokumentacją DRBD.

Alternatywnie, możesz zastosować szyfrowanie ruchu między węzłami klastra, używając własnego rozwiązania VPN.

Geograficznie rozproszony klaster trybu failover Kaspersky Security Center Linux został zainstalowany. Następnie musisz zainstalować Kaspersky Security Center Web Console na obu węzłach klastra.

Instalowanie Kaspersky Security Center Web Console na geograficznie rozproszonych węzłach klastra trybu failover

W przypadku wdrożenia geograficznie rozproszonego klastra trybu failover Kaspersky Security Center Linux, wymagana jest obsługa wysokiej dostępności Kaspersky Security Center Web Console. Aby to osiągnąć, Kaspersky Security Center Web Console musi być zainstalowana na obu węzłach klastra.

W celu zainstalowania Kaspersky Security Center Web Console:

1. Na obu węzłach utwórz użytkownika do pracy z Kaspersky Security Center Web Console. Aby to zrobić, uruchom następujące polecenie na koncie z uprawnieniami roota:

   ```
   /opt/kaspersky/ksc64/sbin/kladduser -n kscadmin -p <password>
   ```

   gdzie hasło musi zawierać co najmniej 8 znaków.

2. Na obu węzłach przeczytaj Umowę licencyjną użytkownika końcowego (EULA). Jeśli pakiet dystrybucyjny Kaspersky Security Center Linux nie zawiera pliku TXT z treścią Umowy licencyjnej użytkownika końcowego, możesz pobrać ten plik ze strony internetowej Kaspersky. Jeśli nie akceptujesz warunków Umowy licencyjnej, nie instaluj aplikacji.

3. Utwórz plik odpowiedzi, który zawiera parametry połączenia Kaspersky Security Center Web Console z Serwerem administracyjnym: `/etc/ksc-web-console-setup.json`.

Przykład pliku odpowiedzi zawierającego minimalny zestaw parametrów

Zestaw parametrów pliku odpowiedzi zależy od wersji Serwera administracyjnego, z którym łączy się Kaspersky Security Center Web Console:

- Serwer administracyjny w wersji 16 lub nowszej

  Przykład pliku odpowiedzi z minimalnym zestawem parametrów do logowania się do Serwera administracyjnego w wersji 16 lub nowszej:

```
{
    "address": "ksc-web-console.example.com",
    "port": 8080,
    "trusted":  {
        "Administration Server v16": {
            "iamHost": "ksc16.example.com",
            "iamOAuthPort": 4444,
            "iamProxyPort": 9050,
            "iamCertPath": "/var/opt/kaspersky/klnagent_srv/iam/main_certificate.pem",
            "iamPATPath": "/var/opt/kaspersky/klnagent_srv/iam/initial_token.txt",
            "kscPort": 13299,
            "kscCertPath": "/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer"
        }
    },
    "certDomain":"ksc-web-console.example.com",
    "acceptEula": true
}
```

- Serwer administracyjny w wersji 15.4 lub starszej

  Przykład pliku odpowiedzi z minimalnym zestawem parametrów do logowania się do Serwera administracyjnego w wersji 15.4 lub starszej:

```
{
    "address": "ksc-web-console.example.com",
    "port": 8080,
    "trusted":  {
         "Administration Server v15.4": {
             "kscHost": "ksc.example.com",
             "kscPort": 13299,
             "kscCertPath": "/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer"
         }
    },
    "certDomain":"ksc-web-console.example.com",
    "acceptEula": true
}
```

Możesz zainstalować Kaspersky Security Center Web Console na tym samym urządzeniu, na którym jest zainstalowany Serwer administracyjny, lub na innym. Jeżeli Kaspersky Security Center Web Console jest zainstalowana na innym urządzeniu, adres Kaspersky Security Center Web Console (określony przez `address`) i adres Serwera administracyjnego (określony przez `iamHost` lub `kscHost`) różnią się. Jeśli Kaspersky Security Center Web Console jest zainstalowana na tym samym urządzeniu co Serwer administracyjny, parametry te mają takie same wartości.

Wartość `iamHost` musi być zgodna z adresem IAM określonym podczas instalacji Serwera administracyjnego. Aby uzyskać określony adres IAM, uruchom następujące polecenie na urządzeniu z zainstalowanym Serwerem administracyjnym:

```
grep "iam_address:" /var/opt/kaspersky/klnagent_srv/iam/iam_config.yaml
```

Szczegółowe informacje można znaleźć w artykule: [Parametry instalacji Kaspersky Security Center Web Console](#).

Do listy zaufanych serwerów można dodać wiele Serwerów administracyjnych o różnych wersjach. W takim przypadku serwery mogą używać różnych metod uwierzytelniania.

Zalecamy określenie numerów portów powyżej 1024. Jeśli chcesz, aby Kaspersky Security Center Web Console działał na portach poniżej 1024, po instalacji musisz upewnić się, że masz narzędzie setcap, a następnie uruchom następujące polecenie:

```
sudo setcap 'cap_net_bind_service=+ep' /var/opt/kaspersky/ksc-web-console/node
```

Jeśli nie masz narzędzia setcap, możesz je zainstalować. **Kliknij ten link, aby wyświetlić polecenia**.

W przypadku systemów operacyjnych Debian i Ubuntu uruchom jedno z następujących poleceń:

- `sudo apt-get install libcap2-bin`
- `sudo apt install libcap2-bin`

W przypadku SUSE Linux Enterprise Server i Red Hat Enterprise Linux uruchom polecenie:

- `sudo zypper install libcap-progs`

4. Na obu węzłach uruchom plik instalacji z poziomu konta z uprawnieniami administratora.

```
sudo apt-get install ksc-web-console-<build number>.x86_64.deb
```

Rozpocznie się wypakowywanie pliku instalacji. Zaczekaj na zakończenie instalacji. Kaspersky Security Center Web Console jest instalowany w następującym katalogu: `/var/opt/kaspersky/ksc-web-console`.

5. Na jednym z węzłów klastra utwórz zasób Pacemaker dla usługi KSCWebConsole, aby uczynić KSCWebConsole usługą zarządzaną przez Pacemaker:

```
crm configure primitive ksc_webconsole systemd:KSCWebConsole \
op monitor interval=30s timeout=60s \
op start timeout=120s \
op stop timeout=120s \
meta target-role=Stopped
```

6. Na obu węzłach zatrzymaj usługę KSCWebConsole i wyłącz jej automatyczne uruchamianie:

```
sudo systemctl stop KSCWebConsole
sudo systemctl disable KSCWebConsole
```

7. Na jednym z węzłów klastra dodaj zasób `ksc_webconsole` do grupy `group_klfoc`:

```
crm configure edit klfoc_group
```

8. Dołącz `ksc_webconsole` na końcu wiersza grupy, po `klfocsvc_dbms`, na przykład:

```
group klfoc_group {
...
klfocsvc_dbms
ksc_webconsole
}
```

Po zakończeniu instalacji możesz użyć przeglądarki internetowej do otwarcia i zalogowania się do Kaspersky Security Center Web Console.

Konta do pracy z DBMS

Aby zainstalować Serwer administracyjny i pracować z nim, potrzebujesz wewnętrznego konta DBMS. To konto umożliwia dostęp do DBMS i wymaga określonych uprawnień. Zestaw wymaganych uprawnień zależy od następujących kryteriów:

- Typ DBMS:
  - MySQL lub MariaDB
  - PostgreSQL lub Postgres Pro
- Metoda tworzenia bazy danych Serwera administracyjnego:
  - **Automatyczne**. Podczas instalacji Serwera administracyjnego możesz automatycznie utworzyć bazę danych Serwera administracyjnego (zwaną dalej także bazą danych Serwera) przy użyciu instalatora Serwera administracyjnego (instalatora).
  - **Ręcznie**. Możesz użyć aplikacji innej firmy lub skryptu, aby utworzyć pustą bazę danych. Następnie możesz określić tę bazę danych jako bazę danych Serwera podczas instalacji Serwera administracyjnego.

Przestrzegaj zasady najmniejszych uprawnień, gdy przyznajesz prawa i uprawnienia do kont. Oznacza to, że przyznane uprawnienia powinny wystarczyć tylko do wykonania wymaganych działań.

Nie wprowadzaj żadnych ręcznych zmian w bazie danych Serwera administracyjnego ani w bazie danych IAM, w tym modyfikacji wartości, usuwania lub dodawania schematów, tabel i indeksów. Wszelkie zmiany w bazach danych niewykonane przez sam Serwer administracyjny zakłócają prawidłowe działanie Serwera administracyjnego albo natychmiast albo później, na przykład po aktualizacji do nowszej wersji lub podczas przywracania z kopii zapasowej itd. Edycja baz danych jest dozwolona wyłącznie po otrzymaniu wyraźnych instrukcji od pomocy technicznej Kaspersky.

Poniższe tabele zawierają informacje o DBMS, które należy nadać kontom przed zainstalowaniem i uruchomieniem Serwera administracyjnego.

MySQL i MariaDB

Jeśli wybierzesz MySQL lub MariaDB jako DBMS, utwórz wewnętrzne konto DBMS, aby uzyskać dostęp do DBMS, a następnie nadaj temu kontu wymagane uprawnienia. Należy pamiętać, że sposób tworzenia bazy danych nie wpływa na zestaw uprawnień. Wymagane uprawnienia są wymienione poniżej:

- Uprawnienia dotyczące schematu:
  - Baza danych Serwera administracyjnego: ALL (oprócz GRANT OPTION).
  - Schematy systemowe (mysql i sys): SELECT, SHOW VIEW.
  - Procedura składowana sys.table_exists: EXECUTE (jeśli używasz MariaDB 10.5 lub wcześniejszej jako DBMS, nie musisz nadawać uprawnienia EXECUTE).
- Globalne uprawnienia dla wszystkich schematów: PROCESS, SUPER.

Aby uzyskać więcej informacji na temat konfigurowania uprawnień konta, zobacz Konfigurowanie konta DBMS do pracy z MySQL i MariaDB.

Szczegółowe informacje na temat przenoszenia danych ze współdzielonej przestrzeni tabel do przestrzeni tabel typu plik-tabela, zobacz Przenoszenie danych ze współdzielonej przestrzeni tabel do przestrzeni tabel typu plik-tabela w systemach DBMS MySQL i MariaDB.

Konfigurowanie uprawnień do odzyskiwania danych Serwera administracyjnego

Uprawnienia nadane wewnętrznemu kontu DBMS wystarczą do przywrócenia danych Serwera administracyjnego z kopii zapasowej.

PostgreSQL lub Postgres Pro

Jeśli wybierzesz PostgreSQL lub Postgres Pro jako DBMS, możesz użyć *użytkownika Postgres* (domyślna rola Postgres) lub utworzyć nową rolę Postgres (zwaną dalej także rolą), aby uzyskać dostęp do DBMS. W zależności od metody tworzenia bazy danych Serwera, nadaj roli wymagane uprawnienia zgodnie z opisem w poniższej tabeli. Aby uzyskać więcej informacji na temat konfigurowania uprawnień roli, zobacz Konfigurowanie konta DBMS do pracy z PostgreSQL lub Postgres Pro.

Uprawnienia roli Postgres

Automatyczne tworzenie bazy danych		Ręczne tworzenie bazy danych
Użytkownik *Postgres* nie wymaga dodatkowych uprawnień.	Uprawnienia nowej roli: CREATEDB.	Do nowej roli: • Uprawnienia w bazie danych Serwera administracyjnego: ALL. • Uprawnienia do wszystkich tabel w schemacie publicznym: ALL. • Uprawnienia do wszystkich sekwencji w schemacie publicznym: ALL.

Używając klastra Postgres o wysokiej dostępności (wersja 14 lub późniejsza) jako bazy danych, użytkownik bazy danych musi mieć uprawnienia `pg_read_all_stats`. Możesz przyznać takie uprawnienie uruchamiając następujące polecenie:

```
GRANT pg_read_all_stats TO "%1";
```

Gdzie `%1` to nazwa użytkownika bazy danych.

Nazwa użytkownika jest określana w trakcie instalacji Serwera administracyjnego w parametrze `KLSRV_UNATT_DBMS_LOGIN`.

Konfigurowanie uprawnień do odzyskiwania danych Serwera administracyjnego

Aby przywrócić dane Serwera administracyjnego z kopii zapasowej, rola Postgres używana do uzyskiwania dostępu do DBMS musi mieć uprawnienia właściciela do bazy danych Serwera administracyjnego.

Konfiguracja konta DBMS do pracy z MySQL i MariaDB

Wymagania wstępne

Przed przypisaniem uprawnień do konta DBMS wykonaj następujące czynności:

1. Upewnij się, że logujesz się do systemu na konto administratora lokalnego.
2. Zainstaluj środowisko do pracy z MySQL lub MariaDB.

> Nie wprowadzaj żadnych ręcznych zmian w bazie danych Serwera administracyjnego ani w bazie danych IAM, w tym modyfikacji wartości, usuwania lub dodawania schematów, tabel i indeksów. Wszelkie zmiany w bazach danych niewykonane przez sam Serwer administracyjny zakłócają prawidłowe działanie Serwera administracyjnego albo natychmiast albo później, na przykład po aktualizacji do nowszej wersji lub podczas przywracania z kopii zapasowej itd. Edycja baz danych jest dozwolona wyłącznie po otrzymaniu wyraźnych instrukcji od pomocy technicznej Kaspersky.

Konfigurowanie konta DBMS do instalacji Serwera administracyjnego

W celu skonfigurowania konta DBMS instalacji Serwera administracyjnego:

1. Uruchom środowisko do pracy z MySQL lub MariaDB na koncie root, które utworzono podczas instalacji DBMS.
2. Utwórz wewnętrzne konto DBMS z hasłem. Instalator Serwera administracyjnego (zwany dalej także instalatorem) oraz usługa Serwera administracyjnego będą używać tego wewnętrznego konta DBMS do uzyskiwania dostępu do DBMS.

   Aby utworzyć konto DBMS z hasłem, wykonaj następujące polecenie:

   ```
   /* Utwórz użytkownika o nazwie kscdbadmin i podaj hasło dla kscdbadmin */
   ```

```
CREATE USER 'kscdbadmin' IDENTIFIED BY '<hasło>';
```

3. Nadaj następujące uprawnienia utworzonemu kontu DBMS:

   - Uprawnienia dotyczące schematu:

     - Baza danych Serwera administracyjnego: ALL (oprócz GRANT OPTION)

     - Schematy systemowe (mysql i sys): SELECT, SHOW VIEW

     - Procedura składowana sys.table_exists: EXECUTE

   - Globalne uprawnienia dla wszystkich schematów: PROCESS, SUPER

   Aby nadać wymagane uprawnienia utworzonemu kontu DBMS, uruchom następujący skrypt:

   ```
   /* Przyznaj uprawnienia kscdbadmin */
   GRANT USAGE ON *.* TO 'kscdbadmin';
   GRANT ALL ON kav.* TO 'kscdbadmin';
   GRANT SELECT, SHOW VIEW ON mysql.* TO 'kscdbadmin';
   GRANT SELECT, SHOW VIEW ON sys.* TO 'kscdbadmin';
   GRANT EXECUTE ON PROCEDURE sys.table_exists TO 'kscdbadmin';
   GRANT PROCESS ON *.* TO 'kscdbadmin';
   GRANT SUPER ON *.* TO 'kscdbadmin';
   ```

   Jeśli używasz MariaDB 10.5 lub wersji starszej jako DBMS, nie musisz nadawać uprawnienia EXECUTE. W takim przypadku wyklucz następujące polecenie ze skryptu: `GRANT EXECUTE ON PROCEDURE sys.table_exists TO 'kscdbadmin'`.

4. Aby wyświetlić listę uprawnień nadanych kontu DBMS, wykonaj następującą komendę:

   ```
   SHOW grants for 'kscdbadmin';
   ```

5. Utwórz konto DBMS dla IAM. Wykonaj następujące polecenie:

   ```
   /* Utwórz użytkownika o nazwie iamdbadmin i podaj hasło dla iamdbadmin */
   CREATE USER 'iamdbadmin' IDENTIFIED BY '<password>';
   ```

   Jeśli używasz MySQL 8.0 lub starszego jako DBMS, pamiętaj, że dla tych wersji uwierzytelnianie „Caching SHA2 password” nie jest obsługiwane. Zmień domyślne uwierzytelnianie z „Caching SHA2 password” na „Native password MySQL”:

   - Aby utworzyć konto DBMS korzystające z uwierzytelniania „Natywne hasło MySQL”, wykonaj następujące polecenie:

     ```
     CREATE USER 'iamdbadmin'@'%' IDENTIFIED WITH mysql_native_password BY '<hasło>';
     ```

   - Aby zmienić uwierzytelnianie dla istniejącego konta DBMS, wykonaj następujące polecenie:

     ```
     ALTER USER 'iamdbadmin'@'%' IDENTIFIED WITH mysql_native_password BY '<hasło>';
     ```

6. Nadaj następujące uprawnienia utworzonemu kontu DBMS:

   - Uprawnienia dotyczące schematu:

     - Baza danych Serwera administracyjnego: ALL (oprócz GRANT OPTION)

     - Schematy systemowe (mysql i sys): SELECT, SHOW VIEW

     - Procedura składowana sys.table_exists: EXECUTE

   - Globalne uprawnienia dla wszystkich schematów: PROCESS, SUPER

   Aby nadać wymagane uprawnienia utworzonemu kontu DBMS, uruchom następujący skrypt:

   ```
   /* Przyznaj uprawnienia iamdbadmin */
   GRANT USAGE ON *.* TO 'iamdbadmin';
   GRANT ALL ON iamdb.* TO 'iamdbadmin';
   GRANT SELECT, SHOW VIEW ON mysql.* TO 'iamdbadmin';
   GRANT SELECT, SHOW VIEW ON sys.* TO 'iamdbadmin';
   GRANT EXECUTE ON PROCEDURE sys.table_exists TO 'iamdbadmin';
   GRANT PROCESS ON *.* TO 'iamdbadmin';
   GRANT SUPER ON *.* TO 'iamdbadmin';
   ```

   Jeśli używasz MariaDB 10.5 lub wersji starszej jako DBMS, nie musisz nadawać uprawnienia EXECUTE. W takim przypadku wyklucz następujące polecenie ze skryptu: `GRANT EXECUTE ON PROCEDURE sys.table_exists TO 'iamdbadmin'`.

7. Aby wyświetlić listę uprawnień nadanych kontu DBMS, wykonaj następującą komendę:

   ```
   SHOW grants for 'iamdbadmin';
   ```

8. Aby ręcznie utworzyć bazę danych Serwera administracyjnego uruchom następujące polecenie (w tym poleceniu nazwa bazy danych Serwera administracyjnego to *kav*):

   ```
   CREATE DATABASE kav
   ```

   Użyj tej samej nazwy bazy danych co określona w skrypcie tworzącym konto DBMS.

9. Aby ręcznie utworzyć bazę danych IAM, uruchom następujący skrypt (w tym poleceniu nazwa bazy danych IAM to *iam*):

   ```
   CREATE DATABASE iam
   ```

   Serwer administracyjny nie usuwa bazy danych IAM automatycznie podczas odinstalowywania lub przenoszenia serwera na inne urządzenie, należy usunąć bazę danych ręcznie.

10. Zainstaluj Serwera administracyjnego.

Po zakończeniu instalacji baza danych Serwera administracyjnego jest tworzona i Serwer administracyjny jest gotowy do użycia.

Konfiguracja konta DBMS do pracy z PostgreSQL i Postgres Pro

Wymagania wstępne

Przed przypisaniem uprawnień do konta DBMS wykonaj następujące czynności:

1. Upewnij się, że logujesz się do systemu na konto administratora lokalnego.
2. Zainstaluj środowisko do pracy z PostgreSQL i Postgres Pro.
3. Konfigurowanie serwera PostgreSQL lub Postgres Pro do pracy z Kaspersky Security Center Linux.

Nie wprowadzaj żadnych ręcznych zmian w bazie danych Serwera administracyjnego ani w bazie danych IAM, w tym modyfikacji wartości, usuwania lub dodawania schematów, tabel i indeksów. Wszelkie zmiany w bazach danych niewykonane przez sam Serwer administracyjny zakłócają prawidłowe działanie Serwera administracyjnego albo natychmiast albo później, na przykład po aktualizacji do nowszej wersji lub podczas przywracania z kopii zapasowej itd. Edycja baz danych jest dozwolona wyłącznie po otrzymaniu wyraźnych instrukcji od pomocy technicznej Kaspersky.

Konfigurowanie konta DBMS do instalacji Serwera administracyjnego

W celu skonfigurowania konta DBMS do instalacji Serwera administracyjnego:

1. Uruchom środowisko do pracy z Postgres.
2. Zaloguj się jako użytkownik *Postgres* w bazie danych *Postgres*.
3. Utwórz nową rolę Postgres (w tym przykładzie jest to rola *kscdbadmin*):

   ```
   CREATE USER "kscdbadmin" WITH PASSWORD '<password>';
   ```

4. Utwórz bazę danych Serwera administracyjnego (w tym przykładzie, nazwa bazy danych Serwera administracyjnego to `kav`):

   ```
   CREATE DATABASE "kav" ENCODING 'UTF8' OWNER "kscdbadmin";
   ```

   Zalecamy określenie roli Postgres utworzonej w kroku 3 tej instrukcji jako właściciela bazy danych (w tym przykładzie jest to rola *kscdbadmin*).

   Określanie innego użytkownika jako właściciela bazy danych

   Jeśli musisz określić inną rolę Postgres, połącz się z bazą danych Serwera administracyjnego przy użyciu roli właściciela (lub superużytkownika) i uruchom następujące polecenia:

   ```
   GRANT ALL PRIVILEGES ON DATABASE "kav" TO "kscdbadmin";
   GRANT USAGE ON SCHEMA public TO "kscdbadmin";
   ```

```
GRANT CREATE ON SCHEMA public TO "kscdbadmin";
GRANT ALL PRIVILEGES ON ALL TABLES IN SCHEMA "public" TO "kscdbadmin";
GRANT ALL PRIVILEGES ON ALL SEQUENCES IN SCHEMA "public" TO "kscdbadmin";
```

Upewnij się, że rola właściciela bazy danych ma uprawnienia CONNECT i TEMPORARY.

> Jeżeli pojawi się błąd „Nowe kodowanie (UTF8) jest niezgodne z kodowaniem bazy szablonów" utwórz bazę danych za pomocą polecenia:
> `CREATE DATABASE "kav" ENCODING 'UTF8' OWNER "kscdbadmin" TEMPLATE template0;`
> zamiast:
> `CREATE DATABASE "kav" ENCODING 'UTF8' OWNER "kscdbadmin";`

5. Utwórz nową rolę Postgres dla IAM (w tym przykładzie jest to rola `iamdbadmin`):

```
CREATE USER "iamdbadmin" WITH PASSWORD '<password>';
```

6. Utwórz bazę danych IAM (w tym przykładzie: nazwa bazy danych IAM to `iam`):

```
CREATE DATABASE "iam" ENCODING 'UTF8' OWNER "iamdbadmin";
```

Zalecamy określenie roli Postgres utworzonej w kroku 5 tej instrukcji jako właściciela bazy danych (w tym przykładzie rolą jest *iamdbadmin*).

Określanie innego użytkownika jako właściciela bazy danych IAM

Jeśli musisz określić inną rolę Postgres, połącz się z bazą danych IAM przy użyciu roli właściciela (lub superużytkownika) i uruchom następujące polecenia:

```
GRANT ALL PRIVILEGES ON DATABASE "iam" TO "iamdbadmin";
GRANT USAGE ON SCHEMA public TO "iamdbadmin";
GRANT CREATE ON SCHEMA public TO "iamdbadmin";
GRANT ALL PRIVILEGES ON ALL TABLES IN SCHEMA "public" TO "iamdbadmin";
GRANT ALL PRIVILEGES ON ALL SEQUENCES IN SCHEMA "public" TO "iamdbadmin";
```

Upewnij się, że rola właściciela bazy danych ma uprawnienia CONNECT i TEMPORARY.

> Jeżeli pojawi się błąd „Nowe kodowanie (UTF8) jest niezgodne z kodowaniem bazy szablonów" utwórz bazę danych za pomocą polecenia:
> `CREATE DATABASE "iam" ENCODING 'UTF8' OWNER "iamdbadmin" TEMPLATE template0;`
> zamiast:
> `CREATE DATABASE "iam" ENCODING 'UTF8' OWNER "iamdbadmin";`

Serwer administracyjny nie usuwa bazy danych IAM automatycznie podczas odinstalowywania lub przenoszenia serwera na inne urządzenie, należy usunąć bazę danych ręcznie.

7. Zainstaluj Serwera administracyjnego.

Po zakończeniu instalacji Serwer administracyjny użyje utworzonej bazy danych do przechowywania danych Serwera administracyjnego. Serwer administracyjny jest gotowy do użycia.

Przenoszenie danych ze współdzielonej przestrzeni tabel do przestrzeni tabel typu plik-tabela w systemach DBMS MySQL lub MariaDB

W przypadku systemów DBMS MySQL i MariaDB dane można przechowywać w następujący sposób:

- Jako współdzielona przestrzeń tabel, gdy dane wszystkich baz danych użytkownika są przechowywane w jednym pliku (zwykle w pliku `ibdata1`).
- Jako przestrzeń tabel typu plik-tabela, gdy dla każdej tabeli tworzona jest oddzielna przestrzeń danych jako oddzielny plik.

Korzystanie ze współdzielonej przestrzeni tabel zwiększa ryzyko fragmentacji przestrzeni tabel. Ponieważ nie da się wykonać operacji `SHRINK`, plik w przestrzeni tabel współdzielonych może zająć około 90% miejsca na dysku. Ma to negatywny wpływ na wydajność podsystemu dyskowego. Dlatego też warto zdecydować się na przestrzeń tabel typu plik-tabela.

W tym artykule opisano sposób przenoszenia danych ze współdzielonej przestrzeni tabel do przestrzeni tabel typu plik-tabela. Jeśli systemy DBMS MySQL lub MariaDB są używane również przez inne aplikacje, należy przenieść bazy danych tych aplikacji do przestrzeni tabel typu plik-tabela.

> Zalecamy wykonywanie tej procedury tylko wtedy, gdy na potrzeby Serwera administracyjnego używany jest system DBMS MySQL lub MariaDB.
> Przeniesienie danych ze współdzielonej przestrzeni tabel do przestrzeni tabel typu plik-tabela może zwiększyć obciążenie podsystemu dyskowego.

Wymagania wstępne

Zanim zaczniesz, upewnij się, że:

- Utworzyłeś kopię zapasową danych Serwera administracyjnego, uruchamiając zadanie tworzenia kopii zapasowej danych lub narzędzie klbackup.
- Utworzyłeś kopię zapasową innych aplikacji, których bazy danych są zarządzane przez system DBMS MySQL lub MariaDB (jeśli dotyczy).
- Na urządzeniu z zainstalowanym systemem DBMS, na partycji z bazą danych, znajduje się wolna przestrzeń dyskowa.

Wymagana ilość miejsca na dysku wynosi 150% bieżącego całkowitego rozmiaru bazy danych (bieżący rozmiar pliku `ibdata1`).

Proces

Aby przenieść dane ze współdzielonej przestrzeni tabel do przestrzeni tabel typu plik-tabela:

1. Zatrzymaj usługę Serwer administracyjny Kaspersky Security Center i inne aplikacje korzystające z instancji systemu DBMS, dla którego chcesz wykonać tę procedurę.

2. Zaloguj się do systemu DBMS jako superużytkownik, a następnie w dowolnej dogodnej aplikacji uruchom skrypt `fix_tablespace.sql`.

   Możesz wyświetlać skrypty `fix_tablespace.sql` klikając te odnośniki:

   Wyświetl skrypt dla MySQL 5.7 i MariaDB 10.1+

```
DROP PROCEDURE IF EXISTS upgd_alter_all_tables_for_all_databases_to_innodb;
DELIMITER //
CREATE PROCEDURE `upgd_alter_all_tables_for_all_databases_to_innodb` ()
BEGIN
    DECLARE __st_FETCH_STATUS INT;
    DECLARE `schemaName` VARCHAR(192);
    DECLARE `tableName` VARCHAR(192);
    DECLARE `curIX` CURSOR FOR
    SELECT `TABLE_SCHEMA` , `TABLE_NAME`
    FROM information_schema.TABLES
    WHERE `TABLE_SCHEMA` NOT IN ('mysql', 'performance_schema', 'sys') AND TABLE_TYPE = 'BASE TABLE';
    DECLARE CONTINUE HANDLER FOR SQLSTATE '02000' SET __st_FETCH_STATUS = 1;
    OPEN `curIX`;
    SET `__st_FETCH_STATUS` = 0; FETCH `curIX` INTO `schemaName`, `tableName`;
    while1 : WHILE (0 = 0 AND __st_FETCH_STATUS = 0 ) DO
        SET @`strSQL` = CONCAT( 'ALTER TABLE `' , `schemaName`, '`.`',`tableName`, '` ENGINE=''InnoDB'';' );
        PREPARE stmt1 FROM @`strSQL`;
        EXECUTE stmt1;
        DEALLOCATE PREPARE stmt1;
        SET `__st_FETCH_STATUS` = 0; FETCH `curIX` INTO `schemaName`, `tableName`;
    END WHILE;
    CLOSE `curIX`;
END
//
DELIMITER ;
SET GLOBAL innodb_file_per_table = 1;
CALL upgd_alter_all_tables_for_all_databases_to_innodb();
DROP PROCEDURE IF EXISTS upgd_alter_all_tables_for_all_databases_to_innodb;
```

   Wyświetl skrypt dla MySQL 8.0+

```
DROP PROCEDURE IF EXISTS upgd_alter_all_tables_for_all_databases_to_innodb;
DELIMITER //
CREATE PROCEDURE `upgd_alter_all_tables_for_all_databases_to_innodb` ()
BEGIN
    DECLARE __st_FETCH_STATUS INT;
    DECLARE `schemaName` VARCHAR(192);
    DECLARE `tableName` VARCHAR(192);
    DECLARE `curIX` CURSOR FOR
    SELECT `TABLE_SCHEMA` , `TABLE_NAME`
    FROM information_schema.TABLES
    WHERE `TABLE_SCHEMA` NOT IN ('mysql', 'performance_schema', 'sys') AND TABLE_TYPE = 'BASE TABLE';
    DECLARE CONTINUE HANDLER FOR SQLSTATE '02000' SET __st_FETCH_STATUS = 1;
    OPEN `curIX`;
    SET `__st_FETCH_STATUS` = 0; FETCH `curIX` INTO `schemaName`, `tableName`;
    while1 : WHILE (0 = 0 AND __st_FETCH_STATUS = 0 ) DO
        SET @`strSQL` = CONCAT( 'ALTER TABLE `' , `schemaName`, '`.`',`tableName`, '` ENGINE=''InnoDB'';' );
        PREPARE stmt1 FROM @`strSQL`;
        EXECUTE stmt1;
        DEALLOCATE PREPARE stmt1;
        SET @`strSQL` = CONCAT( 'ALTER TABLE `' , `schemaName`, '`.`',`tableName`, '` TABLESPACE =
innodb_file_per_table;' );
        PREPARE stmt2 FROM @`strSQL`;
        EXECUTE stmt2;
        DEALLOCATE PREPARE stmt2;
        SET `__st_FETCH_STATUS` = 0; FETCH `curIX` INTO `schemaName`, `tableName`;
    END WHILE;
```

```
    CLOSE `curIX`;
END
//
DELIMITER ;
SET GLOBAL innodb_file_per_table = 1;
CALL upgd_alter_all_tables_for_all_databases_to_innodb();
DROP PROCEDURE IF EXISTS upgd_alter_all_tables_for_all_databases_to_innodb;
```

Nie wolno przerywać wykonywania skryptu.
Jeśli nie wystąpiły błędy DBMS, ale przerwano wykonywanie skryptu, należy uruchomić skrypt ponownie albo przerwać wykonywanie czynności opisanych w tej procedurze, ponownie uruchomić usługę DBMS i przywrócić dane Serwera administracyjnego z kopii zapasowej.

3. W sekcji `[mysqld]` pliku my.cnf ustaw parametr `innodb_file_per_table` na `1`.
4. Uruchom ponownie usługę MySQL lub MariaDB.
5. Uruchom ponownie usługę Serwera administracyjnego Kaspersky Security Center.

Dane są przenoszone ze współdzielonej przestrzeni tabel do przestrzeni tabel typu plik-tabela.

Certyfikaty do pracy z Kaspersky Security Center Linux

Ta sekcja zawiera informacje o certyfikatach Kaspersky Security Center Linux i opisuje sposób wystawiania i zastępowania certyfikatów dla konsoli internetowej Kaspersky Security Center Web Console oraz odnawiania certyfikatu dla serwera administracyjnego, jeśli serwer współpracuje z konsolą internetową Kaspersky Security Center Web Console.

Informacje o certyfikatach Kaspersky Security Center

Kaspersky Security Center używa następujących typów certyfikatów w celu włączenia interakcji między składnikami aplikacji:

- Certyfikatu Serwera administracyjnego
- Certyfikat mobilny
- Certyfikat serwera sieciowego
- Certyfikat Kaspersky Security Center Web Console
- Certyfikat Menedżera tożsamości i dostępu (IAM)

Domyślnie, Kaspersky Security Center używa certyfikatów z podpisem własnym (czyli takich, które zostały opublikowane przez sam program Kaspersky Security Center), ale możesz zastąpić je z certyfikatami niestandardowymi, aby lepiej spełniały wymagania sieci w Twojej organizacji i były zgodne ze standardami bezpieczeństwa. Podczas używania niestandardowego certyfikatu, plik certyfikatu musi zawierać pełny łańcuch kluczy publicznych, w tym wszystkie certyfikaty pośrednie aż do głównego Urzędu Certyfikacji (CA). Po zweryfikowaniu przez Serwer administracyjny, czy certyfikat niestandardowy spełnia wszystkie odpowiednie wymagania, ten certyfikat obejmuje ten sam obszar funkcyjny jak certyfikat z podpisem własnym. Jedyna różnica to taka, że certyfikat niestandardowy nie jest ponownie publikowany automatycznie po wygaśnięciu. Możesz zastąpić certyfikaty certyfikatami niestandardowymi przy użyciu narzędzia klsetsrvcert lub poprzez sekcję Właściwości Serwera administracyjnego w Kaspersky Security Center Web Console, w zależności od typu certyfikatu. Podczas korzystania z narzędzia klsetsrvcert należy określić typ certyfikatu przy użyciu jednej z następujących wartości:

- C – typowy certyfikat dla portów 13000 i 13291
- CR – typowy rezerwowy certyfikat dla portów 13000 i 13291
- M – certyfikat mobilny dla portu 13292
- MR – rezerwowy certyfikat mobilny dla portu 13292
- MCA – mobilny urząd certyfikacji dla automatycznie wygenerowanych certyfikatów użytkowników

Maksymalny okres ważności dowolnego certyfikatu Serwera administracyjnego nie może przekraczać 397 dni.

Certyfikaty Serwera administracyjnego

Certyfikat Serwera administracyjnego jest wymagany do następujących celów:

- Uwierzytelnianie Serwera administracyjnego, gdy łączy się z nim Kaspersky Security Center Web Console.
- Bezpieczna interakcja pomiędzy Serwerem administracyjnym a Agentem sieciowym na zarządzanych urządzeniach.
- Uwierzytelnianie, gdy główne Serwery administracyjne są połączone z podrzędnymi Serwerami administracyjnymi.

Certyfikat Serwera administracyjnego jest tworzony automatycznie w trakcie instalacji modułu Serwera administracyjnego i jest przechowywany w folderze /var/opt/kaspersky/klnagent_srv/1093/cert/. Certyfikat Serwera administracyjnego określasz podczas tworzenia pliku odpowiedzi w celu zainstalowania Kaspersky Security Center Web Console. Ten certyfikat jest nazywany standardowym („C”).

Certyfikat Serwera administracyjnego jest ważny przez 397 dni. Kaspersky Security Center automatycznie generuje wspólny certyfikat rezerwowy („CR”) 90 dni przed wygaśnięciem certyfikatu wspólnego. Wspólny certyfikat rezerwowy jest dalej używany dla bezproblemowego zastąpienia certyfikat Serwera administracyjnego. Jeśli certyfikat standardowy wkrótce wygaśnie, wspólny certyfikat rezerwowy jest używany do zachowania połączenia z instancjami Agenta sieciowego, zainstalowanymi na zarządzanych urządzeniach. Wspólny certyfikat rezerwowy automatycznie staje się nowym certyfikatem standardowym na 24 godziny przed wygaśnięciem starego certyfikatu standardowego.

Maksymalny okres ważności dowolnego certyfikatu Serwera administracyjnego nie może przekraczać 397 dni.

Jeśli to konieczne, możesz przypisać certyfikat innej firmy dla Serwera administracyjnego. Na przykład, to może być konieczne w celu zapewnienia lepszej integracji z istniejącą PKI Twojej firmy lub w celu przeprowadzenia konfiguracji niestandardowej pól certyfikatu. Podczas zamiany certyfikatu, wszystkie Agenty sieciowe, które wcześniej były połączone z Serwerem administracyjnym za pomocą protokołu SSL, utracą połączenie i zwrócą „Błąd autoryzacji Serwera administracyjnego". Aby wyeliminować ten błąd, będziesz musiał przywrócić połączenie po zastąpieniu certyfikatu.

Po zastąpieniu certyfikatu Serwera administracyjnego certyfikatem zapasowym lub niestandardowym określ nowy certyfikat w pliku odpowiedzi, a następnie ponownie zainstaluj Kaspersky Security Center Web Console przy użyciu tego pliku. W przeciwnym razie Kaspersky Security Center Web Console nie będzie mógł nawiązać połączenia z Serwerem administracyjnym.

Jeśli certyfikat Serwera administracyjnego zostanie utracony, aby go odzyskać, musisz ponownie zainstalować moduł Serwera administracyjnego, a następnie przywrócić dane.

Możesz utworzyć kopię zapasową certyfikatu Serwera administracyjnego oddzielnie od innych ustawień Serwera administracyjnego w celu usunięcia Serwera administracyjnego z jednego urządzenia na inne bez utraty danych.

Jeżeli otworzysz Kaspersky Security Center Web Console w różnych przeglądarkach i pobierzesz plik certyfikatu Serwera administracyjnego w oknie właściwości Serwera administracyjnego, pobrane pliki będą miały różne nazwy.

Certyfikaty mobilne

Certyfikat mobilny („M") jest wymagany do autoryzacji Serwera administracyjnego na urządzeniu mobilnym. Certyfikat mobilny należy wskazać we właściwościach Serwera administracyjnego.

Poza tym, dostępny jest zapasowy certyfikat mobilny („MR"): jest on używany dla bezproblemowego zastąpienia certyfikatu mobilnego. Kaspersky Security Center automatycznie generuje ten certyfikat na 60 dni przed wygaśnięciem certyfikatu standardowego. Jeśli certyfikat mobilny wkrótce wygaśnie, zapasowy certyfikat mobilny jest używany do zachowania połączenia z instancjami Agenta sieciowego, zainstalowanymi na zarządzanych urządzeniach mobilnych. Zapasowy certyfikat mobilny automatycznie staje się nowym certyfikatem standardowym na 24 godziny przed wygaśnięciem starego certyfikatu mobilnego.

Jeśli scenariusz połączenia wymaga użycia certyfikatu klienckiego na urządzeniach mobilnych (połączenie obejmujące dwuetapową autoryzację SSL), możesz wygenerować te certyfikaty przy użyciu urzędu certyfikacji dla automatycznie wygenerowanych certyfikatów używanych („MCA"). Poza tym we właściwościach Serwera administracyjnego można wskazać niestandardowe certyfikaty klienckie opublikowane przez inny urząd certyfikacji, podczas gdy integracja z domeną infrastruktury kluczy publicznych (PKI) Twojej organizacji włącza publikację certyfikatów klienckich przy użyciu urzędu certyfikacji domeny.

Ponadto do uwierzytelnienia Serwera administracyjnego na urządzeniach mobilnych z systemem operacyjnym iOS wymagany jest certyfikat serwera iOS MDM. Więcej informacji znajdziesz w artykule Konfigurowanie certyfikatu serwera iOS MDM.

Certyfikat serwera sieciowego

Serwer sieciowy, składnik Serwera administracyjnego Kaspersky Security Center, używa specjalnego typu certyfikatu. Ten certyfikat jest wymagany do publikowania pakietów instalacyjnych Agenta sieciowego, które są następnie pobierane na zarządzane urządzenia, oraz do pakietów instalacyjnych Kaspersky Security for Mobile. W tym celu serwer sieciowy może użyć różnych certyfikatów.

Jeśli obsługa urządzenia mobilnego jest wyłączona, serwer sieciowy używa jednego z następujących certyfikatów w kolejności priorytetów:

1. Niestandardowy certyfikat serwer sieciowy, który określiłeś ręcznie przy użyciu Konsoli administracyjnej
2. Niestandardowy certyfikat Serwera administracyjnego („C")

Jeśli obsługa urządzenia mobilnego jest włączona, serwer sieciowy używa jednego z następujących certyfikatów w kolejności priorytetów:

1. Niestandardowy certyfikat serwer sieciowy, który określiłeś ręcznie przy użyciu Konsoli administracyjnej
2. Niestandardowy certyfikat mobilny
3. Certyfikat mobilny z podpisem własnym („M")
4. Niestandardowy certyfikat Serwera administracyjnego („C")

Certyfikat Kaspersky Security Center Web Console

Serwer Kaspersky Security Center Web Console (zwany dalej Web Console) posiada własny certyfikat. Po otwarciu witryny przeglądarka sprawdza, czy połączenie jest zaufane. Certyfikat Web Console umożliwia uwierzytelnianie Web Console i jest używany do szyfrowania ruchu między przeglądarką a Web Console.

Po otworzeniu Web Console przeglądarka informuje użytkownika, że połączenie z Web Console nie jest prywatne oraz że certyfikat Web Console jest nieprawidłowy. Takie ostrzeżenie pojawia się, ponieważ certyfikat Web Console jest certyfikatem z podpisem własnym i jest automatycznie generowany przez Kaspersky Security Center. Aby usunąć to ostrzeżenie, możesz wykonać jedną z następujących czynności:

- Zastąp certyfikat Web Console certyfikatem niestandardowym (opcja zalecana). Utwórz certyfikat, który jest zaufany w Twojej infrastrukturze i spełnia wymagania certyfikatów niestandardowych.
- Dodaj certyfikat Web Console do listy zaufanych certyfikatów przeglądarki. Zalecamy korzystanie z tej opcji tylko wtedy, gdy nie można utworzyć certyfikatu niestandardowego.

Certyfikat Menedżera tożsamości i dostępu (IAM)

Certyfikat Menedżera tożsamości i dostępu (certyfikat IAM) jest wymagany do następujących celów:

- Uwierzytelniania Serwera administracyjnego, gdy przeglądarka użytkownika łączy się z nim za pomocą protokołu OAuth.
- Uwierzytelnianie Serwera administracyjnego, gdy łączy się z nim Kaspersky Security Center Web Console.

Certyfikat IAM jest tworzony automatycznie przy pierwszym uruchomieniu Serwera administracyjnego. Certyfikat jest przechowywany na urządzeniu Serwera administracyjnego w katalogu: /var/opt/kaspersky/klnagent_srv/iam/main_certificate.pem (dla klastra trybu failover Kaspersky Security Center: <udostępniony folder danych>/iam/main_certificate.pem). Musisz określić ścieżkę do certyfikatu IAM za pomocą parametru `iamCertPath` podczas tworzenia pliku odpowiedzi do instalacji Kaspersky Security Center Web Console.

Certyfikat IAM jest ważny przez 365 dni. Kaspersky Security Center automatycznie generuje certyfikat rezerwowy IAM 48 godzin przed wygaśnięciem bieżącego certyfikatu. Certyfikat rezerwowy jest dalej używany dla bezproblemowego zastąpienia nieważnego certyfikatu IAM.

Maksymalny okres ważności dowolnego certyfikatu IAM nie może przekraczać 397 dni.

W razie potrzeby możesz przypisać niestandardowy certyfikat IAM. Na przykład, to może być konieczne w celu zapewnienia lepszej integracji z istniejącą PKI Twojej firmy lub w celu przeprowadzenia konfiguracji niestandardowej pól certyfikatu.

> Po zastąpieniu certyfikatu IAM certyfikatem zapasowym lub niestandardowym określ nowy certyfikat w pliku odpowiedzi, a następnie zainstaluj ponownie Kaspersky Security Center Web Console przy użyciu tego pliku. W przeciwnym razie Kaspersky Security Center Web Console nie będzie mógł nawiązać połączenia z Serwerem administracyjnym.

Po zalogowaniu się do Kaspersky Security Center Web Console przeglądarka jest przekierowywana na stronę logowania Serwera administracyjnego (https://< `adres Serwera administracyjnego`>:4444) w celu uwierzytelnienia. Ruch pomiędzy przeglądarką a Serwerem administracyjnym jest szyfrowany przy użyciu protokołu TLS i certyfikatu IAM.

Przeglądarka może poinformować, że połączenie z Serwerem administracyjnym nie jest prywatne, a certyfikat IAM jest nieprawidłowy. Takie ostrzeżenie pojawia się, ponieważ certyfikat IAM jest certyfikatem z podpisem własnym i jest automatycznie generowany przez Kaspersky Security Center. Aby usunąć to ostrzeżenie, możesz wykonać jedną z następujących czynności:

- Zastąp certyfikat IAM certyfikatem niestandardowym (opcja zalecana). Utwórz certyfikat, który jest zaufany w Twojej infrastrukturze i spełnia wymagania certyfikatów niestandardowych.
- Dodaj certyfikat IAM do listy zaufanych certyfikatów przeglądarki. Zalecamy korzystanie z tej opcji tylko wtedy, gdy nie można utworzyć certyfikatu niestandardowego.

Wymagania dotyczące niestandardowych certyfikatów stosowanych w Kaspersky Security Center Linux

Poniższa tabela wyświetla wymagania odnośnie niestandardowych certyfikatów określonych dla różnych komponentów Kaspersky Security Center Linux.

Wymagania wobec certyfikatów Kaspersky Security Center Linux

Typ certyfikatu	Wymagania	Komentarze
Wspólny certyfikat, wspólny certyfikat rezerwowy („C", „CR")	Minimalna długość klucza: 2048. Podstawowe ograniczenia: • Ograniczenie długości ścieżki: brak Użycie klucza: • Podpis cyfrowy • Podpisywanie certyfikatów • Szyfrowanie kluczy • Podpisywanie CRL Rozszerzone użycie klucza (opcjonalnie): uwierzytelnianie serwera, uwierzytelnianie klienta. Certyfikat musi zawierać prawidłową Alternatywną nazwę podmiotu (SAN), która zawiera adres pętli zwrotnej Serwera administracyjnego: • Dla IPv4: 127.0.0.1 • Dla IPv6: 0:0:0:0:0:0:0:1	Parametr Rozszerzone użycie klucza jest opcjonalny. Wartość ograniczenia długości ścieżki może być całkowicie inna niż „Brak", ale nie mniejsza niż „1".
Certyfikat serwera sieciowego	Rozszerzone użycie klucza: uwierzytelnianie serwera. Kontener PKCS #12 / PEM, z którego certyfikat jest określony, zawiera cały łańcuch kluczy publicznych. Alternatywna nazwa podmiotu (SAN) certyfikatu jest obecna; czyli wartość pola `subjectAltName` jest ważna. Certyfikat spełnia faktyczne wymagania przeglądarek internetowych nałożone na certyfikaty serwera, a także bieżące podstawowe wymagania CA/Browser Forum.	—
Certyfikat Kaspersky Security Center Web Console	Rozszerzone użycie klucza: uwierzytelnianie serwera, uwierzytelnianie klienta. Kontener PEM, z którego certyfikat jest określony, zawiera cały łańcuch kluczy publicznych. Alternatywna nazwa podmiotu (SAN) certyfikatu jest obecna; czyli wartość pola `subjectAltName` jest ważna. Wartość musi być zgodna z adresem IAM określonym podczas instalacji Serwera administracyjnego. Aby uzyskać określony adres IAM, uruchom następujące polecenie na hoście Serwera administracyjnego: `grep "iam_address:" /var/opt/kaspersky/klnagent_srv/iam/iam_config.yaml` Certyfikat spełnia faktyczne wymagania przeglądarek internetowych nałożone na certyfikaty serwera, a także bieżące podstawowe wymagania CA/Browser Forum.	Zaszyfrowane certyfikaty nie są obsługiwane przez Kaspersky Security Center Web Console.
Certyfikat Menedżera tożsamości i dostępu (certyfikat IAM)	Rozszerzone użycie klucza: uwierzytelnianie serwera. Kontener PEM, z którego certyfikat jest określony, zawiera cały łańcuch kluczy publicznych. Certyfikat musi być ważny i obsługiwać uwierzytelnianie klienta. Certyfikat spełnia faktyczne wymagania przeglądarek internetowych nałożone na certyfikaty serwera, a także bieżące podstawowe wymagania CA/Browser Forum.	Zaszyfrowane certyfikaty nie są obsługiwane przez Kaspersky Security Center Web Console.

Ponowne wystawianie certyfikatu dla Kaspersky Security Center Web Console

Większość przeglądarek nakłada ograniczenie na okres ważności certyfikatu. Okres ważności certyfikatu Kaspersky Security Center Web Console jest ograniczony do 397 dni, aby mógł się zmieścić w nałożonym ograniczeniu. Możesz zastąpić istniejący certyfikat otrzymany z urzędu certyfikacji, ręcznie publikując nowy certyfikat z podpisem własnym. Możesz ponownie opublikować certyfikat Kaspersky Security Center Web Console, który utracił ważność.

Automatyczne ponowne wystawianie certyfikatu dla Kaspersky Security Center Web Console nie jest obsługiwane. Musisz ręcznie wystawić ponownie wygasły certyfikat.

Po otworzeniu Kaspersky Security Center Web Console przeglądarka może poinformować użytkownika, że połączenie z Kaspersky Security Center Web Console nie jest prywatne oraz że certyfikat Kaspersky Security Center Web Console jest nieprawidłowy. Takie ostrzeżenie pojawia się, ponieważ certyfikat Web Console jest certyfikatem z podpisem własnym i jest automatycznie generowany przez Kaspersky Security Center Linux. Aby usunąć to ostrzeżenie, możesz wykonać jedną z następujących czynności:

- Określ certyfikat niestandardowy podczas jego ponownego wystawiania (opcja zalecana). Utwórz certyfikat, który jest zaufany w Twojej infrastrukturze i spełnia wymagania certyfikatów niestandardowych.
- Dodaj certyfikat Kaspersky Security Center Web Console do listy zaufanych certyfikatów przeglądarki po ponownym wystawieniu certyfikatu. Zalecamy korzystanie z tej opcji tylko wtedy, gdy nie można utworzyć certyfikatu niestandardowego.

W celu ponownego opublikowania certyfikatu Kaspersky Security Center Web Console, który utracił ważność:

Zainstaluj ponownie Kaspersky Security Center Web Console, wykonując jedną z następujących czynności:

- Jeśli chcesz użyć tego samego pliku instalacyjnego co Kaspersky Security Center Web Console, usuń Kaspersky Security Center Web Console, a następnie zainstaluj tę samą wersję Kaspersky Security Center Web Console.
- Jeśli chcesz użyć pliku instalacyjnego zaktualizowanej wersji, uruchom polecenie upgrade.

Certyfikat dla Kaspersky Security Center Web Console jest ponownie publikowany dla innego okresu ważności wynoszącego 397 dni.

Zastępowanie certyfikatu dla Kaspersky Security Center Web Console

Domyślnie, gdy instalujesz Kaspersky Security Center Web Console Server (zwany także Kaspersky Security Center Web Console), certyfikat przeglądarki dla aplikacji jest generowany automatycznie. Możesz zastąpić automatycznie wygenerowany certyfikat certyfikatem niestandardowym.

W celu zastąpienia certyfikatu dla Kaspersky Security Center Web Console certyfikatem niestandardowym:

1. Otwórz plik odpowiedzi, który utworzyłeś podczas instalacji Kaspersky Security Center Web Console.

   Jeśli chcesz, możesz utworzyć nowy plik odpowiedzi.

2. W pliku podaj następujące ścieżki:

   - Do pliku niestandardowego certyfikatu Kaspersky Security Center Web Console za pomocą parametru `certPath`

   - Do klucza prywatnego skojarzonego z niestandardowym certyfikatem Kaspersky Security Center Web Console przy użyciu parametru `keyPath`.

     Musisz określić obie ścieżki. W przeciwnym wypadku przeglądarka internetowa będzie Cię informować, że połączenie nie jest prywatne.

3. Zainstaluj ponownie Kaspersky Security Center Web Console, określając nowy plik odpowiedzi. Wykonaj jedną z poniższych czynności:

   - Jeśli chcesz użyć tego samego pliku instalacyjnego co Kaspersky Security Center Web Console, usuń Kaspersky Security Center Web Console, a następnie zainstaluj tę samą wersję Kaspersky Security Center Web Console.

   - Jeśli chcesz użyć pliku instalacyjnego zaktualizowanej wersji, uruchom polecenie upgrade.

Kaspersky Security Center Web Console działa z określonym certyfikatem.

Konwersja certyfikatu PFX do formatu PEM

Aby użyć certyfikatu PFX w Kaspersky Security Center Web Console, musisz najpierw przekonwertować go do formatu PEM za pomocą dowolnego wygodnego narzędzia wieloplatformowego opartego na OpenSSL.

Aby przekonwertować certyfikat PFX na format PEM w systemie operacyjnym Linux:

1. W wieloplatformowym narzędziu opartym na OpenSSL wykonaj następujące polecenia:

   ```
   openssl pkcs12 -in <nazwapliku.pfx> -clcerts -nokeys | sed -ne '/-BEGIN CERTIFICATE-/,/-END CERTIFICATE-/p' > server.crt
   ```

   ```
   openssl pkcs12 -in <nazwapliku.pfx> -nocerts -nodes | sed -ne '/-BEGIN PRIVATE KEY-/,/-END PRIVATE KEY-/p' > key.pem
   ```

2. Upewnij się, że plik certyfikatu i klucz prywatny są generowane w tym samym katalogu, w którym przechowywany jest plik .pfx.

3. Kaspersky Security Center Web Console nie obsługuje certyfikatów chronionych hasłem. Dlatego uruchom następujące polecenie w wieloplatformowym narzędziu opartym na OpenSSL, aby usunąć hasło z pliku .pem:

   ```
   openssl rsa -in key.pem -out key-without-passphrase.pem
   ```

   Nie używaj tej samej nazwy dla wejściowych i wyjściowych plików .pem.

   W rezultacie nowy plik .pem jest niezaszyfrowany. Nie musisz wpisywać hasła, aby z niego skorzystać.

Pliki .crt i .pem są gotowe do użycia, więc możesz je określić w instalatorze Kaspersky Security Center Web Console.

Scenariusz: Określanie niestandardowego certyfikatu Serwera administracyjnego

Możesz przypisać niestandardowy certyfikat Serwera administracyjnego, na przykład, w celu lepszej integracji z istniejącą infrastrukturą kluczy publicznych (PKI) przedsiębiorstwa lub w celu niestandardowej konfiguracji pól certyfikatu. Dobrym rozwiązaniem jest zastąpienie certyfikatu natychmiast po zainstalowaniu Serwera administracyjnego, a przed zakończeniem działania kreatora wstępnej konfiguracji.

Maksymalny okres ważności dowolnego certyfikatu Serwera administracyjnego nie może przekraczać 397 dni.

Wymagania wstępne

Muszą być spełnione następujące warunki:

- Nowy certyfikat musi zostać utworzony w formacie PKCS#12 (na przykład za pomocą infrastruktury klucza publicznego (PKI) organizacji).
- W przypadku nowego certyfikatu należy spełnić wymagania wymienione w poniższej tabeli.

  W poniższej tabeli zwróć uwagę na wymaganie „CA: true", które oznacza, że nowy certyfikat musi zostać wydany przez zaufany urząd certyfikacji (CA). Nowy certyfikat z wymaganiem „CA: true", musi zawierać cały łańcuch zaufania oraz klucz prywatny, który musi być przechowywany w pliku z rozszerzeniem pfx lub p12.

Wymagania dotyczące certyfikatów Serwera administracyjnego

Typ certyfikatu	Wymagania
Certyfikat standardowy, standardowy certyfikat zapasowy („C", „CR")	Minimalna długość klucza: 2048. Podstawowe ograniczenia: • Ograniczenie długości ścieżki: brak Wartość ograniczenia długości ścieżki może być całkowicie inna niż „Brak", ale nie mniejsza niż „1". Użycie klucza: • Podpis cyfrowy • Podpisywanie certyfikatów • Szyfrowanie klucza • Podpisywanie CRL Rozszerzone użycie klucza (EKU): uwierzytelnianie serwera i uwierzytelnianie klienta. Jednostka EKU jest opcjonalna, ale jeśli zawiera ją certyfikat, dane uwierzytelniania serwera i klienta muszą być określone w jednostce EKU. Certyfikat musi zawierać prawidłową Alternatywną nazwę podmiotu (SAN), która zawiera adres pętli zwrotnej Serwera administracyjnego: • Dla IPv4: 127.0.0.1 • Dla IPv6: 0:0:0:0:0:0:0:1

Typ certyfikatu	Wymagania
Certyfikat mobilny, zapasowy certyfikat mobilny („M", „MR")	Minimalna długość klucza: 2048. Podstawowe ograniczenia: • Urząd certyfikacji (CA): prawda • Ograniczenie długości ścieżki: brak Wartość ograniczenia długości ścieżki może być całkowicie inna niż „Brak", jeśli standardowy certyfikat ma wartość ograniczenia długości ścieżki nie mniejszą niż 1. Użycie klucza: • Podpis cyfrowy • Podpisywanie certyfikatów • Szyfrowanie klucza • Podpisywanie CRL Rozszerzone użycie klucza (EKU): uwierzytelnianie serwera. Jednostka EKU jest opcjonalna, ale jeśli zawiera ją certyfikat, dane uwierzytelniania serwera muszą być określone w jednostce EKU.
Certyfikat Urzędu certyfikacji (CA) dla automatycznie generowanych certyfikatów użytkowników („MCA")	Minimalna długość klucza: 2048. Podstawowe ograniczenia: • Urząd certyfikacji (CA): prawda • Ograniczenie długości ścieżki: brak Wartość ograniczenia długości ścieżki może być całkowicie inna niż „Brak", jeśli Standardowy certyfikat ma wartość ograniczenia długości ścieżki nie mniejszą niż 1. Użycie klucza: • Podpis cyfrowy • Podpisywanie certyfikatów • Szyfrowanie klucza • Podpisywanie CRL Rozszerzone użycie klucza (EKU): uwierzytelnianie klienta. Jednostka EKU jest opcjonalna, ale jeśli zawiera ją certyfikat, dane uwierzytelniania klienta muszą być określone w jednostce EKU.

Certyfikaty wystawione przez publiczny urząd certyfikacji nie mają uprawnień do podpisywania certyfikatów. Aby korzystać z takich certyfikatów, upewnij się, że zainstalowałeś Agenta sieciowego w wersji 13 lub nowszej w punktach dystrybucji lub bramach połączeń w swojej sieci. W przeciwnym razie nie będziesz mógł korzystać z certyfikatów bez pozwolenia na podpisywanie.

Etapy

Określanie certyfikatu Serwera administracyjnego odbywa się w etapach:

1. **Zastępowanie certyfikatu Serwera administracyjnego**

   W tym celu użyj polecenia narzędzie klsetsrvcert.

2. **Określanie nowego certyfikatu i przywracanie połączenia Agentów sieciowych z Serwerem administracyjnym**

   Podczas zamiany certyfikatu, wszystkie Agenty sieciowe, które wcześniej były połączone z Serwerem administracyjnym za pomocą protokołu SSL, utracą połączenie i zwrócą „Błąd autoryzacji Serwera administracyjnego". Aby określić nowy certyfikat i przywrócić połączenie, użyj polecenia narzędzia klmover.

3. **Określenie nowego certyfikatu w ustawieniach Kaspersky Security Center Web Console**

   Po zastąpieniu certyfikatu należy go określić w pliku odpowiedzi, a następnie zaktualizować Kaspersky Security Center Web Console przy użyciu tego pliku. W przeciwnym razie Kaspersky Security Center Web Console nie będzie mógł nawiązać połączenia z Serwerem administracyjnym.

Wyniki

Po zakończeniu scenariusza, certyfikat Serwera administracyjnego jest zastępowany i serwer zostaje uwierzytelniony przez Agentów sieciowych na zarządzanych urządzeniach.

Zastępowanie certyfikatu Serwera administracyjnego za pomocą narzędzia klsetsrvcert

Aby uniknąć utraty kontroli nad urządzeniami, przed kontynuowaniem zapoznaj się ze Scenariuszem: Określanie niestandardowego certyfikatu serwera administracyjnego.

W celu zastąpienia certyfikatu Serwera administracyjnego:

W wierszu polecenia uruchom następujące narzędzie:

```
/opt/kaspersky/ksc64/sbin/klsetsrvcert [-t <certificate type> {-i <path to new certificate> [-p <password>] [-o
<validation parameters>] | -g <dns name>}][-f <replacement time>][-r <root certificates>][-l <log file path>]
```

Opis parametrów narzędzia klsetsrvcert przedstawia poniższa tabela.

Wartości parametrów narzędzia klsetsrvcert

Parametr	Wartość
`-t < typ certyfikatu >`	Typ zastępowanego certyfikatu. Możliwe wartości parametru `< typ certyfikatu >` to: • `C` – zastępuje certyfikat standardowy dla portów 13000 i 13291. • `CR` – zastępuje zapasowy certyfikat standardowy dla portów 13000 i 13291.
`-f < czas zastąpienia >`	Terminarz zmiany certyfikatu w formacie „DD-MM-YYYY hh:mm" (dla portów: 13000 i 13291). Użyj tego parametru, jeśli chcesz zastąpić certyfikat standardowy zapasowym certyfikatem standardowym przed wygaśnięciem certyfikatu standardowego. Określ czas, w którym zarządzane urządzenia muszą synchronizować się z Serwerem administracyjnym na nowym certyfikacie.
`-i < ścieżka do nowego certyfikatu >`	Kontener z certyfikatem i kluczem prywatnym w formacie PKCS#12 (plik z rozszerzeniem .p12 lub .pfx).
`-p < hasło >`	Hasło używane do ochrony kontenera p12. Certyfikat i klucz prywatny są przechowywane w kontenerze, dlatego do odszyfrowania pliku z kontenerem wymagane jest hasło.
`-o < parametry walidacji >`	Parametry legalizacji certyfikatu (oddzielone średnikiem). Aby użyć certyfikatu niestandardowego bez uprawnień do podpisywania, określ `-o NoCA` w narzędziu klsetsrvcert. Jest to przydatne w przypadku certyfikatów wydanych przez publiczny urząd certyfikacji. Aby zmienić długość klucza szyfrowania dla certyfikatów typu C lub CR, w narzędziu klsetsrvcert określ parametr `-o RsaKeyLen:< długość klucza >`, gdzie parametr `< długość klucza >` jest wymaganą wartością długości klucza. W przeciwnym razie używana jest bieżąca długość klucza certyfikatu.
`-g < nazwa DNS >`	Zostanie utworzony nowy certyfikat dla określonej nazwy DNS (nazwa wspólna i alternatywna nazwa podmiotu).
`-r < certyfikaty główne >`	Lista zaufanych urzędów certyfikacji w formacie PEM.
`-l < ścieżka do pliku dziennika >`	Zapisuje dane wynikowe. Domyślnie dane wynikowe są przekierowywane do standardowego strumienia wyjściowego.

Na przykład, aby określić niestandardowy certyfikat Serwera administracyjnego, użyj następującego polecenia:

```
klsetsrvcert -t C -i <ścieżka do nowego certyfikatu> -p <hasło> -o NoCA
```

Po zastąpieniu certyfikatu wszystkie Agenty sieciowe połączone z Serwerem administracyjnym przez SSL tracą połączenie. Aby je przywrócić, użyj polecenia narzędzia klmover.

Aby uniknąć utraty połączeń z Agentami sieciowymi, użyj następującego polecenia:

1. Aby zainstalować nowy certyfikat,

   ```
   klsetsrvcert -t CR -i <ścieżka do nowego certyfikatu> -p <hasło> -o NoCA
   ```

2. Aby określić datę stosowania nowego certyfikatu,

   ```
   klsetsrvcert -f "DD-MM-YYYY hh:mm"
   ```

gdzie „`DD-MM-YYYY hh:mm`" to data 3–4 tygodnie po dacie bieżącej. Przesunięcie czasowe zmiany certyfikatu na nowy pozwoli na rozesłanie nowego certyfikatu do wszystkich Agentów sieciowych.

Pytania i odpowiedzi

Jakie dodatkowe kroki są wymagane po zastąpieniu wspólnego certyfikatu Serwera administracyjnego?

1. Upewnij się, że **spełnione są wymagania dotyczące certyfikatów niestandardowych**.

   Jeśli używasz certyfikatu niestandardowego zamiast certyfikatu z podpisem własnym, przed aktualizacją Kaspersky Security Center Linux do nowszej wersji upewnij się, że certyfikat zawiera Alternatywną nazwę podmiotu (SAN). Jeżeli nie zawiera, ważne jest, aby wymienić certyfikat przed aktualizacją Kaspersky Security Center Linux. W przeciwnym razie nie będziesz mógł zalogować się do Web Console po aktualizacji.

   Aby upewnić się, że certyfikat zawiera Alternatywną nazwę podmiotu (SAN):

   1. Na urządzeniu z zainstalowanym Serwerem administracyjnym, wykonaj następujące polecenie:

      - W przypadku urządzenia z systemem Linux:

        ```
        sudo openssl x509 -in /var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer -noout -ext subjectAltName
        ```

      - W przypadku urządzenia z systemem Windows:

        ```
        certutil -dump %ProgramData%\KasperskyLab\adminkit\1093\cert\klserver.cer
        ```

   2. Upewnij się, że Alternatywna nazwa podmiotu jest obecna w wynikach polecenia i zawiera adres urządzenia Serwera administracyjnego.

   3. Jeśli Alternatywna nazwa podmiotu jest niedostępna, użyj narzędzia klsetsrvcert, aby zastąpić certyfikat niestandardowy tym, który spełnia wymagania.

2. Upewnij się, że plik konfiguracyjny Serwera IAM zawiera aktualny adres Serwera administracyjnego. Jeśli nie, dodaj adres do pliku konfiguracyjnego.

3. Zainstaluj ponownie Web Console, aby uniknąć następującego błędu:

   Serwer administracyjny używa niezaufanego certyfikatu. Skonfiguruj ponownie aplikację, określając prawidłowy certyfikat lub skontaktuj się z głównym administratorem.

Podłączanie Agentów sieciowych do Serwera administracyjnego przy użyciu narzędzia klmover

Użyj narzędzia klmover, aby przywrócić połączenie z niekontrolowanych urządzeń do Serwera administracyjnego, na przykład po awarii Serwera administracyjnego, jeśli nie jest możliwe przywrócenie z kopii zapasowej.

Aby przywrócić połączenie, uruchom narzędzie klmover z wiersza poleceń:

- Dla systemu Linux:
  - Dla systemów 32-bitowych: `/opt/kaspersky/klnagent/bin/klmover [-address <adres serwera>] [-pn <numer portu>] [-ps <numer portu SSL>] [-nossl] [-cert <ścieżka pliku certyfikacji>]`
  - Dla systemów 64-bitowych: `/opt/kaspersky/klnagent64/bin/klmover [-address <adres serwera>] [-pn <numer portu>] [-ps <numer portu SSL>] [-nossl] [-cert <ścieżka pliku certyfikacji>]`
- Dla systemu Windows:
  - Dla systemów 32-bitowych: `<ścieżka>\klmover.exe [-address <adres serwera>] [-pn <numer portu>] [-ps <numer portu SSL>] [-nossl] [-cert <ścieżka pliku certyfikacji>]`
  - Dla systemów 64-bitowych: `<ścieżka>\klmover.exe [-address <adres serwera>] [-pn <numer portu>] [-ps <numer portu SSL>] [-nossl] [-cert <ścieżka pliku certyfikacji>]`
- W przypadku macOS:

  `/Library/Application Support/Kaspersky Lab/klnagent/Binaries/klmover [-address <adres serwera>] [-pn <numer portu>] [-ps <numer portu SSL>] [-nossl] [-cert <ścieżka pliku certyfikacji>]`

gdzie `<ścieżka>` to domyślna ścieżka instalacji Agenta sieciowego lub ścieżka instalacji określona przez Ciebie w ustawieniach pakietu instalacyjnego Agenta sieciowego.

Aby uniemożliwić intruzom przeniesienie urządzeń poza Serwer administracyjny kontrolujący, zdecydowanie zalecamy włączenie ochrony hasłem podczas uruchamiania narzędzia klmover. Aby włączyć ochronę hasłem, wybierz opcję **Użyj hasła dezinstalacyjnego** w ustawieniach zasady Agenta sieciowego.

> Jeśli zgubisz lub zapomnisz hasła do chronionego hasłem Agenta sieciowego zainstalowanego na urządzeniu, które nie jest już zarządzane przez Kaspersky Security Center Linux, nie będziesz mógł usunąć Agenta sieciowego przy użyciu narzędzia klmover ani wiersza poleceń. W takim przypadku należy ponownie zainstalować system operacyjny na urządzeniu z zainstalowanym Agentem sieciowym chronionym hasłem.

Narzędzie klmover wymaga uprawnień administratora lokalnego.

Włączenie opcji **Użyj hasła dezinstalacyjnego** na urządzeniach Windows umożliwia również ochronę hasłem narzędzia Cleaner (cleaner.exe).

Narzędzia klmover nie można używać w przypadku urządzeń klienckich podłączonych do Serwera administracyjnego poprzez bramy połączeń. W przypadku takich urządzeń należy albo ponownie skonfigurować Agenta sieciowego, albo ponownie zainstalować Agenta sieciowego i określić bramę połączenia.

Opis parametrów narzędzia klmover przedstawia poniższa tabela.

Wartości parametrów narzędzia klmover

Parametr	Wartość
`-address < adres serwera >`	Adres Serwera administracyjnego do nawiązania połączenia. Można określić adres IP lub nazwę DNS.
`-pn < numer portu >`	Numer portu użytego do nawiązania nieszyfrowanego połączenia z Serwerem administracyjnym. Domyślny numer portu to 14000.
`-ps < numer portu SSL >`	Numer portu SSL, przez który nawiązywane jest połączenie szyfrowane z Serwerem administracyjnym (przy użyciu protokołu SSL). Domyślny numer portu to 13000.
`-nossl`	Użycie nieszyfrowanego połączenia z Serwerem administracyjnym. Jeżeli klucz ten nie zostanie użyty, Agent sieciowy nawiąże z Serwerem administracyjnym połączenie szyfrowane przy użyciu szyfrowanego protokołu SSL.
`-cert < ścieżka do pliku certyfikatu >`	Użycie określonego pliku certyfikatu do autoryzacji podczas uzyskiwania dostępu do Serwera administracyjnego.
`-nauninstpwd < hasło >`	Użyj tego parametru, aby określić hasło dezinstalacyjne Agenta sieciowego. Parametr nie jest obowiązkowy.

Ponowne wystawianie certyfikatu serwera sieciowego

Certyfikat serwera sieciowego używany w Kaspersky Security Center Linux jest wymagany do publikowania pakietów instalacyjnych Agenta sieciowego, które są następnie pobierane na zarządzane urządzenia, a także do publikowania profili iOS MDM, aplikacji iOS oraz pakietów instalacyjnych Kaspersky Endpoint Security for Mobile. W zależności od bieżącej konfiguracji aplikacji różne certyfikaty mogą funkcjonować jako certyfikat serwera sieciowego (aby uzyskać więcej informacji, zobacz Informacje o certyfikatach Kaspersky Security Center Linux).

Ponowne wystawienie certyfikatu serwera sieciowego może być konieczne w celu spełnienia określonych wymagań bezpieczeństwa organizacji lub utrzymania ciągłego połączenia z zarządzanymi urządzeniami przed rozpoczęciem aktualizacji aplikacji. Kaspersky Security Center Linux zapewnia dwa sposoby ponownego wystawienia certyfikatu serwera sieciowego. Wybór między tymi dwiema metodami zależy od tego, czy masz podłączone urządzenia mobilne i zarządzane za pośrednictwem protokołu mobilnego (tj. przy użyciu certyfikatu mobilnego).

Jeśli nigdy nie określono własnego certyfikatu niestandardowego jako certyfikatu serwera sieciowego w sekcji **Serwer WWW** właściwości Serwera administracyjnego, certyfikat mobilny działa jako certyfikat serwera sieciowego. W tym przypadku ponowne wystawienie certyfikatu serwera sieciowego odbywa się poprzez ponowne wystawienie samego protokołu mobilnego.

Aby ponownie wystawić certyfikat serwera sieciowego, gdy masz jakiekolwiek urządzenia mobilne zarządzane za pośrednictwem protokołu mobilnego:

1. Wygeneruj swój certyfikat niestandardowy i przygotuj go do użycia w Kaspersky Security Center Linux. Sprawdź, czy Twój certyfikat niestandardowy spełnia wymagania Kaspersky Security Center Linux. W razie potrzeby zmodyfikuj certyfikat.

2. W menu głównym kliknij nazwę Serwera administracyjnego.

   Zostanie otwarte okno właściwości Serwera administracyjnego.

3. Na zakładce **Ogólne** wybierz sekcję **Serwer WWW**.

4. W podsekcji **Przez HTTP** zaznacz opcję **Prześlij certyfikat z pliku** i kliknij przycisk **Zmień certyfikat**.

5. W otwartym oknie, w polu **Format certyfikatu** wybierz typ swojego certyfikatu:

   - Jeśli został wybrany typ **Kontener PKCS #12**, kliknij przycisk **Przeglądaj** obok pola **Certyfikat** i określ plik certyfikatu na dysku twardym. Jeśli plik certyfikatu jest chroniony hasłem, wprowadź hasło w polu **Hasło**.

   - Jeśli został wybrany typ **Certyfikat X.509**, kliknij przycisk **Przeglądaj** obok pola **Klucz prywatny** i określ klucz prywatny na dysku twardym. Jeśli klucz prywatny jest chroniony hasłem, wprowadź hasło w polu **Hasło**.

6. Kliknij przycisk **Zapisz**, a następnie kliknij **OK**.

   Okno jest zamknięte.

7. Jeśli to konieczne, w polu **Port HTTPS serwera WWW** zmień numer portu HTTPS dla serwera WWW i kliknij przycisk **Zapisz**.

Certyfikat serwera sieciowego został ponownie wystawiony.

Aby ponownie wystawić certyfikat serwera sieciowego, gdy nie masz żadnych urządzeń mobilnych zarządzanych za pośrednictwem protokołu mobilnego:

1. W menu głównym kliknij nazwę Serwera administracyjnego.

   Zostanie otwarte okno właściwości Serwera administracyjnego.

2. Na zakładce **Ogólne** wybierz sekcję **Certyfikaty**.

3. Jeśli planujesz nadal używać certyfikatu wystawionego przez Kaspersky Security Center, wykonaj następujące czynności:

   a. Wybierz opcję **Certyfikat wydany przez Serwer administracyjny** i kliknij przycisk **Przeglądaj**.

   b. W otwartym oknie, w grupach ustawień **Adres połączenia** i **Czas aktywacji** wybierz odpowiednie opcje i kliknij przycisk **OK**.

Alternatywnie, jeśli planujesz używać własnego certyfikatu niestandardowego, wykonaj następujące czynności:

a. Sprawdź, czy Twój certyfikat niestandardowy spełnia wymagania Kaspersky Security Center Linux. W razie potrzeby zmodyfikuj certyfikat.

b. Wybierz opcję **Inny certyfikat**, kliknij przycisk **Zarządzaj certyfikatami**, a następnie w oknie, które zostanie otwarte, kliknij przycisk **Przeglądaj**.

c. W otwartym oknie, w polu **Format certyfikatu** wybierz typ swojego certyfikatu:

- Jeśli został wybrany typ **Kontener PKCS #12**, kliknij przycisk **Przeglądaj** obok pola **Certyfikat** i określ plik certyfikatu na dysku twardym. Jeśli plik certyfikatu jest chroniony hasłem, wprowadź hasło w polu **Hasło**.
- Jeśli został wybrany typ **Certyfikat X.509**, kliknij przycisk **Przeglądaj** obok pola **Klucz prywatny** i określ klucz prywatny na dysku twardym. Jeśli klucz prywatny jest chroniony hasłem, wprowadź hasło w polu **Hasło**.

d. Kliknij przycisk **Zapisz**, a następnie kliknij **OK**.

Certyfikat mobilny został ponownie wystawiony w celu używania go jako certyfikat serwera sieciowego.

Zmiana domyślnego certyfikatu IAM na niestandardowy

Aby zmienić domyślny certyfikat IAM:

1. Wygeneruj swój certyfikat niestandardowy i przygotuj go do użycia w Kaspersky Security Center Linux. Sprawdź, czy Twój certyfikat niestandardowy spełnia wymagania Kaspersky Security Center Linux.
2. Upewnij się, że grupa kladmins ma dostęp do plików certyfikatu IAM.
3. Zlokalizuj plik konfiguracyjny IAM: `/var/opt/kaspersky/klnagent_srv/iam/iam_config.yaml`

   W tym pliku dodaj ścieżki do plików certyfikatów IAM do sekcji `server_iam`:

   - `certificates.main.cert`: Ścieżka do pliku certyfikatu podstawowego.
   - `certificates.main.key`: Ścieżka do klucza prywatnego certyfikatu podstawowego. Klucz prywatny nie może być chroniony hasłem.
4. Znajdź plik konfiguracyjny Web Console: `/etc/ksc-web-console-setup.json`

   W tym pliku ustaw wartość pola `iamCertPath` na ścieżkę do klucza publicznego certyfikatu podstawowego.
5. Uruchom ponownie usługę kliam, wykonując następujące polecenie:

   ```
   sudo service kliam_srv restart
   ```
6. Zainstaluj ponownie Web Console.

   Po ponownej instalacji Web Console używa niestandardowego certyfikatu IAM.

Aby zmienić certyfikat rezerwowy IAM:

1. Zlokalizuj plik konfiguracyjny IAM: `/var/opt/kaspersky/klnagent_srv/iam/iam_config.yaml`

   W tym pliku określ ścieżki do plików certyfikatu IAM:

   - `server_iam.certificates.reserve.cert`: Ścieżka do pliku certyfikatu podstawowego.
   - `server_iam.certificates.reserve.key`: Ścieżka do klucza prywatnego certyfikatu podstawowego. Klucz prywatny nie może być chroniony hasłem.
2. Uruchom ponownie usługę kliam, wykonując następujące polecenie:

   ```
   sudo systemctl restart kliam_srv.service
   ```

   Po wygaśnięciu pliku certyfikatu podstawowego używany jest certyfikat rezerwowy IAM.

Dodawanie adresu Serwera Administracyjnego do konfiguracji Serwera IAM

Po zmianie standardowego certyfikatu Serwera administracyjnego („C") podczas aktualizacji, przeniesienia lub migracji należy określić adres Serwera administracyjnego w pliku konfiguracyjnym serwera IAM, aby zapewnić poprawną walidację certyfikatu między serwerem IAM a Serwerem administracyjnym.

Aby dodać adres Serwera administracyjnego do konfiguracji serwera IAM:

1. Pobierz wartość Alternatywnej nazwy podmiotu (SAN) ze standardowego certyfikatu Serwera administracyjnego („C"), wykonując następujące polecenie:

```
sudo openssl x509 -in /var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer -noout -ext subjectAltName
```

2. W zależności od wyniku polecenia, wykonaj jedną z następujących czynności:

   - Jeśli wynik wskazuje na brak wartości, sprawdź **wymagania dotyczące certyfikatu niestandardowego**.

     Jeśli używasz certyfikatu niestandardowego zamiast certyfikatu z podpisem własnym, przed aktualizacją Kaspersky Security Center Linux do nowszej wersji upewnij się, że certyfikat zawiera Alternatywną nazwę podmiotu (SAN). Jeżeli nie zawiera, ważne jest, aby wymienić certyfikat przed aktualizacją Kaspersky Security Center Linux. W przeciwnym razie nie będziesz mógł zalogować się do Web Console po aktualizacji.

     Aby upewnić się, że certyfikat zawiera Alternatywną nazwę podmiotu (SAN):

     1. Na urządzeniu z zainstalowanym Serwerem administracyjnym, wykonaj następujące polecenie:

        - W przypadku urządzenia z systemem Linux:

          ```
          sudo openssl x509 -in /var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer -noout -ext subjectAltName
          ```

        - W przypadku urządzenia z systemem Windows:

          ```
          certutil -dump %ProgramData%\KasperskyLab\adminkit\1093\cert\klserver.cer
          ```

     2. Upewnij się, że Alternatywna nazwa podmiotu jest obecna w wynikach polecenia i zawiera adres urządzenia Serwera administracyjnego.

     3. Jeśli Alternatywna nazwa podmiotu jest niedostępna, użyj narzędzia klsetsrvcert, aby zastąpić certyfikat niestandardowy tym, który spełnia wymagania.

     Jeśli nie spełnia wymagań, zastąp standardowy certyfikat Serwera administracyjnego na poprzednim Serwerze administracyjnym za pomocą narzędzia klsetsrvcert. Następnie powtórz procedurę aktualizacji, przeniesienia lub migracji.

   - Jeśli wartość jest zgodna z wartością określoną podczas instalacji Kaspersky Security Center Linux (w kroku **Wprowadź nazwę serwera DNS IAM** kreatora instalacji lub, w przypadku instalacji cichej, w parametrze `KLSRV_UNATT_IAM_ADDRESS`), nie jest wymagane żadne dalsze działanie. Serwer IAM i Serwer administracyjny będą współdziałać poprawnie.

   - Jeśli wartość zawiera adresy pętli zwrotnej (127.0.0.1 i/lub 0:0:0:0:0:0:0:1), użyj jednego z nich w pliku konfiguracyjnym. Zalecane jest użycie 127.0.0.1.

3. Dodaj jedną z wartości adresu SAN ze standardowego certyfikatu Serwera administracyjnego do bloku `server_iam` w pliku konfiguracyjnym serwera IAM w następującym formacie: `ksc_address: "<SAN_address>"`.

   Plik konfiguracyjny serwera IAM można zmodyfikować za pomocą edytora tekstu, na przykład vi. Poniższe polecenie otwiera plik w edytorze tekstu vi:

   ```
   vi /var/opt/kaspersky/klnagent_srv/iam/iam_config.yaml
   ```

   Przykład bloku server_iam w pliku konfiguracyjnym serwera IAM:

   ```
   server_iam:
       iam_address: "ksc.example.com"
       server_display_name: "ksc.example.com"
       ksc_address: "oldksc.example.internal"
       ksc_ca: "/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer"
   ```

   Upewnij się, że używasz tych samych odstępów, co w przykładzie.

4. Sprawdź, czy nazwa sieci w parametrze `ksc_address` przekierowuje na adres IP Serwera administracyjnego. W tym celu można użyć narzędzia Ping na Serwerze administracyjnym.

   Jeśli adres, na który nastąpiło przekierowanie jest inny, upewnij się, że stary Serwer administracyjny jest odłączony od sieci i że nie pozostały żadne rekordy DNS ze starym adresem IP. Jeśli nie można rozpoznać adresu, zmapuj go przy użyciu rekordu DNS w firmowym systemie DNS lub dodaj wpis do pliku hostów na Serwerze administracyjnym.

5. Uruchom ponownie usługę serwera IAM, aby zastosować zmiany konfiguracji, uruchamiając następujące polecenie:

   ```
   sudo systemctl restart kliam_srv.service
   ```

Adres Serwera administracyjnego zostanie dodany do pliku konfiguracyjnego serwera IAM ze standardowego certyfikatu Serwera administracyjnego.

Rozwiązywanie problemów

Problemy z konfiguracją na serwerze IAM mogą powodować błędy podczas logowania do Web Console. Poniższa tabela opisuje możliwe błędy i rozwiązania.

Błąd	Opis	Rozwiązanie
Nie można teraz przetworzyć Twojego żądania. Proszę poczekać i spróbować ponownie.	Oprócz procesu inicjalizacji danych po aktualizacji lub przywróceniu Kaspersky Security Center Linux, ten błąd może wystąpić, jeśli połączenie z Serwerem administracyjnym przy użyciu określonego adresu sieciowego nie powiedzie się.	Sprawdź, do jakiego adresu IP przekierowuje nazwa sieciowa, używając narzędzia ping.
Serwer administracyjny używa niezaufanego certyfikatu. Skonfiguruj ponownie aplikację, określając prawidłowy certyfikat lub skontaktuj się z głównym administratorem.	Błąd może wystąpić, jeśli wartość adresu w pliku konfiguracyjnym serwera IAM nie jest zgodna z wartością atrybutu Alternatywna nazwa podmiotu (SAN) standardowego certyfikatu Serwera administracyjnego.	Postępuj zgodnie z powyższymi instrukcjami.
Nazwa użytkownika lub hasło są niepoprawne.	Oprócz nieprawidłowych poświadczeń, ten błąd może wystąpić, jeśli w sieci istnieje inny Serwer administracyjny o tej samej nazwie.	Sprawdź, czy określony adres przekierowuje na adres IP bieżącego Serwera administracyjnego.

Określanie folderu współdzielonego

Po zainstalowaniu Serwera administracyjnego możesz określić lokalizację folderu współdzielonego we właściwościach Serwera administracyjnego. Domyślnie folder współdzielony jest tworzony na urządzeniu z Serwerem administracyjnym. Jednakże w niektórych przypadkach (takich, jak duże obciążenie sieci, konieczność uzyskania dostępu z odizolowanej sieci) przydatne może być umiejscowienie folderu współdzielonego w dedykowanym zasobie plików.

Folder współdzielony jest sporadycznie używany podczas wdrożenia Agenta sieciowego.

Uwzględnianie wielkości liter dla folderu współdzielonego musi być wyłączone.

Logowanie do Kaspersky Security Center Web Console i wylogowywanie

Możesz zalogować się do Kaspersky Security Center Web Console po zainstalowaniu Serwera administracyjnego i serwera Web Console Server. Musisz znać adres internetowy Serwera administracyjnego oraz numer portu określony podczas instalacji (domyślnie jest to port o numerze 8080). W swojej przeglądarce włącz JavaScript.

Możesz zalogować się do Kaspersky Security Center Web Console przy użyciu następujących metod:

- Korzystając z uwierzytelniania domeny (pojedynczego logowania)

  Ta metoda jest używana do bezpiecznego uwierzytelniania w Kaspersky Security Center Web Console połączonej z Serwerem administracyjnym w wersji 16 i nowszych. Jeśli chcesz użyć uwierzytelniania domeny, musisz określić dodatkowe parametry do interakcji z Menedżerem tożsamości i dostępu (IAM) podczas instalacji Kaspersky Security Center Web Console.

- Określając nazwę i hasło użytkownika domeny

  Zanim zalogujesz się przy użyciu konta użytkownika domeny, przeszukaj kontroler domeny, aby uzyskać listę użytkowników domeny. Następnie musisz określić nazwę użytkownika domeny i hasło, aby zalogować się do Serwera administracyjnego. Ta metoda jest obsługiwana wyłącznie w przypadku uwierzytelniania za pośrednictwem usługi Microsoft Active Directory.

- Określając nazwę i hasło użytkownika wewnętrznego

Konto użytkownika, za pomocą którego chcesz zalogować się do Kaspersky Security Center Web Console musi mieć przypisaną rolę. Przed zalogowaniem upewnij się, że domena lub konto użytkownika wewnętrznego mają przypisaną rolę. W przeciwnym razie wystąpi błąd logowania.

Logowanie korzystając z uwierzytelniania domeny (pojedynczego logowania)

W celu zalogowania się do Kaspersky Security Center Web Console przy użyciu uwierzytelniania domeny:

1. W przeglądarce przejdź do https://`<adres Kaspersky Security Center Web Console>`:`<numer portu>`.

   Zostanie wyświetlona strona wyboru Serwera administracyjnego.

2. Jeśli dodałeś kilka zaufanych serwerów, na liście Serwerów administracyjnych wybierz Serwer administracyjny, z którym chcesz nawiązać połączenie.

   Jeśli dodano tylko jeden Serwer administracyjny, lista Serwery administracyjne nie jest wyświetlana.

   Przeglądarka zostanie przekierowana do adresu https://`<adres Serwera administracyjnego>`:4444.

3. Skonfiguruj uwierzytelnianie domeny Kerberos.

4. Wykonaj jedną z poniższych czynności:

   - Kliknij przycisk **Użyj uwierzytelniania domeny**.
   - Jeżeli jeden lub więcej wirtualnych Serwerów administracyjnych jest utworzonych na Serwerze i chcesz zalogować się do Serwera wirtualnego przy użyciu uwierzytelniania domeny:

     a. Kliknij **Pokaż opcje serwera wirtualnego**.

     b. Wpisz nazwę wirtualnego Serwera administracyjnego określoną podczas tworzenia wirtualnego Serwera.

     c. Kliknij przycisk **Użyj uwierzytelniania domeny**.

5. Wygeneruj jednorazowy kod bezpieczeństwa z użyciem aplikacji uwierzytelniającej na urządzeniu mobilnym.

   Podczas pierwszego logowania skonfiguruj uwierzytelnianie dwuskładnikowe dla swojego konta. Jeśli konfiguracja uwierzytelniania dwuskładnikowego nie jest dla Ciebie dostępna, skontaktuj się z użytkownikiem, który ma uprawnienie Modyfikuj listy ACL obiektów w obszarze funkcjonalnym **Funkcje ogólne**: **Uprawnienia użytkownika** i skonfigurował uwierzytelnianie dwuskładnikowe, aby dodać swoje konto do listy dozwolonych uwierzytelniania dwuskładnikowego.

Po zalogowaniu zostanie wyświetlona strona główna Kaspersky Security Center Web Console zawierająca ostatnio używany język i motyw. Możesz poruszać się po konsoli Kaspersky Security Center Web Console i użyć jej do pracy z Kaspersky Security Center Linux.

Logowanie poprzez podanie nazwy i hasła użytkownika domeny lub użytkownika wewnętrznego

W celu zalogowania się do Kaspersky Security Center Web Console poprzez podanie nazwy użytkownika i hasła administratora:

1. W przeglądarce przejdź do https://`<adres Kaspersky Security Center Web Console>`:`<numer portu>`.

   Zostanie wyświetlona strona wyboru Serwera administracyjnego.

2. Jeśli dodałeś kilka zaufanych serwerów, na liście Serwerów administracyjnych wybierz Serwer administracyjny, z którym chcesz nawiązać połączenie.

   Jeśli dodano tylko jeden Serwer administracyjny, lista Serwery administracyjne nie jest wyświetlana.

Przeglądarka zostanie przekierowana do adresu https://<adres Serwera administracyjnego>:4444.

3. Wykonaj jedną z poniższych czynności:

   - Aby zalogować się do Serwera administracyjnego przy użyciu konta użytkownika domeny, wprowadź nazwę użytkownika i hasło użytkownika domeny.

     Nazwę użytkownika domeny możesz wprowadzić w jednym z następujących formatów:

     - `Nazwa użytkownika @ dns.domena`
     - `NTDOMAIN\Nazwa użytkownika`

     > Zanim zalogujesz się na konto użytkownika domeny, przeszukaj kontroler domeny, aby uzyskać listę użytkowników domeny.

   - Aby zalogować się do Serwera administracyjnego, podając nazwę użytkownika i hasło administratora, wprowadź nazwę użytkownika i hasło użytkownika wewnętrznego.

   - Jeżeli jeden lub więcej wirtualnych Serwerów administracyjnych jest utworzonych na Serwerze i chcesz zalogować się do Serwera wirtualnego:

     a. Kliknij **Pokaż opcje serwera wirtualnego**.

     b. Wpisz nazwę wirtualnego Serwera administracyjnego określoną podczas tworzenia wirtualnego Serwera.

     c. Wprowadź nazwę użytkownika i hasło administratora, który ma uprawnienia na wirtualnym Serwerze administracyjnym.

4. Kliknij przycisk **Zaloguj się**.

5. Wygeneruj jednorazowy kod bezpieczeństwa z użyciem aplikacji uwierzytelniającej na urządzeniu mobilnym.

   Podczas pierwszego logowania skonfiguruj uwierzytelnianie dwuskładnikowe dla swojego konta. Jeśli konfiguracja uwierzytelniania dwuskładnikowego nie jest dla Ciebie dostępna, skontaktuj się z użytkownikiem, który ma uprawnienie Modyfikuj listy ACL obiektów w obszarze funkcjonalnym **Funkcje ogólne**: **Uprawnienia użytkownika** i skonfigurował uwierzytelnianie dwuskładnikowe, aby dodać swoje konto do listy dozwolonych uwierzytelniania dwuskładnikowego.

6. Jeśli dla Twojego konta włączona jest funkcja wymuszonej zmiany hasła lub Twoje hasło wygasło, zostanie wyświetlone okno dialogowe zmiany hasła. Ustaw nowe hasło, aby zalogować się do Kaspersky Security Center Web Console.

Po zalogowaniu zostanie wyświetlona strona główna Kaspersky Security Center Web Console zawierająca ostatnio używany język i motyw. Możesz poruszać się po konsoli Kaspersky Security Center Web Console i użyć jej do pracy z Kaspersky Security Center Linux.

Wylogowanie

W celu wylogowania się z Kaspersky Security Center Web Console:

W górnym panelu przejdź do menu konta, klikając nazwę swojego konta a następnie wybierz **Wyloguj się**.

Konsola Kaspersky Security Center Web Console zostanie zamknięta i zostanie wyświetlona strona logowania.

Interfejs Kaspersky Security Center Web Console

Zarządzanie Kaspersky Security Center Linux odbywa się poprzez interfejs Kaspersky Security Center Web Console.

Okno Kaspersky Security Center Web Console zawiera następujące elementy:

- Menu główne w lewej części okna
- Górny panel w górnej części okna
- Obszar roboczy w prawej części okna

Menu główne

Menu główne zawiera następujące sekcje:

- **Serwer administracyjny**. Wyświetla nazwę aktualnie połączonego Serwera administracyjnego. Właściwości serwera administracyjnego można otworzyć, klikając nazwę Serwera administracyjnego.
- **Poruszanie się po konsoli**. Wyświetla mapę menu głównego. Większość wyświetlanych sekcji można dodać do zakładek lub ustawić jako stronę główną. Domyślnie **Poruszanie się po konsoli** ustawione są jako strona główna. Możesz zmienić te ustawienia.
- **Monitorowanie**. Zapewnia ogląd infrastruktury, stanów ochrony i statystyk.
- **Zarządzanie zasobami**. Zawiera narzędzia do zarządzania urządzeniami i sprzętem oraz zasady aplikacji Kaspersky.
- **Zadania**. Zawiera narzędzia do tworzenia i uruchamiania zadań.
- **Użytkownicy i role**. Umożliwia zarządzanie użytkownikami i rolami, konfigurowanie praw użytkowników poprzez przypisywanie ról użytkownikom oraz kojarzenie profili zasad z rolami.
- **Repozytoria**. Zapewnia dostęp do repozytoriów aplikacji.
- **Zarządzanie oprogramowaniem**. Umożliwia zarządzanie aplikacjami Kaspersky i innych firm, a także pakietami instalacyjnymi i poprawkami.
- **Operacje**. Zawiera różne operacje, w tym licencjonowanie aplikacji oraz wyświetlanie zaszyfrowanych dysków i zdarzeń szyfrowania i zarządzanie nimi.
- **Wykrywanie i wdrażanie**. Umożliwia przeszukiwanie sieci w celu wykrycia urządzeń klienckich i dystrybucję urządzeń do grup administracyjnych ręcznie lub automatycznie. Ta sekcja zawiera także kreator wstępnej konfiguracji i kreator wdrażania ochrony.

- **Platforma handlowa**. Zawiera informacje o całej gamie rozwiązań biznesowych Kaspersky i pozwala wybrać te, których potrzebujesz, a następnie przystąpić do zakupu tych rozwiązań na stronie internetowej Kaspersky.

- **Ustawienia**. Umożliwia wykonanie kopii zapasowej bieżącego stanu wtyczki webowej, aby móc później przywrócić zapisany stan. Zawiera Twoje osobiste ustawienia związane z wyglądem interfejsu, takie jak język lub motyw interfejsu.

W razie potrzeby można zminimalizować menu główne do ikon, klikając znak strzałki (<<) u dołu ekranu.

Górny panel

Górny panel jest zawsze wyświetlany we wszystkich sekcjach konsoli i nie można go ukryć.

Lewa strona panelu zawiera nazwę i logo aplikacji. Po kliknięciu nazwy lub logo aplikacji zostanie otwarta strona główna Kaspersky Security Center Web Console.

Po prawej stronie panelu wyświetlane są następujące ustawienia:

- Ikona powiadomień (🔔). Po kliknięciu ikony otworzy się panel z powiadomieniami.

- Menu Twojego konta. Zawiera łącze do pomocy Kaspersky Security Center Linux. Umożliwia także wylogowanie się z Kaspersky Security Center Linux, zmianę hasła do Twojego konta i przeglądanie wersji Kaspersky Security Center Web Console oraz listy zainstalowanych webowych wtyczek administracyjnych.

Miejsce pracy

Obszar roboczy wyświetla informacje, które wybrano do przeglądania w sekcjach okna interfejsu Kaspersky Security Center Web Console. Zawiera także elementy sterujące, za pomocą których można skonfigurować sposób wyświetlania informacji.

> Zalecamy korzystanie z jednej zakładki przeglądarki w trakcie pracy z Kaspersky Security Center Web Console.

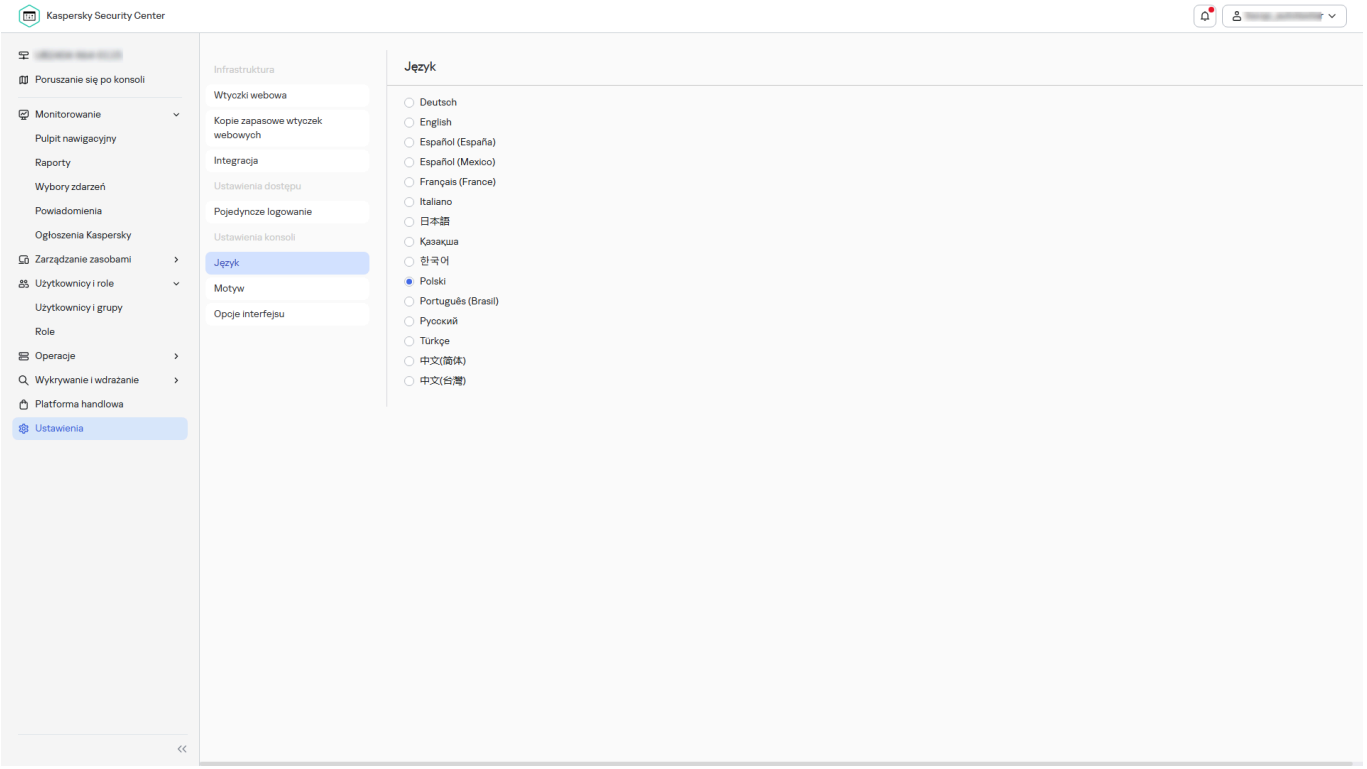
Zmiana języka interfejsu oprogramowania Kaspersky Security Center Web Console

Możesz wybrać język interfejsu Kaspersky Security Center Web Console.

Aby zmienić język interfejsu:

1. W menu głównym przejdź do sekcji **Ustawienia** → **Język**.

2. Wybierz jeden z obsługiwanych języków lokalizacji.



Zmiana języka interfejsu Kaspersky Security Center Web Console

Zmiana strony głównej Kaspersky Security Center Web Console

Strona główna jest wyświetlana po zalogowaniu się do Kaspersky Security Center Web Console.

Domyślnie sekcja **Poruszanie się po konsoli**jest ustawiona jako strona główna. Jeśli to konieczne, możesz zmienić stronę główną.

Aby zmienić stronę główną:

1. W sekcji **Poruszanie się po konsoli** najedź kursorem myszy na element, który chcesz ustawić jako stronę główną.

2. Zostanie wyświetlona ikona domku (), kliknij ją.

Strona główna zostaje zmieniona, na ekranie wyświetla się odpowiedni komunikat, a element wybrany jako strona główna zostaje oznaczony ikoną domku ().

Sekcji **Platforma handlowa** i **Ustawienia** nie można ustawić jako strony głównej.

Dodawanie i usuwanie z ulubionych

Możesz przypiąć często używane sekcje Kaspersky Security Center Web Console do ulubionych, aby uzyskać do nich szybki dostęp z sekcji **Zakładki** w menu głównym.

Jeśli nie dodałeś żadnej sekcji do ulubionych, sekcja **Zakładki** nie będzie wyświetlana w menu głównym.

Do ulubionych możesz dodać tylko te sekcje, w których wyświetlane są strony. Przykładowo, jeśli przejdziesz do **Zarządzanie zasobami** → **Zasoby (urządzenia)**, otworzy się strona z tabelą urządzeń, co oznacza, że możesz przypiąć tą sekcję. Jeśli po wybraniu sekcji w menu głównym wyświetli się okno lub nie wyświetli się żaden element, nie będzie możliwości przypięcia takiej sekcji.

Aby dodać sekcję do ulubionych:

1. W menu głównym najedź kursorem myszy na sekcję, którą chcesz przypiąć.
2. Zostanie wyświetlona ikona pinezki (), kliknij ją.

   Sekcja zostanie przypięta i będzie wyświetlana w sekcji **Zakładki**.

Aby usunąć sekcję z ulubionych:

1. W menu głównym przejdź do sekcji **Zakładki**.
2. Najedź kursorem myszy na sekcję, którą chcesz odpiąć, a następnie kliknij ikonę pinezki ().

   Sekcja zostanie usunięta z ulubionych.

Możesz również dodawać i usuwać sekcje z ulubionych w sekcji **Poruszanie się po konsoli**, najeżdżając na nie kursorem myszy i klikając ikonę pinezki (). Wybrany element zostanie oznaczony ikoną pinezki () i będzie wyświetlany w sekcji **Zakładki** w menu głównym. Jeśli chcesz usunąć element z ulubionych, kliknij ikonę pinezki ().

Sekcja **Zakładki** wyświetlana jest tylko w menu głównym. Nigdy nie jest wyświetlana na stronie **Poruszanie się po konsoli**.

Usuwanie Kaspersky Security Center Web Console

Konieczne może być usunięcie Kaspersky Security Center Web Console Server (nazywanego również Kaspersky Security Center Web Console) w następujących przypadkach:

- Przywracanie danych z kopii zapasowej przy użyciu innego standardowego certyfikatu.
- Ponowne wydawanie standardowego certyfikatu Serwera administracyjnego.
- Zastępowanie certyfikatu Web Console certyfikatem niestandardowym.
- Kaspersky Security Center Web Console nie jest już używana na urządzeniu.

W celu usunięcia Kaspersky Security Center Web Console:

1. W zależności od dystrybucji Linux uruchom jedno z następujących poleceń:

   - `sudo dnf remove ksc-web-console`

   - `sudo apt remove ksc-web-console`

2. Sprawdź wynik, wykonując następujące polecenie:

   `sudo systemctl status KSC*`

   Kaspersky Security Center Web Console musi być nieobecna w wynikach polecenia.

Aby przywrócić Kaspersky Security Center Web Console, zainstaluj ją na urządzeniu zgodnie z opisem w artykule: Instalowanie Kaspersky Security Center Web Console.

Kreator wstępnej konfiguracji

Kaspersky Security Center Linux umożliwia dostosowanie minimalnego zestawu ustawień niezbędnych do stworzenia systemu scentralizowanego zarządzania ochroną sieci przed zagrożeniami bezpieczeństwa. Taka konfiguracja jest przeprowadzana przez Kreator wstępnej konfiguracji. Przy pierwszym uruchomieniu kreatora możesz wprowadzić w aplikacji następujące zmiany:

- Dodaj pliki klucza lub wprowadź kody aktywacyjne, które mogą być automatycznie przesyłane do urządzeń w grupach administracyjnych.

- Skonfigurować dostarczanie powiadomień informujących o zdarzeniach występujących podczas działania Serwera administracyjnego i zarządzanych aplikacji za pomocą poczty e-mail.

- Utworzyć zasadę ochrony dla stacji roboczych i serwerów, a także zadania skanowania w poszukiwaniu złośliwego oprogramowania, zadania pobierania aktualizacji i zadania tworzenia kopii zapasowej danych dla najwyższego poziomu hierarchii zarządzanych urządzeń.

  Kreator wstępnej konfiguracji tworzy zasady tylko dla tych aplikacji, dla których folder **Zasoby (urządzenia)** nie zawiera żadnych zasad. Kreator wstępnej konfiguracji nie tworzy zadań, jeśli zadania o tych samych nazwach zostały już utworzone dla najwyższego poziomu hierarchii zarządzanych urządzeń.

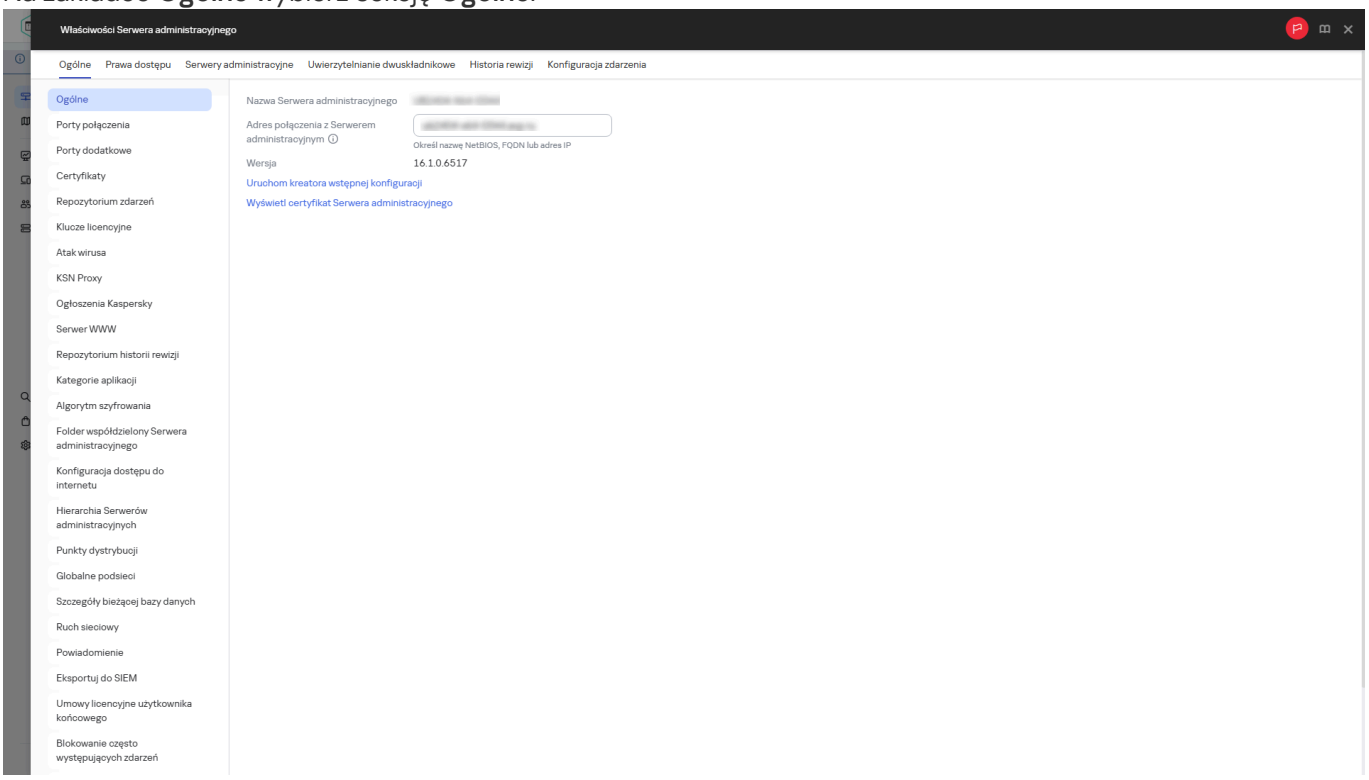
Po zainstalowaniu Serwera administracyjnego, przy pierwszym nawiązaniu połączenia z nim, aplikacja automatycznie wyświetli pytanie dotyczące uruchomienia kreatora wstępnej konfiguracji. Kreator wstępnej konfiguracji można również uruchomić ręcznie w dowolnym momencie.

W celu ręcznego uruchomienia kreatora wstępnej konfiguracji:

1. W menu głównym kliknij nazwę Serwera administracyjnego.

   Zostanie otwarte okno właściwości Serwera administracyjnego.

2. Na zakładce **Ogólne** wybierz sekcję **Ogólne**.



Okno właściwości Serwera administracyjnego

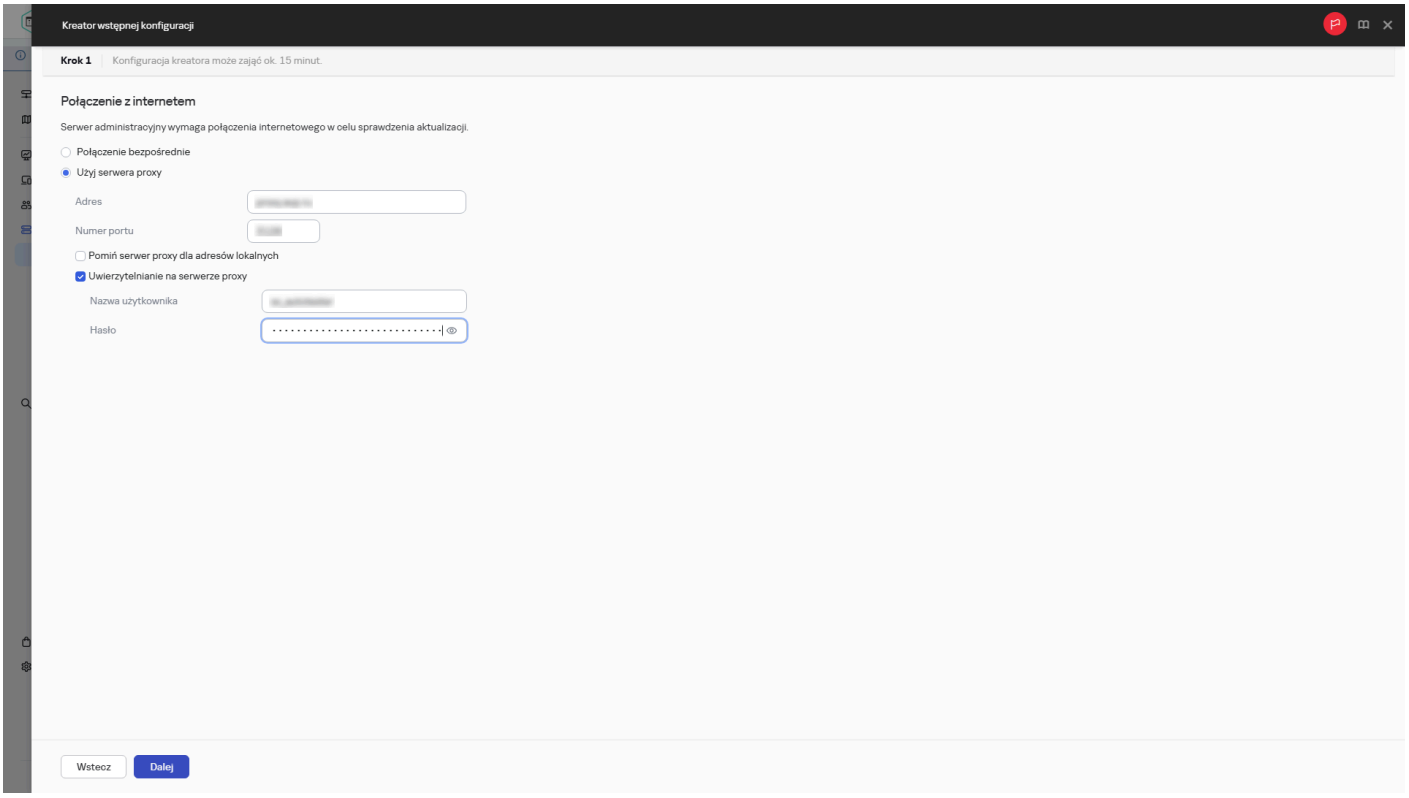
3. Kliknij **Uruchom kreatora wstępnej konfiguracji**.

kreator wyświetli pytanie o przeprowadzenie wstępnej konfiguracji Serwera administracyjnego. Postępuj zgodnie z instrukcjami kreatora. Przejdź przez kroki kreatora, korzystając z przycisku **Dalej**.

Krok 1. Określenie ustawień połączenia internetowego

Określ ustawienia dostępu do Internetu dla Serwera administracyjnego. Należy skonfigurować dostęp do internetu w taki sposób, aby korzystać z Kaspersky Security Network i pobierać aktualizacje antywirusowych baz danych dla Kaspersky Security Center Linux i zarządzanych aplikacji Kaspersky.

Włącz opcję **Użyj serwera proxy**, jeśli podczas łączenia z internetem chcesz korzystać z serwera proxy. Jeśli ta opcja jest włączona, dostępne staną się pola do wprowadzenia ustawień. Dla połączenia z serwerem proxy określ następujące ustawienia:



Ustawienia połączenia z internetem

- **Adres**

  Adres serwera proxy używanego do łączenia Kaspersky Security Center Linux z Internetem.

- **Numer portu**

  Numer portu, poprzez który zostanie nawiązane połączenie proxy Kaspersky Security Center Linux.

- **Pomiń serwer proxy dla adresów lokalnych**

  Żaden serwer proxy nie będzie używany do nawiązywania połączenia z urządzeniami w sieci lokalnej.

- **Uwierzytelnianie na serwerze proxy**

  Jeśli to pole jest zaznaczone, w polach wejściowych możesz określić dane uwierzytelniające do autoryzacji na serwerze proxy.

  To pole wejściowe jest dostępne, jeśli opcja **Użyj serwera proxy** jest zaznaczona.

- **Nazwa użytkownika**

  Konto użytkownika, z poziomu którego nawiązywane jest połączenie z serwerem proxy (to pole jest dostępne, jeśli pole **Uwierzytelnianie na serwerze proxy** jest wybrane).

- **Hasło**

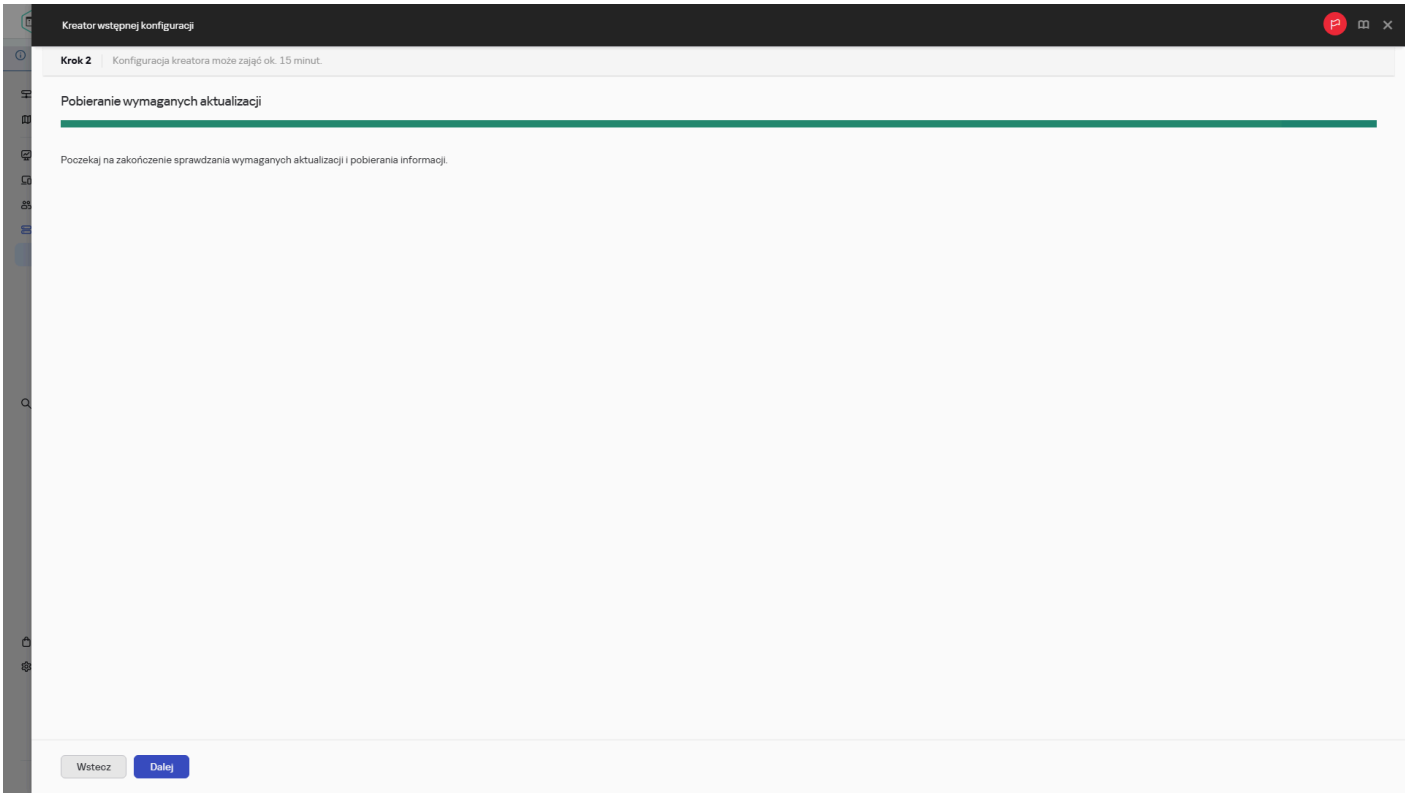
  Hasło ustawione przez użytkownika, którego konto jest używane do nawiązywania połączenia z serwerem proxy (to pole jest dostępne, jeśli pole **Uwierzytelnianie na serwerze proxy** jest zaznaczone).

  Aby zobaczyć wprowadzone hasło, trzymaj kliknięty przycisk **Pokaż** tak długo, jak potrzebujesz.

Możesz skonfigurować dostęp do Internetu później, niezależnie od kreatora wstępnej konfiguracji.

Krok 2. Pobieranie żądanych uaktualnień

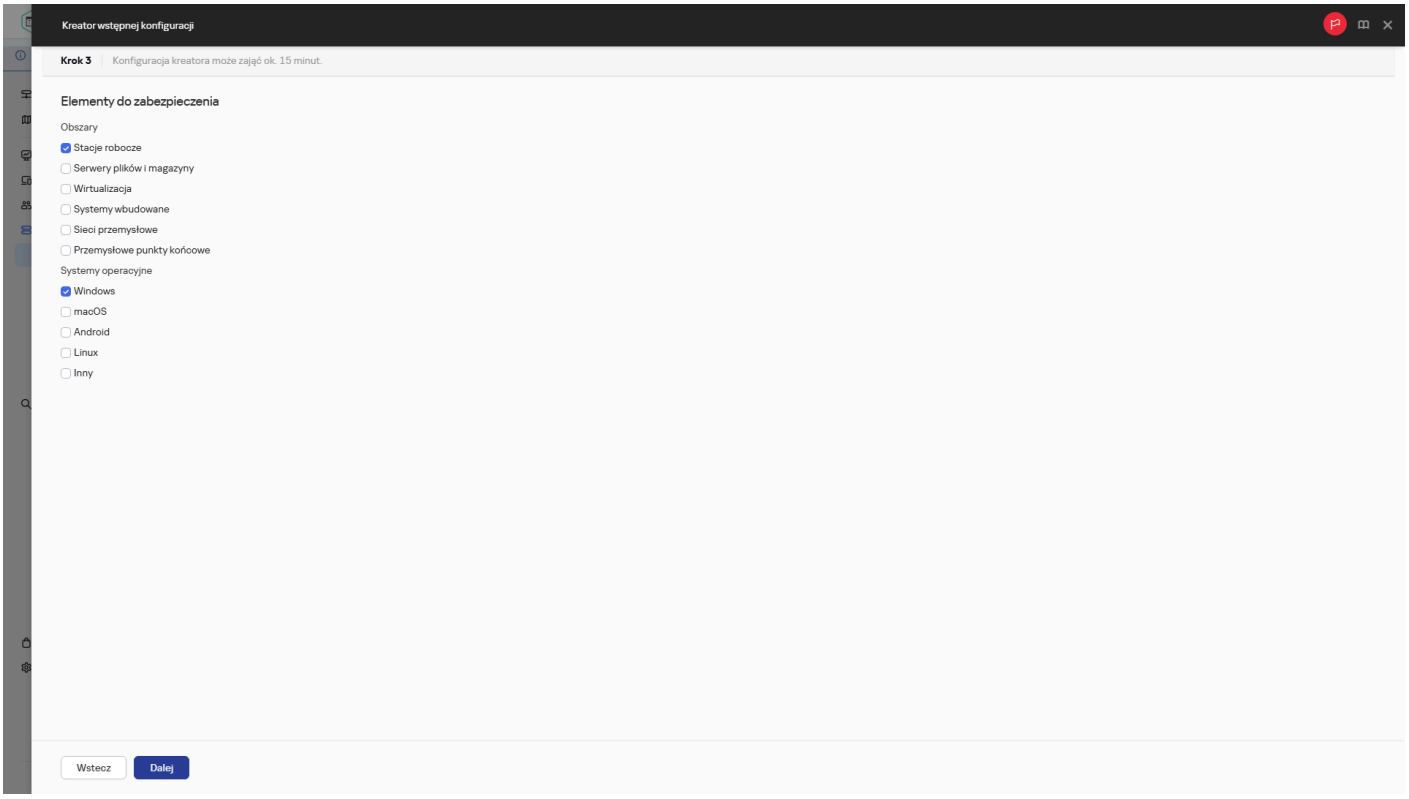
Wymagane aktualizacje są automatycznie pobierane z serwerów Kaspersky.



Pobieranie żądanych uaktualnień

Krok 3. Wybór elementów do zabezpieczenia

Wybierz obszary ochrony i systemy operacyjne używane w Twojej sieci. Jeśli wybierzesz te opcje, określ filtry dla wtyczek zarządzających aplikacjami i pakietami dystrybucyjnymi na serwerach Kaspersky, które możesz pobrać do zainstalowania na urządzeniach klienckich w Twojej sieci.



Wybór elementów do zabezpieczenia

Wybierz opcje:

- **Obszary**

  Możesz wybrać następujące obszary ochrony:

  - **Stacje robocze**
  - **Serwery plików i magazyny**
  - **Wirtualizacja**
  - **Systemy wbudowane**
  - **Sieci przemysłowe**
  - **Przemysłowe punkty końcowe**

- **Systemy operacyjne**

  Możesz wybrać następujące platformy:

  - Microsoft Windows
  - macOS
  - Android
  - Linux
  - Inne

  Aby uzyskać informacje na temat obsługiwanych systemów operacyjnych, zobacz Wymagania sprzętowe i programowe dla Kaspersky Security Center Web Console.

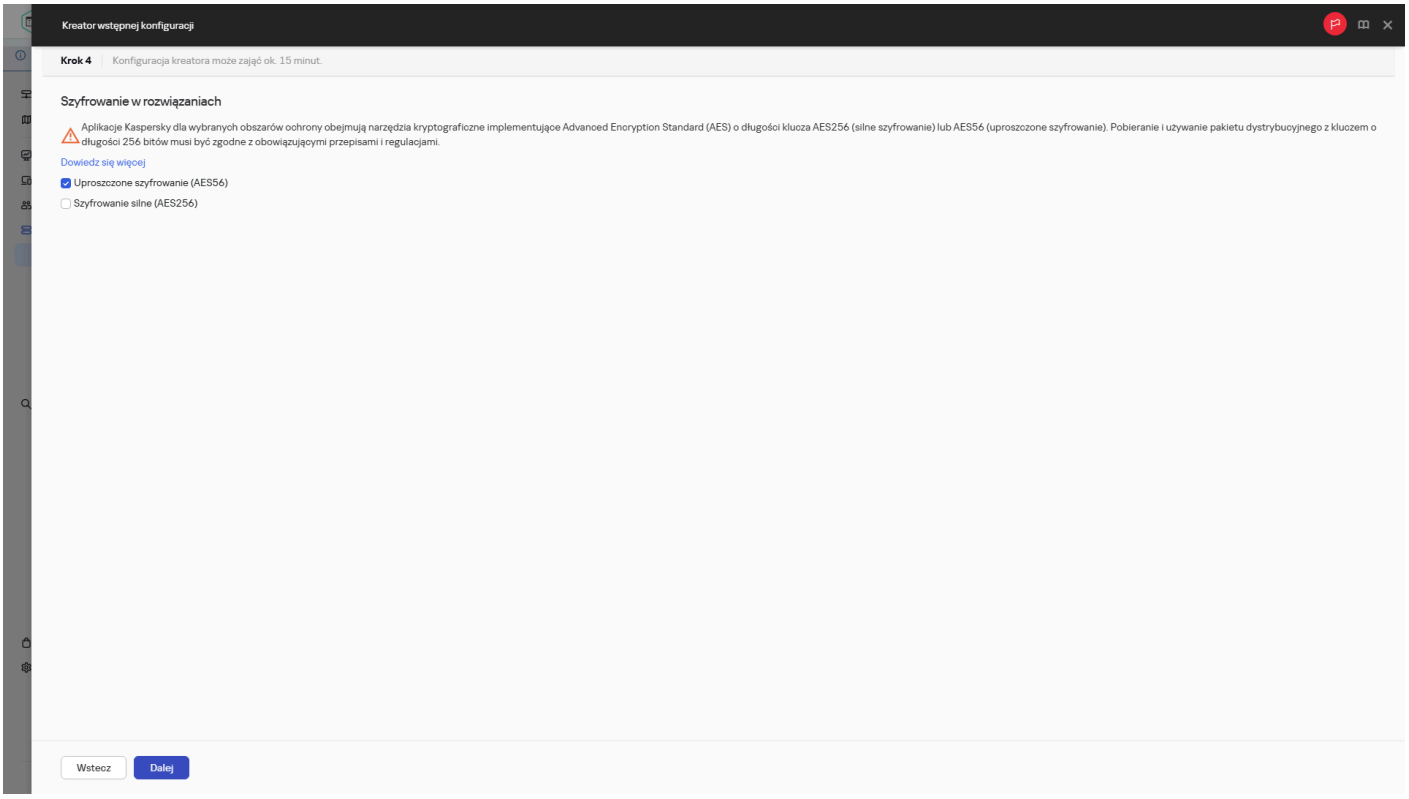
Możesz wybrać pakiety aplikacji Kaspersky z listy dostępnych pakietów później, niezależnie od kreatora wstępnej konfiguracji. Aby uprościć wyszukiwanie potrzebnych pakietów, możesz filtrować listę dostępnych pakietów według różnych kryteriów.

Krok 4. Wybieranie szyfrowania w rozwiązaniach

Okno **Szyfrowanie w rozwiązaniach** jest wyświetlane tylko wtedy, gdy wybrano **Stacje robocze** jako obszar ochrony.

Kaspersky Endpoint Security for Windows zawiera narzędzia do szyfrowania informacji przechowywanych na urządzeniach klienckich z systemem Windows. Te narzędzia szyfrujące mają zaimplementowany standard Advanced Encryption Standard (AES) z kluczem o długości 256-bitowej lub 56-bitowej.

Pobieranie i korzystanie z pakietu dystrybucyjnego z kluczem o długości 256 bitów musi odbywać się zgodnie z obowiązującymi przepisami i regulacjami. Aby pobrać pakiet dystrybucyjny Kaspersky Endpoint Security for Windows potrzebny w Twojej organizacji, miej na uwadze ustawodawstwo kraju, w którym znajdują się urządzenia klienckie Twojej organizacji.



Wybieranie szyfrowania w rozwiązaniach

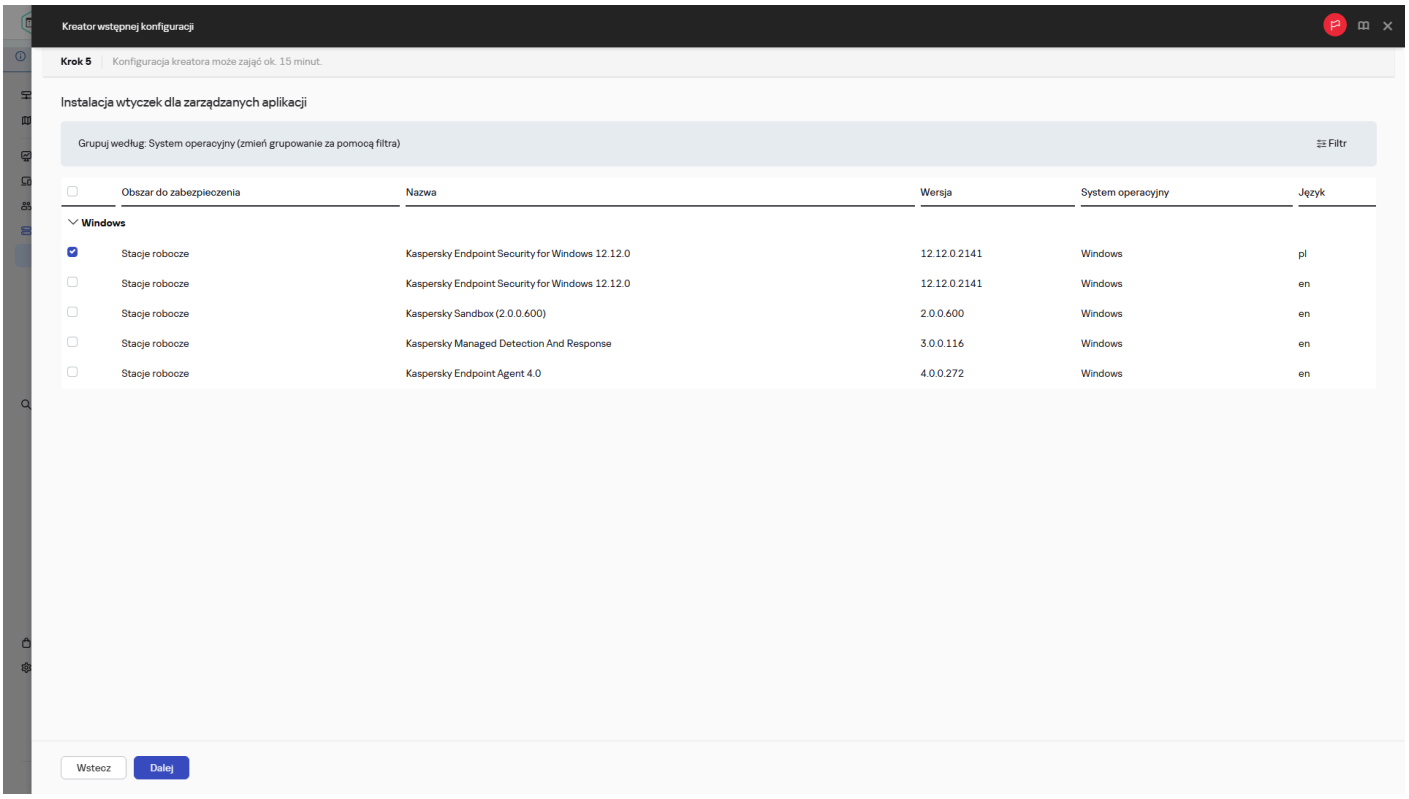
W oknie **Szyfrowanie w rozwiązaniach** wybierz jeden z następujących typów szyfrowania:

- Lite encryption (Szyfrowanie podstawowe). Ten typ szyfrowania używa klucza o długości 56 bitów.
- Strong encryption (Silne szyfrowanie). Ten typ szyfrowania używa klucza o długości 256 bitów.

Możesz wybrać pakiet dystrybucyjny dla Kaspersky Endpoint Security for Windows z wymaganym typem szyfrowania później, niezależnie od kreatora wstępnej konfiguracji.

Krok 5. Konfigurowanie instalacji wtyczek dla zarządzanych aplikacji

Wybierz wtyczki dla zarządzanych aplikacji, które mają zostać zainstalowane. Zostanie wyświetlona lista wtyczek znajdujących się na serwerach Kaspersky. Lista jest filtrowana zgodnie z opcjami wybranymi w poprzednim kroku kreatora. Domyślnie, pełna lista zawiera wtyczki we wszystkich językach. Aby wyświetlić tylko wtyczkę w określonym języku, użyj filtru.



Instalacja wtyczek dla zarządzanych aplikacji

Lista wtyczek zawiera następujące kolumny:

- **Obszar do zabezpieczenia**

  W tej kolumnie wyświetlane są wybrane obszary do zabezpieczenia.

- **Typ**

  W tej kolumnie wyświetlane są typy wtyczek.

- **Nazwa**

  Zostały wybrane wtyczki zależne od obszarów ochrony i platform, które wybrano w poprzednim kroku.

- **Wersja**

  Lista zawiera wtyczki we wszystkich wersjach umieszczone na serwerach Kaspersky. Domyślnie zostaną wybrane wtyczki w najnowszych wersjach.

- **Najnowsza wersja**

  Ta kolumna wskazuje, czy wersja wtyczki jest najnowsza. Jeśli wyświetlana jest wartość **true**, odpowiednia wtyczka posiada najnowszą wersję. Jeśli wyświetlana jest wartość **false**, odpowiednia wtyczka posiada starszą wersję.

- **System operacyjny**

  W tej kolumnie wyświetlane są systemy operacyjne wtyczek.

- **Język**

  Domyślnie wersja językowa wtyczki jest definiowana przez wersję językową Kaspersky Security Center Linux, którą wybrałeś w momencie instalacji. Możesz określić inne wersje językowe na liście rozwijalnej **Wskaż język dla Konsoli administracyjnej lub**.

Po wybraniu wtyczek kliknij przycisk **Dalej**, aby rozpocząć instalację.

Wtyczki administracyjne dla aplikacji Kaspersky można zainstalować ręcznie, niezależnie od kreatora wstępnej konfiguracji.

Kreator wstępnej konfiguracji automatycznie instaluje wybrane wtyczki. Aby zainstalować niektóre wtyczki, należy zaakceptować warunki Umowy licencyjnej użytkownika końcowego. Zapoznaj się z treścią wyświetlonej Umowy licencyjnej użytkownika końcowego, zaznacz pole **Zgadzam się na korzystanie z Kaspersky Security Network** i kliknij przycisk **Zainstaluj**. Jeśli nie akceptujesz warunków Umowy licencyjnej użytkownika końcowego, wtyczka nie zostanie zainstalowana.

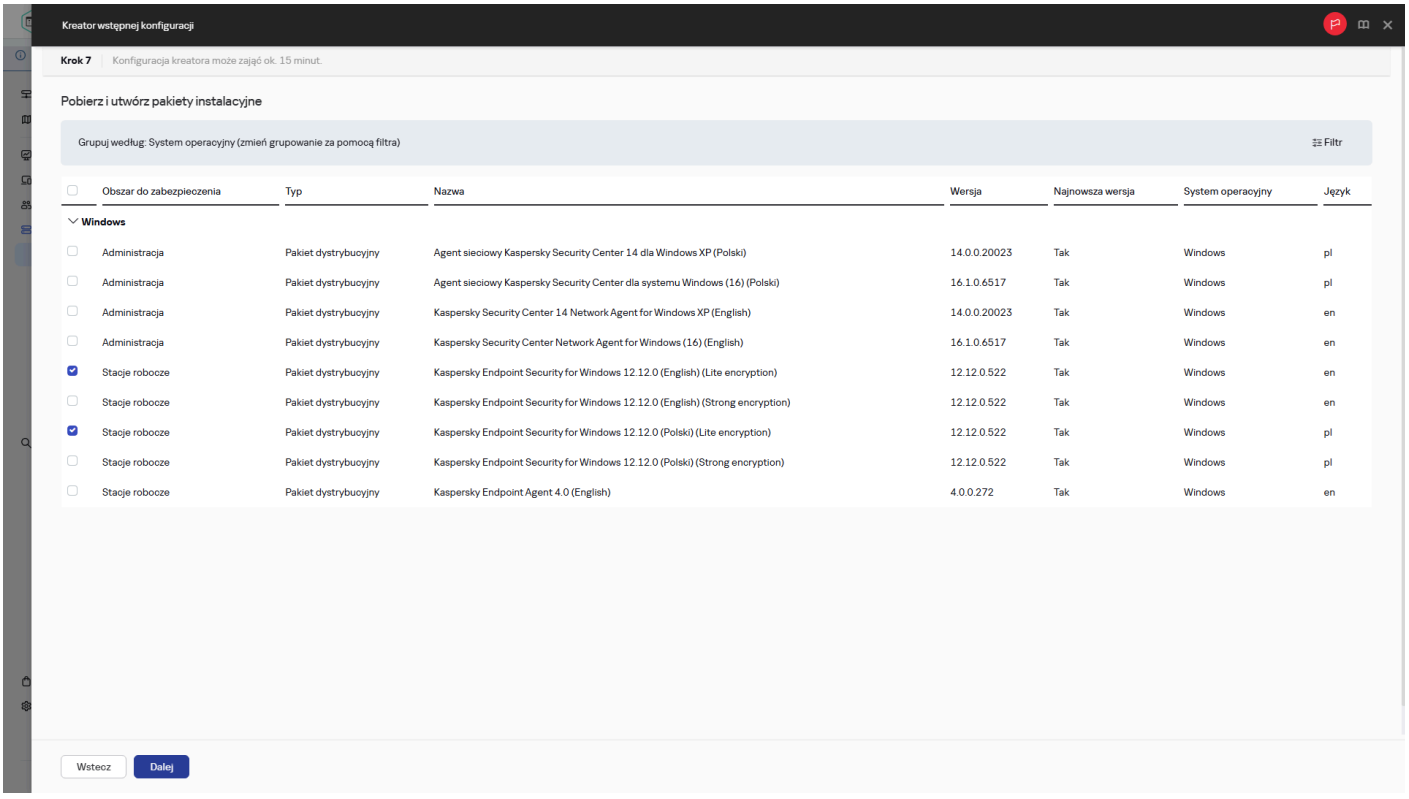
Po zainstalowaniu wszystkich wybranych wtyczek Kreator wstępnej konfiguracji automatycznie przeniesie Cię do następnego kroku.

Krok 6. Pobieranie pakietów dystrybucyjnych i tworzenie pakietów instalacyjnych

Wybierz pakiety dystrybucyjne do pobrania.

> Dystrybutory zarządzanych aplikacji mogą wymagać zainstalowania określonej minimalnej wersji Kaspersky Security Center Linux.

Po wybraniu typu szyfrowania dla Kaspersky Endpoint Security for Windows, zostanie wyświetlona lista pakietów dystrybucyjnych obu typów szyfrowania. Pakiet dystrybucyjny z wybranym typem szyfrowania zostanie wybrany z listy. Możesz wybrać pakiety dystrybucyjne dowolnego typu szyfrowania. Język pakietu dystrybucyjnego odpowiada językowi Kaspersky Security Center Linux. Jeśli pakiet dystrybucyjny aplikacji dla języka Kaspersky Security Center Linux nie istnieje, wybrany zostanie pakiet dystrybucyjny w języku angielskim.



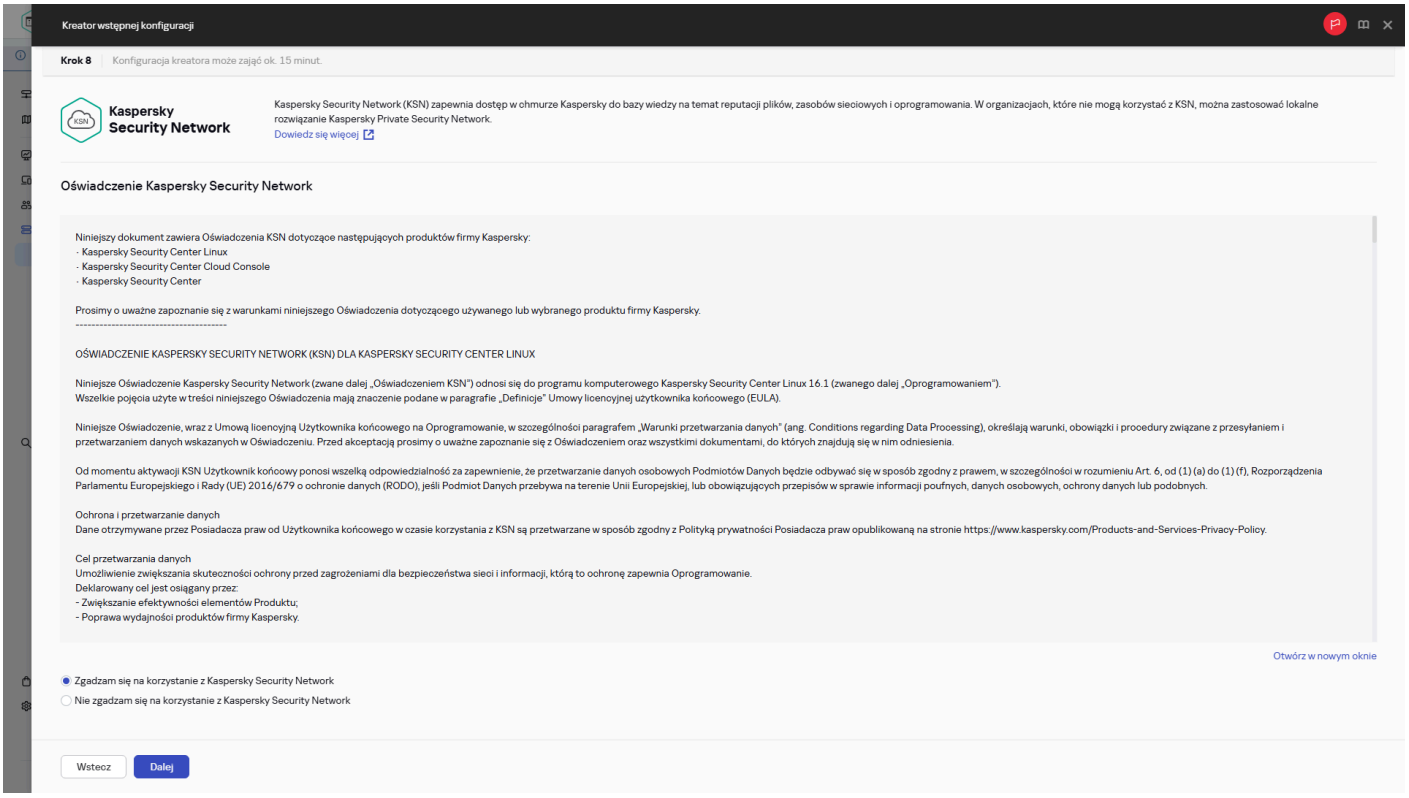
Pobieranie pakietów dystrybucyjnych i tworzenie pakietów instalacyjnych

Aby zakończyć pobieranie niektórych pakietów dystrybucyjnych, należy zaakceptować Umowę licencyjną użytkownika końcowego. Jeśli klikniesz przycisk **Zaakceptuj**, zostanie wyświetlona treść Umowy licencyjnej użytkownika końcowego. Aby przejść do kolejnego kroku kreatora, należy zaakceptować warunki i postanowienia Umowy licencyjnej użytkownika końcowego oraz warunki i postanowienia Polityki prywatności Kaspersky. Jeśli nie akceptujesz warunków i postanowień, pobieranie pakietu zostanie anulowane.

Po zaakceptowaniu warunków i postanowień Umowy licencyjnej użytkownika końcowego oraz warunków i postanowień Polityki prywatności Kaspersky, pobieranie pakietów dystrybucyjnych będzie kontynuowane. W późniejszym czasie możesz wykorzystać pakiety instalacyjne do wdrożenia aplikacji Kaspersky na urządzeniach klienckich.

Krok 7. Konfigurowanie Kaspersky Security Network

Określ ustawienia przekazywania informacji o działaniach Kaspersky Security Center Linux do bazy wiedzy Kaspersky Security Network.



Konfigurowanie Kaspersky Security Network

Wybierz jedną z następujących opcji:

- **Zgadzam się na korzystanie z Kaspersky Security Network**

  Kaspersky Security Center Linux i zarządzane aplikacje zainstalowane na urządzeniach klienckich automatycznie prześlą szczegóły swoich działań do Kaspersky Security Network. Uczestnictwo w Kaspersky Security Network umożliwia szybsze aktualizowanie baz danych zawierających informacje o wirusach i innych zagrożeniach, co zapewnia szybszą reakcję na pojawiające się zagrożenia bezpieczeństwa.

- **Nie zgadzam się na korzystanie z Kaspersky Security Network**

  Kaspersky Security Center Linux i zarządzane aplikacje nie dostarczą informacji do Kaspersky Security Network.

  Jeśli wybierzesz tę opcję, korzystanie z Kaspersky Security Network zostanie wyłączone.

Możesz skonfigurować dostęp do Kaspersky Security Network (KSN) później, niezależnie od kreatora wstępnej konfiguracji.

Krok 8. Wybieranie metody aktywacji aplikacji

Wybierz jedną z poniższych opcji aktywacji Kaspersky Security Center Linux:

- **Wprowadzając kod aktywacyjny**

  Kod aktywacyjny to unikatowa sekwencja 20 znaków alfanumerycznych. Możesz wprowadzić kod aktywacyjny w celu dodania klucza aktywującego Kaspersky Security Center Linux. Możesz otrzymać kod aktywacyjny na adres e-mail, który określiłeś po zakupieniu Kaspersky Security Center.

  Aby aktywować aplikację za pomocą kodu aktywacyjnego, potrzebny jest dostęp do internetu w celu nawiązania połączenia z serwerami aktywacji Kaspersky.

  Jeśli wybrałeś tę opcję aktywacji, możesz włączyć opcję **Automatycznie roześlij klucz licencyjny na zarządzane urządzenia**.

  Jeśli ta opcja jest włączona, klucz licencyjny zostanie automatycznie zainstalowany na zarządzanych urządzeniach.

  Jeśli ta opcja jest wyłączona, możesz wdrożyć klucz licencyjny na zarządzanych urządzeniach później, w sekcji głównego menu **Operacje** → **Licencjonowanie** → **Licencje**.

- **Określając plik klucza**

  Plik klucza to plik z rozszerzeniem .key, dostarczony przez firmę Kaspersky. Plik klucza jest przeznaczony do dodania klucza aktywującego aplikację.

  Możesz otrzymać plik klucza na adres e-mail, który określiłeś po zakupieniu Kaspersky Security Center.

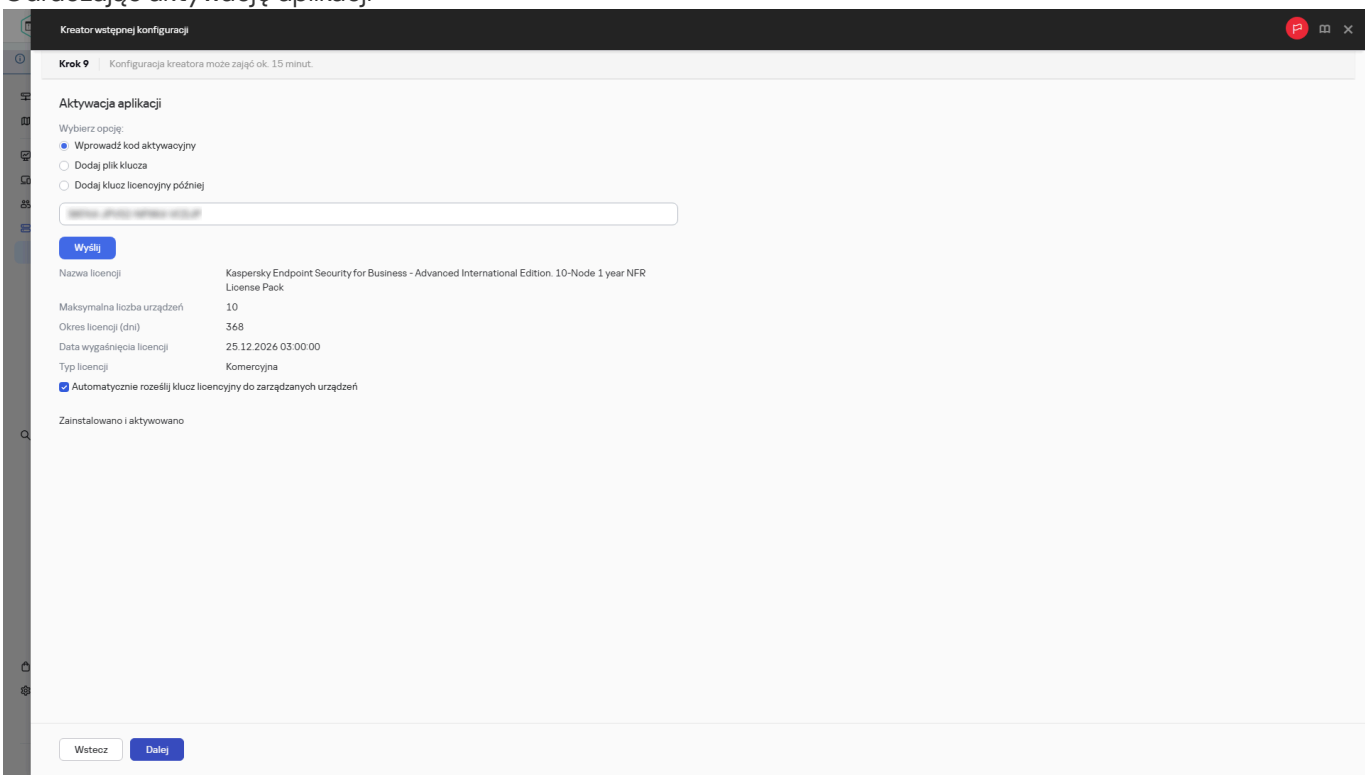
  Aby aktywować aplikację przy pomocy pliku klucza, nie musisz łączyć się z serwerami aktywacji Kaspersky.

  Jeśli wybrałeś tę opcję aktywacji, możesz włączyć opcję **Automatycznie roześlij klucz licencyjny na zarządzane urządzenia**.

  Jeśli ta opcja jest włączona, klucz licencyjny zostanie automatycznie zainstalowany na zarządzanych urządzeniach.

  Jeśli ta opcja jest wyłączona, możesz wdrożyć klucz licencyjny na zarządzanych urządzeniach później, w sekcji głównego menu **Operacje** → **Licencjonowanie** → **Licencje**.

- Odraczając aktywację aplikacji



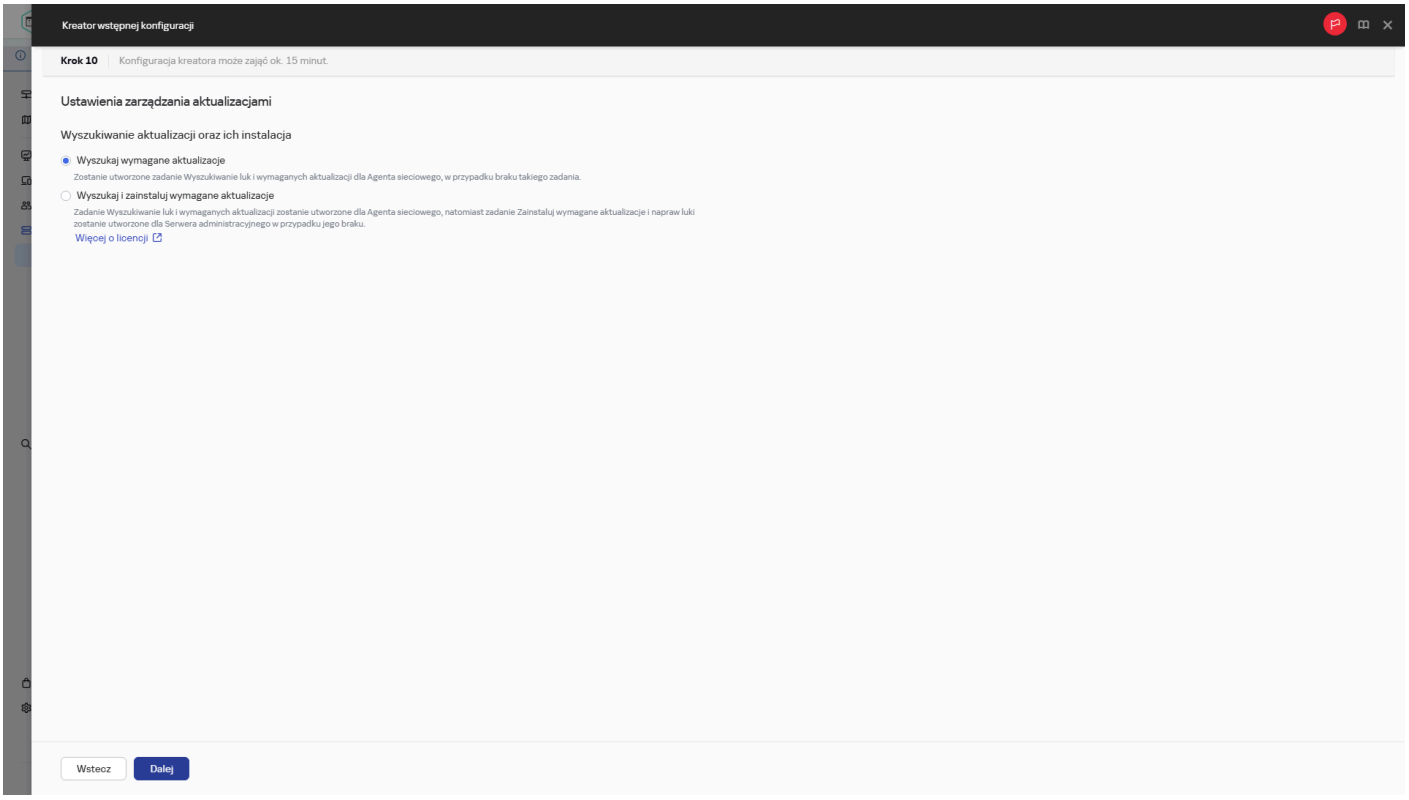
Wybieranie metody aktywacji aplikacji

Jeśli wybierzesz opcję odroczenia aktywacji aplikacji, będziesz mógł dodać klucz licencyjny w późniejszym czasie, wybierając **Operacje** → **Licencjonowanie**.

Podczas pracy z Kaspersky Security Center zainstalowanym z płatnego obrazu AMI lub dla Usage-based monthly billed SKU, nie można określić pliku klucza ani wprowadzić kodu.

Krok 9. Określanie ustawień zarządzania aktualizacjami firm trzecich

Krok **Ustawienia zarządzania aktualizacjami** kreatora wstępnej konfiguracji nie jest wyświetlany, jeśli nie posiadasz licencji na zarządzanie lukami i poprawkami, a zadanie *Wyszukiwanie luk i wymaganych aktualizacji*.



Ustawienia zarządzania aktualizacjami firm trzecich

Dla aktualizacji oprogramowania innych firm wybierz jedną z następujących opcji:

- **Wyszukaj wymagane aktualizacje**

  Zadanie *Wyszukiwanie luk i wymaganych aktualizacji* jest tworzone automatycznie, jeśli ich nie ma.

  Opcja ta jest wybrana domyślnie.

- **Wyszukaj i zainstaluj wymagane aktualizacje**

  Zadania *Wyszukiwanie luk i wymaganych aktualizacji* i *Zainstaluj wymagane aktualizacje i napraw luki* są tworzone automatycznie, jeśli ich nie ma.

  Ta opcja jest dostępna tylko w ramach licencji na Zarządzanie lukami i poprawkami.

W przypadku aktualizacji Windows Update wybierz opcję **Użyj źródeł uaktualnień zdefiniowanych w zasadzie domeny.**

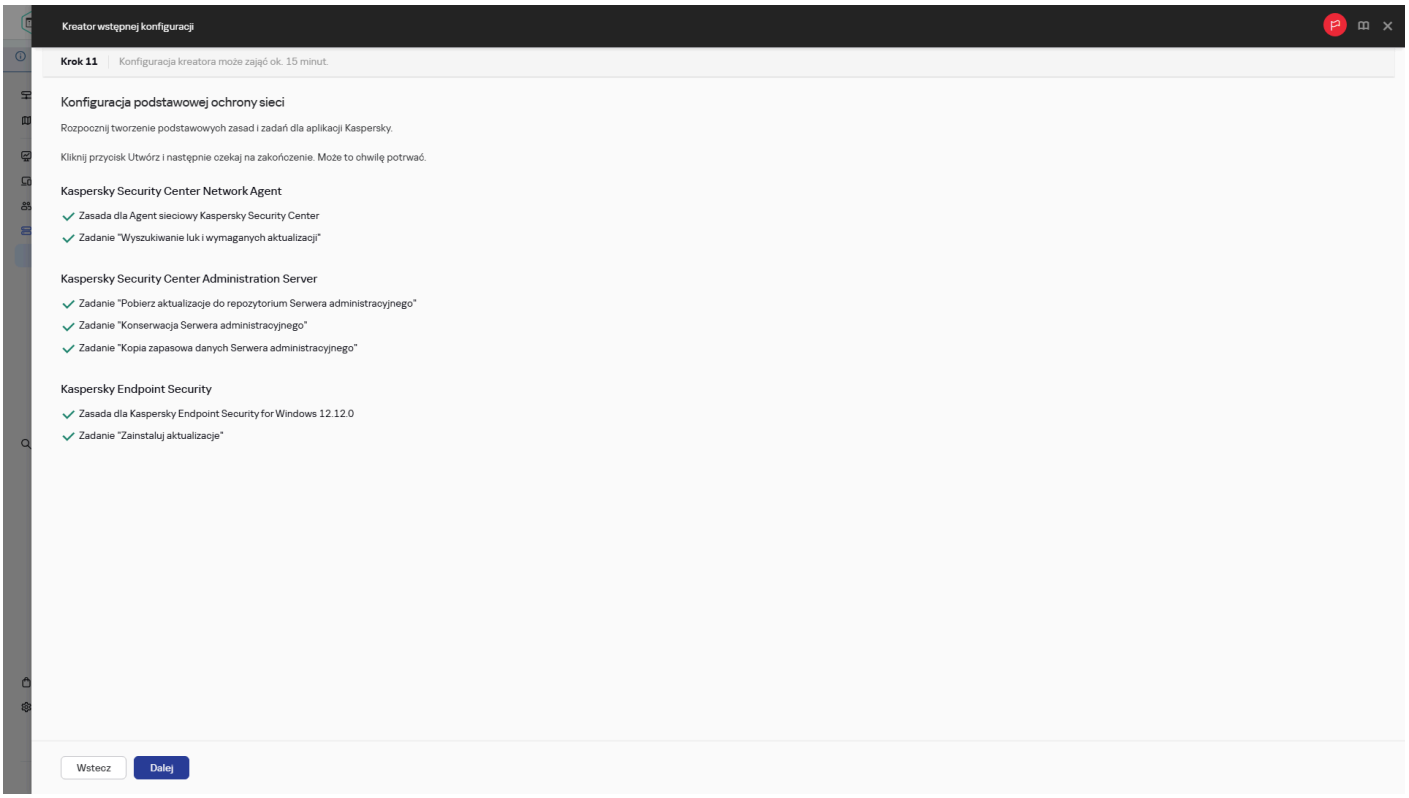
Urządzenia klienckie pobiorą aktualizacje Windows Update zgodnie z ustawieniami zasad domeny. Zasada Agenta sieciowego jest tworzona automatycznie, jeśli jeszcze jej nie masz.

Zadania *Wyszukiwanie luk i wymaganych aktualizacji* oraz *Zainstaluj wymagane aktualizacje i napraw luki* możesz utworzyć niezależnie od kreatora wstępnej konfiguracji.

Krok 10. Tworzenie podstawowej konfiguracji ochrony sieci

Możesz sprawdzić listę utworzonych zasad i zadań.

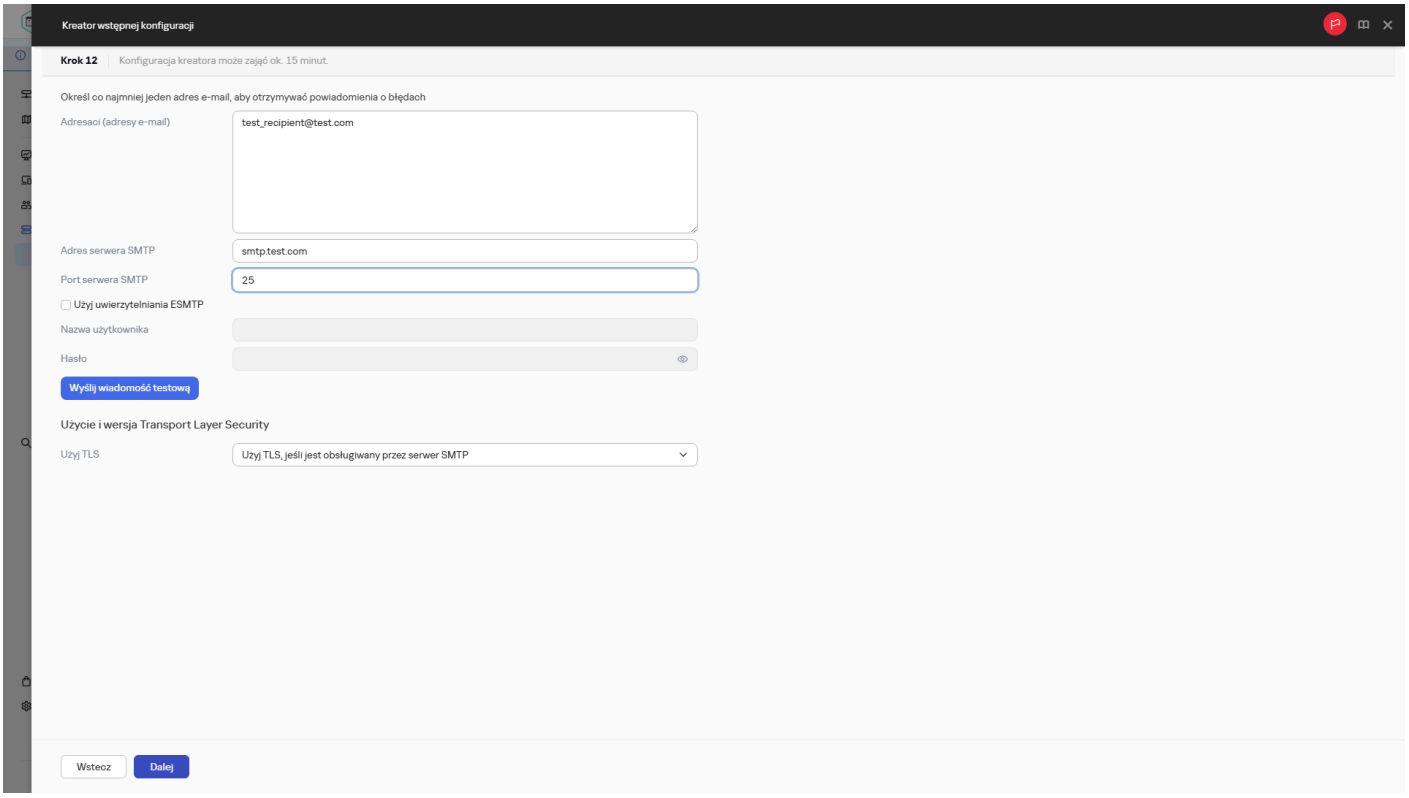
Przed przystąpieniem do następnego kroku kreatora poczekaj na zakończenie tworzenia zasad i zadań.



Tworzenie podstawowej konfiguracji ochrony sieci

Krok 11. Konfigurowanie powiadomień e-mail

Skonfiguruj dostarczanie powiadomień o zdarzeniach zarejestrowanych podczas działania aplikacji firmy Kaspersky na urządzeniach klienckich. Ustawienia te będą używane jako ustawienia domyślne dla zasad aplikacji.



Konfigurowanie powiadomień e-mail

W celu skonfigurowania dostarczania powiadomień o zdarzeniach występujących w aplikacjach firmy Kaspersky użyj następujących ustawień:

- **Adresaci (adresy e-mail)**

  Adresy e-mail użytkowników, którym aplikacja będzie wysyłała powiadomienia. Możesz wprowadzić jeden lub więcej adresów; jeśli wprowadzisz więcej niż jeden adres, oddziel je średnikami.

- **Adres serwera SMTP**

  Adres lub adresy serwerów pocztowych Twojej organizacji.

  Jeśli wprowadzisz więcej niż jeden adres, oddziel je średnikami. Możesz użyć następujących wartości:

  - Adres IPv4 lub IPv6
  - Nazwa DNS serwera SMTP

- **Port serwera SMTP**

  Numer portu komunikacji serwera SMTP. Jeśli korzystasz z kilku serwerów SMTP, połączenie z nimi jest nawiązywane przez określony port komunikacyjny. Domyślny numer portu to 25.

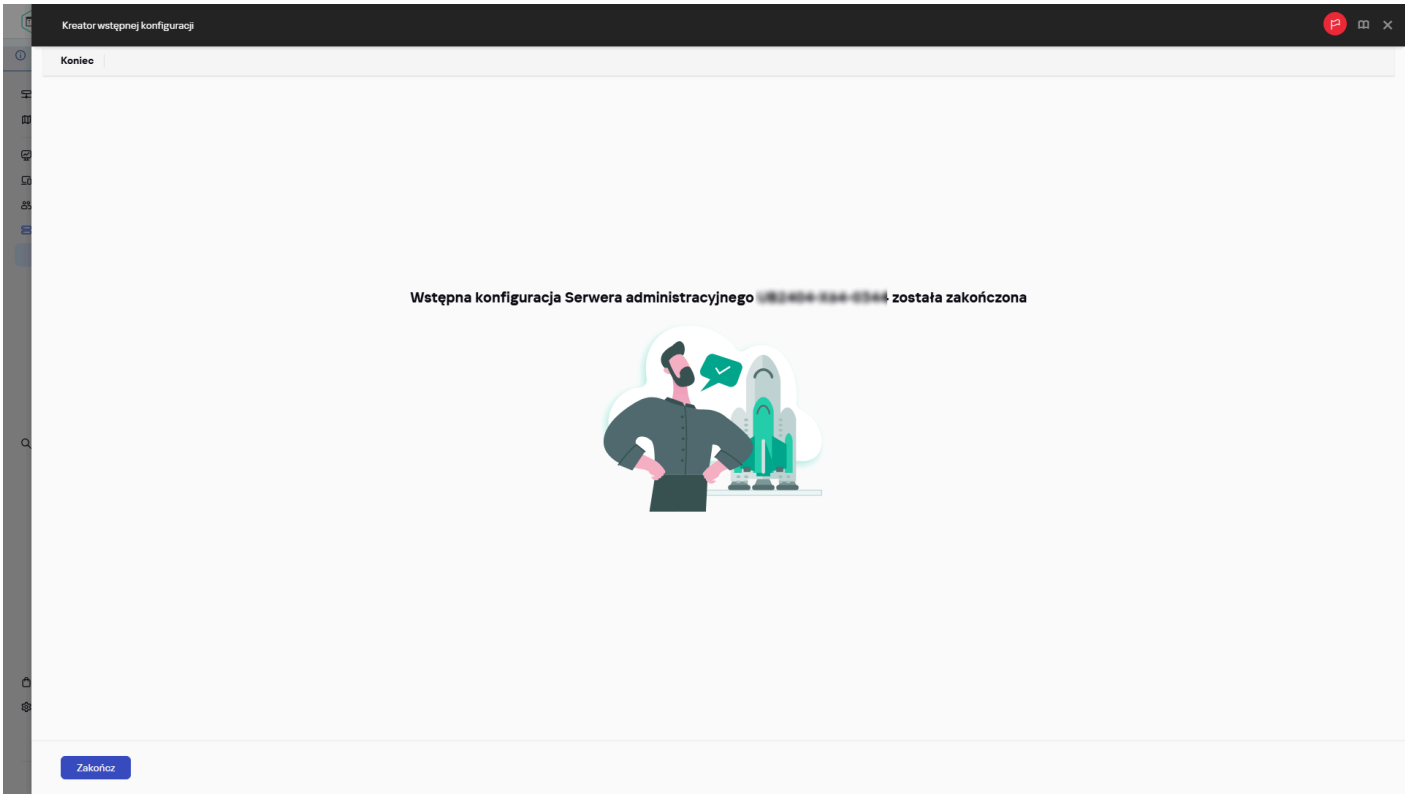
- **Użyj uwierzytelniania ESMTP**

  Włącza obsługę autoryzacji ESMTP. Po zaznaczeniu opcji, w polach **Nazwa użytkownika** i **Hasło** możesz określić ustawienia autoryzacji ESMTP. Domyślnie pole to nie jest zaznaczone.

Możesz przetestować nowe ustawienia powiadomień e-mail, klikając przycisk **Wyślij wiadomość testową**.

Krok 12. Zamykanie kreatora wstępnej konfiguracji

Aby zamknąć kreator, kliknij przycisk **Zakończ**.



Ostatni krok Kreatora wstępnej konfiguracji

Po zakończeniu działania kreatora wstępnej konfiguracji możesz uruchomić kreator wdrażania ochrony, aby automatycznie zainstalować aplikacje antywirusowe lub Agenta sieciowego na urządzeniach w sieci.

Kreator wdrażania ochrony

Do zainstalowania aplikacji firmy Kaspersky można użyć kreatora wdrażania ochrony. Kreator wdrażania ochrony umożliwia przeprowadzenie zdalnej instalacji aplikacji przy pomocy specjalnie utworzonych pakietów instalacyjnych lub bezpośrednio z pakietu dystrybucyjnego.

Kreator wdrażania ochrony wykonuje następujące działania:

- Pobiera pakiet instalacyjny potrzebny do zainstalowania aplikacji (jeśli nie został utworzony wcześniej). Pakiet instalacyjny znajduje się w sekcji **Zarządzanie oprogramowaniem** → **Pakiety instalacyjne**. Możesz użyć tego pakietu instalacyjnego do przyszłej instalacji aplikacji.

- Tworzy i uruchamia zadanie zdalnej instalacji dla określonych urządzeń lub grupy administracyjnej. Nowo utworzone zadanie zdalnej instalacji jest przechowywane w sekcji **Zadania**. Możesz później uruchomić to zadanie ręcznie. Typ zadania to **Zdalna instalacja aplikacji**.

Jeśli chcesz zainstalować Agenta sieciowego na urządzeniach z systemem operacyjnym SUSE Linux Enterprise Server 15, w pierwszej kolejności zainstaluj pakiet insserv-compat, aby skonfigurować Agenta sieciowego.

Krok 1. Uruchamianie kreatora wdrażania ochrony

Możesz ręcznie uruchomić kreator wdrażania ochrony w dowolnym momencie.

W celu ręcznego uruchomienia kreatora wdrażania ochrony:

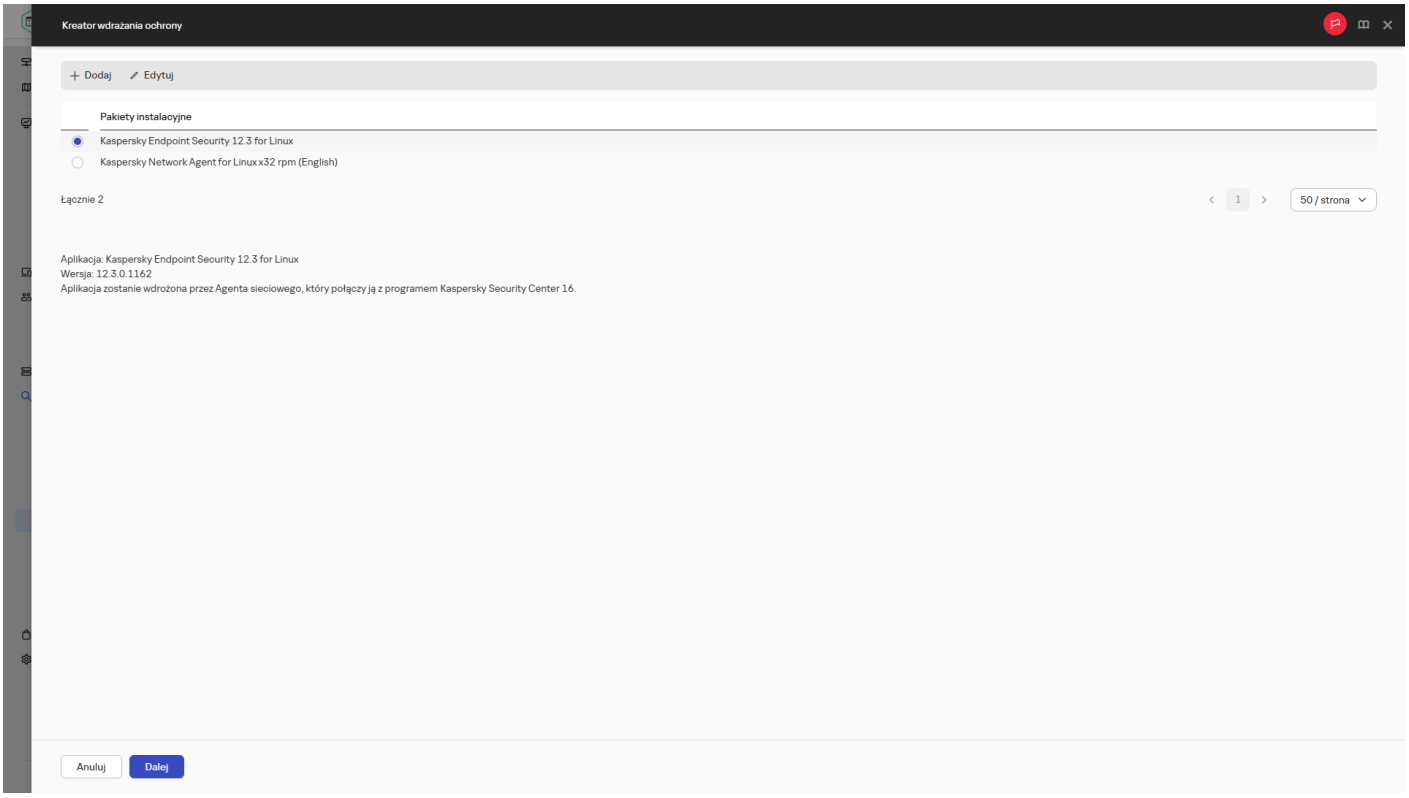
W głównym menu kliknij **Wykrywanie i wdrażanie** → **Wdrażanie i przypisywanie** → **Kreator wdrażania ochrony**.

Zostanie uruchomiony kreatora wdrażania ochrony. Przejdź przez kroki kreatora, korzystając z przycisku **Dalej**.

Krok 2. Wybieranie pakietu instalacyjnego

Wybierz pakiet instalacyjny aplikacji, którą chcesz zainstalować.

Jeśli nie ma pakietu instalacyjnego żądanej aplikacji, kliknij przycisk **Dodaj**, a następnie wybierz aplikację z listy.



Wybierz pakiet instalacyjny

Krok 3. Wybieranie metody rozsyłania pliku klucza lub kodu aktywacyjnego

Wybierz metodę rozesłania pliku klucza lub kodu aktywacyjnego:

- **Nie dodawaj klucza licencyjnego do pakietu instalacyjnego**

  Klucz jest automatycznie rozsyłany na wszystkie urządzenia, z którymi jest kompatybilny:

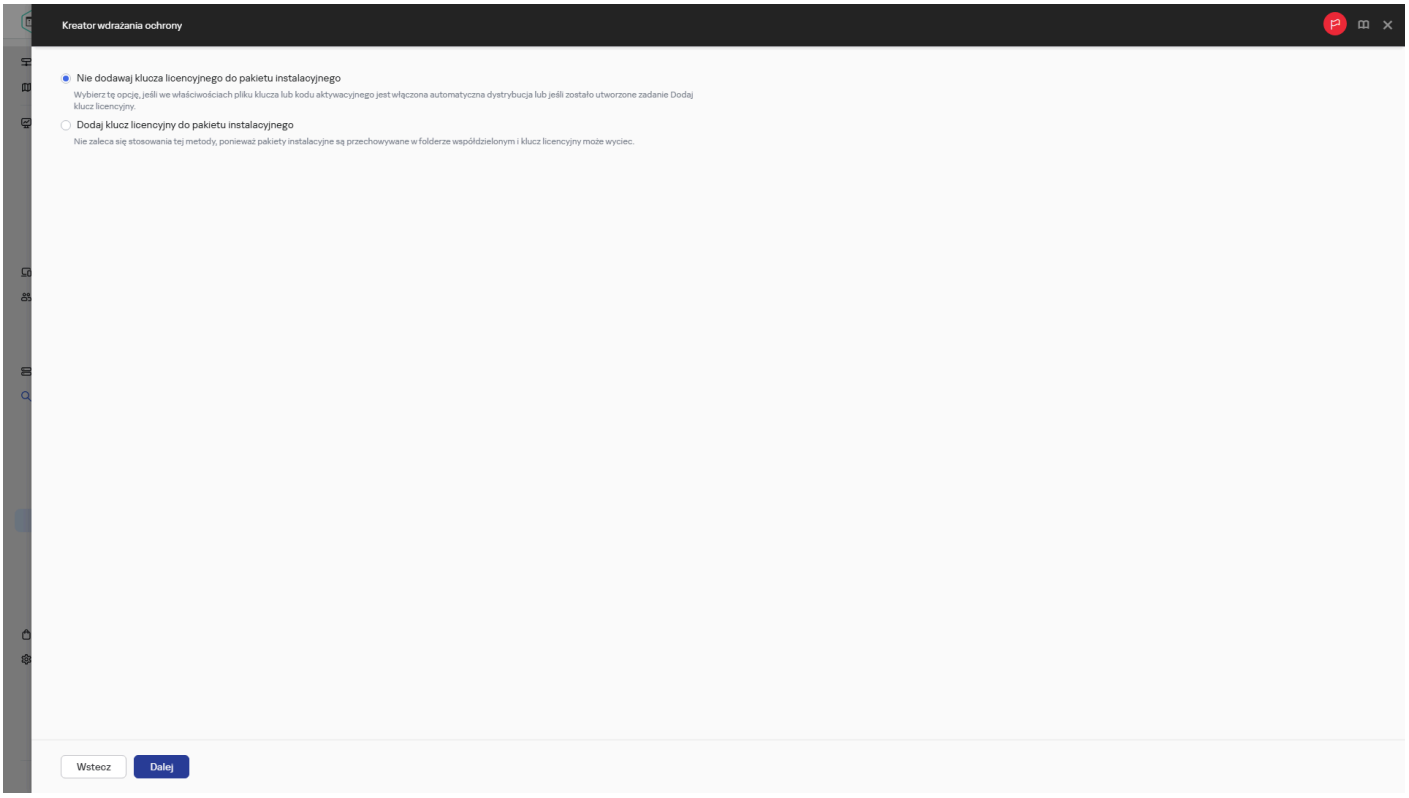
  - Jeśli we właściwościach klucza jest włączona automatyczna dystrybucja.
  - Jeśli utworzono zadanie **Dodaj klucz**.

- **Dodaj klucz licencyjny do pakietu instalacyjnego**

  Klucz jest rozsyłany na urządzenia wraz z pakietem instalacyjnym.

  > Nie zalecamy rozpowszechniania klucza przy użyciu tej metody, ponieważ współdzielone prawa dostępu do odczytu są włączone do repozytorium pakietów instalacyjnych.

Jeśli pakiet instalacyjny już zawiera plik klucza lub kod aktywacyjny, to okno zostanie wyświetlone, ale będzie zawierało tylko informacje dotyczące klucza licencyjnego.

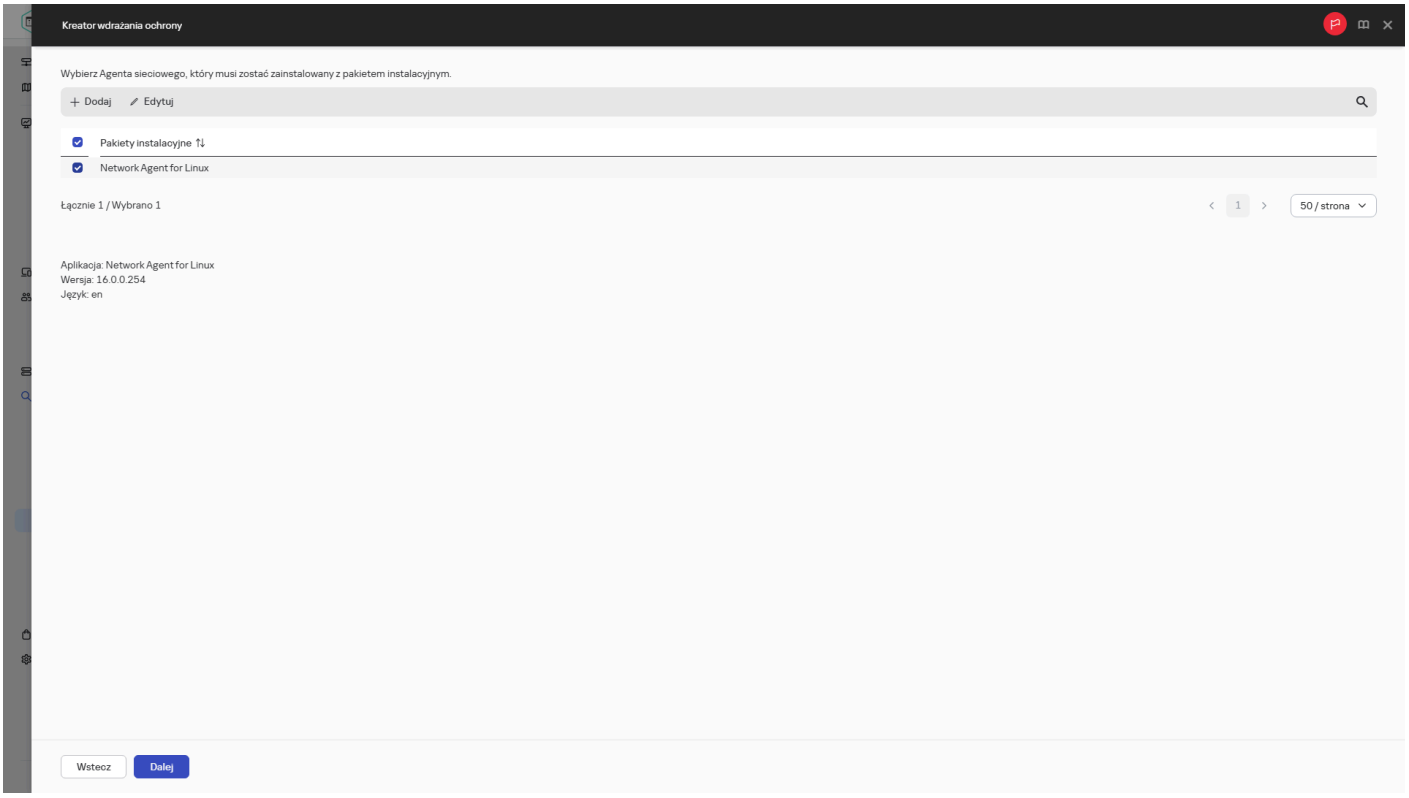


Wybór metody dystrybucji pliku klucza lub kodu aktywacyjnego

Krok 4. Wybieranie wersji Agenta sieciowego

Jeśli wybrano pakiet instalacyjny aplikacji innej niż Agent sieciowy, należy również zainstalować Agenta sieciowego, który łączy aplikację z Serwerem administracyjnym.

Wybierz najnowszą wersję Agenta sieciowego.



Wybieranie wersji Agenta sieciowego

Krok 5. Wybór urządzeń

Określ listę urządzeń, na których zostanie zainstalowana aplikacja:

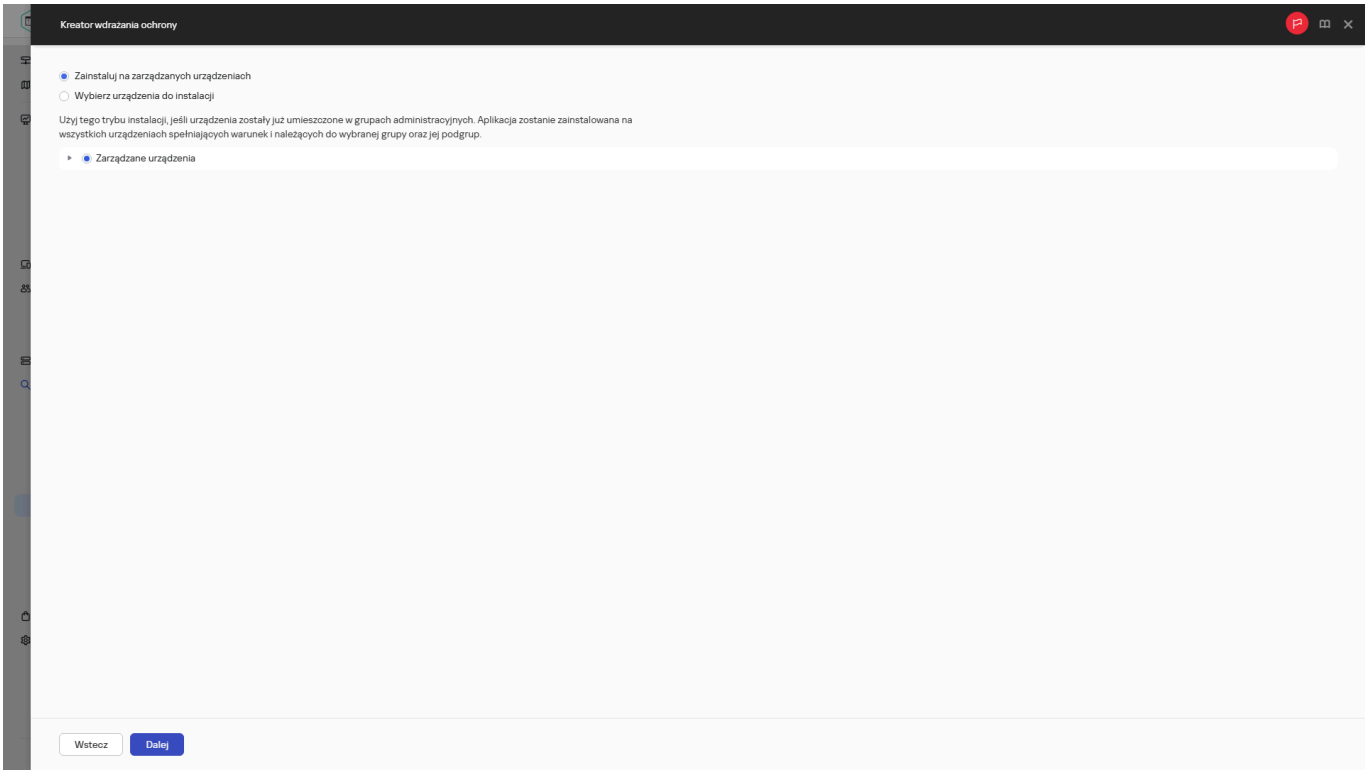
- **Zainstaluj na zarządzanych urządzeniach**

  Jeżeli ta opcja jest zaznaczona, zadanie zdalnej instalacji jest tworzone dla grupy urządzeń.

- **Wybierz urządzenia do instalacji**

  Zadanie jest przypisywane do urządzeń znajdujących się w wyborze urządzeń. Możesz określić jeden z istniejących wyborów.

Na przykład, możesz chcieć użyć tej opcji do uruchomienia zadania na urządzeniach z określoną wersją systemu operacyjnego.



Określanie listy urządzeń, na których zostanie zainstalowana aplikacja

Krok 6. Określanie ustawień zadania zdalnej instalacji

W oknie **Ustawienia zadania zdalnej instalacji** określ ustawienia zdalnej instalacji aplikacji.

W grupie ustawień **Wymuś pobranie pakietu instalacyjnego** określ sposób rozsyłania na urządzenia klienckie plików, które są niezbędne do zainstalowania aplikacji:

- **Przy użyciu Agenta sieciowego**

  Jeśli ta opcja jest włączona, pakiety instalacyjne są dostarczane na urządzenia klienckie przez Agenta sieciowego zainstalowanego na tych urządzeniach klienckich.

  Jeśli ta opcja jest wyłączona, pakiety instalacyjne są dostarczane przy użyciu narzędzi systemu operacyjnego urządzeń klienckich.

  Zalecane jest włączenie tej opcji, jeśli zadanie zostało przypisane do urządzeń z zainstalowanymi Agentami sieciowymi.

  Domyślnie opcja ta jest włączona.

- **Przy użyciu zasobów systemu operacyjnego poprzez punkty dystrybucji**

  Jeśli ta opcja jest włączona, pakiety instalacyjne są przesyłane na urządzenia klienckie przy użyciu narzędzi systemu operacyjnego za pośrednictwem punktów dystrybucyjnych. Możesz wybrać tę opcję, jeżeli w sieci jest przynajmniej jeden punkt dystrybucyjny.

  Jeśli opcja **Przy użyciu Agenta sieciowego** jest włączona, pliki będą dostarczane przy użyciu narzędzi systemu operacyjnego, jeśli narzędzia Agenta sieciowego są niedostępne.

  Domyślnie ta opcja jest włączona dla zadań zdalnej instalacji utworzonych na wirtualnym Serwerze administracyjnym.

Jedynym sposobem zainstalowania aplikacji dla systemu Windows (w tym Agenta sieciowego dla systemu Windows) na urządzeniu, na którym nie ma zainstalowanego Agenta sieciowego, jest użycie punktu dystrybucji opartego na systemie Windows. Dlatego podczas instalowania aplikacji Windows:

- Wybierz tę opcję.
- Upewnij się, że punkt dystrybucji jest przypisany do docelowych urządzeń klienckich.
- Upewnij się, że punkt dystrybucji jest oparty na systemie Windows.

- **Przy użyciu zasobów systemu operacyjnego przez Serwer administracyjny**

  Jeśli ta opcja jest włączona, pliki są przesyłane do urządzeń klienckich przy użyciu narzędzi systemu operacyjnego urządzeń klienckich za pośrednictwem Serwera administracyjnego. Możesz włączyć tę opcję, jeśli na urządzeniu klienckim nie ma zainstalowanego Agenta sieciowego, ale urządzenie klienckie jest w tej samej sieci co Serwer administracyjny.

  Domyślnie opcja ta jest włączona.

Określ ustawienie dodatkowe:

- **Nie instaluj aplikacji ponownie, jeżeli jest już zainstalowana**

  Jeśli ta opcja jest włączona, wybrana aplikacja nie zostanie ponownie zainstalowana, jeśli już jest zainstalowana na tym urządzeniu klienckim.

  Jeśli ta opcja jest wyłączona, aplikacja zostanie zainstalowana mimo wszystko.

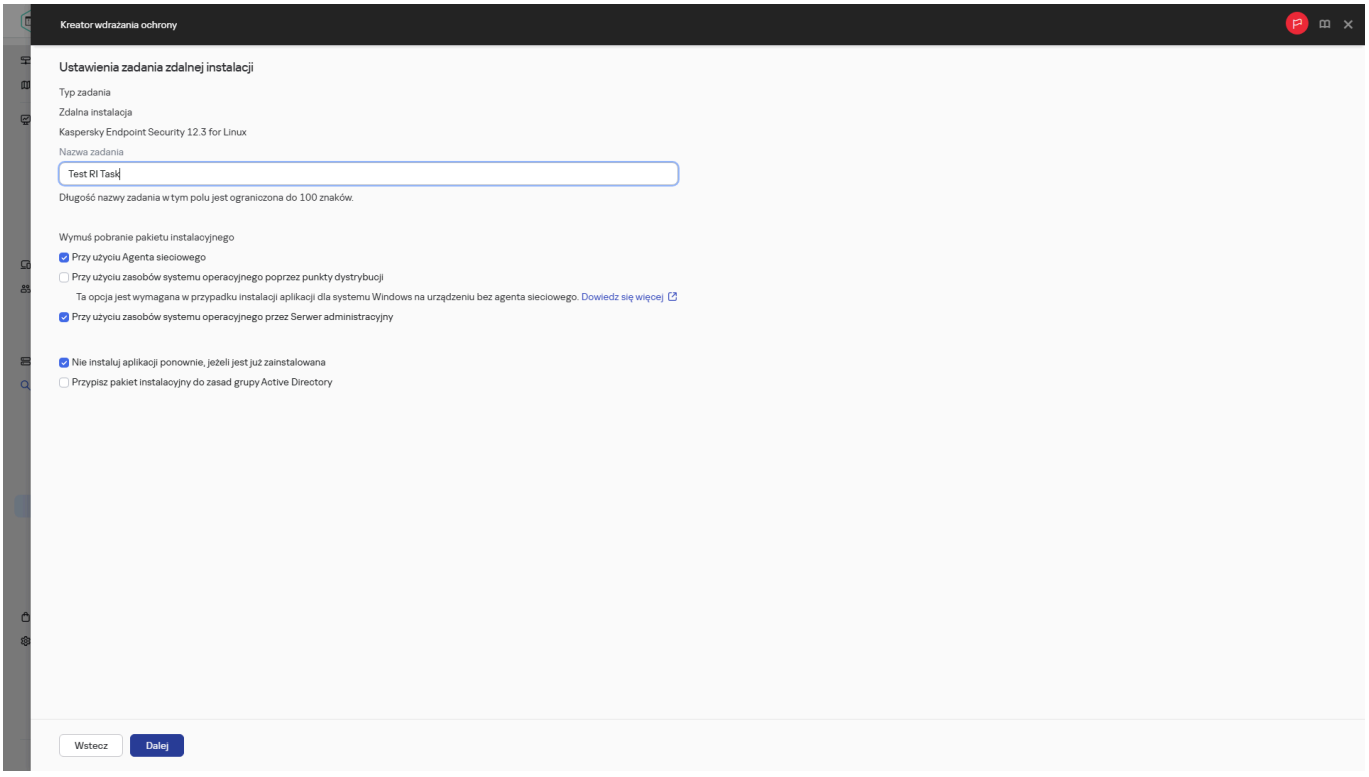
  Domyślnie opcja ta jest włączona.

- **Przypisz pakiet instalacyjny do zasad grupy Active Directory**

  Jeśli ta opcja jest włączona, pakiet instalacyjny jest instalowany przy użyciu zasad grupy Active Directory.

  Ta opcja jest dostępna, jeśli wybrany jest pakiet instalacyjny Agenta sieciowego.

  Domyślnie opcja ta jest wyłączona.



Określanie ustawień zadania zdalnej instalacji

Krok 7. Zarządzanie ponownym uruchomieniem

Określ działanie, jakie ma zostać wykonane, jeśli system operacyjny musi być uruchomiony ponownie podczas instalowania aplikacji:

- **Nie uruchamiaj ponownie urządzenia**

  Urządzenia klienckie nie są automatycznie uruchamiane ponownie po działaniu. Aby zakończyć działanie, należy uruchomić urządzenie ponownie (na przykład ręcznie lub przy użyciu zadania zarządzania urządzeniem). Informacje o wymaganym ponownym uruchomieniu zostaną zapisane w wynikach zadania oraz w statusie urządzenia. Opcja ta jest odpowiednia dla zadań na serwerach i innych urządzeniach, na których działanie ciągłe jest krytyczne.

- **Uruchom urządzenie ponownie**

  Urządzenia klienckie są zawsze automatycznie uruchamiane ponownie, jeśli jest to wymagane do zakończenia działania. Opcja jest przydatna, gdy zadania są uruchamiane na urządzeniach, na których możliwe są regularne przerwy w działaniu (wyłączenie lub ponowne uruchomienie).

- **Pytaj użytkownika o akcję**

  Na urządzeniu klienckim wyświetlane jest przypomnienie o ręcznym ponownym uruchomieniu urządzenia. Dla tej opcji można zdefiniować pewne ustawienia zaawansowane: treść wyświetlanego komunikatu, częstotliwość wyświetlania wiadomości oraz przedział czasu, po upływie którego ponowne uruchomienie zostanie wymuszone (bez potwierdzenia ze strony użytkownika). Ta opcja jest najodpowiedniejsza dla stacji roboczych, na których użytkownicy muszą mieć możliwość wyboru odpowiedniej godziny ponownego uruchomienia.

  Domyślnie opcja ta jest zaznaczona.

  - **Ponawiaj pytanie co (min)**

    Jeśli ta opcja jest włączona, aplikacja wyświetli pytanie o ponowne uruchomienie systemu operacyjnego z określoną częstotliwością.

    Domyślnie opcja ta jest włączona. Domyślnie przedział czasu wynosi 5 minut. Dostępne wartości znajdują się w zakresie od 1 do 1440 minut.

    Jeśli ta opcja jest wyłączona, monit zostaje wyświetlony tylko raz.

  - **Uruchom ponownie po (min)**

    Po wyświetleniu monitu, aplikacja wymusza ponowne uruchomienie systemu operacyjnego po minięciu określonego przedziału czasu.

    Domyślnie opcja ta jest włączona. Domyślne opóźnienie wynosi 30 minut. Dostępne wartości znajdują się w zakresie od 1 do 1440 minut.

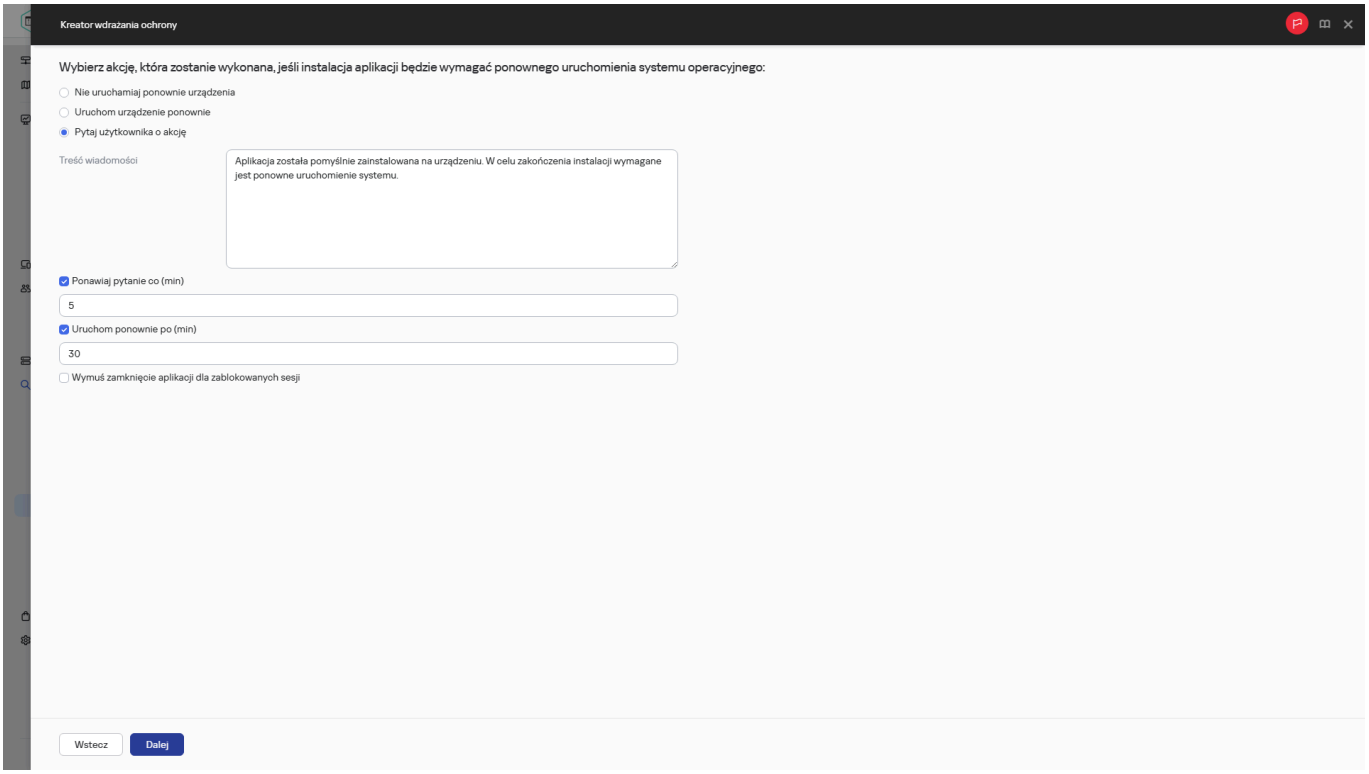
- **Wymuś zamknięcie aplikacji dla zablokowanych sesji**

  Uruchomione aplikacje mogą uniemożliwić ponowne uruchomienie urządzenia klienckiego. Na przykład, jeśli dokument jest edytowany w edytorze tekstu i nie zostanie zapisany, aplikacja nie zezwoli na ponowne uruchomienie urządzenia.

  Jeśli ta opcja jest włączona, zostaje wymuszone zamknięcie takich aplikacji na zablokowanym urządzeniu przed jego ponownym uruchomieniem. W wyniku tego działania użytkownicy mogą utracić niezapisane zmiany.

  Jeśli ta opcja jest wyłączona, zablokowane urządzenie nie zostanie uruchomione ponownie. Stan zadania na tym urządzeniu informuje, że wymagane jest ponowne uruchomienie urządzenia. Użytkownicy muszą ręcznie zamknąć wszystkie aplikacje uruchomione na zablokowanych urządzeniach i uruchomić ponownie te urządzenia.

Domyślnie opcja ta jest wyłączona.



Wybieranie opcji ponownego uruchamiania systemu operacyjnego

Krok 8. Usuwanie niekompatybilnych aplikacji przed instalacją

Ten krok jest dostępny tylko wtedy, gdy wiadomo, że aplikacja, którą instalujesz, jest niekompatybilna z innymi aplikacjami.

Wybierz opcję, jeśli chcesz, aby program Kaspersky Security Center Linux automatycznie usuwał aplikacje, które są niekompatybilne z instalowaną aplikacją.

Lista niekompatybilnych aplikacji także zostanie wyświetlona.

Jeśli nie wybierzesz tej opcji, aplikacja zostanie zainstalowana tylko na urządzeniach, na których nie ma niekompatybilnych aplikacji.

Krok 9. Przenoszenie urządzeń do grupy Zarządzane urządzenia

Określ, czy urządzenia powinny zostać przeniesione do grupy administracyjnej po zainstalowaniu Agenta sieciowego.

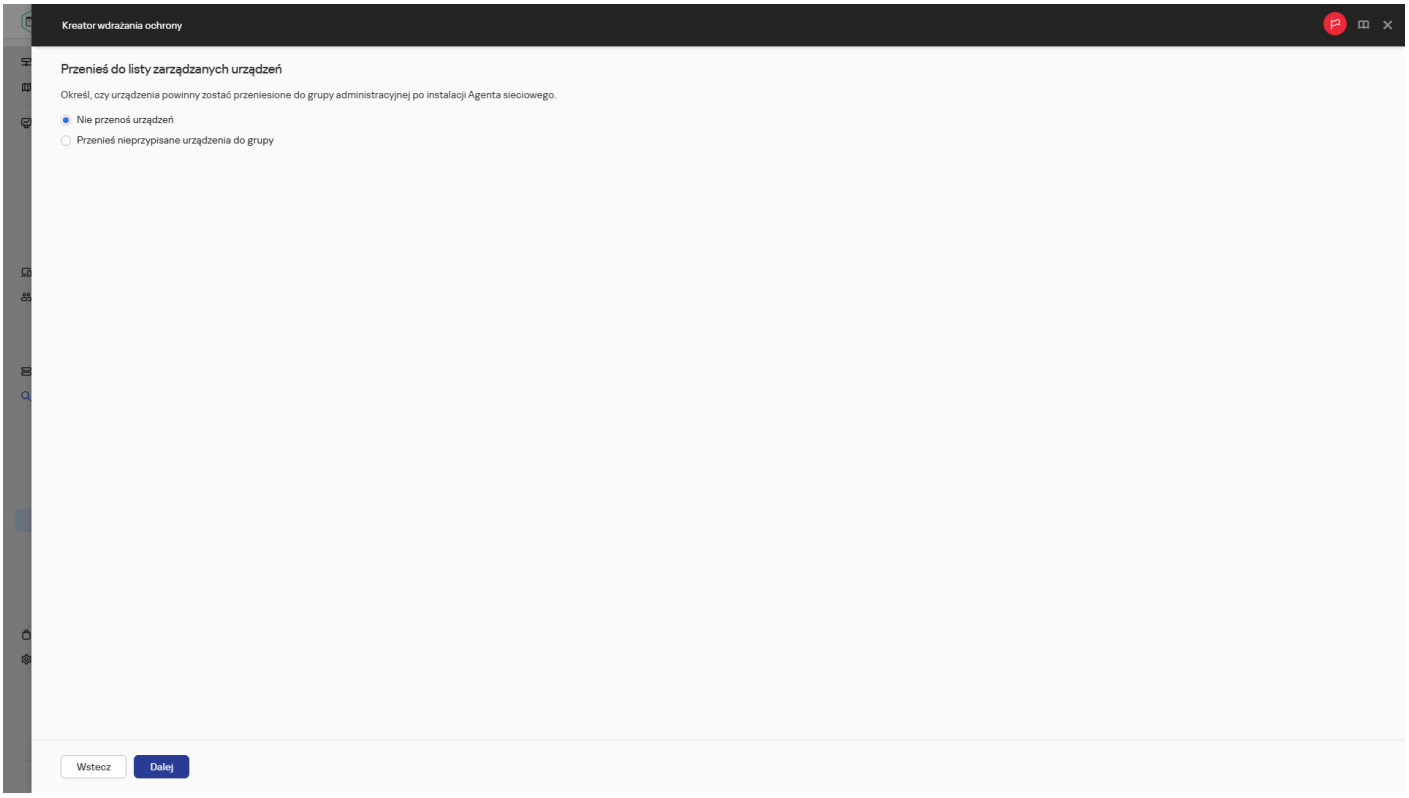
- **Nie przenoś urządzeń**

  Urządzenia pozostają w grupach, w których aktualnie się znajdują. Urządzenia, które zostały umieszczone w dowolnej grupie, pozostaną nieprzypisane.

- **Przenieś nieprzypisane urządzenia do grupy**

  Urządzenia są przenoszone do wybranej grupy administracyjnej.

Opcja **Nie przenoś urządzeń** została wybrana domyślnie. W celach bezpieczeństwa możesz ręcznie przenieść urządzenia.



Wybieranie opcji przeniesienia urządzeń do grupy administracyjnej

Krok 10. Wybieranie kont w celu uzyskania dostępu do urządzeń

Jeśli to konieczne, dodaj konta, które będą używane do uruchamiania zadania zdalnej instalacji:

- **Konto nie jest wymagane (Agent sieciowy jest zainstalowany)**

  Jeśli ta opcja jest zaznaczona, nie musisz określić konta, z poziomu którego zostanie uruchomiony instalator aplikacji. Zadanie zostanie uruchomione z poziomu konta, z którego uruchomiona jest usługa Serwera administracyjnego.

  Jeśli Agent sieciowy nie został zainstalowany na urządzeniach klienckich, ta opcja nie będzie dostępna.

- **Konto wymagane (Agent sieciowy nie jest używany)**

  Wybierz tę opcję, jeśli Agent sieciowy nie jest zainstalowany na urządzeniach, do których przypisano zadanie zdalnej instalacji. W takim przypadku możesz określić konto użytkownika lub certyfikat SSH, aby zainstalować aplikację.

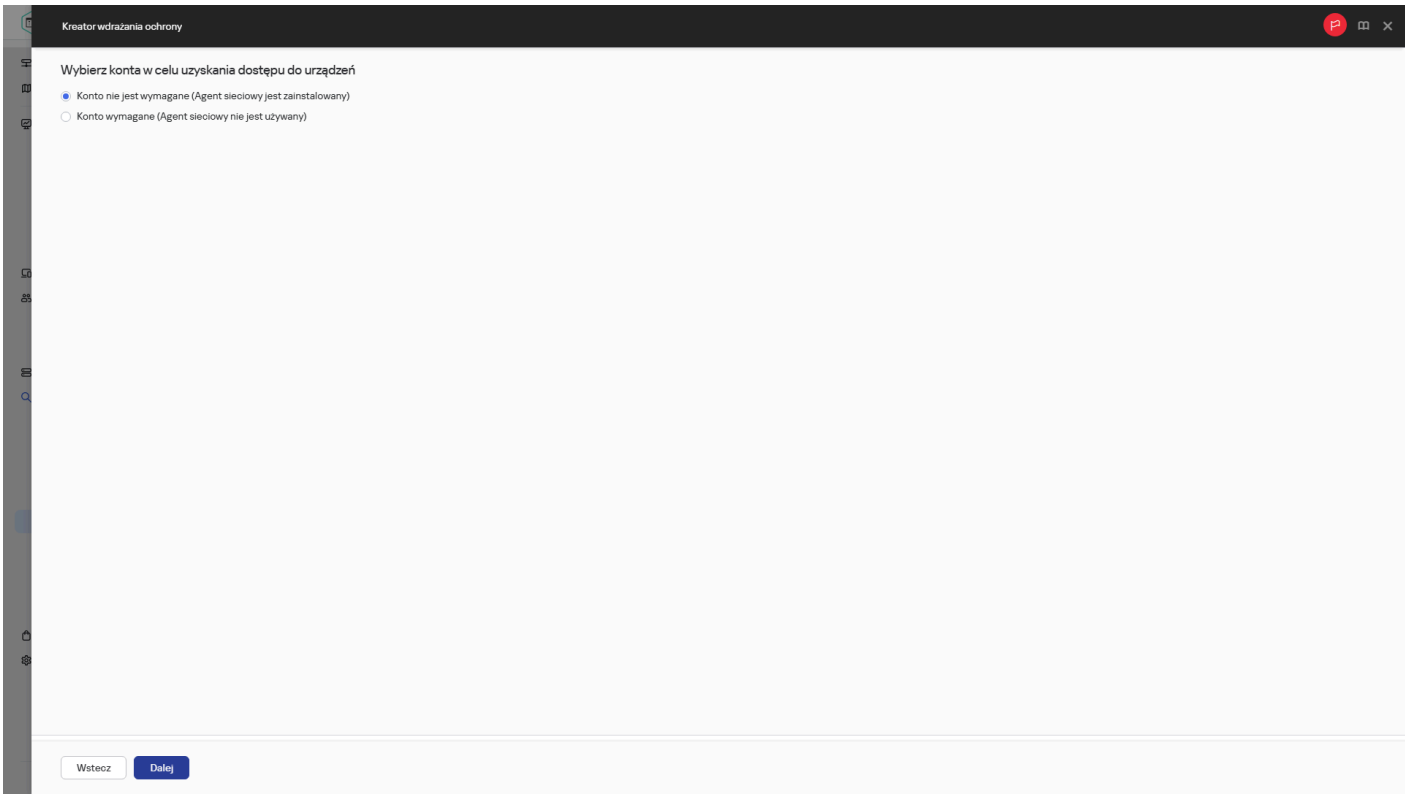
  - **Konto lokalne lub domenowe**. Jeśli ta opcja jest zaznaczona, określ konto użytkownika, z poziomu którego zostanie uruchomiony instalator aplikacji. Kliknij przycisk **Dodaj**, wybierz **Konto lokalne lub domenowe**, a następnie określ poświadczenia konta użytkownika.

    Możesz określić wiele kont użytkowników, jeśli na przykład żadne z nich nie ma wszystkich wymaganych uprawnień na wszystkich urządzeniach, do których przypisujesz zadanie. W tym przypadku wszystkie dodane konta są używane do uruchomienia zadania, zaczynając od góry.

  - **Certyfikat SSH**. Jeśli chcesz zainstalować aplikację na urządzeniu klienckim opartym na systemie Linux, możesz określić certyfikat SSH zamiast konta użytkownika. Kliknij przycisk **Dodaj**, wybierz **Certyfikat SSH**, a następnie określ klucze prywatny i publiczny certyfikatu.

Aby wygenerować klucz prywatny, możesz użyć narzędzia ssh-keygen. Należy zauważyć, że Kaspersky Security Center Linux obsługuje format PEM kluczy prywatnych, ale narzędzie ssh-keygen domyślnie generuje klucze SSH w formacie OPENSSH. Format OPENSSH nie jest obsługiwany przez Kaspersky Security Center Linux. Aby utworzyć klucz prywatny w obsługiwanym formacie PEM, dodaj opcję -m PEM w poleceniu ssh-keygen. Na przykład:

```
ssh-keygen -m PEM -t rsa -b 4096 -C "<adres e-mail użytkownika>"
```



Wybieranie kont w celu uzyskania dostępu do urządzeń

Krok 11. Uruchamianie instalacji

Ten krok to ostatni krok kreatora. W tym kroku **Zadanie zdalnej instalacji** zostało pomyślnie utworzone i skonfigurowane.

Domyślnie opcja **Uruchom zadanie po zakończeniu działania kreatora** nie jest zaznaczona. Jeśli wybierzesz tę opcję, **Zadanie zdalnej instalacji** zostanie uruchomione natychmiast po zakończeniu działania kreatora. Jeśli nie wybierzesz tej opcji, **Zadanie zdalnej instalacji** nie zostanie uruchomione. Możesz później uruchomić to zadanie ręcznie.

Kliknij **OK**, aby zakończyć ostatni krok kreatora wdrażania ochrony.

Aktualizacja Kaspersky Security Center Linux

Możesz zainstalować Serwer administracyjny w wersji 16.3 na urządzeniu, na którym jest zainstalowana wcześniejsza wersja Serwera administracyjnego (począwszy od wersji 13). Podczas aktualizowania do wersji 16.3 wszystkie dane i ustawienia z poprzedniej wersji Serwera administracyjnego zostają zachowane.

Wymagania wstępne

- Utwórz kopię zapasową danych Serwera administracyjnego przed rozpoczęciem aktualizacji.
- Podczas uaktualniania Serwera administracyjnego z wersji 16 lub starszej do wersji 16.1 lub nowszej, uwierzytelnianie dwuskładnikowe jest włączone. Aby uzyskać więcej informacji, zapoznaj się z sekcją Informacje o dwuetapowej weryfikacji dla konta.

  Aby upewnić się, że użytkownicy mogą logować się do Web Console za pomocą swoich istniejących kont, używając skonfigurowanych kluczy tajnych uwierzytelniania dwuskładnikowego, a skrypty automatyzacji OpenAPI będą nadal działać po uaktualnieniu, należy wykonać następujące kroki:

  - Włączanie uwierzytelniania dwuskładnikowego dla wszystkich użytkowników
  - Administratorzy muszą skonfigurować uwierzytelnianie dwuskładnikowe dla swoich kont
  - Wykluczanie kont z uwierzytelniania dwuskładnikowego

    W razie potrzeby dodaj konta integracji używane do uruchamiania skryptów za pośrednictwem OpenAPI do listy wykluczeń.
- Upewnij się, że korzystasz z wersji systemu operacyjnego i systemu DBMS, które są obsługiwane przez wersję 16.3 Serwera administracyjnego. Jeśli to konieczne, możesz przenieść Serwer administracyjny na inne urządzenie z nowszymi wersjami systemu operacyjnego i DBMS.
- Podczas uaktualniania Serwera administracyjnego z wersji 15.4 lub starszej do wersji 16 lub nowszej, na serwerze DBMS utwórz bazę danych dla IAM. Nazwa bazy danych musi być inna niż nazwa bazy danych, którą zainstalowałeś, aby działać z Kaspersky Security Center Linux.

  - W przypadku PostgreSQL uruchom następujące polecenie:

    ```
    sudo -i -u postgres psql -U postgres -c "CREATE DATABASE <iam_db_name>;"
    ```

  - W przypadku MariaDB uruchom następujące polecenie:

    ```
    sudo mysql -u root -p -e "CREATE DATABASE <iam_db_name>;"
    ```
- Podczas uaktualniania Serwera administracyjnego z wersji 15.4 lub starszej do wersji 16 lub nowszej, przygotuj plik odpowiedzi z nowymi parametrami dla IAM. Listę wymaganych parametrów można znaleźć w artykule: Instalowanie Kaspersky Security Center Linux w trybie cichym. Dodaj zmienną środowiskową `KLAUTOANSWERS` i ustaw jej wartość na ścieżkę do pliku odpowiedzi.
- Udostępnij port używany przez proces kliam do uwierzytelniania protokołu OpenID Connect. Domyślnie 4444. Zapoznaj się z opisem parametru `trusted` w następującym artykule: Parametry instalacji Kaspersky Security Center Web Console.

Etapy

1. **Aktualizacja Serwera administracyjnego**

   Wersję Serwera administracyjnego można zaktualizować, korzystając z jednej z następujących metod:

   - Korzystając z pliku instalacyjnego Kaspersky Security Center Linux
   - Tworząc kopię zapasową danych Serwera administracyjnego, instalując nową wersję Serwera administracyjnego i przywracając dane Serwera administracyjnego z kopii zapasowej

   > Podczas aktualizacji równoczesne korzystanie z DBMS przez Serwer administracyjny i inną aplikację jest surowo zabronione.

   Jeżeli Twoja sieć zawiera kilka Serwerów administracyjnych, musisz zaktualizować każdy Serwer ręcznie. Kaspersky Security Center Linux nie obsługuje scentralizowanej aktualizacji.

2. **Uruchomienie skryptu postinstall.pl (krok opcjonalny)**

   Jeśli plik odpowiedzi nie zawiera parametrów IAM lub nie można znaleźć pliku odpowiedzi, podczas aktualizacji w terminalu zostanie wyświetlony komunikat z prośbą o uruchomienie skryptu postinstall.pl.

   Na tym etapie scenariusza wykonaj następujące czynności:

   1. W systemie operacyjnym Serwera administracyjnego utwórz konto użytkownika bez uprawnień „ksciam", które musi należeć do grupy „kladmins":

      ```
      adduser ksciam
      gpasswd -a ksciam kladmins
      usermod -g kladmins ksciam
      ```

   2. Na koncie z uprawnieniami administratora uruchom skrypt /opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl w celu skonfigurowania zaktualizowanego Serwera administracyjnego. Po wyświetleniu monitu wprowadź następujące ustawienia:

      1. Wprowadź nazwę DNS serwera FQDN. Należy użyć nazwy DNS Serwera administracyjnego określonej podczas instalacji Kaspersky Security Center Linux.
      2. Wprowadź nazwę konta, aby uruchomić usługę IAM. Konto musi należeć do wprowadzonej grupy zabezpieczeń. Domyślnie używane jest konto ksciam.
      3. Wybierz DBMS, który zainstalowałeś do pracy z usługą IAM:
         - Jeśli zainstalowałeś MySQL lub MariaDB, wpisz 1.
         - Jeśli zainstalowałeś PostgreSQL lub Postgres Pro, wpisz 2.
      4. Wprowadź adres IAM DBMS, który ma być używany przez usługę IAM.

5. Wprowadź numer portu IAM DBMS. Ten port jest używany do komunikacji z usługą IAM. Domyślnie używane są następujące porty:
   - Port 3306 dla MySQL lub MariaDB
   - Port 5432 dla PostgreSQL lub Postgres Pro
6. Wprowadź nazwę bazy danych IAM, która ma być używana przez usługę IAM. Nazwa bazy danych używanej przez usługę IAM powinna być inna niż nazwa bazy danych używanej przez Serwer administracyjny.

3. **Zaktualizuj Kaspersky Security Center Web Console do nowej wersji**
4. **(Opcjonalnie) Aktualizacja agenta sieciowego na urządzeniach do nowej wersji.**
5. **Upewnij się, że lista dozwolonych kont uwierzytelniania dwuskładnikowego zawiera tylko konta użytkowników, które muszą mieć dostęp do Serwera administracyjnego.**

   Przejrzyj listę dozwolonych kont uwierzytelniania dwuskładnikowego i usuń z niej wszystkie inne konta.

Pamiętaj, że jeśli zaktualizujesz Serwer administracyjny do wersji 16.3, nie będzie można tworzyć nowych pakietów instalacyjnych Agenta sieciowego w wersji 15 lub starszej. Jednakże wcześniej utworzone pakiety instalacyjne będą dostępne.

Podczas gdy aktualizujesz Kaspersky Security Center Linux z poprzedniej wersji, wszystkie zainstalowane wtyczki obsługiwanych aplikacji Kaspersky są zachowywane. Wtyczki Serwera administracyjnego i Agenta sieciowego zostają zaktualizowane automatycznie.

Aktualizacja Kaspersky Security Center Linux z wersji 16 lub nowszej

W tej sekcji opisano następujące opcje aktualizacji Kaspersky Security Center Linux z wersji 16 lub nowszej do najnowszej wersji:

- Aktualizacja przy użyciu pliku instalacyjnego
- Aktualizacja za pomocą kopii zapasowej
- Aktualizacja na węzłach klastra trybu failover Kaspersky Security Center Linux

Aktualizowanie Kaspersky Security Center Linux z wersji 16 lub nowszej przy użyciu pliku instalatora

Aby zaktualizować Serwer administracyjny z wersji 16 do najnowszej wersji, możesz zainstalować nową wersję na wcześniejszej przy użyciu pliku instalacyjnego Kaspersky Security Center Linux.

Aby zaktualizować Kaspersky Security Center Linux z wersji 16 lub nowszej do najnowszej wersji przy użyciu pliku instalatora:

1. Pobierz plik instalacyjny Kaspersky Security Center Linux z pełnym pakietem dla wersji 16.3 ze strony internetowej Kaspersky:

   - W przypadku urządzeń z systemem operacyjnym opartym na RPM — `ksc64-<version number>.x86_64.rpm`

   - W przypadku urządzeń z systemem operacyjnym opartym na Debianie — `ksc64_<version number>_amd64.deb`

2. Rozpocznij aktualizację Kaspersky Security Center Linux. Uruchom następujące polecenie w terminalu wiersza poleceń:

   - W przypadku urządzeń z systemem operacyjnym opartym na RPM:

     ```
     sudo yum install ./ksc64-<version number>.x86_64.rpm
     ```

   - Dla urządzeń z systemem operacyjnym opartym na systemie Debian:

     ```
     sudo apt-get install ./ksc64_<version number>_amd64.deb
     ```

   Po pomyślnym wykonaniu polecenia tworzony jest skrypt `/opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl`. Komunikat o tym jest wyświetlany w terminalu.

3. Uruchom skrypt `/opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl` w celu skonfigurowania zaktualizowanego Serwera administracyjnego:

   ```
   sudo /opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl
   ```

4. Przeczytaj Umowę licencyjną i Politykę prywatności, które pojawiają się w terminalu wiersza poleceń. Jeśli zgadzasz się ze wszystkimi warunkami Umowy licencyjnej i Polityki prywatności:

   a. Wpisz `Y`, aby potwierdzić, że w pełni przeczytałeś, zrozumiałeś i akceptujesz warunki Umowy licencyjnej użytkownika końcowego.

   b. Wpisz ponownie `Y`, aby potwierdzić, że w pełni przeczytałeś, zrozumiałeś i akceptujesz Politykę prywatności opisującą sposób postępowania z danymi.

   Instalacja aplikacji na Twoim urządzeniu będzie kontynuowana po dwukrotnym wpisaniu `Y`.

5. Wpisz `1`, aby wybrać standardowy tryb instalacji Serwera administracyjnego.

Poniższy obrazek przedstawia dwa ostatnie kroki.

```
Enter 'Y' to confirm that you understand and accept the terms of the End
User License Agreement (EULA). You must accept the terms and conditions of
the EULA to install the application. Enter 'N' providing you do not accept
the terms of the EULA or 'R' to view it again [N]:
y

Enter 'Y' to confirm that you accept the terms of the Privacy Policy. You
must accept the terms and conditions of the Privacy Policy to install the
application. Entering 'Y' means that you are aware that your data will be
handled and transmitted (including to third countries) as described in the
Privacy Policy. Enter 'N' providing you do not accept the Privacy Policy
[N]:
y

Choose the Administration Server installation mode:
1) Standard
2) Primary cluster node
3) Secondary cluster node
Enter the range number (1, 2, or 3) [1]:
```

Zaakceptowanie warunków Umowy licencyjnej użytkownika końcowego i Polityki prywatności oraz wybranie standardowego trybu instalacji Serwera administracyjnego w terminalu wiersza poleceń

Następnie instalator konfiguruje i kończy aktualizację Serwera administracyjnego. Podczas aktualizacji nie możesz zmienić ustawień Serwera administracyjnego, które zostały dostosowane przed aktualizacją.

6. Zaktualizuj Kaspersky Security Center Web Console do nowej wersji.

7. Dla urządzeń, na których została zainstalowana wcześniejsza wersja Agenta sieciowego, utwórz i uruchom zadanie zdalnej instalacji nowej wersji Agenta sieciowego.

   Zalecamy aktualizację Agenta sieciowego dla systemu Linux do tej samej wersji co Kaspersky Security Center Linux.

   Po zakończeniu wykonywania zadania zdalnej instalacji, wersja Agenta sieciowego zostanie zaktualizowana.

   Uruchom następujące polecenia na zasobach opartych na systemie Linux, aby usunąć zależności, które nie są już potrzebne:

   - W przypadku zasobów opartych na systemie Debianie uruchom dowolne z następujących poleceń:

     ```
     sudo apt-get -y autoremove
     ```

     ```
     sudo apt -y autoremove
     ```

   - W przypadku zasobów opartych na systemie RPM uruchom dowolne z następujących poleceń:

     ```
     sudo dnf autoremove
     ```

     ```
     sudo yum autoremove
     ```

Aktualizacja Kaspersky Security Center Linux z wersji 16 lub nowszej za pomocą kopii zapasowej

Aby zaktualizować Serwer administracyjny z wersji 16 do najnowszej wersji, możesz utworzyć kopię zapasową danych Serwera administracyjnego i przywrócić te dane po zainstalowaniu nowej wersji Kaspersky Security Center Linux. Jeżeli podczas instalacji Serwera administracyjnego pojawią się problemy, będzie można przywrócić poprzednią wersję Serwera administracyjnego przy pomocy kopii zapasowej danych Serwera administracyjnego utworzonej przed aktualizacją.

Aby zaktualizować Kaspersky Security Center Linux z wersji 16 lub nowszej do najnowszej wersji przy użyciu kopii zapasowej:

1. Przed aktualizacją utwórz kopię zapasową danych Serwera administracyjnego przy użyciu starszej wersji aplikacji.

2. Odinstaluj starszą wersję Kaspersky Security Center Linux.

3. Zainstaluj Kaspersky Security Center Linux w wersji 16.3 na urządzeniu, na którym wcześniej zainstalowano Serwer administracyjny.

   Jeśli schemat bazy danych w kopii zapasowej różni się od schematu aktualnie używanego przez Serwer administracyjny lub IAM, dane zostaną przywrócone do bieżącego schematu.

   Jeśli w kopii zapasowej używany jest schemat publiczny, muszą zostać spełnione następujące warunki:

   - W bazie danych istnieje schemat publiczny.
   - Publiczny schemat bazy danych można modyfikować z poziomu konta DBMS używanego przez Serwer administracyjny lub IAM w celu uzyskania dostępu do bazy danych.

   W przeciwnym razie przywracanie danych zakończy się błędem.

4. Przywróć dane Serwera administracyjnego z kopii zapasowej utworzonej przed aktualizacją.

5. Zainstaluj Kaspersky Security Center Web Console.

   Jeśli Kaspersky Security Center Web Console została zainstalowana wcześniej, zainstaluj ją ponownie z tym samym plikiem odpowiedzi.

   Zaloguj się do Kaspersky Security Center Web Console na koncie użytkownika wewnętrznego administratora.

   Proces inicjalizacji danych trwa zazwyczaj do 15 minut po przywróceniu danych Serwera administracyjnego, lecz czas ten zależy od wydajności sprzętu i rozmiaru danych Serwera administracyjnego. W tym czasie Kaspersky Security Center Web Console może nie nawiązać połączenia i mogą zostać wyświetlone błędy.

6. Dla urządzeń, na których została zainstalowana wcześniejsza wersja Agenta sieciowego, utwórz i uruchom zadanie zdalnej instalacji nowej wersji Agenta sieciowego.

   > Zalecamy aktualizację Agenta sieciowego dla systemu Linux do tej samej wersji co Kaspersky Security Center Linux.

   Po zakończeniu wykonywania zadania zdalnej instalacji, wersja Agenta sieciowego zostanie zaktualizowana.

Uruchom następujące polecenia na zasobach opartych na systemie Linux, aby usunąć zależności, które nie są już potrzebne:

- W przypadku zasobów opartych na systemie Debianie uruchom dowolne z następujących poleceń:

```
sudo apt-get -y autoremove
```

```
sudo apt -y autoremove
```

- W przypadku zasobów opartych na systemie RPM uruchom dowolne z następujących poleceń:

```
sudo dnf autoremove
```

```
sudo yum autoremove
```

Aktualizowanie Kaspersky Security Center Linux od wersji 16 lub nowszej na węzłach klastra trybu failover Kaspersky Security Center Linux

Najnowszą wersję Serwera administracyjnego można zainstalować na każdym węźle klastra trybu failover Kaspersky Security Center Linux, na którym zainstalowano Serwer administracyjny w wersji 16 lub nowszej. Podczas aktualizowania do najnowszej wersji, wszystkie dane i ustawienia z poprzedniej wersji Serwera administracyjnego zostają zachowane.

Jeśli wcześniej instalowałeś lokalnie Kaspersky Security Center Linux na urządzeniach, możesz także zaktualizować Kaspersky Security Center Linux na tych urządzeniach, korzystając z pliku instalacyjnego lub kopii zapasowej.

Aktualizowanie Kaspersky Security Center Linux od wersji 16 lub nowszej na węzłach klastra trybu failover Kaspersky Security Center Linux:

1. Pobierz plik instalacyjny Kaspersky Security Center Linux z pełnym pakietem dla wersji 16.3 ze strony internetowej Kaspersky:

   - W przypadku urządzeń z systemem operacyjnym opartym na RPM — `ksc64-<version number>-<build number>.x86_64.rpm`

   - W przypadku urządzeń z systemem operacyjnym opartym na systemie Debian — `ksc64_<version number>-<build number>_amd64.deb`

2. Zatrzymaj klaster.

3. Na aktywnym węźle klastra uruchom następujące polecenie w terminalu wiersza poleceń, aby uruchomić aktualizację:

   - W przypadku urządzeń z systemem operacyjnym opartym na RPM:

     ```
     sudo yum install ./ksc64-<version number>-<build number>.x86_64.rpm
     ```

   - Dla urządzeń z systemem operacyjnym opartym na systemie Debian:

     ```
     sudo apt-get install ./ksc64_<version number>-<build number>_amd64.deb
     ```

   Po pomyślnym wykonaniu polecenia tworzony jest skrypt `/opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl`. Komunikat o tym jest wyświetlany w terminalu.

4. Uruchom skrypt `/opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl` w celu skonfigurowania zaktualizowanego Serwera administracyjnego:

   ```
   sudo /opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl
   ```

5. Przeczytaj Umowę licencyjną i Politykę prywatności, które pojawiają się w terminalu wiersza poleceń. Jeśli zgadzasz się ze wszystkimi warunkami Umowy licencyjnej i Polityki prywatności:

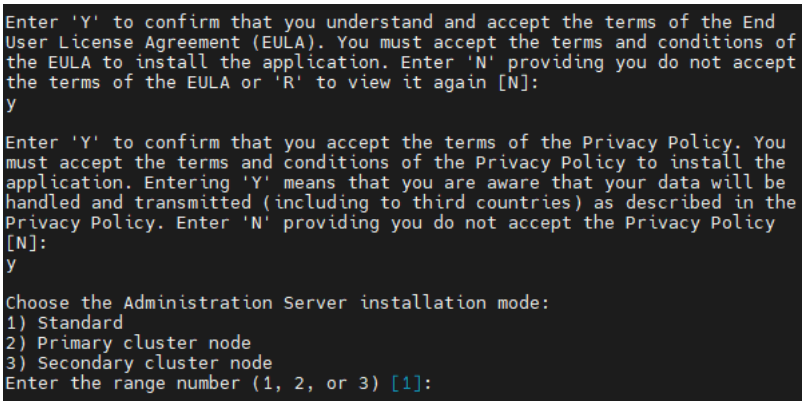
   a. Wpisz `Y`, aby potwierdzić, że w pełni przeczytałeś, zrozumiałeś i akceptujesz warunki Umowy licencyjnej użytkownika końcowego.

   b. Wpisz ponownie `Y`, aby potwierdzić, że w pełni przeczytałeś, zrozumiałeś i akceptujesz Politykę prywatności opisującą sposób postępowania z danymi.

   Instalacja aplikacji na Twoim urządzeniu będzie kontynuowana po dwukrotnym wpisaniu `Y`.

6. Wybierz węzeł, na którym przeprowadzasz aktualizację, wpisując `2`.

   Poniższy obrazek przedstawia dwa ostatnie kroki.



Zaakceptowanie warunków Umowy licencyjnej użytkownika końcowego i Polityki prywatności oraz wybranie trybu instalacji w terminalu wiersza poleceń

   Następnie instalator konfiguruje i kończy aktualizację Serwera administracyjnego. Podczas aktualizacji nie możesz zmienić ustawień Serwera administracyjnego, które zostały dostosowane przed aktualizacją.

7. Wykonaj kroki 3–5 na węźle pasywnym.

   W kroku 6 wprowadź `3`, aby wybrać węzeł.

8. Uruchom klaster.

> Możesz uruchomić klaster na dowolnym węźle. Jeśli uruchomisz klaster w węźle pasywnym, stanie się on węzłem aktywnym.

9. Dla urządzeń, na których jest instalowana wcześniejsza wersja Agenta sieciowego, utwórz i uruchom zadanie zdalnej instalacji nowej wersji Agenta sieciowego.

> Zalecamy aktualizację Agenta sieciowego dla systemu Linux do tej samej wersji co Kaspersky Security Center Linux.

Po zakończeniu wykonywania zadania zdalnej instalacji, wersja Agenta sieciowego zostanie zaktualizowana.

Uruchom następujące polecenia na zasobach opartych na systemie Linux, aby usunąć zależności, które nie są już potrzebne:

- W przypadku zasobów opartych na systemie Debianie uruchom dowolne z następujących poleceń:

```
sudo apt-get -y autoremove
```

```
sudo apt -y autoremove
```

- W przypadku zasobów opartych na systemie RPM uruchom dowolne z następujących poleceń:

```
sudo dnf autoremove
```

```
sudo yum autoremove
```

W rezultacie zainstalowałeś Serwer administracyjny najnowszej wersji na węzłach klastra typu failover Kaspersky Security Center Linux.

Aktualizacja Kaspersky Security Center Linux z wersji 15.4 lub starszej

W tej sekcji opisano następujące opcje aktualizacji Kaspersky Security Center Linux z wersji 15.4 lub starszej do wersji 16 lub nowszej:

- Aktualizacja przy użyciu pliku instalacyjnego
- Aktualizacja za pomocą kopii zapasowej
- Aktualizacja na węzłach klastra trybu failover Kaspersky Security Center Linux

Każda opcja aktualizacji Kaspersky Security Center Linux z wersji 15.4 lub starszej do wersji 16 lub nowszej obejmuje kroki tworzenia i konfigurowania bazy danych IAM na serwerze DBMS, tworzenia konta bez uprawnień „ksciam" w celu uruchomienia usługi IAM oraz dodawania tego konta do grupy zabezpieczeń „kladmins".

Aktualizacja Kaspersky Security Center Linux z wersji 15.4 lub starszej przy użyciu pliku instalacyjnego

Aby zaktualizować Serwer administracyjny z wersji 13—15.4 do wersji 16 lub nowszej, możesz zainstalować nową wersję na wcześniejszej przy użyciu pliku instalacyjnego Kaspersky Security Center Linux.

Przed rozpoczęciem, **sprawdź wymagania dotyczące certyfikatu niestandardowego**.

Jeśli używasz certyfikatu niestandardowego zamiast certyfikatu z podpisem własnym, przed aktualizacją Kaspersky Security Center Linux do nowszej wersji upewnij się, że certyfikat zawiera Alternatywną nazwę podmiotu (SAN). Jeżeli nie zawiera, ważne jest, aby wymienić certyfikat przed aktualizacją Kaspersky Security Center Linux. W przeciwnym razie nie będziesz mógł zalogować się do Web Console po aktualizacji.

Aby upewnić się, że certyfikat zawiera Alternatywną nazwę podmiotu (SAN):

1. Na urządzeniu z zainstalowanym Serwerem administracyjnym, wykonaj następujące polecenie:

   - W przypadku urządzenia z systemem Linux:

     ```
     sudo openssl x509 -in /var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer -noout -ext subjectAltName
     ```

   - W przypadku urządzenia z systemem Windows:

     ```
     certutil -dump %ProgramData%\KasperskyLab\adminkit\1093\cert\klserver.cer
     ```

2. Upewnij się, że Alternatywna nazwa podmiotu jest obecna w wynikach polecenia i zawiera adres urządzenia Serwera administracyjnego.

3. Jeśli Alternatywna nazwa podmiotu jest niedostępna, użyj narzędzia klsetsrvcert, aby zastąpić certyfikat niestandardowy tym, który spełnia wymagania.

Aby zaktualizować Kaspersky Security Center Linux z wersji 15.4 lub starszej do najnowszej wersji przy użyciu pliku instalacyjnego:

1. Pobierz plik instalacyjny Kaspersky Security Center Linux z pełnym pakietem dla wersji 16.3 ze strony internetowej Kaspersky:

   - W przypadku urządzeń z systemem operacyjnym opartym na RPM — `ksc64-<version number>.x86_64.rpm`

   - W przypadku urządzeń z systemem operacyjnym opartym na Debianie — `ksc64_<version number>_amd64.deb`

2. Na serwerze DBMS utwórz bazę danych dla IAM. Nazwa bazy danych IAM musi być inna niż nazwa bazy danych używanej przez Serwer administracyjny.

   - W przypadku PostgreSQL uruchom następujące polecenie:

     ```
     sudo -i -u postgres psql -U postgres -c "CREATE DATABASE <iam_db_name>;"
     ```

- W przypadku MariaDB uruchom następujące polecenie:

```
sudo mysql -u root -p -e "CREATE DATABASE <iam_db_name>;"
```

3. Utwórz nieuprzywilejowane konto „ksciam”, dodaj je do grupy zabezpieczeń „kladmins”, a następnie ustaw grupę „kladmins” jako grupę podstawową dla konta „ksciam”. Aby to zrobić, kolejno uruchom następujące polecenia:

```
sudo adduser ksciam
sudo gpasswd -a ksciam kladmins
sudo usermod -g kladmins ksciam
```

4. Rozpocznij aktualizację Kaspersky Security Center Linux. Uruchom następujące polecenie w terminalu wiersza poleceń:

   - W przypadku urządzeń z systemem operacyjnym opartym na RPM:

   ```
   sudo yum install ./ksc64-<numer wersji>.x86_64.rpm
   ```

   - Dla urządzeń z systemem operacyjnym opartym na systemie Debian:

   ```
   sudo apt-get install ./ksc64_<numer wersji>_amd64.deb
   ```

   Po pomyślnym wykonaniu polecenia tworzony jest skrypt `/opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl`. Komunikat o tym jest wyświetlany w terminalu.

5. Uruchom skrypt `/opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl` w celu skonfigurowania zaktualizowanego Serwera administracyjnego:

```
sudo /opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl
```

6. Przeczytaj Umowę licencyjną i Politykę prywatności, które pojawiają się w terminalu wiersza poleceń. Jeśli zgadzasz się ze wszystkimi warunkami Umowy licencyjnej i Polityki prywatności:

   a. Wpisz `Y`, aby potwierdzić, że w pełni przeczytałeś, zrozumiałeś i akceptujesz warunki Umowy licencyjnej użytkownika końcowego.

   b. Wpisz ponownie `Y`, aby potwierdzić, że w pełni przeczytałeś, zrozumiałeś i akceptujesz Politykę prywatności opisującą sposób postępowania z danymi.

   Instalacja aplikacji na Twoim urządzeniu będzie kontynuowana po dwukrotnym wpisaniu `Y`.

7. Wpisz `1`, aby wybrać standardowy tryb instalacji Serwera administracyjnego.

Poniższy obrazek przedstawia dwa ostatnie kroki.

```
Enter 'Y' to confirm that you understand and accept the terms of the End
User License Agreement (EULA). You must accept the terms and conditions of
the EULA to install the application. Enter 'N' providing you do not accept
the terms of the EULA or 'R' to view it again [N]:
y

Enter 'Y' to confirm that you accept the terms of the Privacy Policy. You
must accept the terms and conditions of the Privacy Policy to install the
application. Entering 'Y' means that you are aware that your data will be
handled and transmitted (including to third countries) as described in the
Privacy Policy. Enter 'N' providing you do not accept the Privacy Policy
[N]:
y

Choose the Administration Server installation mode:
1) Standard
2) Primary cluster node
3) Secondary cluster node
Enter the range number (1, 2, or 3) [1]:
```

Zaakceptowanie warunków Umowy licencyjnej użytkownika końcowego i Polityki prywatności oraz wybranie standardowego trybu instalacji Serwera administracyjnego w terminalu wiersza poleceń

8. Następnie instalator konfiguruje i kończy aktualizację Serwera administracyjnego. Podczas aktualizacji nie możesz zmienić ustawień Serwera administracyjnego, które zostały dostosowane przed aktualizacją. Po wyświetleniu monitu wprowadź następujące ustawienia:

   a. Wprowadź nazwę DNS serwera FQDN.

      Należy użyć nazwy DNS Serwera administracyjnego określonej podczas instalacji Kaspersky Security Center Linux.

   b. Wprowadź nazwę konta, aby uruchomić usługę IAM. Konto musi należeć do wprowadzonej grupy zabezpieczeń. Domyślnie używane jest konto ksciam.

   c. Wybierz DBMS, który zainstalowałeś do pracy z usługą IAM:

      - Jeśli zainstalowałeś MySQL lub MariaDB, wpisz `1`.
      - Jeśli zainstalowałeś PostgreSQL lub Postgres Pro, wpisz `2`.

   d. Wprowadź adres IAM DBMS, który ma być używany przez usługę IAM.

   e. Wprowadź numer portu IAM DBMS. Ten port jest używany do komunikacji z usługą IAM. Domyślnie używane są następujące porty:

      - Port 3306 dla MySQL lub MariaDB
      - Port 5432 dla PostgreSQL lub Postgres Pro

   f. Wprowadź nazwę bazy danych IAM, która ma być używana przez usługę IAM. Nazwa bazy danych używanej przez usługę IAM powinna być inna niż nazwa bazy danych używanej przez Serwer administracyjny.

   g. Wprowadź login i hasło DBMS, który ma być używany przez usługę IAM.

   h. Jeśli zainstalowano PostgreSQL lub Postgres Pro, można określić schemat bazy danych, który ma być używany przez IAM. Aby to zrobić, podaj nazwę schematu.

      Jeśli nie chcesz używać schematu niestandardowego, naciśnij `ENTER`, a zostanie użyty schemat publiczny.

      > W nazwie schematu rozróżniana jest wielkość liter: należy używać wyłącznie małych liter.
      > Nie określaj zarezerwowanych nazw schematów iam: `client, iam, ksc, locker, pat, scope, voltron`.

9. Zaktualizuj Kaspersky Security Center Web Console do nowej wersji.

10. Dla urządzeń, na których została zainstalowana wcześniejsza wersja Agenta sieciowego, utwórz i uruchom zadanie zdalnej instalacji nowej wersji Agenta sieciowego.

    Zalecamy aktualizację Agenta sieciowego dla systemu Linux do tej samej wersji co Kaspersky Security Center Linux.

    Po zakończeniu wykonywania zadania zdalnej instalacji, wersja Agenta sieciowego zostanie zaktualizowana.

    Uruchom następujące polecenia na zasobach opartych na systemie Linux, aby usunąć zależności, które nie są już potrzebne:

    - W przypadku zasobów opartych na systemie Debianie uruchom dowolne z następujących poleceń:

      ```
      sudo apt-get -y autoremove
      ```

      ```
      sudo apt -y autoremove
      ```

    - W przypadku zasobów opartych na systemie RPM uruchom dowolne z następujących poleceń:

      ```
      sudo dnf autoremove
      ```

      ```
      sudo yum autoremove
      ```

Aktualizowanie Kaspersky Security Center Linux z wersji 15.4 lub starszej poprzez kopię zapasową

Aby uaktualnić Serwer administracyjny z wersji 14.2—15.4 do wersji 16 lub nowszej, możesz utworzyć kopię zapasową danych Serwera administracyjnego i przywrócić ją po zainstalowaniu nowej wersji Kaspersky Security Center Linux. Jeżeli podczas instalacji Serwera administracyjnego pojawią się problemy, będzie można przywrócić poprzednią wersję Serwera administracyjnego przy pomocy kopii zapasowej danych Serwera administracyjnego utworzonej przed aktualizacją.

Wymagania wstępne

1. **Sprawdź wymagania dotyczące certyfikatu niestandardowego**.

   Jeśli używasz certyfikatu niestandardowego zamiast certyfikatu z podpisem własnym, przed aktualizacją Kaspersky Security Center Linux do nowszej wersji upewnij się, że certyfikat zawiera Alternatywną nazwę podmiotu (SAN). Jeżeli nie zawiera, ważne jest, aby wymienić certyfikat przed aktualizacją Kaspersky Security Center Linux. W przeciwnym razie nie będziesz mógł zalogować się do Web Console po aktualizacji.

Aby upewnić się, że certyfikat zawiera Alternatywną nazwę podmiotu (SAN):

1. Na urządzeniu z zainstalowanym Serwerem administracyjnym, wykonaj następujące polecenie:

   - W przypadku urządzenia z systemem Linux:

     ```
     sudo openssl x509 -in /var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer -noout -ext subjectAltName
     ```

   - W przypadku urządzenia z systemem Windows:

     ```
     certutil -dump %ProgramData%\KasperskyLab\adminkit\1093\cert\klserver.cer
     ```

2. Upewnij się, że Alternatywna nazwa podmiotu jest obecna w wynikach polecenia i zawiera adres urządzenia Serwera administracyjnego.

3. Jeśli Alternatywna nazwa podmiotu jest niedostępna, użyj narzędzia klsetsrvcert, aby zastąpić certyfikat niestandardowy tym, który spełnia wymagania.

2. Utwórz kopię zapasową danych Serwera administracyjnego przy użyciu starszej wersji aplikacji.

Procedura aktualizacji

Aby uaktualnić Kaspersky Security Center Linux z wersji 15.4 lub starszej do najnowszej wersji poprzez kopię zapasową:

1. Odinstaluj starszą wersję Kaspersky Security Center Linux.

2. Na serwerze DBMS utwórz bazę danych dla IAM. Nazwa bazy danych IAM musi być inna niż nazwa bazy danych używanej przez Serwer administracyjny.

   - W przypadku PostgreSQL uruchom następujące polecenie:

     ```
     sudo -i -u postgres psql -U postgres -c "CREATE DATABASE <iam_db_name>;"
     ```

   - W przypadku MariaDB uruchom następujące polecenie:

     ```
     sudo mysql -u root -p -e "CREATE DATABASE <iam_db_name>;"
     ```

3. Utwórz nieuprzywilejowane konto „ksciam”, dodaj je do grupy zabezpieczeń „kladmins”, a następnie ustaw grupę „kladmins” jako grupę podstawową dla konta „ksciam”. Aby to zrobić, kolejno uruchom następujące polecenia:

   ```
   sudo adduser ksciam
   sudo gpasswd -a ksciam kladmins
   sudo usermod -g kladmins ksciam
   ```

4. Zainstaluj Kaspersky Security Center Linux w wersji 16.3 na urządzeniu, na którym wcześniej zainstalowano Serwer administracyjny.

   Jeśli schemat bazy danych w kopii zapasowej różni się od schematu aktualnie używanego przez Serwer administracyjny lub IAM, dane zostaną przywrócone do bieżącego schematu.

Jeśli w kopii zapasowej używany jest schemat publiczny, muszą zostać spełnione następujące warunki:

- W bazie danych istnieje schemat publiczny.
- Publiczny schemat bazy danych można modyfikować z poziomu konta DBMS używanego przez Serwer administracyjny lub IAM w celu uzyskania dostępu do bazy danych.

W przeciwnym razie przywracanie danych zakończy się błędem.

5. Przywróć dane Serwera administracyjnego z kopii zapasowej utworzonej przed aktualizacją.
6. Skonfiguruj weryfikację certyfikatu przez Serwer administracyjny i Serwer IAM.
7. Zainstaluj Kaspersky Security Center Web Console.

   Jeśli Kaspersky Security Center Web Console została zainstalowana wcześniej, zainstaluj ją ponownie z tym samym plikiem odpowiedzi.

   Zaloguj się do Kaspersky Security Center Web Console na koncie użytkownika wewnętrznego administratora.

   Proces inicjalizacji danych trwa zazwyczaj do 15 minut po przywróceniu danych Serwera administracyjnego, lecz czas ten zależy od wydajności sprzętu i rozmiaru danych Serwera administracyjnego. W tym czasie Kaspersky Security Center Web Console może nie nawiązać połączenia i mogą zostać wyświetlone błędy.
8. Dla urządzeń, na których została zainstalowana wcześniejsza wersja Agenta sieciowego, utwórz i uruchom zadanie zdalnej instalacji nowej wersji Agenta sieciowego.

   > Zalecamy aktualizację Agenta sieciowego dla systemu Linux do tej samej wersji co Kaspersky Security Center Linux.

   Po zakończeniu wykonywania zadania zdalnej instalacji, wersja Agenta sieciowego zostanie zaktualizowana.

   Uruchom następujące polecenia na zasobach opartych na systemie Linux, aby usunąć zależności, które nie są już potrzebne:

   - W przypadku zasobów opartych na systemie Debianie uruchom dowolne z następujących poleceń:

     ```
     sudo apt-get -y autoremove
     ```

     ```
     sudo apt -y autoremove
     ```

   - W przypadku zasobów opartych na systemie RPM uruchom dowolne z następujących poleceń:

     ```
     sudo dnf autoremove
     ```

     ```
     sudo yum autoremove
     ```

Aktualizowanie Kaspersky Security Center Linux od wersji 15.4 lub starszej na węzłach klastra trybu failover Kaspersky Security Center Linux

Możesz zainstalować wersję 16 lub nowszą Serwera administracyjnego na każdym węźle klastra trybu failover Kaspersky Security Center Linux, na którym zainstalowano wersję 14—15.4 Serwera administracyjnego. Podczas aktualizowania wszystkie dane i ustawienia z poprzedniej wersji Serwera administracyjnego zostają zachowane.

Przed rozpoczęciem, **sprawdź wymagania dotyczące certyfikatu niestandardowego**.

Jeśli używasz certyfikatu niestandardowego zamiast certyfikatu z podpisem własnym, przed aktualizacją Kaspersky Security Center Linux do nowszej wersji upewnij się, że certyfikat zawiera Alternatywną nazwę podmiotu (SAN). Jeżeli nie zawiera, ważne jest, aby wymienić certyfikat przed aktualizacją Kaspersky Security Center Linux. W przeciwnym razie nie będziesz mógł zalogować się do Web Console po aktualizacji.

Aby upewnić się, że certyfikat zawiera Alternatywną nazwę podmiotu (SAN):

1. Na urządzeniu z zainstalowanym Serwerem administracyjnym, wykonaj następujące polecenie:

   - W przypadku urządzenia z systemem Linux:

     ```
     sudo openssl x509 -in /var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer -noout
     -ext subjectAltName
     ```

   - W przypadku urządzenia z systemem Windows:

     ```
     certutil -dump %ProgramData%\KasperskyLab\adminkit\1093\cert\klserver.cer
     ```

2. Upewnij się, że Alternatywna nazwa podmiotu jest obecna w wynikach polecenia i zawiera adres urządzenia Serwera administracyjnego.

3. Jeśli Alternatywna nazwa podmiotu jest niedostępna, użyj narzędzia klsetsrvcert, aby zastąpić certyfikat niestandardowy tym, który spełnia wymagania.

Jeśli wcześniej instalowałeś lokalnie Kaspersky Security Center Linux na urządzeniach, możesz także zaktualizować Kaspersky Security Center Linux na tych urządzeniach, korzystając z pliku instalacyjnego lub kopii zapasowej.

Aktualizowanie Kaspersky Security Center Linux z wersji 15.4 lub starszej na węzłach klastra trybu failover Kaspersky Security Center Linux:

1. Pobierz plik instalacyjny Kaspersky Security Center Linux z pełnym pakietem dla wersji 16.3 ze strony internetowej Kaspersky:

   - W przypadku urządzeń z systemem operacyjnym opartym na RPM — `ksc64-<version number>-<build number>.x86_64.rpm`

   - W przypadku urządzeń z systemem operacyjnym opartym na systemie Debian — `ksc64_<version number>-<build number>_amd64.deb`

2. Zatrzymaj klaster.

3. Na serwerze DBMS utwórz bazę danych dla IAM. Nazwa bazy danych IAM musi być inna niż nazwa bazy danych używanej przez Serwer administracyjny.

   - W przypadku PostgreSQL uruchom następujące polecenie:

     ```
     sudo -i -u postgres psql -U postgres -c "CREATE DATABASE <iam_db_name>;"
     ```

   - W przypadku MariaDB uruchom następujące polecenie:

     ```
     sudo mysql -u root -p -e "CREATE DATABASE <iam_db_name>;"
     ```

4. Utwórz nieuprzywilejowane konto „ksciam", dodaj je do grupy zabezpieczeń „kladmins", a następnie ustaw grupę „kladmins" jako grupę podstawową dla konta „ksciam". Aby to zrobić, kolejno uruchom następujące polecenia:

   ```
   sudo adduser ksciam
   sudo gpasswd -a ksciam kladmins
   sudo usermod -g kladmins ksciam
   ```

5. Na aktywnym węźle klastra uruchom jedno z następujących poleceń w terminalu wiersza poleceń, aby rozpocząć aktualizację:

   - W przypadku urządzeń z systemem operacyjnym opartym na RPM:

     ```
     sudo yum install ./ksc64-<numer wersji>-<numer kompilacji>.x86_64.rpm
     ```

   - Dla urządzeń z systemem operacyjnym opartym na systemie Debian:

     ```
     sudo apt-get install ./ksc64_<numer wersji>-<numer kompilacji>_amd64.deb
     ```

   Po pomyślnym wykonaniu polecenia tworzony jest skrypt `/opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl`. Komunikat o tym jest wyświetlany w terminalu.

6. Uruchom skrypt `/opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl` w celu skonfigurowania zaktualizowanego Serwera administracyjnego:

   ```
   sudo /opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl
   ```

7. Przeczytaj Umowę licencyjną i Politykę prywatności, które pojawiają się w terminalu wiersza poleceń. Jeśli zgadzasz się ze wszystkimi warunkami Umowy licencyjnej i Polityki prywatności:

   a. Wpisz `Y`, aby potwierdzić, że w pełni przeczytałeś, zrozumiałeś i akceptujesz warunki Umowy licencyjnej użytkownika końcowego.

   b. Wpisz ponownie `Y`, aby potwierdzić, że w pełni przeczytałeś, zrozumiałeś i akceptujesz Politykę prywatności opisującą sposób postępowania z danymi.

   Instalacja aplikacji na Twoim urządzeniu będzie kontynuowana po dwukrotnym wpisaniu `Y`.

8. Wybierz węzeł, na którym przeprowadzasz aktualizację, wpisując `2`.

Poniższy obrazek przedstawia dwa ostatnie kroki.

```
Enter 'Y' to confirm that you understand and accept the terms of the End
User License Agreement (EULA). You must accept the terms and conditions of
the EULA to install the application. Enter 'N' providing you do not accept
the terms of the EULA or 'R' to view it again [N]:
y

Enter 'Y' to confirm that you accept the terms of the Privacy Policy. You
must accept the terms and conditions of the Privacy Policy to install the
application. Entering 'Y' means that you are aware that your data will be
handled and transmitted (including to third countries) as described in the
Privacy Policy. Enter 'N' providing you do not accept the Privacy Policy
[N]:
y

Choose the Administration Server installation mode:
1) Standard
2) Primary cluster node
3) Secondary cluster node
Enter the range number (1, 2, or 3) [1]:
```

Zaakceptowanie warunków Umowy licencyjnej użytkownika końcowego i Polityki prywatności oraz wybranie trybu instalacji w terminalu wiersza poleceń

9. Następnie instalator konfiguruje i kończy aktualizację Serwera administracyjnego. Podczas aktualizacji nie możesz zmienić ustawień Serwera administracyjnego, które zostały dostosowane przed aktualizacją. Po wyświetleniu monitu wprowadź następujące ustawienia:

   a. Wprowadź nazwę DNS serwera FQDN.

      Należy użyć nazwy DNS Serwera administracyjnego określonej podczas instalacji Kaspersky Security Center Linux.

   b. Wprowadź nazwę konta, aby uruchomić usługę IAM. Konto musi należeć do wprowadzonej grupy zabezpieczeń. Domyślnie używane jest konto ksciam.

   c. Wybierz DBMS, który zainstalowałeś do pracy z usługą IAM:

      - Jeśli zainstalowałeś MySQL lub MariaDB, wpisz `1`.
      - Jeśli zainstalowałeś PostgreSQL lub Postgres Pro, wpisz `2`.

   d. Wprowadź adres IAM DBMS, który ma być używany przez usługę IAM.

   e. Wprowadź numer portu IAM DBMS. Ten port jest używany do komunikacji z usługą IAM. Domyślnie używane są następujące porty:

      - Port 3306 dla MySQL lub MariaDB
      - Port 5432 dla PostgreSQL lub Postgres Pro

   f. Wprowadź nazwę bazy danych IAM, która ma być używana przez usługę IAM. Nazwa bazy danych używanej przez usługę IAM powinna być inna niż nazwa bazy danych używanej przez Serwer administracyjny.

   g. Wprowadź login i hasło DBMS, który ma być używany przez usługę IAM.

10. Wykonaj krok 5 na węźle pasywnym.

    W kroku 6 wprowadź `3`, aby wybrać węzeł.

11. Uruchom klaster.

    Możesz uruchomić klaster na dowolnym węźle. Jeśli uruchomisz klaster w węźle pasywnym, stanie się on węzłem aktywnym.

12. Dla urządzeń, na których jest instalowana wcześniejsza wersja Agenta sieciowego, utwórz i uruchom zadanie zdalnej instalacji nowej wersji Agenta sieciowego.

    Zalecamy aktualizację Agenta sieciowego dla systemu Linux do tej samej wersji co Kaspersky Security Center Linux.

    Po zakończeniu wykonywania zadania zdalnej instalacji, wersja Agenta sieciowego zostanie zaktualizowana.

    Uruchom następujące polecenia na zasobach opartych na systemie Linux, aby usunąć zależności, które nie są już potrzebne:

    - W przypadku zasobów opartych na systemie Debianie uruchom dowolne z następujących poleceń:

      ```
      sudo apt-get -y autoremove
      ```

      ```
      sudo apt -y autoremove
      ```

    - W przypadku zasobów opartych na systemie RPM uruchom dowolne z następujących poleceń:

      ```
      sudo dnf autoremove
      ```

      ```
      sudo yum autoremove
      ```

    W rezultacie zainstalowałeś Serwer administracyjny najnowszej wersji na węzłach klastra typu failover Kaspersky Security Center Linux.

Aktualizowanie Kaspersky Security Center Web Console

W tym artykule opisano sposób aktualizacji Kaspersky Security Center Web Console Server (zwanego również Kaspersky Security Center Web Console) na urządzeniach działających pod kontrolą systemu operacyjnego Linux.

Jeśli musisz zaktualizować Kaspersky Security Center Web Console na Astra Linux w trybie zamkniętego środowiska oprogramowania, postępuj zgodnie z instrukcjami określonymi dla Astra Linux.

Użyj jednego z następujących plików instalacyjnych, które odpowiadają dystrybucji Linux zainstalowanej na Twoim urządzeniu:

- Dla systemów operacyjnych opartych na Debianie — ksc-web-console-<build_number>.x86_64.deb
- Dla systemów operacyjnych opartych na RPM — ksc-web-console-<build_number>.x86_64.rpm

Plik instalacyjny można pobrać ze strony internetowej Kaspersky.

W celu zaktualizowania Kaspersky Security Center Web Console:

1. Upewnij się, że na urządzeniu, na którym chcesz zainstalować Kaspersky Security Center Web Console, działa jedna z obsługiwanych dystrybucji systemu Linux.

2. Przeczytaj i zaakceptuj Umowę licencyjną użytkownika końcowego. Jeśli pakiet dystrybucyjny Kaspersky Security Center Linux nie zawiera pliku TXT z treścią Umowy licencyjnej użytkownika końcowego, możesz pobrać ten plik ze strony internetowej Kaspersky. Jeśli nie akceptujesz warunków Umowy licencyjnej, nie aktualizuj Kaspersky Security Center Web Console przy użyciu pliku instalacyjnego.

3. Użyj tego samego pliku odpowiedzi, który został przygotowany przed instalacją Kaspersky Security Center Web Console. Nazwa pliku odpowiedzi to ksc-web-console-setup.json, a lokalizacja pliku to /etc/ksc-web-console-setup.json.

   Jeśli podczas instalacji Kaspersky Security Center Web Console określono wartości parametrów `webConsoleAccount`, `managementServiceAccount`, `serviceWebConsoleAccount`, `pluginAccount` i `natsMessageQueueAccount`, upewnij się, że wszystkie te parametry zostały określone w pliku odpowiedzi.

   Jeśli plik odpowiedzi nie istnieje, utwórz nowy plik odpowiedzi zawierający parametry umożliwiające połączenie Kaspersky Security Center Web Console z Serwerem administracyjnym. Nadaj plikowi nazwę ksc-web-console-setup.json, a następnie umieść go w katalogu /etc.

   Przykład pliku odpowiedzi zawierającego minimalny zestaw parametrów

   Zestaw parametrów pliku odpowiedzi zależy od wersji Serwera administracyjnego, z którym łączy się Kaspersky Security Center Web Console:

   - Serwer administracyjny w wersji 16 lub nowszej

     Przykład pliku odpowiedzi z minimalnym zestawem parametrów do logowania się do Serwera administracyjnego w wersji 16 lub nowszej:

```
{
    "address": "ksc-web-console.example.com",
    "port": 8080,
    "trusted":  {
        "Administration Server v16": {
            "iamHost": "ksc16.example.com",
            "iamOAuthPort": 4444,
            "iamProxyPort": 9050,
            "iamCertPath": "/var/opt/kaspersky/klnagent_srv/iam/main_certificate.pem",
            "iamPATPath": "/var/opt/kaspersky/klnagent_srv/iam/initial_token.txt",
            "kscPort": 13299,
            "kscCertPath": "/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer"
        }
    },
    "certDomain":"ksc-web-console.example.com",
    "acceptEula": true
}
```

   - Serwer administracyjny w wersji 15.4 lub starszej

     Przykład pliku odpowiedzi z minimalnym zestawem parametrów do logowania się do Serwera administracyjnego w wersji 15.4 lub starszej:

```
{
    "address": "ksc-web-console.example.com",
    "port": 8080,
    "trusted":  {
         "Administration Server v15.4": {
             "kscHost": "ksc.example.com",
             "kscPort": 13299,
             "kscCertPath": "/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer"
         }
    },
    "certDomain":"ksc-web-console.example.com",
    "acceptEula": true
}
```

Możesz zainstalować Kaspersky Security Center Web Console na tym samym urządzeniu, na którym jest zainstalowany Serwer administracyjny, lub na innym. Jeżeli Kaspersky Security Center Web Console jest zainstalowana na innym urządzeniu, adres Kaspersky Security Center Web Console (określony przez `address`) i adres Serwera administracyjnego (określony przez `iamHost` lub `kscHost`) różnią się. Jeśli Kaspersky Security Center Web Console jest zainstalowana na tym samym urządzeniu co Serwer administracyjny, parametry te mają takie same wartości.

Wartość `iamHost` musi być zgodna z adresem IAM określonym podczas instalacji Serwera administracyjnego. Aby uzyskać określony adres IAM, uruchom następujące polecenie na urządzeniu z zainstalowanym Serwerem administracyjnym:

```
grep "iam_address:" /var/opt/kaspersky/klnagent_srv/iam/iam_config.yaml
```

Szczegółowe informacje można znaleźć w artykule: Parametry instalacji Kaspersky Security Center Web Console.

Do listy zaufanych serwerów można dodać wiele Serwerów administracyjnych o różnych wersjach. W takim przypadku serwery mogą używać różnych metod uwierzytelniania.

Jeśli chcesz zaktualizować Kaspersky Security Center Web Console w połączeniu z Serwerem administracyjnym zainstalowanym w węzłach klastra trybu failover Kaspersky Security Center Linux, w pliku odpowiedzi określ parametr zaufanej instalacji, aby umożliwić klastrowi trybu failover Kaspersky Security Center Linux połączenie się z Kaspersky Security Center Web Console.

Składniki parametru `trusted` **instalacji**

Jeśli łączysz się z klastrem trybu failover Kaspersky Security Center Linux za pomocą uwierzytelniania domeny z funkcją SSO, określ parametr zaufany instalacji w następujący sposób: Jeśli łączysz Kaspersky Security Center Web Console z Serwerem administracyjnym w wersji 16 lub nowszej, zostanie użyte uwierzytelnianie domeny z funkcją pojedynczego logowania (SSO) zapewniane przez usługę Menedżera tożsamości i dostępu (IAM). W takim przypadku określ parametr `trusted` instalacji w następujący sposób:

```
"trusted":  {
  "<Nazwa Serwera administracyjnego>": {
    "iamHost": "ksc-iam.example.com",
    "iamOAuthPort": 4444,
    "iamProxyPort": 9050,
    "iamCertPath": "<udostepniony folder danych>/iam/main_certificate.pem",
    "iamPATPath": "<udostepniony folder danych>/iam/initial_token.txt",
    "kscPort": 13299,
    "kscCertPath": "<udostepniony folder danych>/1093/cert/klserver.cer"
  }
}
```

gdzie:

- `<Nazwa Serwera administracyjnego>` to nazwa klastra trybu failover Kaspersky Security Center Linux, która będzie wyświetlana w oknie logowania Kaspersky Security Center Web Console.

- `iamHost` to adres urządzenia, na którym zainstalowane są Serwer administracyjny i IAM. Jeśli utworzyłeś dodatkową kartę sieciową podczas przygotowywania węzłów klastra, użyj FQDN, nazwy hosta lub adresu IP karty jako adresu klastra trybu failover Kaspersky Security Center Linux. W przeciwnym razie określ FQDN lub nazwę hosta modułu równoważenia obciążenia innej firmy, którego używasz.

  Ta wartość `iamHost` musi być zgodna z adresem IAM określonym podczas instalacji Serwera administracyjnego. Aby uzyskać określony adres IAM, uruchom następujące polecenie na hoście Serwera administracyjnego:

  ```
  grep "iam_address:" /var/opt/kaspersky/klnagent_srv/iam/iam_config.yaml
  ```

- `iamOAuthPort` to port używany do wymiany tokenów uwierzytelniania przez protokół uwierzytelniania OpenID Connect (wartość domyślna to 4444). Ten port jest używany zarówno do komunikacji między Kaspersky Security Center Web Console Server a Serwerem administracyjnym, jak i między przeglądarką (używaną z Kaspersky Security Center Web Console) a Serwerem administracyjnym.

- `iamProxyPort` to port, który jest używany przez Kaspersky Security Center Web Console Server do nawiązywania połączenia z Serwerem administracyjnym (domyślnie jest to port 9050).

- `iamCertPath` to ścieżka do certyfikatu IAM. Certyfikat IAM jest tworzony automatycznie przy pierwszym uruchomieniu Serwera administracyjnego. Plik certyfikatu jest przechowywany na urządzeniu, na którym zainstalowany jest Serwer administracyjny. Domyślna ścieżka do certyfikatu: `< udostępniony folder danych >/iam/main_certificate.pem`. Certyfikat Serwera administracyjnego znajduje się we współdzielonym magazynie danych klastra trybu failover Kaspersky Security Center Linux. Certyfikat IAM z podpisem własnym jest automatycznie rotowany.

- `iamPATPath` to ścieżka do tokena używanego do rejestracji Kaspersky Security Center Web Console jako klienta OAuth w IAM. Ten plik jest generowany podczas pierwszego uruchomienia Serwera administracyjnego. Plik certyfikatu jest przechowywany na urządzeniu, na którym zainstalowany jest Serwer administracyjny. Domyślna ścieżka do tokena: <udostępniony folder danych>/iam/initial_token.txt. Token znajduje się we współdzielonym magazynie danych klastra trybu failover Kaspersky Security Center Linux. Token jest ważny bezterminowo i nie wymaga rotacji.

- `kscPort` to port OpenAPI, którego Kaspersky Security Center Web Console używa do łączenia się z Serwerem administracyjnym (wartość domyślna to 13299).

- `kscCertPath` to certyfikat Serwera administracyjnego, który znajduje się we współdzielonym magazynie danych klastra trybu failover Kaspersky Security Center Linux. Domyślna ścieżka do pliku certyfikatu to: `< udostępniony folder danych >\1093\cert\klserver.cer`.

  Skopiuj plik certyfikatu Serwera administracyjnego (określony przez `kscCertPath`), plik certyfikatu IAM (określony przez `iamCertPath`) i plik tokena (określony przez `iamPATPath`) z współdzielonego magazynu danych na urządzenie, na którym instalujesz Kaspersky Security Center Web Console. Określ lokalną ścieżkę do certyfikatu Serwera administracyjnego.

Jeśli łączysz Kaspersky Security Center Web Console z Serwerem administracyjnym w wersji 15.4 lub starszej, zostanie użyte uwierzytelnianie poprzez określenie nazwy i hasła użytkownika domeny lub użytkownika wewnętrznego. W takim przypadku określ parametr zaufany instalacji w następujący sposób:

```
"trusted":  {
  "<Nazwa Serwera administracyjnego>": {
    "kscHost": "ksc.example.com",
    "kscPort": 13299,
    "kscCertPath": "<udostepniony folder danych>/1093/cert/klserver.cer"
  }
}
```

gdzie:

- `< Nazwa Serwera administracyjnego >` to nazwa klastra trybu failover Kaspersky Security Center Linux, która będzie wyświetlana w oknie logowania Kaspersky Security Center Web Console.

- `kscHost` to adres Serwera administracyjnego (FQDN lub nazwa hosta). Jeśli utworzyłeś dodatkową kartę sieciową podczas przygotowywania węzłów klastra, użyj adresu karty jako adresu klastra trybu failover Kaspersky Security Center Linux. W przeciwnym razie określ adres modułu równoważenia obciążenia innej firmy, którego używasz.

- `kscPort` to port OpenAPI, którego Kaspersky Security Center Web Console używa do łączenia się z Serwerem administracyjnym (wartość domyślna to 13299).

- `kscCertPath` to certyfikat Serwera administracyjnego, który znajduje się we współdzielonym magazynie danych klastra trybu failover Kaspersky Security Center Linux. Domyślna ścieżka do pliku certyfikatu to: `<udostępniony folder danych>\1093\cert\klserver.cer`. Skopiuj plik certyfikatu ze współdzielonego magazynu danych na urządzenie, na którym instalujesz Kaspersky Security Center Web Console. Określ lokalną ścieżkę do certyfikatu Serwera administracyjnego.

Kaspersky Security Center Web Console nie można zaktualizować przy użyciu tego samego pliku instalacyjnego. Jeśli chcesz zmienić ustawienia w pliku odpowiedzi i użyć tego pliku do ponownego zainstalowania aplikacji, w pierwszej kolejności musisz usunąć aplikację, a następnie zainstalować ją ponownie z nowym plikiem odpowiedzi.

4. Z poziomu konta z uprawnieniami administratora użyj wiersza polecenia, aby uruchomić plik instalacji z rozszerzeniem .deb lub .rpm, w zależności od posiadanej dystrybucji systemu Linux.

   W celu przeprowadzenia aktualizacji z poprzedniej wersji Kaspersky Security Center Web Console, uruchom jedno z następujących poleceń:

   - W przypadku urządzeń z systemem operacyjnym opartym na RPM:
     ```
     sudo yum install ksc-web-console-<numer_kompilacji>.x86_64.rpm
     ```

   - Dla urządzeń z systemem operacyjnym opartym na systemie Debian:
     ```
     sudo apt-get install ksc-web-console-<numer_kompilacji>.x86_64.deb
     ```

   Rozpocznie się wypakowywanie pliku instalacji. Zaczekaj na zakończenie instalacji.

5. Uruchom ponownie wszystkie usługi Kaspersky Security Center Web Console, uruchamiając następujące polecenie:
   ```
   sudo systemctl restart KSC*
   ```

Po zakończeniu instalacji możesz użyć przeglądarki internetowej do otwarcia i zalogowania się do Kaspersky Security Center Web Console.

Aktualizowanie Kaspersky Security Center Web Console na Astra Linux w trybie zamkniętego środowiska oprogramowania

W tej sekcji opisano sposób aktualizacji Kaspersky Security Center Web Console Server (zwanego również Kaspersky Security Center Web Console) w systemie operacyjnym Astra Linux Special Edition.

W celu zaktualizowania Kaspersky Security Center Web Console:

1. Upewnij się, że na urządzeniu, na którym chcesz zainstalować Kaspersky Security Center Web Console, działa jedna z obsługiwanych dystrybucji systemu Linux.

2. Przeczytaj i zaakceptuj Umowę licencyjną użytkownika końcowego. Jeśli pakiet dystrybucyjny Kaspersky Security Center Linux nie zawiera pliku TXT z treścią Umowy licencyjnej użytkownika końcowego, możesz pobrać ten plik ze strony internetowej Kaspersky. Jeśli nie akceptujesz warunków Umowy licencyjnej, nie aktualizuj Kaspersky Security Center Web Console przy użyciu pliku instalacyjnego.

3. Użyj tego samego pliku odpowiedzi, który został przygotowany przed instalacją Kaspersky Security Center Web Console. Nazwa pliku odpowiedzi to ksc-web-console-setup.json, a lokalizacja pliku to /etc/ksc-web-console-setup.json.

   Jeśli plik odpowiedzi nie istnieje, utwórz nowy plik odpowiedzi zawierający parametry umożliwiające połączenie Kaspersky Security Center Web Console z Serwerem administracyjnym. Nadaj plikowi nazwę ksc-web-console-setup.json, a następnie umieść go w katalogu /etc.

   Przykład pliku odpowiedzi zawierającego minimalny zestaw parametrów

   Zestaw parametrów pliku odpowiedzi zależy od wersji Serwera administracyjnego, z którym łączy się Kaspersky Security Center Web Console:

   - Serwer administracyjny w wersji 16 lub nowszej

     Przykład pliku odpowiedzi z minimalnym zestawem parametrów do logowania się do Serwera administracyjnego w wersji 16 lub nowszej:

```
{
    "address": "ksc-web-console.example.com",
    "port": 8080,
    "trusted":  {
        "Administration Server v16": {
            "iamHost": "ksc16.example.com",
            "iamOAuthPort": 4444,
            "iamProxyPort": 9050,
            "iamCertPath": "/var/opt/kaspersky/klnagent_srv/iam/main_certificate.pem",
            "iamPATPath": "/var/opt/kaspersky/klnagent_srv/iam/initial_token.txt",
            "kscPort": 13299,
            "kscCertPath": "/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer"
        }
    },
    "certDomain":"ksc-web-console.example.com",
    "acceptEula": true
}
```

   - Serwer administracyjny w wersji 15.4 lub starszej

     Przykład pliku odpowiedzi z minimalnym zestawem parametrów do logowania się do Serwera administracyjnego w wersji 15.4 lub starszej:

```
{
    "address": "ksc-web-console.example.com",
    "port": 8080,
    "trusted":  {
         "Administration Server v15.4": {
             "kscHost": "ksc.example.com",
             "kscPort": 13299,
             "kscCertPath": "/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer"
         }
    },
    "certDomain":"ksc-web-console.example.com",
    "acceptEula": true
}
```

   Możesz zainstalować Kaspersky Security Center Web Console na tym samym urządzeniu, na którym jest zainstalowany Serwer administracyjny, lub na innym. Jeżeli Kaspersky Security Center Web Console jest zainstalowana na innym urządzeniu, adres Kaspersky Security Center Web Console (określony przez `address`) i adres Serwera administracyjnego (określony przez `iamHost` lub `kscHost`) różnią się. Jeśli Kaspersky Security Center Web Console jest zainstalowana na tym samym urządzeniu co Serwer administracyjny, parametry te mają takie same wartości.

   Wartość `iamHost` musi być zgodna z adresem IAM określonym podczas instalacji Serwera administracyjnego. Aby uzyskać określony adres IAM, uruchom następujące polecenie na urządzeniu z zainstalowanym Serwerem administracyjnym:

```
grep "iam_address:" /var/opt/kaspersky/klnagent_srv/iam/iam_config.yaml
```

Szczegółowe informacje można znaleźć w artykule: Parametry instalacji Kaspersky Security Center Web Console.

Do listy zaufanych serwerów można dodać wiele Serwerów administracyjnych o różnych wersjach. W takim przypadku serwery mogą używać różnych metod uwierzytelniania.

4. Upewnij się, że w pliku `/etc/digsig/digsig_initramfs.conf` parametr `DIGSIG_ELF_MODE` jest określony w następujący sposób:

   ```
   DIGSIG_ELF_MODE=1
   ```

5. Upewnij się, że zainstalowany jest pakiet zgodności `astra-digsig-oldkeys`.

   Jeśli ten pakiet nie jest zainstalowany, uruchom następujące polecenie:

   ```
   apt install astra-digsig-oldkeys
   ```

6. Utwórz katalog dla klucza aplikacji, jeśli nie istnieje:

   ```
   mkdir -p /etc/digsig/keys/legacy/kaspersky/
   ```

7. Umieść klucz aplikacji /opt/kaspersky/ksc64/share/kaspersky_astra_pub_key.gpg w katalogu utworzonym w poprzednim kroku:

   ```
   cp kaspersky_astra_pub_key.gpg /etc/digsig/keys/legacy/kaspersky/
   ```

   > Jeśli pakiet dystrybucyjny Kaspersky Security Center Linux nie zawiera klucza aplikacji kaspersky_astra_pub_key.gpg, możesz go pobrać, klikając łącze: https://media.kaspersky.com/utilities/CorporateUtilities/kaspersky_astra_pub_key.gpg.

8. Zaktualizuj dyski RAM:

   ```
   update-initramfs -u -k all
   ```

   Uruchom ponownie system.

9. Na koncie z uprawnieniami administratora użyj wiersza poleceń, aby uruchomić plik instalacyjny. Plik konfiguracyjny można pobrać ze strony internetowej Kaspersky.

   W celu przeprowadzenia aktualizacji z poprzedniej wersji Kaspersky Security Center Web Console, uruchom następujące polecenie:

   ```
   sudo apt-get install ksc-web-console-<numer_kompilacji>.x86_64.deb
   ```

   Rozpocznie się wypakowywanie pliku instalacji. Zaczekaj na zakończenie instalacji.

10. Uruchom ponownie wszystkie usługi Kaspersky Security Center Web Console, uruchamiając następujące polecenie:

    ```
    sudo systemctl restart KSC*
    ```

Po zakończeniu instalacji możesz użyć przeglądarki internetowej do otwarcia i zalogowania się do Kaspersky Security Center Web Console.

Migracja do Kaspersky Security Center Linux

Migrację z Kaspersky Security Center Windows do Kaspersky Security Center Linux można wykonać przy użyciu kopii zapasowej danych Serwera administracyjnego (z narzędziem klbackup) i Kreatora migracji.

Poniższa tabela umożliwia porównanie głównych funkcji i ograniczeń migracji przy użyciu kopii zapasowej danych Serwera administracyjnego i Kreatora migracji, aby zdecydować, które podejście jest bardziej odpowiednie dla Twojej organizacji.

Parametry	Kopia zapasowa danych Serwera administracyjnego	Kreator migracji
Proces migracji	Tworzenie pełnej kopii zapasowej danych Serwera administracyjnego Kaspersky Security Center Windows i przywracanie ich na Serwerze administracyjnym Kaspersky Security Center Linux	Wybieranie i eksportowanie danych Serwera administracyjnego do migracji, importowanie tych danych do Serwera administracyjnego Kaspersky Security Center Linux i przełączanie zarządzanych urządzeń w ramach zarządzania Kaspersky Security Center Linux
Funkcje metody migracji	• Migracja wszystkich danych Serwera administracyjnego • Migracja dowolnej liczby zarządzanych urządzeń • Służy do uzyskania kompletnej kopii danych Serwera administracyjnego Kaspersky Security Center Windows i przesłania ich do Serwera administracyjnego Kaspersky Security Center Linux	• Częściowa migracja danych Serwera administracyjnego • Dostępny jest wybór obiektów do migracji • Grupa lub podgrupa administracyjna podlegająca migracji nie może zawierać więcej niż 10 000 urządzeń • Służy do częściowego przesyłania danych Serwera administracyjnego, obejmujących wyłącznie obiekty grupowe w zakresie migracji; obiekty grupowe spoza zakresu migracji muszą zostać przywrócone ręcznie
Zakres migracji	Pełne przesyłanie danych Serwera administracyjnego z nieograniczoną liczbą zarządzanych urządzeń	• Struktura grupy administracyjnej • Urządzenia zarządzane zawarte w grupach administracyjnych (**nie więcej niż 10 000 urządzeń**) • Znaczniki przypisane do urządzeń klienckich • Globalne zadania Agenta sieciowego i zarządzanych aplikacji (nie dla Serwera administracyjnego) • Zadania grupowe Agenta sieciowego i zarządzanych aplikacji • Licencjonowanie zarządzanych aplikacji • Szablony raportów • Użytkownicy i role • Użytkownicy wewnętrzni i grupy zabezpieczeń • Kategorii aplikacji niestandardowych z zawartością dodaną ręcznie • Niestandardowe wybory urządzeń
Zakres nie podlegający migracji	—	• Zadania globalne Serwera administracyjnego • Wydarzenia zapisane na Serwerze administracyjnym • Repozytorium pakietów dystrybucyjnych aplikacji przeznaczonych do zdalnego zainstalowania • Certyfikatu Serwera administracyjnego • Klucze licencyjne używane przez Serwer administracyjny i zarządzane aplikacje • Wirtualne Serwery administracyjne • Ustawienia zasady Agenta sieciowego • Reguły przenoszenia urządzeń • Reguły automatycznego znakowania urządzeń • Punkty dystrybucji • Ustawienia aplikacji Kaspersky zapisane na Serwerze administracyjnym
Wersje Kaspersky Security Center obsługujące migrację	• Dowolna obsługiwana wersja Kaspersky Security Center Windows • Kaspersky Security Center Linux w wersji 15.2 lub nowszej	• Kaspersky Security Center Windows w wersji 14.2 lub nowszej • Kaspersky Security Center Linux w wersji 15 lub nowszej
Systemy DBMS, pomiędzy którymi można przeprowadzić migrację	• Microsoft SQL Server → MySQL, MariaDB • Microsoft SQL Server → PostgreSQL, Postgres Pro (tylko w przypadku migracji z Kaspersky Security Center Windows w wersji 14.2 lub nowszej z zainstalowaną poprawką do Kaspersky Security Center Linux w wersji 15.3 lub nowszej) • MySQL → MySQL, MariaDB • MariaDB → MySQL, MariaDB • PostgreSQL → PostgreSQL Postgres Pro → Postgres Pro (tylko w przypadku migracji z Kaspersky Security Center Windows w wersji 15.1 lub nowszej do Kaspersky Security Center Linux w wersji 16 lub nowszej)	Migracja pomiędzy obsługiwanymi systemami DBMS bez ograniczeń

Migracja do Kaspersky Security Center Linux przy użyciu kopii zapasowej danych Serwera administracyjnego

Za pomocą kopii zapasowej danych możesz przenieść dane z Serwera administracyjnego Kaspersky Security Center Windows do Kaspersky Security Center Linux. Przed migracją upewnij się, że wymagane funkcje Kaspersky Security Center Windows są obsługiwane w Kaspersky Security Center Linux.

Dla ułatwienia dostępny jest film instruktażowy na temat migracji danych Serwera administracyjnego do Kaspersky Security Center Linux przy użyciu kopii zapasowej.

Ograniczenia

- Migrację można przeprowadzić pomiędzy następującymi systemami DBMS:
  - Microsoft SQL Server → MySQL, MariaDB
  - Microsoft SQL Server → PostgreSQL, Postgres Pro
  - MySQL → MySQL, MariaDB
  - MariaDB → MySQL, MariaDB
  - PostgreSQL → PostgreSQL
  - Postgres Pro → Postgres Pro
- Migracja danych Serwera administracyjnego przechowywanych w bazie danych Microsoft SQL Server, MySQL lub MariaDB do bazy danych MySQL lub MariaDB jest obsługiwana w przypadku migracji z dowolnej obsługiwanej wersji programu Kaspersky Security Center Windows do Kaspersky Security Center Linux w wersji 15.2 lub nowszej.
- Migracja danych Serwera administracyjnego przechowywanych w bazie danych PostgresSQL do bazy danych PostgreSQL lub Postgres Pro jest obsługiwana w przypadku migracji z Kaspersky Security Center Windows w wersji 15.1 lub nowszej do Kaspersky Security Center Linux w wersji 16 lub nowszej.
- Migracja danych Serwera administracyjnego przechowywanych w bazie danych Microsoft SQL Server do bazy danych PostgreSQL lub Postgres Pro jest obsługiwana w przypadku migracji z Kaspersky Security Center Windows w wersji 14.2 lub nowszej do Kaspersky Security Center Linux w wersji 15.3 lub nowszej.

  Aby wesprzeć migrację do PostgreSQL lub Postgres Pro, musisz poprosić o pomoc techniczną Kaspersky i zainstalować jedną z następujących poprawek:

  - Dla Kaspersky Security Center 14.2 Windows: 14.2.0.26967-pf5
  - W przypadku rozwiązania Kaspersky Secure Mobility Management opartego na Kaspersky Security Center 14.2 Windows: 14.2.0.48079-pf5

- Dla Kaspersky Security Center 15.1 Windows: 15.1.0.20748-pf2

  Migracja do PostgreSQL lub Postgres Pro staje się również dostępna po zaktualizowaniu Kaspersky Security Center Windows do wersji 15.1.0.22239.

- Jeśli używasz MySQL lub MariaDB jako systemu DBMS dla Kaspersky Security Center Windows i Kaspersky Security Center Linux, parametr `lower_case_table_names` musi być taki sam dla bieżącego i nowego systemu DBMS.

  Przed utworzeniem kopii zapasowej danych sprawdź parametr `lower_case_table_names`. Następnie podczas instalacji MySQL lub MariaDB dla Kaspersky Security Center Linux należy ustawić ten parametr na taką samą wartość, jaka została określona dla tego parametru w systemie Windows.

Wymagania wstępne

Przed rozpoczęciem, **sprawdź wymagania dotyczące certyfikatu niestandardowego**.

Jeśli używasz certyfikatu niestandardowego zamiast certyfikatu z podpisem własnym, przed aktualizacją Kaspersky Security Center Linux do nowszej wersji upewnij się, że certyfikat zawiera Alternatywną nazwę podmiotu (SAN). Jeżeli nie zawiera, ważne jest, aby wymienić certyfikat przed aktualizacją Kaspersky Security Center Linux. W przeciwnym razie nie będziesz mógł zalogować się do Web Console po aktualizacji.

Aby upewnić się, że certyfikat zawiera Alternatywną nazwę podmiotu (SAN):

1. Na urządzeniu z zainstalowanym Serwerem administracyjnym, wykonaj następujące polecenie:

   - W przypadku urządzenia z systemem Linux:

     ```
     sudo openssl x509 -in /var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer -noout
     -ext subjectAltName
     ```

   - W przypadku urządzenia z systemem Windows:

     ```
     certutil -dump %ProgramData%\KasperskyLab\adminkit\1093\cert\klserver.cer
     ```

2. Upewnij się, że Alternatywna nazwa podmiotu jest obecna w wynikach polecenia i zawiera adres urządzenia Serwera administracyjnego.

3. Jeśli Alternatywna nazwa podmiotu jest niedostępna, użyj narzędzia klsetsrvcert, aby zastąpić certyfikat niestandardowy tym, który spełnia wymagania.

Etapy

Migracja z wykorzystaniem kopii zapasowej danych Serwera administracyjnego przebiega etapami:

1. **Sprawdzenie, czy posiadasz wewnętrzne konto użytkownika administratora, za pomocą którego możesz zalogować się do Serwera administracyjnego**

   Konto administratora będzie wykorzystywane do logowania się do Serwera administracyjnego Kaspersky Security Center Linux. Jeśli nie posiadasz tego konta i jesteś zalogowany tylko na lokalnym koncie systemu Windows lub koncie domenowym, nie będziesz mógł zalogować się do Serwera administracyjnego Kaspersky Security Center Linux po przywróceniu kopii zapasowej. Serwer administracyjny Kaspersky Security Center Linux nie obsługuje logowania przy użyciu lokalnego konta systemu Windows. Zalogowanie się na konto domenowe jest możliwe, ale może wymagać dodatkowej konfiguracji Serwera administracyjnego.

   Jeśli nie posiadasz konta administratora, będziesz musiał je utworzyć po przywróceniu kopii zapasowej, korzystając z narzędzia kladduser.

2. **Tworzenie aktualnej kopii zapasowej danych Serwera administracyjnego Kaspersky Security Center Windows**

   W zależności od typu systemu DBMS używanego w Kaspersky Security Center Windows i Kaspersky Security Center Linux wykonaj jedną z następujących czynności:

   - Aby przeprowadzić migrację MySQL lub MariaDB do MySQL lub MariaDB: utwórz kopię zapasową za pomocą narzędzia klbackup lub zadania tworzenia kopii zapasowej danych na urządzeniu z zainstalowanym Serwerem administracyjnym.

   - W celu migracji PostgresSQL do PostgresSQL i PostgresPro do PostgresPro: utwórz kopię zapasową korzystając z narzędzia klbackup lub zadania tworzenia kopii zapasowej danych na urządzeniu, na którym zainstalowano Serwer administracyjny.

   - W celu migracji Microsoft SQL Server do MySQL lub MariaDB: utwórz kopię zapasową korzystając z narzędzia klbackup, z włączoną opcją **Wykonaj migrację do formatu MySQL/MariaDB**.

   - W celu migracji Microsoft SQL Server do PostgreSQL lub Postgres Pro:

     1. Zainstaluj poprawkę dla Serwera administracyjnego, aby umożliwić migrację do PostgreSQL i Postgres Pro. Skontaktuj się z pomocą techniczną Kaspersky, aby uzyskać tę poprawkę.

        Dla Kaspersky Security Center 15.1 Windows, możesz przeprowadzić aktualizację do wersji 15.1.0.22239 zamiast instalować poprawkę.

     2. Utwórz kopię zapasową za pomocą narzędzia klbackup.

        Jeśli uruchamiasz klbackup z wiersza poleceń, użyj flagi `-migrate postgres`.

        Jeśli używasz interfejsu klbackup, włącz opcję **Migruj do formatu Postgres**.

   Po utworzeniu kopii zapasowej odłącz Serwer administracyjny Kaspersky Security Center Windows od sieci.

3. **Przygotowanie nowego urządzenia do instalacji Kaspersky Security Center Linux**

Na tym etapie scenariusza wykonaj następujące czynności:

1. Wybierz nowe urządzenie, na którym chcesz zainstalować Serwer administracyjny. Urządzenie musi spełniać wymagania sprzętowe i programowe. Sprawdź również, czy porty używane na Serwerze administracyjnym są dostępne.

2. Przypisz ten sam adres do nowego urządzenia.

   Nowy Serwer administracyjny może mieć przypisaną nazwę NetBIOS, FQDN i statyczny adres IP. Zależy to od tego, który adres Serwera administracyjnego został ustawiony w pakiecie instalacyjnym Agenta sieciowe w momencie instalacji Agenta sieciowego. Alternatywnie można użyć adresu połączenia, który określa Serwer administracyjny, z którym łączy się Agent sieciowy (możesz uzyskać ten adres na zarządzanych urządzeniach korzystając z narzędzia klnagchk).

4 Instalowanie i konfigurowanie systemu DBMS

Na tym etapie scenariusza wykonaj następujące czynności:

1. Wybierz typ systemu DBMS zapewniający optymalną wydajność. Należy wziąć pod uwagę liczbę urządzeń sieciowych, topologię sieci oraz obciążenie sieci. Możesz wybrać dowolny obsługiwany system DBMS.

2. Zainstaluj system DBMS zgodnie z typem systemu DBMS wybranym podczas tworzenia kopii zapasowej. Informacje o sposobie zainstalowania wybranego systemu DBMS znajdziesz w tym dokumencie.

   Ręcznie utwórz bazę danych dla IAM.

   > Nowa wersja bazy danych nie może być starsza od obecnej.

3. Skonfiguruj system DBMS do pracy z Kaspersky Security Center Linux:

- Konfigurowanie serwera MariaDB x64 do pracy z Kaspersky Security Center Linux
- Konfigurowanie serwera PostgreSQL lub Postgres Pro do pracy z Kaspersky Security Center Linux
- Konfigurowanie serwera MySQL x64 do pracy z Kaspersky Security Center Linux

5 Instalowanie Kaspersky Security Center Linux

Zainstaluj Kaspersky Security Center Linux na nowym urządzeniu.

Wewnętrzne konto użytkownika administratora utworzone podczas instalacji, a także inne obiekty (grupy, zasady, zadania, użytkownicy) utworzone przed przywróceniem danych Serwera administracyjnego z kopii zapasowej zostaną utracone po przywróceniu. Obiekty te zostaną zastąpione obiektami zawartymi w kopii zapasowej.

6 Przywracanie danych Serwera administracyjnego z kopii zapasowej

Na tym etapie scenariusza wykonaj następujące czynności:

1. Przywróć dane Serwera administracyjnego na nowym urządzeniu, korzystając z narzędzia klbackup.

   > Ze względu na ograniczenia PostgreSQL należy tymczasowo przyznać uprawnienia superużytkownika PostgreSQL dla konta, którego Serwer administracyjny używa do łączenia się z systemem DBMS.

2. Jeśli nie posiadasz wewnętrznego konta użytkownika administratora, na którym zalogowałeś się do Serwera administracyjnego Kaspersky Security Center Windows i używasz lokalnego konta systemu Windows lub konta domenowego, utwórz konto administratora, korzystając z narzędzia kladduser w następujący sposób:

   ```
   /opt/kaspersky/ksc64/sbin/kladduser -n kscadmin -p <hasło>
   ```

gdzie parametr < `hasło` > spełnia następujące wymagania:

- Hasło użytkownika nie może mieć mniej niż 8 ani więcej niż 256 znaków.
- Hasło musi zawierać znaki z przynajmniej trzech z poniższych grup:
  - Wielkie litery (A-Z)
  - Małe litery (a-z)
  - Cyfry (0-9)
  - Znaki specjalne (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)

7. **Konfigurowanie weryfikacji certyfikatu przez Serwer administracyjny i Serwer IAM.**

8. **Instalacja Kaspersky Security Center Web Console i konfiguracja Serwera administracyjnego**

   Na tym etapie scenariusza wykonaj następujące czynności:

   1. Zainstaluj Kaspersky Security Center Web Console.

      Jeśli Kaspersky Security Center Web Console została zainstalowana wcześniej, zainstaluj ją ponownie z tym samym plikiem odpowiedzi.

      Zaloguj się do Kaspersky Security Center Web Console na koncie użytkownika wewnętrznego administratora.

      Proces inicjalizacji danych trwa zazwyczaj do 15 minut po przywróceniu danych Serwera administracyjnego, lecz czas ten zależy od wydajności sprzętu i rozmiaru danych Serwera administracyjnego. W tym czasie Kaspersky Security Center Web Console może nie nawiązać połączenia i mogą zostać wyświetlone błędy.

   2. Sprawdź działanie głównych funkcji Serwera administracyjnego po zakończeniu inicjalizacji danych w bazie danych. Sprawdź, czy Serwer administracyjny synchronizuje się z zarządzanymi urządzeniami i czy dane Serwera administracyjnego zostały odzyskane.

   3. Przeprowadź przeszukiwanie kontrolerów domeny w celu przywrócenia informacji o strukturze domeny, kontach użytkowników, grupach zabezpieczeń i nazwach DNS urządzeń uwzględnionych w domenach.

   4. Przejrzyj zmigrowane zadania. Jeżeli którykolwiek z parametrów zawiera ścieżkę do pliku systemu Windows, zastąp ją odpowiednią ścieżką do pliku systemu Linux.

   5. W razie konieczności odinstaluj Serwer administracyjny i serwer bazy danych z poprzedniego urządzenia.

      W tej samej sieci nie może być wiele Serwerów administracyjnych korzystających z tego samego adresu połączenia i certyfikatu Serwera administracyjnego.

Administrator ma dostęp do danych Serwera administracyjnego i zarządzanych urządzeń, do których dostęp jest możliwy w Kaspersky Security Center Windows, z uwzględnieniem funkcjonalności obsługiwanych w Kaspersky Security Center Linux.

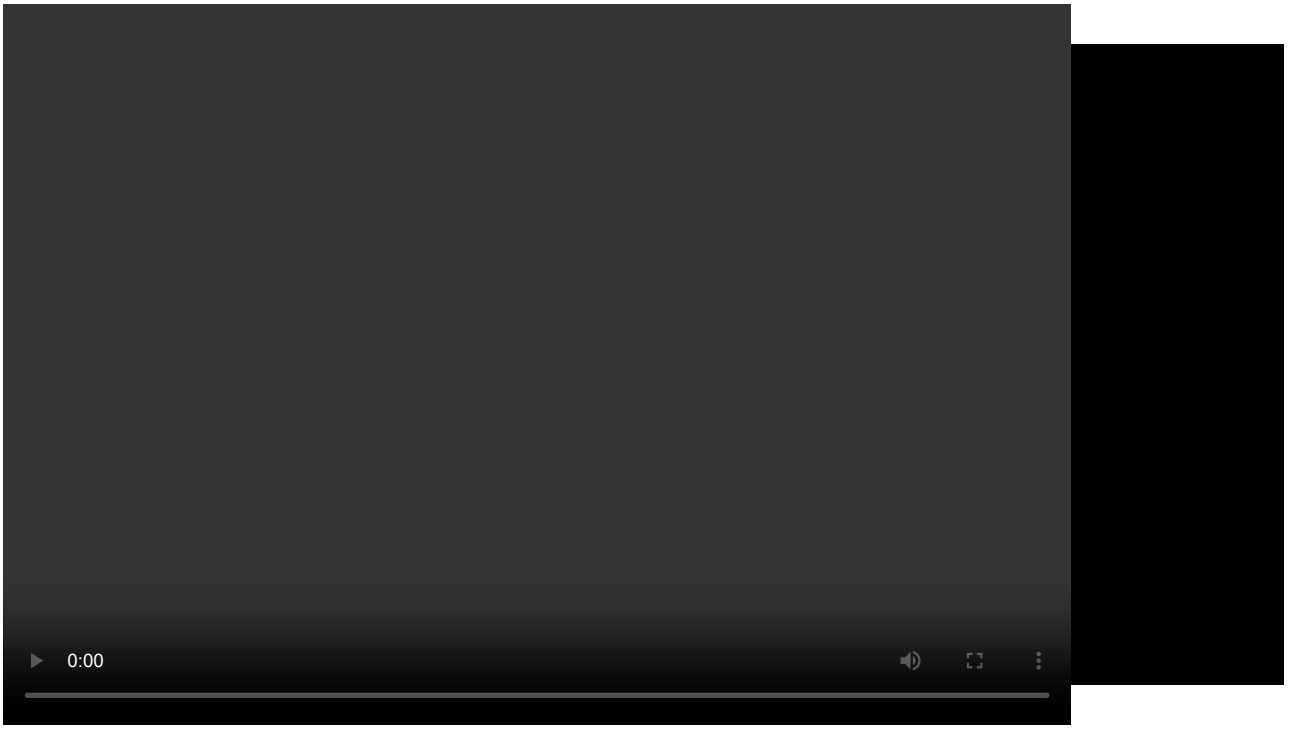
Film instruktażowy: Migracja do Kaspersky Security Center Linux przy użyciu kopii zapasowej danych Serwera administracyjnego

Obejrzyj film, aby dowiedzieć się, jak przenieść dane z Serwera administracyjnego Kaspersky Security Center Windows do Kaspersky Security Center Linux, korzystając z kopii zapasowej danych Serwera administracyjnego (za pomocą narzędzia klbackup).

Aby wesprzeć migrację do PostgreSQL lub Postgres Pro, musisz poprosić o pomoc techniczną Kaspersky i zainstalować jedną z następujących poprawek:

- Dla Kaspersky Security Center 14.2 Windows: 14.2.0.26967-pf5
- Dla Kaspersky Secure Mobility Management opartego na Kaspersky Security Center 14.2 Windows: 14.2.0.48079-pf5
- Dla Kaspersky Security Center 15.1 Windows: 15.1.0.20748-pf2

Migracja do PostgreSQL lub Postgres Pro staje się również dostępna po aktualizacji Kaspersky Security Center Windows do wersji 15.1.0.22239.



Migracja do Kaspersky Security Center Linux przy użyciu kopii zapasowej danych Serwera administracyjnego. Film wideo

Migracji do Kaspersky Security Center Linux za pomocą Kreatora migracji

Postępując zgodnie z tym scenariuszem, możesz przenieść strukturę grupy administracyjnej, dołączone zarządzane urządzenia i inne obiekty grupowe (zasady, zadania, zadania globalne, znaczniki i wybór urządzeń) z Kaspersky Security Center Windows w ramach zarządzania Kaspersky Security Center Linux.

Ograniczenia:

- Migracja jest możliwa wyłącznie z Kaspersky Security Center Windows w wersji 14.2 lub nowszej do Kaspersky Security Center Linux w wersji 15 lub nowszej.
- Możesz wykonać ten scenariusz tylko przy użyciu Kaspersky Security Center Web Console.

Zanim zaczniesz, dowiedz się więcej o funkcjach i ograniczeniach Kaspersky Security Center Linux:

- Różnice funkcjonalne pomiędzy Kaspersky Security Center Windows i Kaspersky Security Center Linux
- Lista aplikacji firmy Kaspersky obsługiwanych przez Kaspersky Security Center Linux

Etapy

Scenariusz migracji przebiega etapami:

1. **Wybierz metodę migracji**

   Migracji do Kaspersky Security Center Linux dokonujesz za pomocą Kreatora migracji. Kroki kreatora migracji zależą od tego, czy Serwery administracyjne Kaspersky Security Center Windows i Kaspersky Security Center Linux są ułożone w hierarchię:

   - Migracja z użyciem hierarchii Serwerów administracyjnych

     Wybierz tę opcję, jeśli Serwer administracyjny Kaspersky Security Center Windows działa jako serwer pomocniczy w stosunku do Serwera administracyjnego Kaspersky Security Center Linux. Zarządzasz procesem migracji i przełączasz się między serwerami w jednej instancji Kaspersky Security Center Web Console. Jeśli wolisz tę opcję, możesz ustawić Serwery administracyjne w hierarchię, aby uprościć procedurę migracji. Aby to zrobić, utwórz hierarchię przed rozpoczęciem migracji.

   - Migracja za pomocą pliku eksportu (archiwum ZIP)

     Wybierz tę opcję, jeśli Serwery administracyjne Kaspersky Security Center Windows i Kaspersky Security Center Linux nie są ułożone w hierarchię. Procesem migracji zarządzasz za pomocą dwóch instancji Kaspersky Security Center Web Console — instancji dla Kaspersky Security Center Windows i drugiej dla Kaspersky Security Center Linux. W takim przypadku użyjesz pliku eksportu, który utworzyłeś i pobrałeś podczas eksportu z Kaspersky Security Center Windows i zaimportujesz ten plik do Kaspersky Security Center Linux.

2. **Utwórz kopię zapasową certyfikatu i klucza prywatnego Serwera administracyjnego Kaspersky Security Center Windows (krok opcjonalny)**

   Możesz poddać zarządzane urządzenia zarządzaniu przez Serwer administracyjny Kaspersky Security Center Linux poprzez przywrócenie certyfikatu i klucza prywatnego Serwera administracyjnego z kopii zapasowej. W takim przypadku wykonaj kopię zapasową certyfikatu i klucza prywatnego Serwera administracyjnego Kaspersky Security Center Windows. Następnie na etapie 6 należy przywrócić certyfikat i klucz prywatny.

3. **Eksportowanie danych z Kaspersky Security Center Windows**

   Otwórz Kaspersky Security Center Windows, a następnie uruchom Kreatora migracji.

4. **Import danych do Kaspersky Security Center Linux**

   Kontynuuj działanie Kreatora migracji, aby zaimportować wyeksportowane dane do Kaspersky Security Center Linux. Jeśli Serwery są ułożone w hierarchię, import rozpoczyna się automatycznie po pomyślnym eksporcie w tym samym kreatorze. Jeśli Serwery nie są ułożone w hierarchię, po przełączeniu do Kaspersky Security Center Linux będziesz kontynuować działanie Kreatora migracji.

5. **Wykonaj dodatkowe czynności, aby ręcznie przenieść obiekty i ustawienia z Kaspersky Security Center Windows do Kaspersky Security Center Linux (krok opcjonalny)**

   Możesz także chcieć przenieść obiekty i ustawienia, których nie można przenieść za pomocą Kreatora migracji. Na przykład możesz dodatkowo wykonać następujące czynności:

   - Przenieś klucze licencyjne używane przez Serwer administracyjny i zarządzane aplikacje
   - Skonfiguruj zadania globalne Serwera administracyjnego
   - Skonfiguruj Ustawienia zasady Agenta sieciowego
   - Utwórz pakiety instalacyjne aplikacji
   - Utwórz wirtualne Serwery
   - Skonfiguruj reguły przenoszenia urządzeń
   - Skonfiguruj reguły automatycznego znakowania urządzeń
   - Utwórz kategorie aplikacji
   - Przypisz i skonfiguruj punkty dystrybucji

     Jeżeli przeniesiesz urządzenie pełniące rolę punktu dystrybucji na inny Serwer administracyjny, urządzenia objęte zasięgiem punktu dystrybucji nie zostaną przeniesione automatycznie. Musisz przenosić każde urządzenie osobno. Jeśli punkt dystrybucji pełni funkcję bramy, musisz uruchomić skrypt `# /opt/kaspersky/klnagent64/bin/setup/postinstall.pl`, aby punkt dystrybucji przestał pełnić funkcję bramy.

6. **Przenieś zaimportowane zarządzane urządzenia do zarządzania przez Kaspersky Security Center Linux**

   Aby zakończyć migrację, przenieść zaimportowane zarządzane urządzenia do zarządzania przez Kaspersky Security Center Linux. Można to zrobić przy użyciu jednej z następujących metod:

   - Za pomocą narzędzia klmover

     Użyj narzędzia klmover i określ ustawienia połączenia dla nowego Serwera administracyjnego.

- Poprzez zadanie *Zmień Serwer administracyjny*

  Utwórz zadanie *Zmień Serwer administracyjny*, określ zaimportowane zarządzane urządzenia, nowy Serwer administracyjny i inne ustawienia zadania. Następnie uruchom zadanie, aby przenieść zarządzane urządzenia pod zarządzanie Serwera administracyjnego Kaspersky Security Center Linux.

- Poprzez usunięcie (jeśli jest już zainstalowany) i ponowną instalację Agenta sieciowego na zarządzanych urządzeniach

  Utwórz nowy pakiet instalacyjny Agenta sieciowego i określ ustawienia połączenia dla nowego Serwera administracyjnego we właściwościach pakietu instalacyjnego. Usuń Agenta sieciowego na zaimportowanych urządzeniach zarządzanych, a następnie użyj pakietu instalacyjnego, aby zainstalować Agenta sieciowego na zaimportowanych urządzeniach zarządzanych za pomocą zadania instalacji zdalnej. Można także utworzyć autonomiczny pakiet instalacyjny i używać go do lokalnej instalacji Agenta sieciowego. Aby uzyskać więcej informacji, zobacz punkt Przełączanie zarządzanych urządzeń na zarządzane przez Kaspersky Security Center Linux.

- Poprzez przywrócenie certyfikatu i klucza prywatnego Serwera administracyjnego z kopii zapasowej (tylko w przypadku migracji do Kaspersky Security Center Linux 15.1 lub nowszej wersji)

  Przypisz urządzeniu z Serwerem administracyjnym Kaspersky Security Center Linux ten sam adres sieciowy, co urządzeniu z Serwerem administracyjnym Kaspersky Security Center Windows. Uruchom narzędzie klbackup z parametrem `-cert_only`, aby przywrócić certyfikat Serwera administracyjnego oraz klucz prywatny z kopii zapasowej, którą zapisałeś w etapie 2. W wierszu poleceń wykonaj następujące polecenie: `/opt/kaspersky/ksc64/sbin/klbackup -path <ścieżka do kopii zapasowej certyfikatu Serwera administracyjnego> -restore -cert_only`. Aby uzyskać więcej informacji, zobacz Używanie narzędzia klbackup w celu przełączania zarządzanych urządzeń na zarządzenie przez inny Serwer administracyjny.

7. **Zaktualizuj Agenta sieciowego do najnowszej wersji**

   Zalecamy aktualizację Agenta sieciowego dla systemu Linux do tej samej wersji, co Kaspersky Security Center.

8. **Upewnij się, że zarządzane urządzenia są widoczne na nowym Serwerze administracyjnym**

   Na Serwerze administracyjnym Kaspersky Security Center Linux otwórz listę zarządzanych urządzeń (**Zarządzanie zasobami** → **Zasoby (urządzenia)**) i sprawdź wartości w kolumnach **Widoczny**, **Agent sieciowy jest zainstalowany** i **Ostatnie połączenie z Serwerem administracyjnym**.

Inne metody migracji danych

Oprócz kreatora migracji istnieją inne metody przesyłania bieżących obiektów, ale te metody umożliwiają przesyłanie tylko zasad i zadań:

- Wyeksportuj zadania z Kaspersky Security Center Windows, a następnie zaimportuj zadania do Kaspersky Security Center Linux.
- Wyeksportuj określone zasady z Kaspersky Security Center Windows, a następnie zaimportuj zasady do Kaspersky Security Center Linux. Powiązane profile zasad są eksportowane i importowane razem z wybranymi zasadami.

Eksportowanie obiektów grupowych z Kaspersky Security Center Windows

Struktura grupy administracyjnej migracji, dołączone zarządzane urządzenia i inne obiekty grupowe z Kaspersky Security Center Windows do Kaspersky Security Center Linux wymaga uprzedniego wybrania danych do eksportu i utworzenia pliku eksportu. Plik eksportu zawiera informacje o wszystkich obiektach grupowych, których migrację chcesz przeprowadzić. Plik eksportowania zostanie użyty do następnego zaimportowania do konsoli Kaspersky Security Center Linux.

Możesz wyeksportować następujące obiekty:

- Zadania i zasady zarządzanych aplikacji
- Zadania globalne
- Niestandardowe wybory urządzeń
- Strukturę grupy administracyjnej i dołączonych urządzeń
- Znaczniki przypisane do przenoszonych urządzeń

Przed rozpoczęciem eksportu przeczytaj ogólne informacje o migracji do Kaspersky Security Center Linux. Wybierz metodę migracji — używając lub nie używając hierarchii Serwerów administracyjnych Kaspersky Security Center Windows i Kaspersky Security Center Linux.

Aby wyeksportować zarządzane urządzenia i powiązane obiekty grupowe za pomocą kreatora migracji:

1. W zależności od tego, czy Serwery administracyjne Kaspersky Security Center Windows i Kaspersky Security Center Linux są ułożone w hierarchię, wykonaj jedną z następujących czynności:
   - Jeśli Serwery są ułożone w hierarchię, otwórz Kaspersky Security Center Web Console, a następnie przełącz się do Serwera Kaspersky Security Center Windows.
   - Jeśli Serwery nie są ułożone w hierarchię, otwórz Kaspersky Security Center Web Console połączoną z Kaspersky Security Center Windows.
2. W menu głównym przejdź do **Operacje** → **Migracja**.
3. Wybierz **Migracja do Kaspersky Security Center Linux lub platformy Open Single Management Platform**, aby uruchomić kreatora i postępować zgodnie z jego instrukcjami.
4. Wybierz grupę administracyjną lub podgrupę do wyeksportowania. Upewnij się, że wybrana grupa lub podgrupa administracyjna zawiera nie więcej niż 10 000 urządzeń.
5. Wybierz zarządzane aplikacje, których zadania i zasady zostaną wyeksportowane. Wybierz tylko te aplikacje, które są obsługiwane przez Kaspersky Security Center Linux. Obiekty nieobsługiwanych aplikacji będą nadal eksportowane, ale nie będą działać.
6. Użyj linków po lewej stronie, aby wybrać zadania globalne, wybrane urządzenia i raporty do wyeksportowania. Łącze **Obiekty grupy** umożliwia wykluczenie niestandardowych ról, użytkowników wewnętrznych i grup zabezpieczeń oraz niestandardowych kategorii aplikacji z eksportu.

Zostanie utworzony plik eksportu (archiwum ZIP). W zależności od tego, czy przeprowadzasz migrację z obsługą hierarchii Serwera administracyjnego, plik eksportu jest zapisywany w następujący sposób:

- Jeśli serwery są ułożone w hierarchię, plik eksportu jest zapisywany w folderze tymczasowym na serwerze Kaspersky Security Center Web Console Server.
- Jeśli Serwery nie są ułożone w hierarchię, plik eksportu zostanie pobrany na Twoje urządzenie.

W przypadku migracji z obsługą hierarchii Serwera administracyjnego import rozpoczyna się automatycznie po udanym eksporcie. W przypadku migracji bez obsługi hierarchii Serwera administracyjnego możesz ręcznie zaimportować zapisany plik eksportu do Kaspersky Security Center Linux.

Importowanie pliku eksportowania do Kaspersky Security Center Linux

Aby przesłać informacje o zarządzanych urządzeniach, obiektach i ich ustawieniach, które zostały wyeksportowane z Kaspersky Security Center Windows, musisz zaimportować je do Kaspersky Security Center Linux lub Kaspersky Next XDR Expert.

Aby zaimportować zarządzane urządzenia i powiązane obiekty grupowe za pomocą kreatora migracji:

1. W zależności od tego, czy Serwery administracyjne Kaspersky Security Center Windows i Kaspersky Security Center Linux są ułożone w hierarchię, wykonaj jedną z następujących czynności:
   - Jeśli serwery są ustawione hierarchicznie, po zakończeniu eksportu przejdź do następnego kroku kreatora migracji. Import rozpoczyna się automatycznie po pomyślnym eksporcie w tym kreatorze (patrz krok 2 tej instrukcji).
   - Jeśli serwery nie są ustawione hierarchicznie:
     a. Otwórz program Kaspersky Security Center Web Console połączony z oprogramowaniem Kaspersky Security Center Linux lub Kaspersky Next XDR Expert.
     b. W menu głównym przejdź do **Operacje** → **Migracja**.
     c. Wybierz plik eksportu (archiwum ZIP), który utworzono i pobrano podczas eksportu z Kaspersky Security Center Windows. Rozpocznie się przesyłanie pliku eksportu.
2. Po pomyślnym przesłaniu pliku eksportu możesz kontynuować importowanie. Jeśli chcesz wskazać inny plik eksportu, kliknij łącze **Zmień**, a następnie wybierz żądany plik.
3. Wyświetlana jest cała hierarchia grup administracyjnych Kaspersky Security Center Linux.

   Zaznacz pole wyboru obok docelowej grupy administracyjnej, w której mają zostać przywrócone obiekty wyeksportowanej grupy administracyjnej (zarządzane urządzenia, zasady, zadania i inne obiekty grupowe).
4. Rozpoczyna się import obiektów grupy. Nie będzie można zminimalizować kreatora migracji i wykonać jakichkolwiek równoczesnych działań w trakcie importowania. Zaczekaj, aż ikony odświeżenia (🔄), znajdujące się obok wszystkich elementów na liście obiektów zostaną zastąpione zielonymi znacznikami wyboru (✓), a importowanie zostanie zakończone.
5. Po zakończeniu importowania, wyeksportowana struktura grup administracyjnych, w tym szczegóły urządzeń, pojawi się pod wybraną docelową grupą administracyjną. Jeśli nazwa obiektu, który przywracasz, jest taka sama jak nazwa istniejącego obiektu, do przywracanego obiektu zostanie dodany sufiks przyrostowy.

Jeżeli w migrowanym zadaniu podane są dane konta, na którym zadanie jest uruchamiane, po zakończeniu importu należy otworzyć zadanie i ponownie wprowadzić hasło.

Jeśli import zakończył się błędem, możesz wykonać jedną z następujących czynności:

- W przypadku migracji z obsługą hierarchii Serwera administracyjnego możesz ponownie rozpocząć importowanie pliku eksportu.
- W przypadku migracji bez obsługi hierarchii Serwera administracyjnego możesz uruchomić Kreator migracji, aby wybrać inny plik eksportu, a następnie zaimportować go ponownie.

Możesz sprawdzić, czy obiekty grupy zawarte w zakresie eksportu zostały pomyślnie zaimportowane do programu Kaspersky Security Center Linux. W tym celu przejdź do sekcji **Zarządzanie zasobami** i upewnij się, czy zaimportowane obiekty są wyświetlane w odpowiednich podsekcjach.

Zwróć uwagę, że zaimportowane zarządzane urządzenia są wyświetlane w podsekcji **Zarządzane urządzenia**, ale są niewidoczne w sieci, a Agent sieciowy nie jest na nich zainstalowany i uruchomiony (wartość *Nie* w kolumnach **Widoczny**, **Agent sieciowy jest zainstalowany** oraz **Agent sieciowy jest uruchomiony**).

Aby zakończyć migrację, musisz przełączyć zarządzane urządzenia na zarządzanie przez Kaspersky Security Center Linux.

Przełączanie zarządzanych urządzeń na zarządzane przez Kaspersky Security Center Linux

Po pomyślnym zaimportowaniu informacji o zarządzanych urządzeniach, obiektach i ich ustawieniach do Kaspersky Security Center Linux, musisz przełączyć zarządzane urządzenia, aby były zarządzane przez Kaspersky Security Center Linux, aby zakończyć migrację.

Możesz przenieść zarządzane urządzenia do Kaspersky Security Center Linux, korzystając z jednej z następujących metod:

- Użycie narzędzia klmover.
- Użycie zadania *Zmień Serwer administracyjny*.
- Przywracanie certyfikatu i klucza prywatnego Serwera administracyjnego z kopii zapasowej (tylko w przypadku migracji do Kaspersky Security Center Linux 15.1 lub nowszego).

  Aby uzyskać szczegółowe informacje, zapoznaj się z etapem 6 głównego scenariusza migracji.
- Zainstalowanie Agenta sieciowego na zarządzanych urządzeniach za pomocą zadania zdalnej instalacji.

W celu przełączenia zarządzanych urządzeń, aby były zarządzane przez Kaspersky Security Center Linux poprzez zainstalowanie Agenta sieciowego:

1. Usuń Agenta sieciowego na importowanych zarządzanych urządzeniach, które zostaną przełączone pod zarządzanie Kaspersky Security Center Linux.
2. Przełącz się na Serwer administracyjny Kaspersky Security Center Windows.

3. Przejdź do **Zarządzanie oprogramowaniem** → **Pakiety instalacyjne**, a następnie otwórz właściwości istniejącego pakietu instalacyjnego Agenta sieciowego.

   Jeżeli na liście pakietów nie ma pakietu instalacyjnego Agenta sieciowego, pobierz nowy.

   Można także utworzyć autonomiczny pakiet instalacyjny i używać go do lokalnej instalacji Agenta sieciowego.

4. Na karcie **Ustawienia** wybierz sekcję **Połączenie**. Określ ustawienia połączenia Serwera administracyjnego Kaspersky Security Center Linux.

5. Utwórz zadanie zdalnej instalacji dla zaimportowanych zarządzanych urządzeń, a następnie określ ponownie skonfigurowany pakiet instalacyjny Agenta sieciowego.

   Możesz zainstalować Agenta sieciowego za pośrednictwem Serwera administracyjnego Kaspersky Security Center Windows lub urządzenia z systemem Windows, które działa jako punkt dystrybucji. Jeśli korzystasz z Serwera administracyjnego, włącz opcję **Przy użyciu zasobów systemu operacyjnego przez Serwer administracyjny**. Jeśli korzystasz z punktu dystrybucji, włącz opcję **Przy użyciu zasobów systemu operacyjnego poprzez punkty dystrybucji**.

6. Uruchom zadanie zdalnej instalacji.

Po pomyślnym zakończeniu zadania zdalnej instalacji przejdź do Serwera administracyjnego Kaspersky Security Center Linux i upewnij się, że zarządzane urządzenia są widoczne w sieci oraz że Agent sieciowy jest na nich zainstalowany i uruchomiony (wartość *Tak* w kolumnach **Widoczny**, **Agent sieciowy jest zainstalowany** oraz **Agent sieciowy jest uruchomiony**).

Konfigurowanie Serwera administracyjnego

W tej sekcji opisano proces konfiguracji oraz właściwości Serwera administracyjnego.

Konfigurowanie adresu połączenia Serwera administracyjnego

Adres połączenia serwera administracyjnego to adres sieciowy używany do następujących celów:

- Jako adres domyślny podczas tworzenia pakietów instalacyjnych Agenta sieciowego

  Po zainstalowaniu Agenta sieciowego zarządzane urządzenia łączą się z Serwerem administracyjnym pod tym adresem.

- Konfigurowanie adresu serwera proxy KSN

  Zarządzane urządzenia łączą się z serwerem proxy KSN za pośrednictwem tego adresu.

Aby skonfigurować adres połączenia Serwera administracyjnego:

1. W menu głównym kliknij nazwę Serwera administracyjnego.

   Zostanie otwarte okno właściwości Serwera administracyjnego.

2. Na zakładce **Ogólne** wybierz sekcję **Ogólne**.

3. W oknie, które zostanie otwarte, w polu **Adres połączenia z Serwerem administracyjnym** należy podać nowy adres połączenia Serwera administracyjnego.

   Maksymalna długość adresu połączenia wynosi 255 znaków.

   Adres połączenia Serwera administracyjnego można określić jako nazwę NetBIOS, FQDN lub adres IP Serwera administracyjnego.

4. Kliknij przycisk **Zapisz**.

Podany adres jest używany jako adres Serwera administracyjnego i adres serwera proxy KSN.

Konfigurowanie połączenia Kaspersky Security Center Web Console z Serwerem administracyjnym

Połączenie Kaspersky Security Center Web Console z Serwerem administracyjnym można skonfigurować za pośrednictwem właściwości Serwera administracyjnego lub korzystając z ustawień zasad Serwera administracyjnego.

W celu określenia portów połączenia we właściwościach Serwera administracyjnego:

1. W menu głównym kliknij nazwę Serwera administracyjnego.

   Zostanie otwarte okno właściwości Serwera administracyjnego.

2. Na zakładce **Ogólne** wybierz sekcję **Porty połączenia**.

3. W razie potrzeby określ **Port SSL dla Web Console** lub określ inne porty połączenia Serwera administracyjnego.

Określono główne ustawienia połączenia wybranego serwera.

Aby ustawić porty połączeń za pomocą ustawień zasad Serwera administracyjnego:

1. W menu głównym przejdź do **Zarządzanie zasobami** → **Zasady**.

2. Kliknij nazwę zasady Serwera administracyjnego, a następnie przejdź do zakładki **Ustawienia aplikacji**.

3. W razie potrzeby określ **Port SSL dla Web Console** lub określ inne porty połączenia Serwera administracyjnego.

   Jeśli wyłączysz opcję **Otwórz port dla Web Console** i to ustawienie zasad zostanie zastosowane do urządzenia, nie będziesz mógł nawiązać połączenia z Serwerem administracyjnym przy użyciu Kaspersky Security Center Web Console. W takim przypadku połączenie zostanie zakończone. Jeśli posiadasz Serwer administracyjny, na którym ta zasada nie jest stosowana, możesz ponownie nawiązać połączenie z tym Serwerem administracyjnym za pośrednictwem Kaspersky Security Center Web Console.

Określono główne ustawienia połączenia wybranego serwera.

Konfigurowanie listy dozwolonych adresów IP do łączenia się z Kaspersky Security Center Linux

Domyślnie połączenia z Kaspersky Security Center Linux są dozwolone z dowolnego urządzenia. Możesz na przykład zainstalować Kaspersky Security Center Web Console Server na dowolnym urządzeniu spełniającym wymagania, a Kaspersky Security Center Web Console Server będzie komunikować się z Kaspersky Security Center Linux. Możesz jednak skonfigurować Serwer administracyjny tak, aby połączenia były dozwolone wyłącznie z urządzeń o określonych przez Ciebie adresach IP. W takim przypadku, jeśli intruz spróbuje nawiązać połączenie z Kaspersky Security Center Linux za pośrednictwem Kaspersky Security Center Web Console Server zainstalowanego na urządzeniu, które nie znajduje się na liście zezwolonych, nie będzie mógł zalogować się do Kaspersky Security Center Linux.

Adres IP jest sprawdzany, gdy użytkownik loguje się do Kaspersky Security Center Linux lub uruchamia aplikację, która współdziała z Serwerem administracyjnym poprzez Kaspersky Security Center Linux OpenAPI. W tym momencie aplikacja na urządzeniu próbuje nawiązać połączenie z Serwerem administracyjnym. Jeśli adresu IP urządzenia nie ma na liście zezwolonych, wystąpi błąd uwierzytelniania, a zdarzenie KLAUD_EV_SERVERCONNECT powiadamia, że połączenie z serwerem administracyjnym nie zostało nawiązane.

Wymagania dotyczące listy zezwolonych adresów IP

Adresy IP są weryfikowane tylko wtedy, gdy następujące aplikacje próbują połączyć się z serwerem administracyjnym:

- Kaspersky Security Center Web Console Server

  Jeśli logujesz się do Kaspersky Security Center Linux za pomocą Kaspersky Security Center Web Console, możesz skonfigurować zaporę sieciową na urządzeniu, na którym zainstalowany jest Kaspersky Security Center Web Console Server, przy użyciu standardowych środków systemu operacyjnego. Następnie, jeśli ktoś spróbuje zalogować się do Kaspersky Security Center Linux na jednym urządzeniu, a Kaspersky Security Center Web Console Server zostanie zainstalowany na innym urządzeniu, zapora sieciowa zapobiegnie ingerencji intruzów.

- Aplikacje współpracujące z serwerem administracyjnym za pośrednictwem obiektów automatyzacji klakaut

- Aplikacje współpracujące z serwerem administracyjnym za pośrednictwem interfejsu OpenAPI, takie jak Kaspersky Anti Targeted Attack Platform lub Kaspersky Security for Virtualization

Dlatego należy podać adresy urządzeń, na których zainstalowane są wymienione powyżej aplikacje.

Możesz ustawić adresy IPv4 i IPv6. Nie możesz określić zakresów adresów IP.

Jak ustanowić listę zezwolonych adresów IP

Jeśli wcześniej nie ustawiono listy zezwolonych, postępuj zgodnie z poniższymi instrukcjami.

W celu ustanowienia listy zezwolonych adresów IP do logowania się do Kaspersky Security Center Linux:

1. Na urządzeniu serwera administracyjnego uruchom wiersz poleceń na koncie z uprawnieniami administratora.

2. Zmień bieżący katalog na folder instalacyjny Kaspersky Security Center Linux (zwykle /opt/kaspersky/ksc64/sbin).

3. Na koncie root wpisz następujące polecenie:
   ```
   klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "<adresy IP>" -t s
   ```

   Określ adresy IP, które spełniają powyższe wymagania. Wiele adresów IP należy oddzielać średnikami.

   Przykład — jak zezwolić tylko jednemu urządzeniu na łączenie się z serwerem administracyjnym:

   ```
   klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "192.0.2.0" -t s
   ```

   Przykład — jak zezwolić wielu urządzeniom na łączenie się z serwerem administracyjnym:

   ```
   klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "192.0.2.0; 198.51.100.0; 203.0.113.0" -t s
   ```

4. Uruchom ponownie usługę Serwera administracyjnego.

Możesz dowiedzieć się, czy pomyślnie skonfigurowano listę zezwolonych adresów IP w dzienniku zdarzeń Syslog na serwerze administracyjnym.

Jak zmienić listę zezwolonych adresów IP

Listę zezwolonych adresów można zmienić tak samo, jak podczas jej tworzenia. W tym celu uruchom to samo polecenie i określ nową listę zezwolonych adresów:

```
klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "<adresy IP>" -
t s
```

Jeśli chcesz usunąć niektóre adresy IP z listy zezwolonych, przepisz je. Na przykład, lista zezwolonych zawiera następujące adresy IP: 192.0.2.0; 198.51.100.0; 203.0.113.0. Chcesz usunąć adres IP 198.51.100.0. Aby to zrobić, wpisz następujące polecenie w wierszu polecenia:

```
klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "192.0.2.0;
203.0.113.0" -t s
```

Nie zapomnij ponownie uruchomić usługi serwera administracyjnego.

Jak zresetować skonfigurowaną listę zezwolonych adresów IP

Aby zresetować już skonfigurowaną listę zezwolonych adresów IP:

1. Na koncie root wpisz następujące polecenie w wierszu poleceń:
   ```
   klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "" -t s
   ```
2. Uruchom ponownie usługę Serwera administracyjnego.

Następnie adresy IP nie będą już weryfikowane.

Konfigurowanie ustawień dostępu do Internetu dla Serwera administracyjnego

Należy skonfigurować dostęp do internetu w taki sposób, aby korzystać z Kaspersky Security Network i pobierać aktualizacje antywirusowych baz danych dla Kaspersky Security Center Linux i zarządzanych aplikacji Kaspersky.

Aby określić ustawienia dostępu do Internetu dla Serwera administracyjnego:

1. W menu głównym kliknij nazwę Serwera administracyjnego.

   Zostanie otwarte okno właściwości Serwera administracyjnego.
2. Na zakładce **Ogólne** wybierz sekcję **Konfiguracja dostępu do internetu**.

3. Włącz opcję **Użyj serwera proxy**, jeśli podczas łączenia z internetem chcesz korzystać z serwera proxy. Jeśli ta opcja jest włączona, dostępne staną się pola do wprowadzenia ustawień. Dla połączenia z serwerem proxy określ następujące ustawienia:

   - **Adres serwera proxy**

     Adres serwera proxy używanego do łączenia Kaspersky Security Center Linux z Internetem.

   - **Numer portu**

     Numer portu, poprzez który zostanie nawiązane połączenie proxy Kaspersky Security Center Linux.

   - **Pomiń serwer proxy dla adresów lokalnych**

     Żaden serwer proxy nie będzie używany do nawiązywania połączenia z urządzeniami w sieci lokalnej.

   - **Uwierzytelnianie na serwerze proxy**

     Jeśli to pole jest zaznaczone, w polach wejściowych możesz określić dane uwierzytelniające do autoryzacji na serwerze proxy.

     To pole wejściowe jest dostępne, jeśli opcja **Użyj serwera proxy** jest zaznaczona.

   - **Nazwa użytkownika**

     Konto użytkownika, z poziomu którego nawiązywane jest połączenie z serwerem proxy (to pole jest dostępne, jeśli pole **Uwierzytelnianie na serwerze proxy** jest wybrane).

   - **Hasło**

     Hasło ustawione przez użytkownika, którego konto jest używane do nawiązywania połączenia z serwerem proxy (to pole jest dostępne, jeśli pole **Uwierzytelnianie na serwerze proxy** jest zaznaczone).

     Aby zobaczyć wprowadzone hasło, trzymaj kliknięty przycisk **Pokaż** tak długo, jak potrzebujesz.

Dostęp do Internetu można również skonfigurować za pomocą kreatora wstępnej konfiguracji.

Hierarchia Serwerów administracyjnych

Niektóre firmy klienckie, na przykład MSP, mogą uruchamiać wiele Serwerów administracyjnych. Niewygodne może być zarządzanie kilkoma oddzielnymi Serwerami administracyjnymi, dlatego dobrym wyjściem jest utworzenie hierarchii. W hierarchii serwer administracyjny oparty na systemie Linux może działać zarówno jako serwer podstawowy, jak i serwer pomocniczy. Podstawowy serwer oparty na systemie Linux może zarządzać serwerami pomocniczymi opartymi na systemie Linux i Windows. Podstawowy serwer oparty na systemie Windows może zarządzać dodatkowym serwerem opartym na systemie Linux.

Zastosowanie konfiguracji „główny/podrzędny” dla dwóch Serwerów administracyjnych oferuje następujące możliwości:

- Podrzędny Serwer administracyjny dziedziczy zasady, zadania, role użytkowników i pakiety instalacyjne z głównego Serwera administracyjnego, zapobiegając w ten sposób powielaniu ustawień.

- Wybory urządzeń na głównym Serwerze administracyjnym mogą zawierać urządzenia z podrzędnych Serwerów administracyjnych.

- Raporty na głównym Serwerze administracyjnym mogą zawierać dane (w tym szczegółowe informacje) z podrzędnych Serwerów administracyjnych.

- Główny Serwer administracyjny może być używany jako źródło aktualizacji dla podrzędnego Serwera administracyjnego.

W zakresie wyżej wymienionych opcji główny Serwer administracyjny odbiera dane tylko z niewirtualnych podrzędnych Serwerów administracyjnych. To ograniczenie nie dotyczy wirtualnych Serwerów administracyjnych, które współdzielą bazę danych ze swoim głównym Serwerem administracyjnym.

Hierarchia Serwerów administracyjnych zapewnia obsługę trybu wielodostępu. Tryb ten umożliwia głównemu administratorowi centralne zarządzanie wieloma klientami niezależnie. Każda organizacja lub biuro będące klientem jest odizolowane od pozostałych i nazywane jest dzierżawcą. Można przydzielić dzierżawcy wiele zarządzanych urządzeń wraz z powiązanymi danymi, ustawieniami, zasadami i zadaniami, a także skonfigurować uprawnienia użytkowników dla poszczególnych dzierżawców.

Główny Serwer administracyjny, zainstalowany w głównej infrastrukturze organizacji, pełni rolę głównego dzierżawcy. Główny Serwer administracyjny umożliwia podrzędnym lub wirtualnym Serwerom administracyjnym — jego odizolowanym dzierżawcom — niezależne odbieranie i przetwarzanie własnych zdarzeń oraz pracę z własnymi zasobami, usługami i konfiguracjami.

Dostawca usług, który ma klientów z wielu organizacji klienta, może udostępnić funkcjonalność Kaspersky Security Center Linux, w tym agregację alertów i działania reagowania, każdej organizacji klienta niezależnie. Aby to osiągnąć, dostawca usług łączy podrzędne lub wirtualne Serwery administracyjne jako dzierżawców dla każdej organizacji klienta. Dostawca usług świadczy usługi przy użyciu własnego personelu i zasobów.

Tworzenie hierarchii Serwerów administracyjnych: dodawanie podrzędnego Serwera administracyjnego

W hierarchii serwer administracyjny oparty na systemie Linux może działać zarówno jako serwer podstawowy, jak i serwer pomocniczy. Podstawowy serwer oparty na systemie Linux może zarządzać serwerami pomocniczymi opartymi na systemie Linux i Windows. Podstawowy serwer oparty na systemie Windows może zarządzać dodatkowym serwerem opartym na systemie Linux.

Dodawanie podrzędnego Serwera administracyjnego (wykonywane na przyszłym głównym Serwerze administracyjnym)

Możesz dodać Serwer administracyjny jako podrzędny Serwer administracyjny, a tym samym utworzyć hierarchię „główny/podrzędny".

W celu dodania podrzędnego Serwera administracyjnego, który jest dostępny do połączenia poprzez Kaspersky Security Center Web Console:

1. Upewnij się, że port 13000 przyszłego głównego Serwera administracyjnego jest dostępny.

   Ten port będzie używany do komunikacji między głównym a podrzędnym Serwerem administracyjnym po utworzeniu hierarchii.

2. Przejdź do właściwości przyszłego głównego Serwera administracyjnego:

   a. W menu głównym wybierz dowolną sekcję (z wyjątkiem **Platforma handlowa**, **Poruszanie się po konsoli** i **Ustawień**), a następnie na górze strony kliknij przycisk **Pokaż hierarchię**.

   b. W otwartym panelu nawigacyjnym najedź kursorem myszy na nazwę żądanego Serwera administracyjnego, a następnie kliknij ikonę ustawień (⚙).

   Alternatywnie możesz kliknąć nazwę Serwera administracyjnego, a następnie, po wyświetleniu nazwy w menu głównym, kliknąć ją w menu głównym, aby otworzyć okno właściwości serwera.

3. W otwartym oknie właściwości kliknij zakładkę **Serwery administracyjne**.

4. Zaznacz pole obok nazwy grupy administracyjnej, do której chcesz dodać Serwer administracyjny.

5. W wierszu menu kliknij **Połącz podrzędny Serwer administracyjny**.

   Zostanie uruchomiony Kreator dodawania podrzędnego Serwera administracyjnego. Przejdź przez kroki kreatora, korzystając z przycisku **Next**.

6. Wypełnij następujące pola:

   - **Wyświetlana nazwa podrzędnego Serwera administracyjnego**

     Nazwa, pod którą podrzędny Serwer administracyjny będzie wyświetlany w hierarchii. Jeśli chcesz, możesz wprowadzić adres IP jako nazwę lub możesz użyć nazwy, na przykład „Serwer podrzędny dla grupy 1".

   - **Adres podrzędnego Serwera administracyjnego (opcjonalnie)**

     Określ adres IP lub nazwę domeny podrzędnego Serwera administracyjnego.

     Ten parametr jest wymagany, jeśli włączona jest opcja **Połącz główny Serwer administracyjny z podrzędnym Serwerem administracyjnym w DMZ**.

   - **Port SSL Serwera administracyjnego**

     Określ numer portu SSL, który ma być używany do komunikacji między głównym a podrzędnym Serwerem administracyjnym po utworzeniu hierarchii. Domyślny numer portu to 13000.

   - **Port API Serwera administracyjnego**

     Numer portu, którego Web Console będzie używać do odbierania połączeń od podrzędnego Serwera administracyjnego za pośrednictwem OpenAPI. Domyślny numer portu to 13299.

     Podczas tworzenia hierarchii Web Console łączy się z przyszłym podrzędnym Serwerem administracyjnym, żąda poświadczeń, pobiera certyfikat publiczny i przeprowadza konfigurację początkową.

     Po utworzeniu hierarchii Serwerów administracyjnych port 13299 nie będzie już używany. Serwery administracyjne będą komunikować się przez port 13000.

   - **Połącz główny Serwer administracyjny z podrzędnym Serwerem administracyjnym w DMZ**

     Wybierz tę opcję, jeśli podrzędny Serwer administracyjny znajduje się w strefie zdemilitaryzowanej (DMZ).

     Jeżeli ta opcja jest zaznaczona, główny Serwer administracyjny inicjuje połączenie z podrzędnym Serwerem administracyjnym. W przeciwnym razie podrzędny Serwer administracyjny inicjuje połączenie z głównym Serwerem administracyjnym.

- **Użyj serwera proxy**

  Wybierz tę opcję, jeśli używasz serwera proxy do łączenia się z podrzędnym Serwerem administracyjnym.

  W tym przypadku musisz także określić następujące ustawienia serwera proxy:

  - **Adres serwera proxy**
  - **Nazwa użytkownika**
  - **Hasło**

7. Określ ustawienia połączenia:

   - Wprowadź adres przyszłego głównego Serwera administracyjnego.
   - Jeśli przyszły podrzędny Serwer administracyjny będzie korzystał z serwera proxy, wprowadź adres serwera proxy i poświadczenia użytkownika, aby połączyć się z serwerem proxy.

8. Wprowadź poświadczenia użytkownika, który ma prawa dostępu na przyszłym podrzędnym Serwerze administracyjnym.

Kreator kończy działanie, zostaje nawiązane połączenie z przyszłym podrzędnym Serwerem administracyjnym i zostaje utworzona hierarchia „główny/podrzędny".

Połączenie między głównym i podrzędnym Serwerem administracyjnym jest nawiązywane przez port 13000. Zostaną pobrane i zastosowane zadania i zasady z głównego Serwera administracyjnego. Podrzędny Serwer administracyjny jest wyświetlany na głównym Serwerze administracyjnym w grupie administracyjnej, do której został dodany.

Połączenie nie zostanie nawiązane w następujących przypadkach:

- Ustawienia połączenia są nieprawidłowe.

  Należy sprawdzić ustawienia lub ręcznie określić certyfikat przyszłego podrzędnego Serwera administracyjnego.

- Przyszły podrzędny Serwer administracyjny jest uwierzytelniany za pomocą automatycznie podpisanego certyfikatu, który został automatycznie wygenerowany przez Kaspersky Security Center Linux. W rezultacie przeglądarka może zablokować pobieranie automatycznie podpisanego certyfikatu.

  Możesz wykonać jedną z następujących czynności:

  - Dla przyszłego serwera pomocniczego utwórz certyfikat zaufany w Twojej infrastrukturze i spełniający wymagania dotyczące certyfikatów niestandardowych.
  - Dodaj automatycznie podpisany certyfikat przyszłego serwera pomocniczego do listy zaufanych certyfikatów przeglądarki. Zalecamy korzystanie z tej opcji tylko wtedy, gdy nie można utworzyć certyfikatu niestandardowego. Informacje na temat dodawania certyfikatu do listy zaufanych certyfikatów znajdziesz w dokumentacji swojej przeglądarki.

Dodawanie podrzędnego Serwera administracyjnego (wykonywane na przyszłym podrzędnym Serwerze administracyjnym)

Jeśli nie możesz połączyć się z przyszłym podrzędnym Serwerem administracyjnym (na przykład ponieważ był on tymczasowo odłączony lub niedostępny albo ponieważ plik certyfikatu podrzędnego Serwera administracyjnego jest samopodpisany), nadal możesz dodać podrzędny Serwer administracyjny.

W celu dodania podrzędnego Serwera administracyjnego, który nie jest dostępny do połączenia poprzez Kaspersky Security Center Web Console:

1. Wyślij plik certyfikatu przyszłego głównego Serwera administracyjnego do administratora systemu biura, w którym znajduje się przyszły podrzędny Serwer administracyjny (możesz, na przykład, zapisać plik na urządzeniu zewnętrznym, takim jak dysk flash, lub wysłać go przez pocztę e-mail).

   Plik certyfikatu znajduje się na przyszłym głównym serwerze administracyjnym w katalogu /var/opt/kaspersky/klnagent_srv/1093/cert/.

2. Poproś administratora systemu zarządzającego przyszłym podrzędnym Serwerem administracyjnym o wykonanie następujących czynności:

   a. Kliknij nazwę Serwera administracyjnego.

   b. W otwartym oknie właściwości przejdź do sekcji **Hierarchia Serwerów administracyjnych** zakładki **Ogólne**.

   c. Wybierz opcję **Ten Serwer administracyjny jest podrzędnym w hierarchii**.

   d. W polu **Adres głównego Serwera administracyjnego** wprowadź nazwę sieci przyszłego głównego Serwera administracyjnego.

   e. Wybierz wcześniej zapisany plik z certyfikatem przyszłego głównego Serwera administracyjnego, klikając **Przeglądaj**.

   f. Jeśli to konieczne, zaznacz pole **Połącz główny Serwer administracyjny z podrzędnym Serwerem administracyjnym w DMZ**.

   g. Jeśli połączenie z przyszłym głównym Serwerem administracyjnym odbywa się poprzez serwer proxy, wybierz opcję **Użyj serwera proxy** i określ ustawienia połączenia.

   h. Kliknij **Zapisz**.

Zostanie utworzona hierarchia „główny/podrzędny". Główny Serwer administracyjny rozpocznie odbieranie połączenia od podrzędnego Serwera administracyjnego za pośrednictwem portu 13000. Zostaną pobrane i zastosowane zadania i zasady z głównego Serwera administracyjnego. Podrzędny Serwer administracyjny jest wyświetlany na głównym Serwerze administracyjnym w grupie administracyjnej, do której został dodany.

Przeglądanie listy podrzędnych Serwerów administracyjnych

W celu przejrzenia listy podrzędnych (w tym wirtualnych) Serwerów administracyjnych:

1. W menu głównym wybierz dowolną sekcję (z wyjątkiem **Platforma handlowa**, **Poruszanie się po konsoli** i **Ustawień**).

2. U góry listy kliknij przycisk **Pokaż hierarchię**.

   W otwartym panelu nawigacyjnym wyświetlana jest lista podrzędnych (w tym wirtualnych) Serwerów administracyjnych. Możesz przejść do dowolnego z tych Serwerów administracyjnych, klikając jego nazwę.

Nie można przejść do wirtualnych Serwerów administracyjnych, jeśli panel nawigacyjny otwarto z poziomu sekcji **Zakresy IP** lub **Usunięte obiekty**.
Wyświetlane są również grupy administracyjne. Grupy są dostępne do zarządzania po otwarciu panelu nawigacyjnego z następujących sekcji: **Zasoby (urządzenia)**, **Zasady**, **Zadania** oraz **Punkty dystrybucji**. W przeciwnym razie grupy są wyszarzone.

Jeżeli jesteś połączony(-a) z głównym Serwerem administracyjnym w Kaspersky Security Center Web Console i nie możesz połączyć się z wirtualnym Serwerem administracyjnym zarządzanym przez podrzędny Serwer administracyjny, możesz skorzystać z jednego z następujących sposobów:

- **Zmodyfikuj istniejącą instalację Kaspersky Security Center Web Console, aby dodać serwer pomocniczy do listy zaufanych Serwerów administracyjnych**. Następnie będzie można połączyć się z wirtualnym Serwerem administracyjnym w Kaspersky Security Center Web Console.

  1. Na urządzeniu, na którym zainstalowana jest Kaspersky Security Center Web Console, uruchom plik instalacyjny Kaspersky Security Center Web Console odpowiadający dystrybucji Linuksa zainstalowanej na Twoim urządzeniu z poziomu konta z uprawnieniami administratora.

     Uruchomi się Kreator instalacji. Przejdź przez kroki kreatora, korzystając z przycisku **Next**.

  2. Wybierz opcję **Aktualizuj**.

  3. W kroku **Typ modyfikacji** wybierz opcję **Edycja ustawień połączenia**.

  4. W kroku **Zaufane Serwery administracyjne** dodaj wymagany podrzędny Serwer administracyjny.

  5. W ostatnim kroku kliknij opcję **Modyfikuj**, aby zastosować nowe ustawienia.

  6. Po pomyślnym zakończeniu ponownej konfiguracji aplikacji, kliknij przycisk **Zakończ**.

- Użyj Kaspersky Security Center Web Console, aby połączyć się bezpośrednio z podrzędnym serwerem administracyjnym, na którym utworzono wirtualny serwer. Następnie będzie można przełączyć się na wirtualny Serwer administracyjny w Kaspersky Security Center Web Console.

Zarządzanie wirtualnymi Serwerami administracyjnymi

W tej sekcji opisano następujące czynności zarządzania wirtualnymi Serwerami administracyjnymi:

- Utwórz wirtualne Serwery administracyjne
- Włącz i wyłącz wirtualny Serwer administracyjny
- Przypisz administratora wirtualnego Serwera administracyjnego
- Zmień Serwer administracyjny dla urządzeń klienckich
- Usuń wirtualne Serwery administracyjne

Tworzenie wirtualnego Serwera administracyjnego

Możesz utworzyć wirtualne Serwery administracyjne i dodać je do grup administracyjnych.

Podczas tworzenia wirtualnego Serwera administracyjnego dziedziczy on listę użytkowników i wszystkie uprawnienia użytkownika głównego Serwera administracyjnego. Jeśli użytkownik ma prawa dostępu do Serwera podstawowego, ten użytkownik ma również prawa dostępu do Serwera wirtualnego. Po utworzeniu samodzielnie konfigurujesz prawa dostępu do Serwerów.

W celu utworzenia i dodania wirtualnego Serwera administracyjnego:

1. W menu głównym kliknij nazwę Serwera administracyjnego.
2. W otwartym oknie przejdź na zakładkę **Serwery administracyjne**.
3. Wybierz grupę administracyjną, do której chcesz dodać wirtualny Serwer administracyjny.
   Wirtualny serwer administracyjny będzie zarządzać urządzeniami z wybranej grupy (łącznie z podgrupami).
4. W wierszu menu kliknij **Nowy wirtualny Serwer administracyjny**.
5. W otwartym oknie zdefiniuj właściwości nowego wirtualnego Serwera administracyjnego:
   - **Nazwa wirtualnego Serwera administracyjnego**.
   - **Adres połączenia z Serwerem administracyjnym**
     Możesz określić nazwę lub adres IP serwera administracyjnego.
6. Z listy użytkowników wybierz administratora wirtualnego serwera administracyjnego. Jeśli chcesz, możesz edytować jedno z istniejących kont przed przypisaniem do niego roli administratora lub utworzyć nowe konto użytkownika.

   W razie potrzeby możesz utworzyć nowe konto, które będzie pełniło rolę administratora wirtualnego Serwera administracyjnego, korzystając z narzędzia kladduser. Aby to zrobić należy użyć następującego polecenia:

   ```
   kladduser -n <nazwa_użytkownika> -p <hasło> -vs <virtual_server_name>
   ```

gdzie `virtual_server_name` jest nazwą wirtualnego Serwera administracyjnego.

7. Kliknij **Zapisz**.

Nowy wirtualny Serwer administracyjny zostanie utworzony, dodany do grupy administracyjnej i wyświetlony na zakładce **Serwery administracyjne**.

Jeżeli jesteś połączony(-a) z głównym Serwerem administracyjnym w Kaspersky Security Center Web Console i nie możesz połączyć się z wirtualnym Serwerem administracyjnym zarządzanym przez podrzędny Serwer administracyjny, możesz skorzystać z jednego z następujących sposobów:

- **Zmodyfikuj istniejącą instalację Kaspersky Security Center Web Console, aby dodać serwer pomocniczy do listy zaufanych Serwerów administracyjnych**. Następnie będzie można połączyć się z wirtualnym Serwerem administracyjnym w Kaspersky Security Center Web Console.

  1. Na urządzeniu, na którym zainstalowana jest Kaspersky Security Center Web Console, uruchom plik instalacyjny Kaspersky Security Center Web Console odpowiadający dystrybucji Linuksa zainstalowanej na Twoim urządzeniu z poziomu konta z uprawnieniami administratora.

     Uruchomi się Kreator instalacji. Przejdź przez kroki kreatora, korzystając z przycisku **Next**.

  2. Wybierz opcję **Aktualizuj**.

  3. W kroku **Typ modyfikacji** wybierz opcję **Edycja ustawień połączenia**.

  4. W kroku **Zaufane Serwery administracyjne** dodaj wymagany podrzędny Serwer administracyjny.

  5. W ostatnim kroku kliknij opcję **Modyfikuj**, aby zastosować nowe ustawienia.

  6. Po pomyślnym zakończeniu ponownej konfiguracji aplikacji, kliknij przycisk **Zakończ**.

- Użyj Kaspersky Security Center Web Console, aby połączyć się bezpośrednio z podrzędnym serwerem administracyjnym, na którym utworzono wirtualny serwer. Następnie będzie można przełączyć się na wirtualny Serwer administracyjny w Kaspersky Security Center Web Console.

Włączanie i wyłączanie wirtualnego Serwera administracyjnego

Jeśli tworzysz nowy wirtualny Serwer administracyjny, jest on domyślnie włączony. Możesz go wyłączyć lub ponownie włączyć w dowolnym momencie. Wyłączenie lub włączenie wirtualnego Serwera administracyjnego jest równoznaczne z wyłączeniem lub włączeniem fizycznego Serwera administracyjnego.

W celu włączenia lub wyłączenia wirtualnego Serwera administracyjnego:

1. W menu głównym kliknij nazwę Serwera administracyjnego.

2. W otwartym oknie przejdź na zakładkę **Serwery administracyjne**.

3. Wybierz wirtualny Serwer administracyjny, który chcesz włączyć lub wyłączyć.

4. W wierszu menu kliknij przycisk **Włącz / wyłącz wirtualny Serwer administracyjny**.

Stan wirtualnego Serwera administracyjnego jest zmieniany na włączony lub wyłączony, w zależności od jego poprzedniego stanu. Zaktualizowany stan jest wyświetlany obok nazwy Serwera administracyjnego.

Przypisywanie administratora do wirtualnego Serwera administracyjnego

Gdy używasz wirtualnych Serwerów administracyjnych w swojej organizacji, możesz chcieć przypisać dedykowanego administratora dla każdego wirtualnego Serwera administracyjnego. Na przykład, może to być przydatne podczas tworzenia wirtualnych Serwerów administracyjnych do zarządzania oddzielnymi biurami lub działami Twojej organizacji lub jeśli jesteś dostawcą MSP i zarządzasz swoimi dzierżawcami za pośrednictwem wirtualnych Serwerów administracyjnych.

Podczas tworzenia wirtualnego Serwera administracyjnego dziedziczy on listę użytkowników i wszystkie uprawnienia użytkownika głównego Serwera administracyjnego. Jeśli użytkownik ma prawa dostępu do Serwera podstawowego, ten użytkownik ma również prawa dostępu do Serwera wirtualnego. Po utworzeniu samodzielnie konfigurujesz prawa dostępu do Serwerów. Jeśli chcesz przypisać administratora tylko do wirtualnego Serwera administracyjnego, upewnij się, że administrator nie ma praw dostępu na głównym Serwerze administracyjnym.

Administratora wirtualnego Serwera administracyjnego przypisujesz poprzez nadanie praw dostępu administratora do wirtualnego Serwera administracyjnego. Możesz nadać wymagane prawa dostępu na jeden z następujących sposobów:

- Skonfiguruj ręcznie prawa dostępu administratora
- Przypisz jedną lub więcej ról użytkownika dla administratora

Aby zalogować się do Kaspersky Security Center Web Console, administrator wirtualnego Serwera administracyjnego określa nazwę wirtualnego Serwera administracyjnego, nazwę użytkownika i hasło. Kaspersky Security Center Web Console uwierzytelnia administratora i otwiera wirtualny Serwer administracyjny, do którego administrator ma prawa dostępu. Administrator nie może przełączać się między Serwerami administracyjnymi.

Wymagania wstępne

Przed rozpoczęciem upewnij się, że spełnione są następujące warunki:

- Tworzony jest wirtualny Serwer administracyjny.
- Na głównym Serwerze administracyjnym utworzono konto dla administratora, którego chcesz przypisać do wirtualnego Serwera administracyjnego.
- Masz uprawnienia **Modyfikacja list ACL obiektu** w obszarze funkcjonalnym **Funkcje ogólne** → **Uprawnienia użytkownika**.

Ręczne konfigurowanie praw dostępu

Przypisywanie administratora wirtualnego Serwera administracyjnego:

1. Przełącz się na wymagany wirtualny Serwer administracyjny:

   a. W menu głównym wybierz dowolną sekcję (z wyjątkiem **Platforma handlowa**, **Poruszanie się po konsoli** i **Ustawień**), a następnie na górze strony kliknij przycisk **Pokaż hierarchię**.

   b. W otwartym panelu nawigacyjnym kliknij nazwę wymaganego wirtualnego Serwera administracyjnego.

   > Nie można przełączyć się na wirtualny Serwer administracyjny z sekcji **Zakresy IP** i **Usunięte obiekty**.

   W menu głównym Serwer administracyjny zmienia się na wybrany.

2. Przejdź do właściwości Serwera administracyjnego, klikając jego nazwę w menu głównym.

   W panelu nawigacyjnym najedź kursorem myszy na nazwę żądanego wirtualnego Serwera administracyjnego, a następnie kliknij ikonę ustawień (⚙).

   Zostanie otwarte okno właściwości Serwera administracyjnego.

3. Na zakładce **Prawa dostępu** kliknij przycisk **Dodaj**.

   Zostanie otwarta ujednolicona lista użytkowników głównego Serwera administracyjnego i bieżącego wirtualnego Serwera administracyjnego.

4. Z listy użytkowników wybierz konto administratora, którego chcesz przypisać do wirtualnego Serwera administracyjnego, a następnie kliknij przycisk **OK**.

   Aplikacja dodaje wybranego użytkownika do listy użytkowników na zakładce **Prawa dostępu**.

5. Zaznacz pole wyboru obok dodanego konta, a następnie kliknij przycisk **Prawa dostępu**.

6. Skonfiguruj uprawnienia, jakie będzie miał administrator na wirtualnym Serwerze administracyjnym.

   W celu pomyślnego uwierzytelnienia administrator musi mieć co najmniej następujące uprawnienia:

   - **Odczyt** bezpośrednio w obszarze funkcjonalnym **Funkcje ogólne** → **Podstawowa funkcjonalność**
   - **Odczyt** bezpośrednio w obszarze funkcjonalnym **Funkcje ogólne** → **Wirtualne Serwery administracyjne**

Aplikacja zapisuje zmodyfikowane uprawnienia użytkownika na koncie administratora.

Przypisywanie administratora do wielu wirtualnych Serwerów administracyjnych:

1. W menu głównym kliknij nazwę głównego Serwera administracyjnego.

2. Na otwartej stronie przejdź na zakładkę **Prawa dostępu**, a następnie kliknij **Przypisz**.

   W otwartym oknie **Dodaj użytkowników lub grupy** zaznacz pole wyboru obok użytkownika, którego chcesz wyznaczyć na administratora.

3. Możesz przejść na zakładkę **Grupy**, aby wybrać grupy użytkowników.

4. Kliknij **Dalej**.

5. Wybierz serwery, do których chcesz przypisać administratora, a następnie kliknij **Dalej**.

6. W razie potrzeby wybierz role administratora, które chcesz przypisać użytkownikowi.

   Jeśli chcesz ustawić role niestandardowe dla użytkownika na bieżącym Serwerze administracyjnym, przejdź do właściwości wymaganego Serwera administracyjnego, kliknij **Ustaw role**, a następnie wybierz role niestandardowe.

7. Kliknij **Zakończ**, aby zastosować zmiany.

Administrator z wybranymi rolami został przypisany do wielu wirtualnych Serwerów administracyjnych.

Cofanie uprawnień dostępu administratora:

1. Przełącz się na wymagany Serwer administracyjny.

2. W menu głównym kliknij nazwę Serwera administracyjnego.

3. Na otwartej stronie przejdź do zakładki **Prawa dostępu**.

4. Zaznacz pole wyboru obok użytkownika, któremu chcesz cofnąć prawa dostępu.

5. Kliknij **Cofnij** i potwierdź działanie.

Prawa dostępu wybranego użytkownika zostały cofnięte.

Konfigurowanie praw dostępu poprzez przypisywanie ról użytkownikom

Alternatywnie możesz przyznać prawa dostępu administratorowi wirtualnego Serwera administracyjnego poprzez role użytkownika. Na przykład, może to być przydatne, jeśli chcesz przypisać kilku administratorów do tego samego wirtualnego Serwera administracyjnego. W takim przypadku można przypisać kontom administratorów identyczne role użytkownika (jedną lub więcej) zamiast konfigurować te same uprawnienia użytkownika w odniesieniu do kilku administratorów.

W celu przypisania administratora wirtualnego Serwera administracyjnego poprzez przypisanie ról użytkownika:

1. Na głównym Serwerze administracyjnym utwórz nową rolę użytkownika, a następnie określ wszystkie wymagane prawa dostępu, które musi posiadać administrator na wirtualnym Serwerze administracyjnym. Możesz utworzyć kilka ról, na przykład jeśli chcesz oddzielić dostęp do różnych obszarów funkcjonalnych.

2. Przełącz się na wymagany wirtualny Serwer administracyjny:

   a. W menu głównym wybierz dowolną sekcję (z wyjątkiem **Platforma handlowa**, **Poruszanie się po konsoli** i **Ustawień**), a następnie na górze strony kliknij przycisk **Pokaż hierarchię**.

   b. W otwartym panelu nawigacyjnym kliknij nazwę wymaganego wirtualnego Serwera administracyjnego.

   Nie można przełączyć się na wirtualny Serwer administracyjny z sekcji **Zakresy IP** i **Usunięte obiekty**.

W menu głównym Serwer administracyjny zmienia się na wybrany.

3. Przypisz nową rolę lub kilka ról do konta administratora.

Aplikacja przypisuje role do konta administratora.

Konfigurowanie praw dostępu na poziomie obiektu

Oprócz przypisywania praw dostępu na poziomie obszaru funkcjonalnego, możesz skonfigurować dostęp do określonych obiektów na wirtualnym Serwerze administracyjnym, na przykład do określonej grupy administracyjnej lub zadania. W tym celu przełącz się na wirtualny Serwer administracyjny, a następnie skonfiguruj prawa dostępu we właściwościach obiektu.

Zmienianie Serwera administracyjnego dla urządzeń klienckich

Można zmienić Serwer administracyjny zarządzający urządzeniami klienckimi na inny, używając zadania *Zmiana Serwera administracyjnego*. Po zakończeniu zadania wybrane urządzenia klienckie zostaną objęte zarządzaniem przez określony Serwer administracyjny.

Nie możesz użyć zadania *Zmiana Serwera administracyjnego* w przypadku urządzeń klienckich podłączonych do Serwera administracyjnego poprzez bramy połączeń. W przypadku takich urządzeń należy albo ponownie skonfigurować Agenta sieciowego, albo ponownie zainstalować Agenta sieciowego i określić bramę połączenia.

W celu zmiany Serwera administracyjnego zarządzającego urządzeniami klienckimi na inny Serwer:

1. W menu głównym przejdź do **Zadania**.

2. Kliknij **Dodaj**.

   Zostanie uruchomiony Kreator tworzenia nowego zadania. Przejdź przez kroki kreatora, korzystając z przycisku **Dalej**.

3. W kroku **Ustawienia nowych zadań** kreatora określ następujące ustawienia:

   a. Z listy rozwijanej **Aplikacja** wybierz **Kaspersky Security Center**.

   b. W polu **Typ zadania** wybierz opcję **Zmiana Serwera administracyjnego**.

   c. W oknie **Nazwa zadania** określ nazwę dla zadania, które tworzysz.

   Nazwa zadania nie może zawierać więcej niż 100 znaków oraz nie może zawierać żadnych znaków specjalnych ("*<>?\:|).

   d. Wybierz urządzenia, do których zadanie zostanie przypisane:

   - **Przypisz zadanie do grupy administracyjnej**

     Zadanie jest przypisywane do urządzeń znajdujących się w grupie administracyjnej. Możesz określić jedną z istniejących grup lub utworzyć nową grupę.

Na przykład, możesz chcieć użyć tej opcji do uruchomienia zadania wysyłania wiadomości do użytkowników, jeśli wiadomość jest specyficzna dla urządzeń znajdujących się w określonej grupie administracyjnej.

Jeśli zadanie jest przypisane do grupy administracyjnej, zakładka **Zabezpieczenia** nie jest wyświetlana w oknie właściwości zadania, ponieważ zadania grupowe podlegają ustawieniom zabezpieczeń grup, do których się odnoszą.

- **Określ adresy urządzeń ręcznie lub zaimportuj adresy z listy**

  Możesz określić nazwy NetBIOS, nazwy DNS, adresy IP oraz podsieci IP urządzeń, do których chcesz przydzielić zadanie.

  Możesz użyć tej opcji do wykonania zadania dla określonej podsieci. Na przykład, możesz chcieć zainstalować pewną aplikację na urządzeniach księgowych lub przeskanować urządzenia w podsieci, która jest prawdopodobnie zainfekowana.

- **Przypisz zadanie do wyboru urządzeń**

  Zadanie jest przypisywane do urządzeń znajdujących się w wyborze urządzeń. Możesz określić jeden z istniejących wyborów.

  Na przykład, możesz chcieć użyć tej opcji do uruchomienia zadania na urządzeniach z określoną wersją systemu operacyjnego.

4. W kroku **Zakres zadania** kreatora określ grupę administracyjną, urządzenia o określonych adresach lub wybór urządzeń.

5. W tym kroku kreatora potwierdź, że akceptujesz warunki zmiany Serwera administracyjnego dla urządzeń klienckich.

6. W tym kroku kreatora wybierz Serwer administracyjny, którego chcesz używać do zarządzania wybranymi urządzeniami:

   - **Zmień na inny główny Serwer administracyjny**

     Aby przenieść urządzenia klienckie na inny główny Serwer administracyjny, należy określić następujące ustawienia połączenia z Serwerem administracyjnym:

     1. W polu **Adres Serwera administracyjnego** należy podać adres nowego głównego Serwera administracyjnego.

     2. W polu **Numer portu** należy określić numer portu, za pomocą którego ma zostać nawiązane połączenie z Serwerem administracyjnym.

        Domyślny numer portu to 14000.

     3. W polu **Port SSL** określ numer portu SSL na głównym Serwerze administracyjnym.

        Domyślny numer portu to 13000.

     4. W razie potrzeby włącz opcję **Użyj serwera proxy**.

        Jeżeli ta opcja jest wyłączona, do połączenia urządzenia z Serwerem administracyjnym wykorzystywane jest połączenie bezpośrednie.

        Jeżeli ta opcja jest włączona, określ parametry serwera proxy:

        - **Adres serwera proxy**

        - **Port serwera proxy**

Jeżeli Twój serwer proxy wymaga uwierzytelnienia, w polach **Nazwa użytkownika** i **Hasło**, określ poświadczenia konta, w ramach którego nawiązywane jest połączenie z serwerem proxy. Zalecamy określenie poświadczeń konta, które ma minimalne uprawnienia wymagane tylko do uwierzytelnienia serwera proxy.

5. W razie potrzeby prześlij nowy certyfikat Serwera administracyjnego.

- **Zmień na inny wirtualny Serwer na głównym Serwerze**

  Wybierz tę opcję, aby przenieść urządzenia klienckie na wirtualny Serwer administracyjny na bieżącym głównym Serwerze administracyjnym. Aby to zrobić, z listy rozwijanej **Nazwa wirtualnego Serwera administracyjnego** wybierz żądany wirtualny Serwer administracyjny.

7. W kroku **Wybieranie konta do uruchomienia zadania** kreatora określ ustawienia konta:

- **Konto domyślne**

  Zadanie zostanie uruchomione z poziomu tego samego konta co aplikacja, która wykonuje to zadanie.

  Domyślnie opcja ta jest zaznaczona.

- **Określ konto**

  Uzupełnij pola **Konto** i **Hasło**, aby określić szczegóły konta, z poziomu którego uruchamiane jest zadanie. Konto musi posiadać wystarczające uprawnienia dla tego zadania.

  - **Konto**

    Konto, z poziomu którego zadanie jest uruchamiane.

  - **Hasło**

    Hasło do konta, z poziomu którego zadanie będzie uruchamiane.

8. Jeśli chcesz zmienić domyślne ustawienia zadania, w kroku **Zakończ tworzenie zadania** kreatora zaznacz opcję **Otwórz szczegóły zadania po jego utworzeniu**.

   Jeśli nie włączysz tej opcji, zadanie zostanie utworzone z domyślnymi ustawieniami. Możesz zmodyfikować domyślne ustawienia później w dowolnym momencie.

9. Kliknij przycisk **Zakończ**.

   Zadanie zostanie utworzone i będzie wyświetlane na liście zadań.

10. Kliknij nazwę utworzonego zadania, aby otworzyć okno właściwości zadania.

11. Jeśli chcesz zmienić domyślne ustawienia zadania, w oknie właściwości zadania określ ogólne ustawienia zadania według swoich potrzeb.

12. Kliknij przycisk **Zapisz**.

    Zadanie zostało utworzone i skonfigurowane.

13. Uruchom utworzone zadanie.

Po zakończeniu wykonywania zadania, urządzenia klienckie, dla których zostało ono utworzone, zostaną przekazane Serwerowi administracyjnemu określonemu w ustawieniach zadania.

Usuwanie wirtualnego Serwera administracyjnego

Jeśli usuniesz wirtualny Serwer administracyjny, wszystkie obiekty utworzone na Serwerze administracyjnym, w tym zasady i zadania, również zostaną usunięte. Zarządzane urządzenia z grup administracyjnych, którymi zarządzał wirtualny Serwer administracyjny, zostaną usunięte z grup administracyjnych. Aby przywrócić urządzenia zarządzane przez Kaspersky Security Center Linux, uruchom przeszukiwanie sieci, a następnie przenieś wykryte urządzenia z grupy Urządzenia nieprzypisane do grup administracyjnych.

W celu usunięcia wirtualnego Serwera administracyjnego:

1. Przejdź do głównego fizycznego Serwera administracyjnego, do którego należy wirtualny Serwer administracyjny przeznaczony do usunięcia:

   a. W menu głównym wybierz dowolną sekcję (z wyjątkiem **Platforma handlowa**, **Poruszanie się po konsoli** i **Ustawień**), a następnie na górze strony kliknij przycisk **Pokaż hierarchię**.

   b. W otwartym panelu nawigacyjnym kliknij nazwę głównego fizycznego Serwera administracyjnego.

   W menu głównym Serwer administracyjny zmienia się na wybrany.

2. Przejdź do właściwości głównego fizycznego Serwera administracyjnego w jeden z następujących sposobów:

   - W panelu nawigacyjnym najedź kursorem myszy na nazwę żądanego Serwera administracyjnego, a następnie kliknij ikonę ustawień (⚙).

   - W menu głównym kliknij nazwę Serwera administracyjnego.

3. W otwartym oknie właściwości przejdź na zakładkę **Serwery administracyjne**.

4. Wybierz wirtualny Serwer administracyjny, który chcesz usunąć.

5. W wierszu menu kliknij **Usuń**.

Wirtualny Serwer administracyjny zostanie usunięty.

Konfigurowanie rejestrowania zdarzeń połączenia serwera administracyjnego

Historia połączeń i prób nawiązania połączenia z Serwerem administracyjnym podczas jego działania może zostać zapisana w pliku raportu. Informacje w pliku umożliwiają śledzenie nie tylko połączeń w obrębie infrastruktury sieci, ale także nieautoryzowanych prób uzyskania dostępu do serwera.

W celu zapisania zdarzeń nawiązania połączenia z Serwerem administracyjnym:

1. W menu głównym kliknij nazwę Serwera administracyjnego.

   Zostanie otwarte okno właściwości Serwera administracyjnego.

2. Na zakładce **Ogólne** wybierz sekcję **Porty połączenia**.

3. Włącz opcję **Zapisuj zdarzenia połączenia z Serwerem administracyjnym**.

   Wszystkie dalsze zdarzenia przychodzących połączeń z Serwerem administracyjnym, wyniki autoryzacji i błędy SSL zostaną zapisane do pliku /var/opt/kaspersky/klnagent_srv/logs/SC.syslog.

Określanie maksymalnej liczby zdarzeń w repozytorium zdarzeń

W sekcji **Repozytorium zdarzeń** okna właściwości Serwera administracyjnego możesz zmodyfikować ustawienia przechowywania zdarzeń w bazie danych Serwera administracyjnego, ograniczając liczbę wpisów zdarzeń i czas przechowywania wpisów. Jeśli określisz maksymalną liczbę zdarzeń, aplikacja oblicza przybliżoną ilość miejsca przechowywania, wymaganą dla określonej liczby. Możesz użyć tego przybliżonego obliczenia do oszacowania wystarczającej ilości wolnego miejsca na dysku, aby uniknąć przepełnienia bazy danych. Domyślna pojemność bazy danych Serwera administracyjnego wynosi 400 000 zdarzeń. Maksymalną dozwoloną pojemnością bazy danych jest 45 milionów zdarzeń.

Aplikacja sprawdza bazę danych co 10 minut. Jeśli liczba zdarzeń osiągnie określoną maksymalną wartość plus 10 000, aplikacja usunie najstarsze zdarzenia, tak aby pozostała tylko określona maksymalna liczba zdarzeń.

Jeśli Serwer administracyjny usuwa starsze zdarzenia, nie może zapisywać nowych zdarzeń do bazy danych. W tym czasie informacje o odrzuconych zdarzeniach są zapisywane w dzienniku systemu operacyjnego. Nowe zdarzenia zostają zakolejkowane, a następnie zapisane do bazy danych po zakończeniu operacji usuwania. Domyślnie kolejka zdarzeń jest ograniczona do 20 000 zdarzeń. Możesz dostosować limit kolejki, edytując wartość flagi KLEVP_MAX_POSTPONED_CNT.

Aby ograniczyć liczbę zdarzeń, które mogą być przechowywane w repozytorium zdarzeń na Serwerze administracyjnym:

1. W menu głównym kliknij nazwę Serwera administracyjnego.

   Zostanie otwarte okno właściwości Serwera administracyjnego.

2. Na zakładce **Ogólne** wybierz sekcję **Repozytorium zdarzeń**. Określ maksymalną liczbę zdarzeń przechowywanych w bazie danych.

3. Kliknij przycisk **Zapisz**.

Dodatkowo możesz wykonać następujące czynności:

- Zmienić ustawienia dowolnego zadania, aby zapisywać zdarzenia związane z postępem zadania lub zapisywać tylko wyniki wykonania zadania.

- Skrócić lub wyłączyć okres przechowywania zdarzeń Serwera administracyjnego, Agenta sieciowego i aplikacji Kaspersky zainstalowanych na zarządzanych urządzeniach.

Postępując w ten sposób, zmniejszysz liczbę zdarzeń w bazie danych, zwiększysz prędkość wykonywania scenariuszy skojarzonych z analizą tabeli zdarzeń w bazie danych, a także zmniejszysz ryzyko nadpisania krytycznych zdarzeń przez dużą liczbę zdarzeń.

Przenoszenie Serwera administracyjnego na inne urządzenie

Jeśli chcesz użyć Serwera administracyjnego na nowym urządzeniu, możesz je przenieść w jeden z następujących sposobów:

- Przenieś Serwer administracyjny i serwer bazy danych na nowe urządzenie (serwer bazy danych może być zainstalowany na nowym urządzeniu wraz Serwerem administracyjnym, lub na innym urządzeniu).
- Zachowaj serwer bazy danych na poprzednim urządzeniu i przenieś tylko Serwer administracyjny na nowe urządzenie.

W celu przeniesienia Serwera administracyjnego i serwera bazy danych na nowe urządzenie:

1. Na poprzednim urządzeniu utwórz kopię zapasową danych Serwera administracyjnego.

   W tym celu możesz uruchomić zadanie tworzenia kopii zapasowej danych poprzez Kaspersky Security Center Web Console lub uruchomić narzędzie klbackup.

2. Na poprzednim urządzeniu odłącz Serwer administracyjny od sieci.

3. Wybierz nowe urządzenie, na którym chcesz zainstalować Serwer administracyjny. Upewnij się, że sprzęt i oprogramowanie na wybranym urządzeniu spełniają wymagania Serwera administracyjnego, Kaspersky Security Center Web Console oraz Agenta sieciowego. Sprawdź również, czy dostępne są porty używane na Serwerze administracyjnym.

4. Przypisz ten sam adres do nowego urządzenia.

   Nowy Serwer administracyjny może mieć przypisaną nazwę NetBIOS, FQDN i statyczny adres IP. Zależy to od tego, który adres Serwera administracyjnego został ustawiony w pakiecie instalacyjnym Agenta sieciowe w momencie instalacji Agenta sieciowego. Alternatywnie można użyć adresu połączenia, który określa Serwer administracyjny, z którym łączy się Agent sieciowy (możesz uzyskać ten adres na zarządzanych urządzeniach korzystając z narzędzia klnagchk).

5. W razie konieczności, na innym urządzeniu, zainstaluj system zarządzania bazą danych (DBMS), którego będzie używał Serwer administracyjny.

   Bazę danych można zainstalować na nowym urządzeniu razem z Serwerem administracyjnym lub na innym urządzeniu. Upewnij się, że urządzenia spełnia wymagania sprzętowe i programowe. Kiedy wybierasz DBMS, weź pod uwagę liczbę urządzeń obsługiwanych przez Serwer administracyjny.

6. Zainstaluj Serwer administracyjny na wybranym urządzeniu.

   Zwróć uwagę, że jeśli przenosisz serwer bazy danych na inne urządzenie, należy określić adres lokalny jako adres IP urządzenia, na którym zainstalowana jest baza danych (element „h" w instrukcji Instalowanie Kaspersky Security Center Linux). Jeśli chcesz zachować serwer bazy danych na poprzednim urządzeniu, wprowadź adres IP poprzedniego urządzenia w pozycji „h" instrukcji Instalowanie Kaspersky Security Center Linux.

7. Po zakończeniu instalacji odzyskaj dane Serwera administracyjnego na nowym urządzeniu za pomocą narzędzia klbackup.

8. Otwórz Kaspersky Security Center Web Console i połącz się z Serwerem administracyjnym.

9. Sprawdź, czy wszystkie zarządzane urządzenia są podłączone do Serwera administracyjnego.

10. Odinstaluj Serwer administracyjny i serwer bazy danych z poprzedniego urządzenia.

Zmiana nazwy Serwera administracyjnego

Czynności wymagane do zmiany nazwy serwera mogą się różnić w zależności od środowiska. Możesz wybrać jeden z następujących scenariuszy zmiany nazwy serwera:

- Zachowanie połączeń przez dodanie nowego rekordu DNS.
- Zachowanie połączeń przez przejście na łączność opartą na adresie IP.
- Przywrócenie przerwanych połączeń po zmianie nazwy serwera.

Jeśli masz trudności ze zmianą nazwy serwera, skontaktuj się z Pomocą techniczną.

Zachowanie połączeń przez dodanie nowego rekordu DNS

W tym scenariuszu zarządzane urządzenia oraz Kaspersky Security Center Web Console nadal łączą się ze starym adresem Serwera administracyjnego po zmianie nazwy Serwera administracyjnego. Aby to skonfigurować, dodaj jeden z następujących typów rekordów DNS:

- Rekord A dla starego adresu Serwera administracyjnego wskazujący nowy adres IP Serwera administracyjnego.
- Rekord CNAME mapujący starą nazwę Serwera administracyjnego na nową nazwę Serwera administracyjnego.

  Więcej informacji o konfigurowaniu wymaganych rekordów można znaleźć w dokumentacji Serwera DNS.

Aby zachować połączenia przez dodanie nowego rekordu DNS:

1. **Zmień nazwę serwera**.

   Ze względu na sposób konfigurowania komponentów podczas instalacji nie można zmienić nazwy Serwera administracyjnego bez ponownej instalacji Serwera administracyjnego.

   Aby zmienić nazwę serwera:

   1. Utwórz nową kopię zapasową Serwera administracyjnego za pomocą narzędzia klbackup.
   2. Odinstaluj Kaspersky Security Center Linux i Kaspersky Security Center Web Console na wszystkich stacjach roboczych administratorów.
   3. Ręcznie usuń bazę danych Serwera administracyjnego oraz bazę danych IAM. Serwer administracyjny nie usuwa ich automatycznie podczas dezinstalacji.
   4. Zmień nazwę urządzenia w systemie operacyjnym Serwera administracyjnego zgodnie z dokumentacją używanego systemu operacyjnego.
   5. Zainstaluj Serwer administracyjny Kaspersky Security Center Linux, używając nowej nazwy FQDN Serwera administracyjnego.

6. Przywróć wcześniej przygotowaną kopię zapasową Serwera administracyjnego po instalacji.

7. Sprawdź konfigurację serwera IAM i w razie potrzeby dodaj adres Serwera administracyjnego do pliku konfiguracyjnego serwera IAM.

8. Zainstaluj Web Console na wszystkich stacjach roboczych administratorów, podając nową nazwę FQDN Serwera administracyjnego w pliku odpowiedzi.

2. Dodaj nowy rekord DNS dla starego adresu Serwera administracyjnego.

3. Określ nowy adres w ustawieniach Serwera administracyjnego w Kaspersky Security Center Web Console.

4. Uruchom zadanie **Zmiana Serwera administracyjnego** na urządzeniach mających bezpośrednią widoczność Serwera administracyjnego. Następnie zarządzane urządzenia będą mogły łączyć się z Serwerem administracyjnym przy użyciu nowej nazwy.

   Nie uruchamiaj zadania na urządzeniach bez bezpośredniej widoczności Serwera administracyjnego, w przeciwnym razie utracą one połączenie z Serwerem administracyjnym i bramami połączeń.

   Zarządzane urządzenia połączone przez bramy połączeń nie sprawdzają nazwy Serwera administracyjnego. W związku z tym nie są w ich przypadku wymagane żadne dodatkowe działania. Informacje o adresie Serwera administracyjnego nie zostaną zaktualizowane w danych wyjściowych polecenia diagnostycznego klnagchk.

Połączenie z Serwerem administracyjnym zostaje zachowane po zmianie nazwy Serwera administracyjnego.

Po zmianie nazwy Serwera administracyjnego informacje o certyfikacie staną się nieaktualne. Ponieważ nie ma to wpływu na działanie komponentów, nie zalecamy wymiany certyfikatów z podpisem własnym poza harmonogramem. Te certyfikaty są generowane podczas instalacji Kaspersky Security Center i automatycznie odnawiane przez serwer. Zostaną one ponownie wystawione z nową nazwą Serwera administracyjnego podczas następnej automatycznej wymiany certyfikatu.

Podczas ponownej instalacji zostaną wydane nowe certyfikaty dla serwera IAM i serwera Web Console Server. W razie potrzeby zastąp je niestandardowymi certyfikatami wydanymi przez Twój urząd certyfikacji dla nowej nazwy Serwera administracyjnego. Szczegółowe informacje zawiera następujący artykuł: Informacje o certyfikatach Kaspersky Security Center Linux.

Zachowanie połączeń przez przełączenie na łączność opartą na adresie IP

W tym scenariuszu zmienia się sposób łączenia zarządzanych urządzeń z Serwerem administracyjnym. Urządzenia łączą się przy użyciu adresu IP Serwera administracyjnego zamiast nazwy Serwera administracyjnego. Przełączenie wszystkich zarządzanych urządzeń może zająć trochę czasu w zależności od liczby urządzeń oraz częstotliwości, z jaką pojawiają się one w sieci z Serwerem administracyjnym.

Aby zachować połączenia przez przełączenie na łączność opartą na adresach IP:

1. **Przygotuj infrastrukturę Kaspersky Security Center przed zmianą nazwy Serwera administracyjnego**.

   1. Połącz zarządzane urządzenia z Serwerem administracyjnym przy użyciu adresu IP. Po zmianie nazwy Serwera administracyjnego urządzenia, które używają jego nazwy do nawiązywania połączenia, zostaną odłączone od Serwera. Aby nawiązać połączenie za pośrednictwem adresu IP, uruchom zadanie Zmień Serwer administracyjny na urządzeniach mających bezpośrednią widoczność Serwera administracyjnego, w tym na urządzeniach działających jako bramy połączeń.

      > Nie uruchamiaj zadania na urządzeniach bez bezpośredniej widoczności Serwera administracyjnego, w przeciwnym razie utracą one połączenie z Serwerem administracyjnym i bramami połączeń.

      Zarządzane urządzenia połączone przez bramy połączeń nie sprawdzają nazwy Serwera administracyjnego. Dlatego w ich przypadku nie są wymagane żadne dodatkowe działania. Informacje o adresie Serwera administracyjnego nie zostaną zaktualizowane w danych wyjściowych polecenia diagnostycznego klnagchk.

   2. Upewnij się, że wszystkie zarządzane urządzenia są połączone z Serwerem administracyjnym za pośrednictwem adresu IP. W tym celu sprawdź następujące elementy:

      - Wyniki polecenia diagnostycznego klnagchk w wierszu adresu Serwera administracyjnego na zarządzanych urządzeniach z bezpośrednią widocznością Serwera administracyjnego.

      - Informacje o właściwościach pakietu instalacyjnego Agenta sieciowego w momencie instalacji na urządzeniach.

        Agenta sieciowego należy początkowo skonfigurować tak, aby łączył się z Serwerem administracyjnym przy użyciu adresu IP.

        > Jeśli zainstalujesz Agenta sieciowego na istniejącej instalacji bez jej wcześniejszego odinstalowania, adres połączenia z Serwerem administracyjnym i certyfikat określone w konfiguracji Agenta sieciowego nie zostaną zaktualizowane.

   3. Określ nową nazwę w istniejących profilach połączeń Serwera administracyjnego.

   4. Jeśli używasz roli Zarządzanie urządzeniami mobilnymi (zarządzanie urządzeniami z systemem Android i iOS), postępuj zgodnie z instrukcjami Jak zmienić adres Serwera administracyjnego na urządzeniach mobilnych, które używają Kaspersky Endpoint Security for Android z rolą MDM lub KSMM.

2. **Zmień nazwę serwera**.

   Ze względu na sposób konfigurowania komponentów podczas instalacji nie można zmienić nazwy Serwera administracyjnego bez ponownej instalacji Serwera administracyjnego.

   Aby zmienić nazwę serwera:

   1. Utwórz nową kopię zapasową Serwera administracyjnego za pomocą narzędzia klbackup.

   2. Odinstaluj Kaspersky Security Center Linux i Kaspersky Security Center Web Console na wszystkich stacjach roboczych administratorów.

   3. Ręcznie usuń bazę danych Serwera administracyjnego oraz bazę danych IAM. Serwer administracyjny nie usuwa ich automatycznie podczas dezinstalacji.

4. Zmień nazwę urządzenia w systemie operacyjnym Serwera administracyjnego zgodnie z dokumentacją używanego systemu operacyjnego.

5. Zainstaluj Serwer administracyjny Kaspersky Security Center Linux, używając nowej nazwy FQDN Serwera administracyjnego.

6. Przywróć wcześniej przygotowaną kopię zapasową Serwera administracyjnego po instalacji.

7. Sprawdź konfigurację serwera IAM i w razie potrzeby dodaj adres Serwera administracyjnego do pliku konfiguracyjnego serwera IAM.

8. Zainstaluj Web Console na wszystkich stacjach roboczych administratorów, podając nową nazwę FQDN Serwera administracyjnego w pliku odpowiedzi.

3. **Zaktualizuj adres Serwera administracyjnego w ustawieniach Serwera administracyjnego**.

   Po zmianie nazwy Serwera administracyjnego określ nowy adres FQDN w ustawieniach Serwera administracyjnego w Kaspersky Security Center Web Console. W tym celu sprawdź i zaktualizuj adres FQDN w każdym z następujących ustawień:

   - Adres serwera proxy Kaspersky Security Network
   - Serwer sieciowy
   - Właściwości pakietów instalacyjnych Agenta sieciowego
   - Nazwa wystawcy kodu zabezpieczającego (2FA)

   Ponadto wykonaj następujące czynności:

   - Określ nową nazwę serwera w zasadach i ustawieniach innych aplikacji Kaspersky.
   - Opublikuj ponownie każdy opublikowany pakiet autonomiczny i pakiet urządzenia mobilnego.
   - Ponownie połącz podrzędne Serwery administracyjne, jeśli używasz hierarchii Serwerów administracyjnych i jeśli serwery są połączone według nazwy, a nie według adresu IP.

4. Uruchom zadanie **Zmiana Serwera administracyjnego** na urządzeniach, z których Serwer administracyjny jest bezpośrednio widoczny, aby zmienić adres połączenia na zarządzanych urządzeniach na nową nazwę Serwera administracyjnego.

   Połączenie z Serwerem administracyjnym zostaje zachowane po zmianie nazwy Serwera administracyjnego.

Po zmianie nazwy Serwera administracyjnego informacje o certyfikacie staną się nieaktualne. Ponieważ nie ma to wpływu na działanie komponentów, nie zalecamy wymiany certyfikatów z podpisem własnym poza harmonogramem. Te certyfikaty są generowane podczas instalacji Kaspersky Security Center i automatycznie odnawiane przez serwer. Zostaną one ponownie wystawione z nową nazwą Serwera administracyjnego podczas następnej automatycznej wymiany certyfikatu.

Podczas ponownej instalacji zostaną wydane nowe certyfikaty dla serwera IAM i serwera Web Console Server. W razie potrzeby zastąp je niestandardowymi certyfikatami wydanymi przez Twój urząd certyfikacji dla nowej nazwy Serwera administracyjnego. Szczegółowe informacje zawiera następujący artykuł: Informacje o certyfikatach Kaspersky Security Center Linux.

Przywracanie przerwanych połączeń po zmianie nazwy serwera

Scenariusz ten ma zastosowanie w następujących przypadkach:

- Jeśli utracono własność nazwy domenowej urządzenia Serwera administracyjnego, ale dostęp do Serwera administracyjnego nadal jest możliwy.
- Jeśli Serwer administracyjny nie zarządza już zarządzanymi urządzeniami.
- Jeśli dodanie rekordów DNS dla starego adresu Kaspersky Security Center Linux nie jest możliwe z innych przyczyn.

Aby przywrócić przerwane połączenia po zmianie nazwy serwera:

1. **Zmień nazwę serwera**.

   Ze względu na sposób konfigurowania komponentów podczas instalacji nie można zmienić nazwy Serwera administracyjnego bez ponownej instalacji Serwera administracyjnego.

   Aby zmienić nazwę serwera:

   1. Utwórz nową kopię zapasową Serwera administracyjnego za pomocą narzędzia klbackup.
   2. Odinstaluj Kaspersky Security Center Linux i Kaspersky Security Center Web Console na wszystkich stacjach roboczych administratorów.
   3. Ręcznie usuń bazę danych Serwera administracyjnego oraz bazę danych IAM. Serwer administracyjny nie usuwa ich automatycznie podczas dezinstalacji.
   4. Zmień nazwę urządzenia w systemie operacyjnym Serwera administracyjnego zgodnie z dokumentacją używanego systemu operacyjnego.
   5. Zainstaluj Serwer administracyjny Kaspersky Security Center Linux, używając nowej nazwy FQDN Serwera administracyjnego.
   6. Przywróć wcześniej przygotowaną kopię zapasową Serwera administracyjnego po instalacji.
   7. Sprawdź konfigurację serwera IAM i w razie potrzeby dodaj adres Serwera administracyjnego do pliku konfiguracyjnego serwera IAM.
   8. Zainstaluj Web Console na wszystkich stacjach roboczych administratorów, podając nową nazwę FQDN Serwera administracyjnego w pliku odpowiedzi.

2. **Zaktualizuj adres Serwera administracyjnego w ustawieniach Serwera administracyjnego**.

   Po zmianie nazwy Serwera administracyjnego określ nowy adres FQDN w ustawieniach Serwera administracyjnego w Kaspersky Security Center Web Console. W tym celu sprawdź i zaktualizuj adres FQDN w każdym z następujących ustawień:

   - Adres serwera proxy Kaspersky Security Network
   - Serwer sieciowy

- Właściwości pakietów instalacyjnych Agenta sieciowego
- Nazwa wystawcy kodu zabezpieczającego (2FA)

Ponadto wykonaj następujące czynności:

- Określ nową nazwę serwera w zasadach i ustawieniach innych aplikacji Kaspersky.
- Opublikuj ponownie każdy opublikowany pakiet autonomiczny i pakiet urządzenia mobilnego.
- Ponownie połącz podrzędne Serwery administracyjne, jeśli używasz hierarchii Serwerów administracyjnych i jeśli serwery są połączone według nazwy, a nie według adresu IP.

3. Przywróć połączenie z Serwerem administracyjnym na wcześniej zarządzanych urządzeniach:

   - Na urządzeniach mających bezpośrednią widoczność Serwera administracyjnego użyj narzędzia klmover, aby określić adres połączenia z nową nazwą Serwera administracyjnego. Szczegółowe informacje znajdziesz w następującym artykule: Łączenie Agentów sieciowych z Serwerem administracyjnym za pomocą narzędzia klmover.
   - Na urządzeniach działających jako bramy połączeń ponownie zainstaluj Agenta sieciowego i ponownie skonfiguruj rolę bramy połączeń. Szczegółowe informacje można znaleźć w następującym artykule: Dodawanie bramy połączeń w strefie DMZ jako punktu dystrybucji.
   - Urządzenia podłączone za pośrednictwem bram połączeń automatycznie połączą się ponownie po przywróceniu bram połączeń. Agent sieciowy nie używa nazwy Serwera administracyjnego podczas łączenia się z bramami połączeń.

     Nie używaj narzędzia klmover na urządzeniach połączonych za pośrednictwem bram połączeń. Szczegółowe informacje znajdziesz w następującym artykule: Przenoszenie urządzeń połączonych z Serwerem administracyjnym za pośrednictwem bram połączeń do innego Serwera administracyjnego.

Po zmianie nazwy serwera połączenie z Serwerem administracyjnym zostanie przywrócone.

Po zmianie nazwy Serwera administracyjnego informacje o certyfikacie staną się nieaktualne. Ponieważ nie ma to wpływu na działanie komponentów, nie zalecamy wymiany certyfikatów z podpisem własnym poza harmonogramem. Te certyfikaty są generowane podczas instalacji Kaspersky Security Center i automatycznie odnawiane przez serwer. Zostaną one ponownie wystawione z nową nazwą Serwera administracyjnego podczas następnej automatycznej wymiany certyfikatu.

Podczas ponownej instalacji zostaną wydane nowe certyfikaty dla serwera IAM i serwera Web Console Server. W razie potrzeby zastąp je niestandardowymi certyfikatami wydanymi przez Twój urząd certyfikacji dla nowej nazwy Serwera administracyjnego. Szczegółowe informacje zawiera następujący artykuł: Informacje o certyfikatach Kaspersky Security Center Linux.

Zmiana poświadczeń DBMS

Czasami może zajść potrzeba zmiany poświadczeń DBMS, na przykład w celu wykonania rotacji poświadczeń ze względów bezpieczeństwa.

Zmiana poświadczeń bazy danych Serwera administracyjnego

Aby zmienić poświadczenia baz danych Serwera administracyjnego i IAM w środowisku Linux:

1. Zatrzymaj Serwer administracyjny. W zależności od typu wdrożenia Kaspersky Security Center Linux uruchom jedno z następujących poleceń z poziomu konta root:

   - W przypadku klastra pracy awaryjnej Kaspersky Security Center Linux:

     Na aktywnym węźle uruchom następujące polecenie:

     ```
     /opt/kaspersky/ksc64/sbin/klfoc -stopcluster --stp klfoc
     ```

   - W przypadku rozproszonego geograficznie klastra pracy awaryjnej Kaspersky Security Center Linux:

     Na obu węzłach uruchom następujące polecenie:

     ```
     crm node standby
     ```

   - W przypadku wdrożenia Serwera administracyjnego poza klastrem:

     Uruchom następujące polecenia:

     ```
     systemctl stop kladminserver_srv.service
     systemctl stop kliam_srv.service
     ```

2. Połącz się z bazą danych Serwera administracyjnego z uprawnieniami superużytkownika systemu DBMS i uruchom następujące polecenie:

   ```
   REASSIGN OWNED BY <old_kscdbadmin> TO <new_kscdbadmin>;
   ```

   gdzie `<old_kscdbadmin>` to poprzednie konto systemu DBMS używane przez Serwer administracyjny do łączenia się z jego bazą danych, a `<new_kscdbadmin>` to nowe konto systemu DBMS.

3. Połącz się z bazą danych IAM z uprawnieniami superużytkownika systemu DBMS i uruchom następujące polecenie:

   ```
   REASSIGN OWNED BY <old_iamdbadmin> TO <new_iamdbadmin>;
   ```

   gdzie `<old_iamdbadmin>` to poprzednie konto systemu DBMS używane przez Serwer administracyjny do łączenia się z jego bazą danych, a `<new_iamdbadmin>` to nowe konto systemu DBMS.

4. Zlokalizuj plik konfiguracyjny IAM: /var/opt/kaspersky/klnagent_srv/iam/iam_config.yaml

5. W sekcji `dbms_iam`, w polach użytkownika i hasła podaj nowe poświadczenia do konta. Upewnij się, że konto istnieje w systemie DBMS i jest wskazane jako właściciel bazy danych IAM.

6. Uruchom Serwer administracyjny. W zależności od typu wdrożenia Kaspersky Security Center Linux uruchom jedno z następujących poleceń przy użyciu konta root:

   - W przypadku klastra pracy awaryjnej Kaspersky Security Center Linux:

     Na aktywnym węźle uruchom następujące polecenie:

     ```
     /opt/kaspersky/ksc64/sbin/klfoc -startcluster --stp klfoc
     ```

   - W przypadku rozproszonego geograficznie klastra pracy awaryjnej Kaspersky Security Center Linux:

     Na obu węzłach uruchom następujące polecenie:

     ```
     crm node online
     ```

   - W przypadku wdrożenia Serwera administracyjnego poza klastrem:

     Uruchom następujące polecenia:

     ```
     systemctl start kladminserver_srv.service
     systemctl start kliam_srv.service
     ```

7. Uruchom narzędzie klsrvconfig:

   ```
   sudo /opt/kaspersky/ksc64/sbin/klsrvconfig -set_dbms_cred
   ```

8. Podaj nową nazwę konta. Powinieneś określić poświadczenia konta, które istnieje w DBMS.

9. Wpisz nowe hasło.

10. Podaj nowe hasło w celu potwierdzenia.

11. Poczekaj, aż Serwer administracyjny wznowi działanie, a na aktywnym węźle pojawi się wpis w dzienniku syslog informujący, że Serwer administracyjny jest gotowy do wykonywania operacji w interfejsie graficznym.

Zmieniono poświadczenia bazy danych Serwera administracyjnego.

Tworzenie kopii zapasowej i przywracanie danych Serwera administracyjnego

Tworzenie kopii zapasowej danych umożliwia przeniesienie Serwera administracyjnego z jednego urządzenia na inne, bez utraty danych. Dzięki kopii zapasowej możesz przywrócić dane podczas przenoszenia bazy danych Serwera administracyjnego na inne urządzenie lub podczas aktualizacji do nowej wersji Kaspersky Security Center. Możesz również wykorzystać kopię zapasową danych do przeniesienia danych Serwera administracyjnego z Kaspersky Security Center Windows pod zarządzanie Kaspersky Security Center Linux (przenoszenie danych z Kaspersky Security Center Linux do Kaspersky Security Center Windows nie jest obsługiwane).

Nie są tworzone kopie zapasowe zainstalowanych wtyczek zarządzających. Po przywróceniu danych Serwera administracyjnego z kopii zapasowej należy pobrać i ponownie zainstalować wtyczki dla zarządzanych aplikacji.

Przed utworzeniem kopii zapasowej danych Serwera administracyjnego wykonaj następujące czynności:

- **Postępuj zgodnie z wymaganiami dotyczącymi tworzenia kopii zapasowej na Serwerze administracyjnym w wersji 16 lub starszej i przywracania jej na Serwerze administracyjnym w wersji 16.1 lub nowszej**

  - Jeśli utworzysz kopię zapasową danych na Serwerze administracyjnym w wersji 16 lub starszej i przywrócisz ją na Serwerze administracyjnym w wersji 16.1 lub nowszej, uwierzytelnianie dwuskładnikowe jest włączone. Aby uzyskać więcej informacji, zapoznaj się z artykułem Informacje o uwierzytelnianiu dwuskładnikowym dla konta.

    Aby mieć pewność, że użytkownicy będą mogli logować się do Web Console przy użyciu swoich istniejących kont, używając skonfigurowanych kluczy tajnych uwierzytelniania dwuskładnikowego, a skrypty automatyzacji OpenAPI będą nadal działać po przywróceniu, należy wykonać następujące kroki:

    - Włączanie uwierzytelniania dwuskładnikowego dla wszystkich użytkowników
    - Administratorzy muszą skonfigurować uwierzytelnianie dwuskładnikowe dla swoich kont
    - Wykluczanie kont z uwierzytelniania dwuskładnikowego

      W razie potrzeby dodaj konta integracji używane do uruchamiania skryptów za pośrednictwem OpenAPI do listy wykluczeń.

    Jeśli nie jest możliwe skonfigurowanie uwierzytelniania dwuskładnikowego przed utworzeniem kopii zapasowej, konta użytkowników zostaną dodane do listy dozwolonych uwierzytelniania dwuskładnikowego i będą mogły skonfigurować uwierzytelnianie dwuskładnikowe podczas logowania do Web Console. Bardziej szczegółowe warunki dodawania konta do listy dozwolonych opisano w temacie Zezwalanie użytkownikom na konfigurowanie uwierzytelniania dwuskładnikowego.

- Sprawdź, czy wirtualny Serwer administracyjny jest dodany do grupy administracyjnej. Jeśli dodany jest wirtualny Serwer administracyjny, przed utworzeniem kopii zapasowej upewnij się, że do tego wirtualnego Serwera administracyjnego został przypisany administrator. Po utworzeniu kopii zapasowej nie możesz nadać administratorowi praw dostępu do wirtualnego Serwera administracyjnego. Należy pamiętać, że w przypadku utraty poświadczeń konta administratora nie będzie można przypisać nowego administratora do wirtualnego Serwera administratora.

- Aby utworzyć kopię zapasową lub przywrócić klaster pracy awaryjnej Kaspersky Security Center Linux, należy zatrzymać cały klaster w celu przeprowadzenia konserwacji, a następnie ponownie go uruchomić po zakończeniu tworzenia kopii zapasowej lub przywracania.

Możesz utworzyć kopię zapasową danych Serwera administracyjnego w jeden z następujących sposobów:

- Tworząc i uruchamiając zadanie tworzenia kopii zapasowej danych za pomocą Kaspersky Security Center Web Console.

- Uruchamiając narzędzie klbackup na urządzeniu, na którym jest zainstalowany Serwer administracyjny. To narzędzie znajduje się w pakiecie dystrybucyjnym Kaspersky Security Center. Po zainstalowaniu Serwera administracyjnego, narzędzie jest umieszczane w katalogu głównym folderu docelowego, określonego podczas instalacji aplikacji (zazwyczaj /opt/kaspersky/ksc64/sbin/klbackup).

W kopii zapasowej Serwera administracyjnego zapisywane są następujące dane:

- Baza danych Serwera administracyjnego (zasady, zadania, ustawienia aplikacji, zdarzenia zapisane na Serwerze administracyjnym).

- Informacje o konfiguracji struktury grup administracyjnych i urządzeń klienckich.

- Repozytorium pakietów dystrybucyjnych aplikacji przeznaczonych do zdalnego zainstalowania.

- Certyfikat Serwera administracyjnego.
- Klucze tajne uwierzytelniania dwuskładnikowego skonfigurowane dla kont użytkowników.
- Lista kont użytkowników wykluczonych z uwierzytelniania dwuskładnikowego.

Możesz utworzyć kopię zapasową danych Serwera administracyjnego tworząc i uruchamiając zadanie tworzenia kopii zapasowej danych lub korzystając z narzędzia klbackup. Odzyskanie danych Serwera administracyjnego jest możliwe tylko przy użyciu narzędzia klbackup. Należy wykonać przywracanie kopii zapasowej na działającej instancji Serwera administracyjnego, który został właśnie zainstalowany i posiada tę samą wersję (lub nowszą), dla której kopia zapasowa została utworzona. Nie używaj żadnych narzędzi innych firm do tworzenia kopii zapasowych lub przywracania, a jeśli to możliwe, nie usuwaj poprzedniej instalacji Kaspersky Security Center Linux, dopóki konfiguracja i przesyłanie danych nie zostaną w pełni zakończone.

Tworzenie zadania kopii zapasowej danych Serwera administracyjnego

Zadania kopii zapasowej są zadaniami Serwera administracyjnego i są tworzone podczas działania kreatora wstępnej konfiguracji. Jeśli zadanie kopii zapasowej utworzone przez Kreator wstępnej konfiguracji zostało usunięte, możesz je utworzyć ręcznie.

Zadanie *Kopia zapasowa danych Serwera administracyjnego* może zostać utworzone tylko w jednej kopii. Jeśli dla Serwera administracyjnego już utworzono zadanie tworzenia kopii zapasowych danych Serwera administracyjnego, nie będzie wyświetlane w oknie wyboru.

W celu utworzenia zadania kopii zapasowej danych Serwera administracyjnego:

1. W menu głównym przejdź do **Zadania**.
2. Kliknij **Dodaj**.

   Zostanie uruchomiony Kreator tworzenia nowego zadania. Przejdź przez kroki kreatora, korzystając z przycisku **Next**.
3. Na liście **Aplikacja** wybierz **Kaspersky Security Center 16.3**, a na liście **Typ zadania** wybierz **Kopia zapasowa danych Serwera administracyjnego**.
4. W odpowiednim kroku podaj następujące informacje:
   - Folder do przechowywania kopii zapasowych
   - Hasło do kopii zapasowej (opcjonalnie)
   - Maksymalna liczba kopii zapasowych do zapisania

5. Jeśli w kroku **Zakończ tworzenie zadania** włączysz opcję **Otwórz szczegóły zadania po jego utworzeniu**, możesz zmodyfikować domyślne ustawienia zadania. Jeśli nie włączysz tej opcji, zadanie zostanie utworzone z domyślnymi ustawieniami. Możesz zmodyfikować domyślne ustawienia później w dowolnym momencie.

6. Kliknij przycisk **Zakończ**.

Zadanie zostanie utworzone i będzie wyświetlane na liście zadań.

Używanie narzędzia klbackup do tworzenia kopii zapasowych i odzyskiwania danych

Możesz utworzyć kopie danych Serwera administracyjnego w celu przechowywania kopii zapasowych oraz przyszłego ich odzyskania przy użyciu narzędzia klbackup stanowiącego część pakietu dystrybucyjnego Kaspersky Security Center.

Instancja Serwera administracyjnego, na którym kopia zapasowa ma zostać przywrócona, musi korzystać z systemu DBMS tego samego typu. Wersja Serwera administracyjnego może być taka sama (z tą samą lub późniejszą łatą) lub nowsza.

Jeśli kopia zapasowa danych Serwera administracyjnego zawartego w Kaspersky Security Center Linux 15 lub wcześniejszej wersji została utworzona przy użyciu MariaDB DBMS wcześniejszej wersji, a następnie odzyskasz dane na urządzeniu z nowszą wersją MariaDB, może wystąpić błąd. Aby uzyskać więcej informacji, przejdź do Jak przywrócić dane Serwera administracyjnego z kopii zapasowej utworzonej we wcześniejszej wersji DBMS.

Flagi Agenta sieciowego nie są przywracane podczas korzystania z narzędzia klbackup. Należy ręcznie skonfigurować flagi Agenta sieciowego.

W celu utworzenia kopii zapasowej lub odzyskania danych Serwera administracyjnego w trybie cichym,

Uruchom narzędzie klbackup z żądanym zestawem przełączników z poziomu wiersza poleceń urządzenia, na którym jest zainstalowany Serwer administracyjny.

Składnia wiersza poleceń narzędzia:

```
klbackup -path <ścieżka dostępu do kopii zapasowej> [-linux_path <ścieżka dostępu do kopii zapasowej DBMS>-node_cert <ścieżka do certyfikatu>] [-logfile <plik dziennika> [-use_ts]|[-restore] [-password <hasło>] [-cert_only]
```

Jeśli w wierszu polecenia narzędzia klbackup nie określono hasła, narzędzie zażąda wprowadzenie hasła interaktywnie.

Opisy przełączników:

- `-path <ścieżka dostępu do kopii zapasowej>`—Zapisuje informacje w folderze kopii zapasowej, lub używa danych z folderu zawierającego kopię zapasową do ich przywrócenia (wymagany parametr).

- `-linux_path <ścieżka dostępu do kopii zapasowej danych DBMS>`—Lokalna ścieżka do folderu zawierającego kopię zapasową danych DBMS.

  Konto serwera bazy danych i narzędzie klbackup powinny mieć uprawnienia do zmiany danych w folderze zawierającym kopię zapasową DBMS.

- `-node_cert <ścieżka do certyfikatu>`—Plik certyfikatu serwera do konfigurowania nieaktywnego węzła klastra trybu failover po odzyskaniu. Jeśli nie zostanie ustawiony, zostanie automatycznie pobrany z Serwera.

- `-logfile <plik raportu>`—Zapisuje raport dotyczący tworzenia kopii zapasowej i przywracania danych Serwera administracyjnego.

  Konto serwera bazy danych i narzędzie klbackup powinny mieć uprawnienia do zmiany danych w folderze zawierającym kopię zapasową.

- `-use_ts`—Podczas zapisywania danych kopiuje informacje do folderu zawierającego kopię zapasową, do podfolderu o nazwie w formacie `klbackup YYYY-MM-DD # HH-MM-SS`, zawierającego bieżącą datę i godzinę operacji w formacie UTC. Jeśli klucz nie został określony, informacje są zapisywane w głównym folderze folderu zawierającego kopię zapasową.

  Podczas próby zapisu informacji do folderu, w którym już znajduje się kopia zapasowa, zostaje wyświetlona wiadomość o błędzie. Żadne informacje nie zostaną zaktualizowane.

  Dostępność klucza `-use_ts` pozwala zachować archiwum danych Serwera administracyjnego. Na przykład, jeśli klucz `-path` wskazuje folder `/tmp/KLBackups`, wówczas folder `klbackup 2022/6/19 # 11-30-18` przechowuje informacje o stanie Serwera administracyjnego na dzień 19 czerwca, 2022 roku, godzinę 11:30:18.

- `-restore`—przywraca dane Serwera administracyjnego. Przywracanie danych odbywa się w oparciu o informacje znajdujące się w folderze zawierającym kopię zapasową. Jeśli żaden klucz nie jest dostępny, kopie zapasowe danych są tworzone w folderze zawierającym kopię zapasową.

- `-password <hasło>`—Hasło chroniące poufne dane.

  Zapomnianego hasła nie można odzyskać. Nie ma wymagań dotyczących hasła. Długość hasła jest nieograniczona i możliwa jest również długość zerowa (brak hasła).

  Podczas przywracania danych powinieneś określić to samo hasło, które wprowadziłeś podczas tworzenia kopii zapasowej. Jeśli po utworzeniu kopii zapasowej ścieżka do folderu współdzielonego uległa zmianie, sprawdź działanie zadań wykorzystujących przywrócone dane (zadania przywracania i zadania zdalnej instalacji). Jeśli jest to konieczne, zmodyfikuj ustawienia tych zadań. Podczas przywracania danych z pliku kopii zapasowej nikt nie może mieć dostępu do folderu współdzielonego Serwera administracyjnego. Konto, z poziomu którego uruchamiane jest narzędzie klbackup, musi mieć pełen dostęp do folderu współdzielonego. Aby przywrócić dane Serwera administracyjnego z kopii zapasowej, zalecamy uruchomienie narzędzia na nowo zainstalowanym Serwerze administracyjnym.

- `-cert_only`—zapisz lub odzyskaj tylko certyfikat i klucz prywatny Serwera administracyjnego.

  Ta flaga może być użyteczna podczas wykonywania migracji z Serwera administracyjnego Kaspersky Security Center Windows do Serwera administracyjnego Kaspersky Security Center Linux. Możesz również migrować zarządzane urządzenia pomiędzy Serwerami administracyjnymi Kaspersky Security Center Linux, a także pomiędzy Serwerami administracyjnymi Kaspersky Security Center Windows.

Za pomocą kopii zapasowej danych możesz przenieść dane z Serwera administracyjnego Kaspersky Security Center Windows pod zarządzanie Kaspersky Security Center Linux.
Jeśli używasz MySQL lub MariaDB jako systemu zarządzania bazami danych dla Kaspersky Security Center Windows i Kaspersky Security Center Linux, parametr `lower_case_table_names` musi mieć taką samą wartość w obecnym i nowym systemie zarządzania bazami danych.
Przed utworzeniem kopii zapasowej danych sprawdź parametr `lower_case_table_names`. Następnie podczas instalacji MySQL lub MariaDB dla Kaspersky Security Center Linux należy ustawić parametr `lower_case_table_names` na taką samą wartość, jaka została określona dla tego parametru w systemie Windows.

Jeżeli podczas przywracania standardowy certyfikat Serwera administracyjnego zostanie zastąpiony innym certyfikatem z kopii zapasowej, należy wykonać następujące czynności, aby zapewnić prawidłowe działanie:
1. Zainstaluj ponownie Web Console, aby uniknąć następującego błędu:
Serwer administracyjny używa niezaufanego certyfikatu. Skonfiguruj ponownie aplikację, określając prawidłowy certyfikat lub skontaktuj się z głównym administratorem.
2. Sprawdź konfigurację serwera IAM i w razie potrzeby dodaj adres Serwera administracyjnego do pliku konfiguracyjnego serwera IAM.

Korzystanie z narzędzia klbackup w celu przełączania zarządzanych urządzeń pod kontrolą innego Serwera administracyjnego

Narzędzie klbackup umożliwia przełączanie zarządzanych urządzeń pod zarządzanie innego Serwera administracyjnego. Możesz zmienić Serwer administracyjny Kaspersky Security Center Windows na Serwer administracyjny Kaspersky Security Center Linux, korzystając z narzędzia klbackup podczas wykonywania migracji. Możesz również migrować zarządzane urządzenia pomiędzy Serwerami administracyjnymi Kaspersky Security Center Linux, a także pomiędzy Serwerami administracyjnymi Kaspersky Security Center Windows.

Przed rozpoczęciem, **sprawdź wymagania dotyczące certyfikatu niestandardowego**.

Jeśli używasz certyfikatu niestandardowego zamiast certyfikatu z podpisem własnym, przed aktualizacją Kaspersky Security Center Linux do nowszej wersji upewnij się, że certyfikat zawiera Alternatywną nazwę podmiotu (SAN). Jeżeli nie zawiera, ważne jest, aby wymienić certyfikat przed aktualizacją Kaspersky Security Center Linux. W przeciwnym razie nie będziesz mógł zalogować się do Web Console po aktualizacji.

Aby upewnić się, że certyfikat zawiera Alternatywną nazwę podmiotu (SAN):

1. Na urządzeniu z zainstalowanym Serwerem administracyjnym, wykonaj następujące polecenie:

   - W przypadku urządzenia z systemem Linux:

     ```
     sudo openssl x509 -in /var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer -noout
     -ext subjectAltName
     ```

- W przypadku urządzenia z systemem Windows:

  ```
  certutil -dump %ProgramData%\KasperskyLab\adminkit\1093\cert\klserver.cer
  ```

2. Upewnij się, że Alternatywna nazwa podmiotu jest obecna w wynikach polecenia i zawiera adres urządzenia Serwera administracyjnego.

3. Jeśli Alternatywna nazwa podmiotu jest niedostępna, użyj narzędzia klsetsrvcert, aby zastąpić certyfikat niestandardowy tym, który spełnia wymagania.

Aby przełączyć zarządzane urządzenia pod zarządzanie innego Serwera administracyjnego przy użyciu narzędzia klbackup:

1. Na poprzednim urządzeniu utwórz kopię zapasową certyfikatu Serwera administracyjnego i klucza prywatnego.

   Możesz utworzyć kopię zapasową na jeden z następujących sposobów:

   - Za pomocą interfejsu narzędzia klbackup (tylko dla Serwera administracyjnego Kaspersky Security Center Windows)

     Uruchom narzędzie klbackup znajdujące się w folderze instalacyjnym Kaspersky Security Center, a następnie utwórz kopię zapasową, korzystając z opcji **Przywróć lub wykonaj kopię zapasową jedynie certyfikatu Serwera administracyjnego**.

   - Za pomocą wiersza poleceń (dla Serwerów administracyjnych Kaspersky Security Center Windows i Kaspersky Security Center Linux w wersji 15.1 lub nowszej)

     Uruchom narzędzie klbackup z kluczem `-cert_only` z poziomu wiersza poleceń, aby utworzyć kopię zapasową certyfikatu i klucza prywatnego Serwera administracyjnego:

     ```
     klbackup -path <ścieżka do kopii zapasowej certyfikatu Serwera administracyjnego> -cert_only
     ```

2. Na poprzednim urządzeniu odłącz Serwer administracyjny od sieci.

3. Przypisz urządzeniu tą samą nazwę domeny za pomocą innego Serwera administracyjnego.

   Nowy Serwer administracyjny może mieć przypisaną nazwę NetBIOS, FQDN i statyczny adres IP. Zależy to od tego, który adres Serwera administracyjnego został ustawiony w pakiecie instalacyjnym Agenta sieciowe w momencie instalacji Agenta sieciowego. Alternatywnie można użyć adresu połączenia, który określa Serwer administracyjny, z którym łączy się Agent sieciowy (możesz uzyskać ten adres na zarządzanych urządzeniach korzystając z narzędzia klnagchk).

   Jeśli nie jest możliwe przypisanie tego samego adresu do urządzenia z innym Serwerem administracyjnym, należy wygenerować nowy certyfikat Serwera administracyjnego i określić ten certyfikat w pliku konfiguracyjnym IAM. Po zainstalowaniu Serwera administracyjnego należy ręcznie przełączyć Agentów sieciowych na nowy Serwer administracyjny.

4. Na urządzeniu z innym serwerem administracyjnym przywróć certyfikat Serwera administracyjnego i klucz prywatny z kopii zapasowej.

   Możesz przywrócić kopię zapasową na jeden z następujących sposobów:

   - Za pomocą interfejsu narzędzia klbackup (tylko dla Serwera administracyjnego Kaspersky Security Center Windows)

     Uruchom narzędzie klbackup, a następnie przywróć kopię zapasową, korzystając z opcji **Przywróć lub wykonaj kopię zapasową jedynie certyfikatu Serwera administracyjnego**.

   - Za pomocą wiersza poleceń (dla Serwerów administracyjnych Kaspersky Security Center Windows i Kaspersky Security Center Linux w wersji 15.1 lub nowszej)

Uruchom narzędzie klbackup z kluczem `-cert_only` z poziomu wiersza poleceń, aby przywrócić kopię zapasową certyfikatu i klucza prywatnego Serwera administracyjnego:

```
klbackup -path < ścieżka do kopii zapasowej certyfikatu Serwera administracyjnego >
-restore -cert_only
```

5. Skonfiguruj weryfikację certyfikatu przez Serwer administracyjny i Serwer IAM.

Zarządzane urządzenia są przekazywane pod kontrolę innego Serwera administracyjnego. Możesz przejść do tego Serwera administracyjnego i sprawdzić, czy zarządzane urządzenia są widoczne w sieci oraz czy Agent sieciowy jest na nich zainstalowany i uruchomiony (wartość *Tak* w kolumnach **Widoczny**, **Agent sieciowy jest zainstalowany** i **Agent sieciowy jest uruchomiony**).

Tworzenie kopii zapasowej i przywracanie danych Serwera administracyjnego podczas korzystania z MySQL lub MariaDB

Możesz użyć kopii zapasowej danych do migracji danych Serwera administracyjnego z Kaspersky Security Center Windows pod zarządzanie Kaspersky Security Center Linux. Migracja przy użyciu kopii zapasowej danych Serwera administracyjnego jest obsługiwana wyłącznie w przypadku migracji do Kaspersky Security Center Linux 15.2 lub nowszej wersji z dowolnej obsługiwanej wersji Kaspersky Security Center dla systemu Windows.

Jeśli używasz MySQL lub MariaDB jako systemu DBMS dla Kaspersky Security Center Windows i Kaspersky Security Center Linux, parametr `lower_case_table_names` musi być taki sam dla bieżącego i nowego systemu DBMS. W przeciwnym wypadku dane Serwera administracyjnego zostaną nieprawidłowo zmigrowane.

Przed utworzeniem kopii zapasowej danych Serwera administracyjnego w Kaspersky Security Center Windows należy sprawdzić wartość parametru `lower_case_table_names`. Jeżeli ten parametr nie zostanie określony wcześniej podczas instalacji systemu DBMS, użyta zostanie wartość domyślna parametru. Wartość domyślna parametru `lower_case_table_names` w systemie Windows wynosi `1`.

Podczas instalacji MySQL lub MariaDB dla Kaspersky Security Center Linux należy ustawić parametr `lower_case_table_names` na taką samą wartość, jaka została określona dla tego parametru w systemie Windows, korzystając z instrukcji ze strony internetowej MySQL. Jeżeli nie określisz tego parametru, używana jest wartość domyślna parametru. W systemach operacyjnych opartych na systemie Linux wartość domyślna parametru `lower_case_table_names` jest inna niż domyślna wartość w systemie Windows.

Jeśli chcesz zainstalować MySQL 8.0, określenie parametru `lower_case_table_names` zgodnie z tą instrukcją może nie zadziałać. W takim przypadku należy najpierw zainstalować MySQL 5.7, określić parametr `lower_case_table_names` za pomocą instrukcji, a następnie wykonać uaktualnienie MySQL 5.7 do wersji MySQL 8.0. Jeżeli parametr `lower_case_table_names` nie jest zgodny z bieżącym i nowym systemem DBMS, dane Serwera administracyjnego zostaną przywrócone nieprawidłowo.

Konserwacja Serwera administracyjnego

Konserwacja Serwera administracyjnego umożliwia zwolnienie miejsca w folderze Serwera administracyjnego i zmniejszenie objętości bazy danych poprzez usunięcie obiektów, które nie są już potrzebne. Pomaga to poprawić wydajność i niezawodność działania aplikacji. Zalecamy przeprowadzanie konserwacji Serwera administracyjnego przynajmniej raz w tygodniu.

Konserwacja Serwera administracyjnego jest wykonywana przy pomocy dedykowanego zadania. Podczas konserwacji Serwera administracyjnego aplikacja wykonuje następujące działania:

- Usuwa niepotrzebne foldery i pliki z folderu przechowywania.
- Usuwa niepotrzebne rekordy z tabel (znane również jako „dangling pointers" (zwisające wskaźniki)).
- Czyści pamięć podręczną.
- Przeprowadza konserwację bazy danych (jeśli używasz PostgreSQL jako DBMS):
  - Reorganizuje indeksy w bazie danych.
  - Aktualizuje statystyki bazy danych.
  - Zmniejsza bazę danych (jeśli to konieczne).

Zadanie Konserwacja Serwera administracyjnego obsługuje wersję MariaDB 10.3 i nowsze. Jeśli używasz MariaDB w wersji 10.2 lub wcześniejszej, administratorzy muszą samodzielnie utrzymywać ten DBMS.

Zadanie Konserwacja Serwera administracyjnego jest tworzone automatycznie podczas instalacji Kaspersky Security Center Linux. Jeżeli zadanie Konserwacja Serwera administracyjnego zostało usunięte, możesz je utworzyć ręcznie.

W celu utworzenia zadania Konserwacja Serwera administracyjnego:

1. W menu głównym przejdź do **Zadania**.
2. Kliknij przycisk **Dodaj**.

   Zostanie uruchomiony Kreator tworzenia nowego zadania.
3. W oknie **Ustawienia nowych zadań** wybierz **Konserwacja Serwera administracyjnego** jako typ zadania i kliknij przycisk **Dalej**.
4. Wykonaj pozostałe instrukcje kreatora.

Nowo utworzone zadanie będzie wyświetlane na liście zadań. Dla jednego Serwera administracyjnego można uruchomić tylko jedno zadanie Konserwacja Serwera administracyjnego. Jeśli zadanie Konserwacja Serwera administracyjnego zostało już utworzone dla Serwera administracyjnego, nie będzie można utworzyć nowego zadania Konserwacja Serwera administracyjnego.

Usuwanie hierarchii Serwerów administracyjnych

Jeśli nie chcesz mieć hierarchii Serwerów administracyjnych, możesz odłączyć je od tej hierarchii.

W celu usunięcia hierarchii Serwerów administracyjnych:

1. W menu głównym kliknij nazwę Serwera administracyjnego.
2. W otwartym oknie przejdź na zakładkę **Serwery administracyjne**.

3. W grupie administracyjnej, z której chcesz usunąć podrzędny Serwer administracyjny, wybierz podrzędny Serwer administracyjny.

4. W wierszu menu kliknij **Usuń**.

5. W otwartym oknie kliknij **OK**, aby potwierdzić chęć usunięcia podrzędnego Serwera administracyjnego.

Poprzedni główny Serwer administracyjny i poprzedni podrzędny Serwer administracyjny są teraz od siebie niezależne. Hierarchia już nie istnieje.

Dostęp do publicznych serwerów DNS

Jeśli dostęp do serwerów Kaspersky przy użyciu systemowego DNS nie jest możliwy, Kaspersky Security Center Linux może korzystać z następujących publicznych serwerów DNS w następującej kolejności:

1. Google Public DNS (8.8.8.8)

2. Cloudflare DNS (1.1.1.1)

3. Alibaba Cloud DNS (223.6.6.6)

4. Quad9 DNS (9.9.9.9)

5. CleanBrowsing (185.228.168.168)

Żądania kierowane do tych serwerów DNS mogą zawierać adresy domen oraz publiczny adres IP Serwera administracyjnego, ponieważ aplikacja nawiązuje połączenie TCP/UDP z serwerem DNS. Jeśli Kaspersky Security Center Linux korzysta z publicznego serwera DNS, przetwarzanie danych podlega polityce prywatności odpowiedniej usługi.

Aby skonfigurować korzystanie z publicznego DNS z użyciem narzędzia klscflag:

1. Uruchom wiersz poleceń, a następnie zmień bieżący katalog na katalog z narzędziem klscflag. Narzędzie klscflag znajduje się w katalogu, w którym zainstalowany jest serwer administracyjny. Domyślna ścieżka instalacji to /opt/kaspersky/ksc64/sbin.

2. Aby wyłączyć korzystanie z publicznego DNS, wpisz na koncie root następujące polecenie:

```
klscflag -fset -pv ".core/.independent" -s Transport -n ForceUseSystemDNS -t d -v 1
```

3. Aby włączyć korzystanie z publicznego DNS, wpisz na koncie root następujące polecenie:

```
klscflag -fset -pv ".core/.independent" -s Transport -n ForceUseSystemDNS -t d -v 0
```

Konfigurowanie interfejsu

Możesz skonfigurować interfejs konsoli Kaspersky Security Center Web Console, aby wyświetlał i ukrywał sekcje i elementy interfejsu, w zależności od używanych funkcji.

W celu skonfigurowania interfejsu Kaspersky Security Center Web Console zgodnie z aktualnie używanym zestawem funkcji:

1. W menu głównym przejdź do sekcji **Ustawienia** → **Opcje interfejsu**.
2. Włącz lub wyłącz wymagane opcje:
   - **Pokaż ochronę i szyfrowanie danych**
   - **Pokaż funkcje MDR**
   - **Pokaż alerty EDR**
3. Kliknij **Zapisz**.

Po włączeniu wymaganych opcji konsola wyświetli odpowiednie sekcje w menu głównym. Na przykład jeśli włączysz opcję **Pokaż alerty EDR**, w menu głównym pojawi się sekcja **Monitorowanie** → **Alerty**.

Nawiązywanie szyfrowanego połączenia z Serwerem administracyjnym

Wymiana danych pomiędzy urządzeniami klienckimi a Serwerem administracyjnym może odbywać się z wykorzystaniem protokołu TLS (Transport Layer Security). Protokół TLS może identyfikować współdziałające strony, szyfrować przesyłane dane oraz chronić je przed modyfikacją podczas transferu. Protokół TLS używa kluczy publicznych do autoryzowania współdziałających stron oraz szyfrowania danych.

Podczas pierwszego łączenia urządzenia klienckiego z Serwerem administracyjnym Agent sieciowy na urządzeniu pobiera certyfikat Serwera administracyjnego i zapisuje go lokalnie.

Jeśli instalujesz Agenta sieciowego lokalnie na urządzeniu, możesz ręcznie wybrać certyfikat Serwera administracyjnego.

Pobrana kopia certyfikatu jest używana do weryfikowania praw i przyzwoleń Serwera administracyjnego podczas kolejnych połączeń.

W trakcie następnych sesji Agent sieciowy będzie żądał certyfikatu Serwera administracyjnego przy każdym połączeniu urządzenia z Serwerem administracyjnym i będzie go porównywał z lokalną kopią. W przypadku, gdy obie kopie nie będą do siebie pasowały, urządzenie nie uzyska pozwolenia na dostęp do Serwera administracyjnego.

Szyfrowanie komunikacji z TLS

Aby usunąć luki w sieci korporacyjnej organizacji, możesz włączyć szyfrowanie ruchu sieciowego przy użyciu protokołu TLS. Możesz włączyć protokoły szyfrowania TLS i obsługiwane zestawy szyfrów na serwerze administracyjnym. Kaspersky Security Center Linux obsługuje wersje protokołu TLS 1.0, 1.1, 1.2 i 1.3. Możesz wybrać wymagany protokół szyfrowania i zestawy szyfrowania.

Kaspersky Security Center Linux używa certyfikatów z podpisem własnym. Możesz także użyć swoich własnych certyfikatów. Specjaliści z Kaspersky zalecają użycie certyfikatów wydanych przez zaufane urzędy certyfikacji.

W celu skonfigurowania dozwolonych protokołów szyfrowania i zestawów szyfrowania na Serwerze administracyjnym:

1. Uruchom wiersz poleceń, a następnie zmień bieżący katalog na katalog z narzędziem klscflag. Narzędzie klscflag znajduje się w katalogu, w którym zainstalowany jest serwer administracyjny. Domyślna ścieżka instalacji to /opt/kaspersky/ksc64/sbin.

2. Użyj flagi SrvUseStrictSslSettings w celu skonfigurowania dozwolonych protokołów szyfrowania i zestawów szyfrowania na Serwerze administracyjnym. Na koncie root wykonaj następujące polecenie w wierszu poleceń:

   ```
   ./klscflag -fset -pv ".core/.independent" -s Transport -n SrvUseStrictSslSettings -v <wartość> -t d
   ```

   Określ parametr <wartość> flagi SrvUseStrictSslSettings:

   - `4` — Włączone są tylko protokoły TLS 1.2 i TLS 1.3. Włączone są także zestawy szyfrów z TLS_RSA_WITH_AES_256_GCM_SHA384 (te zestawy szyfrów są potrzebne do zapewnienia kompatybilności z wcześniejszymi wersjami z Kaspersky Security Center Linux). To jest wartość domyślna.

     Zestawy szyfrów obsługiwane dla protokołu TLS 1.2:

     - ECDHE-RSA-AES256-GCM-SHA384
     - ECDHE-RSA-AES256-SHA384
     - ECDHE-RSA-CHACHA20-POLY1305
     - AES256-GCM-SHA384 (zestaw szyfrów z TLS_RSA_WITH_AES_256_GCM_SHA384)
     - ECDHE-RSA-AES128-GCM-SHA256
     - ECDHE-RSA-AES128-SHA256

     Zestawy szyfrów obsługiwane dla protokołu TLS 1.3:

     - TLS_AES_256_GCM_SHA384
     - TLS_CHACHA20_POLY1305_SHA256
     - TLS_AES_128_GCM_SHA256
     - TLS_AES_128_CCM_SHA256

   - `5` — Włączone są tylko protokoły TLS 1.2 i TLS 1.3. W przypadku protokołów TLS 1.2 i TLS 1.3 obsługiwane są określone zestawy szyfrów wymienione poniżej.

     Zestawy szyfrów obsługiwane dla protokołu TLS 1.2:

     - ECDHE-RSA-AES256-GCM-SHA384
     - ECDHE-RSA-AES256-SHA384
     - ECDHE-RSA-CHACHA20-POLY1305
     - ECDHE-RSA-AES128-GCM-SHA256
     - ECDHE-RSA-AES128-SHA256

Zestawy szyfrów obsługiwane dla protokołu TLS 1.3:

- TLS_AES_256_GCM_SHA384
- TLS_CHACHA20_POLY1305_SHA256
- TLS_AES_128_GCM_SHA256
- TLS_AES_128_CCM_SHA256

Nie zalecamy używania wartości 0, 1, 2 lub 3 jako wartości parametru flagi SrvUseStrictSslSettings. Te wartości parametrów odpowiadają niezabezpieczonym wersjom protokołu TLS (protokoły TLS 1.0 i TLS 1.1) oraz niezabezpieczonym zestawom szyfrów i są używane wyłącznie w celu zapewnienia kompatybilności wstecznej z wcześniejszymi wersjami Kaspersky Security Center.

3. Uruchom ponownie następujące usługi Kaspersky Security Center Linux:
   - Serwer administracyjny
   - Serwer sieciowy
   - Activation Proxy

Dzięki temu włączone jest szyfrowanie ruchu sieciowego przy użyciu protokołu TLS.

Możesz użyć flag KLTR_TLS12_ENABLED i KLTR_TLS13_ENABLED, aby włączyć obsługę odpowiednio protokołów TLS 1.2 i TLS 1.3. Te flagi są domyślnie włączone.

Aby włączyć lub wyłączyć obsługę protokołów TLS 1.2 i TLS 1.3:

1. Uruchom narzędzie klscflag.

   Uruchom wiersz poleceń, a następnie zmień bieżący katalog na katalog z narzędziem klscflag. Narzędzie klscflag znajduje się w katalogu, w którym zainstalowany jest serwer administracyjny. Domyślna ścieżka instalacji to /opt/kaspersky/ksc64/sbin.

2. Na koncie root wykonaj jedno z następujących poleceń w wierszu poleceń:
   - Użyj tego polecenia, aby włączyć lub wyłączyć obsługę protokołu TLS 1.2:

     ```
     ./klscflag -fset -pv ".core/.independent" -s Transport -n KLTR_TLS12_ENABLED -v <wartość> -t d
     ```

   - Użyj tego polecenia, aby włączyć lub wyłączyć obsługę protokołu TLS 1.3:

     ```
     ./klscflag -fset -pv ".core/.independent" -s Transport -n KLTR_TLS13_ENABLED -v <wartość> -t d
     ```

   Określ parametr `<wartość>` flagi:

   - `1` — Aby włączyć obsługę protokołu TLS.
   - `0` — Aby wyłączyć obsługę protokołu TLS.

Ustawienia sieciowe dotyczące interakcji z usługami zewnętrznymi

Kaspersky Security Center Linux używa następujących ustawień sieciowych do interakcji z usługami zewnętrznymi.

Ustawienia sieci

Ustawienia sieci	Adres	Opis
Port: 443 Protokół: HTTPS	`https://activation-v2.kaspersky.com`	Aktywacja aplikacji.

Port: 443
Protokół: HTTPS
	`https://s00.upd.kaspersky.com`
	`https://s01.upd.kaspersky.com`
	`https://s02.upd.kaspersky.com`
	`https://s03.upd.kaspersky.com`
	`https://s04.upd.kaspersky.com`
	`https://s05.upd.kaspersky.com`
	`https://s06.upd.kaspersky.com`
	`https://s07.upd.kaspersky.com`
	`https://s08.upd.kaspersky.com`
	`https://s09.upd.kaspersky.com`
	`https://s10.upd.kaspersky.com`
	`https://s11.upd.kaspersky.com`
	`https://s12.upd.kaspersky.com`
	`https://s13.upd.kaspersky.com`
	`https://s14.upd.kaspersky.com`
	`https://s15.upd.kaspersky.com`
	`https://s16.upd.kaspersky.com`
	`https://s17.upd.kaspersky.com`
	`https://s18.upd.kaspersky.com`
	`https://s19.upd.kaspersky.com`
	`https://cm.k.kaspersky-labs.com`
		Aktualizowanie baz danych, modułów i aplikacji Kaspersky.

Port: 443 Protokół: HTTPS	`https://downloads.upd.kaspersky.com`	• Aktualizowanie baz danych, modułów i aplikacji Kaspersky. • Sprawdzanie, czy serwery Kaspersky są dostępne. Przed pobraniem baz danych i modułów oprogramowania Kaspersky oprogramowanie Kaspersky Security Center Linux sprawdza, czy serwery Kaspersky są dostępne. Jeżeli dostęp do serwerów za pomocą systemowego DNS nie jest możliwy, aplikacja korzysta z publicznych serwerów DNS.

Ustawienia sieci	Adres	Opis
Port: 80 Protokół: HTTP	http://p00.upd.kaspersky.com http://p01.upd.kaspersky.com http://p02.upd.kaspersky.com http://p03.upd.kaspersky.com http://p04.upd.kaspersky.com http://p05.upd.kaspersky.com http://p06.upd.kaspersky.com http://p07.upd.kaspersky.com http://p08.upd.kaspersky.com http://p09.upd.kaspersky.com http://p10.upd.kaspersky.com http://p11.upd.kaspersky.com http://p12.upd.kaspersky.com http://p13.upd.kaspersky.com http://p14.upd.kaspersky.com http://p15.upd.kaspersky.com http://p16.upd.kaspersky.com http://p17.upd.kaspersky.com http://p18.upd.kaspersky.com http://p19.upd.kaspersky.com http://downloads0.kaspersky-labs.com http://downloads1.kaspersky-labs.com http://downloads2.kaspersky-labs.com http://downloads3.kaspersky-labs.com http://downloads4.kaspersky-labs.com http://downloads5.kaspersky-labs.com http://downloads6.kaspersky-labs.com http://downloads7.kaspersky-labs.com http://downloads8.kaspersky-labs.com http://downloads9.kaspersky-labs.com http://downloads.kaspersky-labs.com http://cm.k.kaspersky-labs.com	Aktualizowanie baz danych, modułów i aplikacji Kaspersky.
Port: 443 Protokół: HTTPS	https://ds.kaspersky.com https://dc1.ksn.kaspersky-labs.com https://dc1-file.ksn.kaspersky-labs.com https://dc1-pp.ksn.kaspersky-labs.com https://dc1-st.ksn.kaspersky-labs.com/ https://dc1-cert.ksn.kaspersky-labs.com https://dc1-cf.ksn.kaspersky-labs.com https://dc1-file.ksn.kaspersky-labs.com https://dc1-kas.ksn.kaspersky-labs.com https://dc1-ml.ksn.kaspersky-labs.com https://dc1-pp.ksn.kaspersky-labs.com https://dc1-st.ksn.kaspersky-labs.com https://dc1.ksn.kaspersky-labs.com	Używanie Kaspersky Security Network.

Ustawienia sieci	Adres	Opis

Port: 443, 1443
Protokół: HTTPS
	`https://ksn-file-geo.kaspersky-labs.com`
	`https://ksn-verdict-geo.kaspersky-labs.com`
	`https://ksn-url-geo.kaspersky-labs.com`
	`https://ksn-a-p2p-geo.kaspersky-labs.com`
	`https://ksn-info-geo.kaspersky-labs.com`
	`https://ksn-cinfo-geo.kaspersky-labs.com`
		Używanie Kaspersky Security Network.

Port: 443, 1443
Protokół: KSN
	`ksn://ksn-a-p2p-geo.kaspersky-labs.com`
	`ksn://ksn-a-stat-geo.kaspersky-labs.com`
	`ksn://ksn-ca-geo.kaspersky-labs.com`
	`ksn://ksn-cinfo-geo.kaspersky-labs.com`
	`ksn://ksn-crypto-catm-geo.kaspersky-labs.com`
	`ksn://ksn-crypto-dnscheck-geo.kaspersky-labs.com`
	`ksn://ksn-crypto-hash-geo.kaspersky-labs.com`
	`ksn://ksn-crypto-ipm-geo.kaspersky-labs.com`
	`ksn://ksn-crypto-whocalls-geo.kaspersky-labs.com`
	`ksn://ksn-crypto-wifiplus-geo.kaspersky-labs.com`
	`ksn://ksn-eu-stat-kmp.kaspersky-labs.com`
	`ksn://ksn-file-geo.kaspersky-labs.com`
	`ksn://ksn-his-geo.kaspersky-labs.com`
	`ksn://ksn-info-geo.kaspersky-labs.com`
	`ksn://ksn-kas-geo.kaspersky-labs.com`
	`ksn://ksn-kddi.kaspersky-labs.com`
	`ksn://ksn-ml-geo.kaspersky-labs.com`
	`ksn://ksn-oui-geo.kaspersky-labs.com`
	`ksn://ksn-pp.kaspersky-labs.com`
	`ksn://ksn-src.kaspersky-labs.com`
	`ksn://ksn-stat-geo.kaspersky-labs.com`
	`ksn://ksn-tcert-geo.kaspersky-labs.com`
	`ksn://ksn-url-geo.kaspersky-labs.com`
	`ksn://ksn-verdict-geo.kaspersky-labs.com`
	`ksn://mdr.ksn.kaspersky-labs.com`
	`ksn://stat-eu.ksn.kaspersky-labs.com`
	`ksn://stat-hq.ksn.kaspersky-labs.com`
	`ksn://stat-ru.ksn.kaspersky-labs.com`
	`ksn://stat-sa.ksn.kaspersky-labs.com`
	`ksn://stat-sbr.ksn.kaspersky-labs.com`
		Używanie Kaspersky Security Network.

Port: 443 Protokół: HTTPS	`https://click.kaspersky.com` `https://redirect.kaspersky.com`	Klikanie odnośników z poziomu interfejsu.
Port: 80 Protokół: HTTP	`http://crl.kaspersky.com` `http://ocsp.kaspersky.com`	Serwery te stanowią część infrastruktury klucza publicznego (PKI) i są niezbędne do weryfikacji statusu ważności certyfikatów podpisu cyfrowego Kaspersky. Lista CRL to lista unieważnionych certyfikatów. OCSP umożliwia sprawdzenie statusu konkretnego certyfikatu w czasie rzeczywistym. Serwery te pomagają zapewnić bezpieczeństwo interakcji z certyfikatami cyfrowymi i chronią przed możliwymi atakami.

Ustawienia sieci	Adres	Opis
Port: 443 Protokół: HTTPS	`https://ipm-klca.kaspersky.com`	Ogłoszenia marketingowe.
Port: 443 Protokół: HTTPS	`https://tip.kaspersky.com`	Reagowanie na zagrożenia za pośrednictwem Kaspersky Threat Intelligence Portal (w przypadku korzystania z funkcjonalności Kaspersky Next XDR Optimum).
Port: 443 Protokół: HTTPS	Aby zapoznać się z pełną listą adresów, zapoznaj się z artykułem Struktura adresów i domen	Reagowanie na zagrożenia za pośrednictwem Kaspersky Automated Security Awareness Platform (przy użyciu funkcjonalności Kaspersky Next XDR Optimum).

Aby zapewnić prawidłową współpracę Kaspersky Security Center Linux z usługami zewnętrznymi, należy uwzględnić następujące zalecenia:
- Na urządzeniach sieciowych i serwerze proxy organizacji należy zezwolić na nieszyfrowany ruch sieciowy przez porty 443 i 1443.
- Podczas komunikacji Serwera administracyjnego z serwerami aktualizacji Kaspersky i serwerami Kaspersky Security Network należy unikać przechwytywania ruchu sieciowego z podmianą certyfikatu (ataki MITM).

Aby pobrać aktualizacje poprzez protokół HTTP lub HTTPS za pomocą narzędzia klscflag:

1. Uruchom wiersz poleceń, a następnie zmień bieżący katalog na katalog z narzędziem klscflag. Narzędzie klscflag znajduje się w katalogu, w którym zainstalowany jest serwer administracyjny. Domyślna ścieżka instalacji to /opt/kaspersky/ksc64/sbin.

2. Jeśli chcesz pobrać aktualizacje przez protokół HTTP, uruchom na koncie root jedno z następujących poleceń:

   - Na urządzeniu z zainstalowanym Serwerem administracyjnym:

     ```
     klscflag -fset -pv klserver -s Updater -n DisableKLHttps -t d -v 1
     ```

   - W punkcie dystrybucji:

     ```
     klscflag -fset -pv klnagent -s Updater -n DisableKLHttps -t d -v 1
     ```

   Jeśli chcesz pobrać aktualizacje za pośrednictwem protokołu HTTPS, uruchom na koncie root jedno z następujących poleceń:

   - Na urządzeniu z zainstalowanym Serwerem administracyjnym:

     ```
     klscflag -fset -pv klserver -s Updater -n DisableKLHttps -t d -v 0
     ```

   - W punkcie dystrybucji:

     ```
     klscflag -fset -pv klnagent -s Updater -n DisableKLHttps -t d -v 0
     ```

Globalna lista podsieci

Dla każdego używanego Serwera administracyjnego możesz skonfigurować globalną listę podsieci, w której przechowywane będą informacje o podsieciach Twojej sieci. Ta lista pomaga w dopasowaniu par {adres IP, maska} i fizycznych jednostek, takich jak oddziały firmy. Możesz użyć podsieci z tej listy w ustawieniach i regułach sieci.

W celu dodania podsieci do globalnej listy podsieci:

1. W menu głównym kliknij nazwę Serwera administracyjnego.
   Zostanie otwarte okno właściwości Serwera administracyjnego.
2. Na zakładce **Ogólne** wybierz sekcję **Globalne podsieci**.
3. Kliknij przycisk **Dodaj**.
   Zostanie otwarte okno **Nowa podsieć**.
4. Wypełnij następujące pola:
   - **Nazwa**
   - **Adres podsieci**
   - **Maska podsieci**
   - **Opis**
5. Kliknij przycisk **Zapisz**.

Okno zostanie zamknięte, a podsieć pojawi się na liście podsieci.

W razie potrzeby na liście podsieci globalnych możesz wykonać następujące czynności:

- Usunąć podsieci z listy, wybierając wymaganą podsieć i klikając przycisk **Usuń**.
- Zmodyfikować właściwości podsieci, klikając łącze z nazwą wymaganej podsieci, a następnie wykonując czynności opisane w krokach 4–5.

Sprawdzanie integralności modułów za pomocą narzędzi klscmodchk i integrity_checker

Kaspersky Security Center Linux zawiera wiele modułów binarnych w formie bibliotek dołączanych dynamicznie, plików wykonywalnych, plików konfiguracyjnych i plików interfejsu. Intruzi mogą wymienić jeden lub więcej modułów wykonywalnych lub plików aplikacyjnych na inne pliki zawierające szkodliwy kod. Aby nie dopuścić do zamiany modułów i plików, Kaspersky Security Center Linux zapewnia kontrolę integralności komponentów za pomocą narzędzi klscmodchk i integrity_checker. Te narzędzia sprawdzają moduły i pliki pod kątem nieautoryzowanych zmian lub uszkodzeń. Jeżeli moduł lub plik aplikacji ma nieprawidłową sumę kontrolną, jest uznawany za uszkodzony.

Narzędzie klscmodchk wykonuje kontrolę integralności dla następujących komponentów Kaspersky Security Center Linux:

- Serwer administracyjny
- Agent sieciowy

Narzędzie integrity_checker wykonuje kontrolę integralności dla następujących komponentów Kaspersky Security Center Linux:

- Serwer administracyjny
- Agent sieciowy
- Kaspersky Security Center Web Console

Oba narzędzia sprawdzają integralność modułów w oparciu o plik manifestu kl_file_integrity_manifest.xml, który jest częścią kompilacji Kaspersky Security Center Linux i znajduje się w folderze instalacyjnym. Plik manifestu komponentu zawiera pliki, których integralność jest ważna z punktu widzenia prawidłowego działania komponentu Kaspersky Security Center Linux. Integralność samego pliku manifestu jest również sprawdzana.

Zdecydowanie nie zalecamy modyfikacji pliku manifestu kl_file_integrity_manifest.xml, gdyż spowoduje to unieważnienie podpisu cyfrowego i nieudaną kontrolę integralności.

Aby sprawdzić integralność komponentu Kaspersky Security Center Linux, uruchomić jedno z poniższych poleceń:

- `$ klscmodchk [ parametry ]`

  Narzędzie klscmodchk uruchamia narzędzie integrity_checker z parametrem `--verbose` i sprawdza integralność modułów.

  Parametry dla narzędzia klscmodchk:

  - `-logfile < log_file_path >`—Określa ścieżkę do pliku na dysku do logowania. Domyślnie informacja jest wyświetlana na konsoli.
  - `-verbose`—Wyświetla rozszerzone informacje w trakcie sprawdzania integralności.

- `$ integrity_checker [ parametry ] < ścieżka_do_pliku_manifestu >`

  Parametry dla narzędznia integrity_checker:

  - `--help`—Wyświetla pomoc narzędzia integrity_checker.
  - `--version`—Wyświetla wersję narzędzia integrity_checker.
  - `--verbose`—Wyświetla informacje o działaniu narzędzia. Wykonując kontrolę integralności, wystarczy użyć tego parametru w wierszu poleceń.

Wyniki sprawdzenia każdego pliku manifestu są wyświetlane obok nazwy pliku manifestu w następującym formacie:

- SUCCEEDED—Integralność pliku potwierdzona (kod zwrotny 0).
- FAILED—Integralność pliku nie została potwierdzona (niezerowy kod powrotny).

Można również skonfigurować automatyczne uruchamianie sprawdzania integralności podczas uruchamiania aplikacji. Domyślnie automatyczne sprawdzanie integralności jest wyłączone.

Aby włączyć automatyczne sprawdzanie integralności:

1. Na urządzeniu z zainstalowanym Serwerem Administracyjnym, w wierszu poleceń wprowadź następujące polecenie:

   ```
   ./klscflag -fset -pv klserver -n KLMODCHK_ENABLE_CHECKING -t d -v 1
   ```

2. Uruchom urządzenie ponownie.

   Automatyczne sprawdzanie integralności jest włączone.

Przy kolejnym uruchomieniu Kaspersky Security Center narzędzie klscmodchk zostanie uruchomione wraz z Serwerem Administracyjnym i rozpocznie sprawdzanie integralności modułów. Wyniki kontroli integralności są zapisywane do Dziennika zdarzeń aplikacji Kaspersky.

Wykrywanie urządzeń w sieci

Ta sekcja opisuje wyszukiwanie i wykrywanie urządzeń w sieci.

Kaspersky Security Center Linux umożliwia wyszukiwanie urządzeń w oparciu o określone kryteria. Wyniki wyszukiwania możesz zapisać do pliku tekstowego.

Opcja wyszukiwania i wykrywania pozwala znaleźć następujące urządzenia:

- Zarządzane urządzenia w grupach administracyjnych Serwera administracyjnego i jego podrzędnych Serwerów administracyjnych.
- Urządzenia nieprzypisane zarządzane przez Serwer administracyjny i jego podrzędne Serwery administracyjne.

Scenariusz: Wykrywanie urządzeń w sieci

Przed zainstalowaniem aplikacji zabezpieczających musisz przeprowadzić wykrywanie urządzeń. Jeśli wszystkie urządzenia w sieci zostaną wykryte, możesz uzyskać informacje o nich i zarządzać nimi poprzez zasady. Regularne przeszukiwania sieci są potrzebne do sprawdzania, czy w sieci są jakiekolwiek nowe urządzenia oraz czy wciąż znajdują się w niej wcześniej wykryte urządzenia.

Wykrywanie urządzeń w sieci odbywa się w etapach:

1. **Wstępne wykrywanie urządzeń**

   Po zakończeniu działania kreatora wstępnej konfiguracji wykonaj ręczne wykrywanie urządzeń.

2. **Konfigurowanie przyszłych przeszukiwań**

   Upewnij się, że przeszukiwanie zakresu IP jest włączone i że terminarz przeszukiwania spełnia potrzeby organizacji. Podczas konfigurowania terminarza przeszukiwania skorzystaj z zaleceń dotyczących częstotliwości przeszukiwania sieci.

   Możesz także włączyć przesukiwanie Zeroconf, jeśli Twoja sieć zawiera urządzenia IPv6.

   Jeśli w domenie znajdują się urządzenia sieciowe, zaleca się użycie przeszukiwania kontrolera domeny.

   Użyj punktów dystrybucji opartych na systemie Windows do przeszukiwania sieci Windows.

3. **Konfigurowanie reguł dodawania wykrytych urządzeń do grup administracyjnych (opcjonalne)**

   Jeśli nowe urządzenia pojawią się w Twojej sieci, zostaną wykryte podczas regularnych przeszukiwań i zostaną automatycznie uwzględnione w grupie **Urządzenia nieprzypisane**. Jeśli chcesz, możesz skonfigurować reguły automatycznego przenoszenia tych urządzeń do grupy **Zarządzane urządzenia**. Możesz także utworzyć reguły zatrzymania.

   Jeśli pominiesz ten krok konfigurowania reguły, wszystkie nowo wykryte urządzenia zostaną przeniesione do grupy **Urządzenia nieprzypisane** i tam pozostaną. Jeśli chcesz, możesz ręcznie przenieść te urządzenia do grupy **Zarządzane urządzenia**. Jeśli ręcznie przeniesiesz te urządzenia do grupy **Zarządzane urządzenia**, możesz przeanalizować informacje o każdym urządzeniu i zdecydować, czy chcesz przenieść je do grupy administracyjnej i do jakiej grupy.

Wyniki

Zakończenie scenariusza powoduje, że:

- Serwer administracyjny Kaspersky Security Center Linux wykrywa urządzenia, które znajdują się w sieci, i zapewnia informacje o nich.
- Przyszłe przeszukiwania zostają skonfigurowane i przeprowadzone zgodnie z określonym terminarzem.

Nowo wykryte urządzenia zostaną rozmieszczone zgodnie ze skonfigurowanymi regułami (lub jeśli nie ma skonfigurowanych reguł, urządzenia pozostają w grupie **Urządzenia nieprzypisane**).

Przeszukiwanie sieci Windows

Informacje o przeszukiwaniu sieci Windows

Serwer administracyjny Kaspersky Security Center Linux nie obsługuje przeszukiwania sieci systemu Windows. Użyj punktów dystrybucji opartych na systemie Windows do przeszukiwania sieci Windows.

Podczas szybkiego przeszukiwania punkty dystrybucji pobierają wyłącznie informacje o urządzeniach znajdujących się na liście nazw NetBIOS wszystkich domen sieci i grup roboczych. Podczas pełnego przeszukiwania wymagane są następujące informacje o każdym urządzeniu klienckim:

- Nazwa systemu operacyjnego
- Adres IP
- Nazwa DNS
- Nazwa NetBIOS

Szybkie przeszukiwanie i pełne przeszukiwanie wymagają:

- Porty UDP 137/138, TCP 139, UDP 445, TCP 445 muszą być dostępne w sieci.
- Protokół SMB jest włączony.
- Usługa Przeglądarka komputera Microsoft musi być używana, a główna przeglądarka komputera musi być włączona na Serwerze administracyjnym.
- Usługa Przeglądarka komputera Microsoft musi być używana, a główna przeglądarka komputera musi być włączona na urządzeniach klienckich:
    - Przynajmniej na jednym urządzeniu, jeśli liczba urządzeń w sieci nie przekracza 32.
    - Przynajmniej na jednym urządzeniu dla każdego z 32 urządzeń w sieci.

Pełne przeszukiwanie może być uruchomione tylko wtedy, gdy szybkie przeszukiwanie było uruchomione przynajmniej raz.

Przeszukiwanie zakresu IP

Kaspersky Security Center Linux próbuje przeprowadzić odwrotne rozwiązanie nazwy dla każdego adresu IPv4 z określonego zakresu do nazwy DNS przy użyciu standardowych żądań DNS. Jeśli to działanie zakończy się sukcesem, serwer wyśle `ICMP ECHO REQUEST` (to samo co polecenie ping) do otrzymanej nazwy. Jeśli urządzenie odpowie, informacje o nim zostaną dodane do bazy danych Kaspersky Security Center Linux. Odwrotne rozwiązanie nazwy jest potrzebne do wykluczenia urządzeń sieciowych, które mogą mieć adres IP, ale nie komputery, na przykład, drukarki sieciowe lub routery.

Ta metoda przeszukiwania polega na poprawnie skonfigurowanej lokalnej usłudze DNS. Musi mieć strefę wyszukiwania wstecznego. Jeśli ta strefa nie jest skonfigurowana, przeszukiwanie podsieci IP nie zwróci wyników.

Na początku program Kaspersky Security Center Linux uzyskuje zakresy adresów IP dla przeszukiwania z ustawień sieciowych urządzenia, na którym jest zainstalowany. Jeśli adres urządzenia to 192.168.0.1, a maska podsieci to 255.255.255.0, Kaspersky Security Center Linux uwzględnia sieć 192.168.0.0/24 na liście automatycznego przeszukiwania adresów. Kaspersky Security Center Linux przeszukuje wszystkie adresy od 192.168.0.1 do 192.168.0.254.

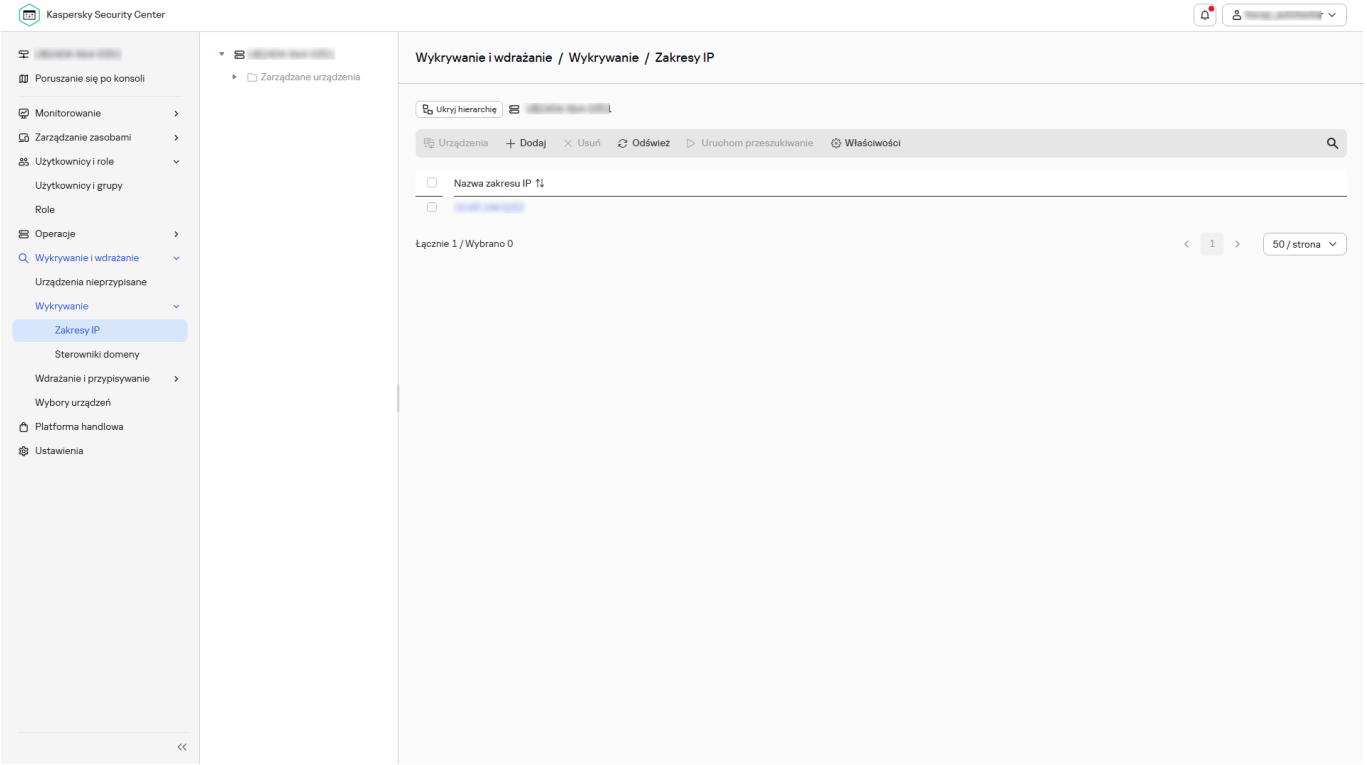
Jeśli włączone jest tylko przeszukiwanie zakresu IP, Kaspersky Security Center Linux wykryje urządzenia tylko z adresami IPv4. Jeśli Twoja sieć zawiera urządzenia IPv6, włącz odpytywanie urządzeń Zeroconf.

Dla wszystkich hostów z systemem Linux w ramach kontrolera domeny Microsoft Active Directory, Samba, FreeIPA lub ALD Pro określ parametry `netbios name` i `workgroup` w pliku `/etc/samba/smb.conf`. W przeciwnym razie wyniki przeszukiwania mogą zawierać zduplikowane hosty.

Przeglądanie i modyfikowanie ustawień przeszukiwania zakresu IP

W celu przejrzenia i zmodyfikowania właściwości przeszukiwania zakresu IP:

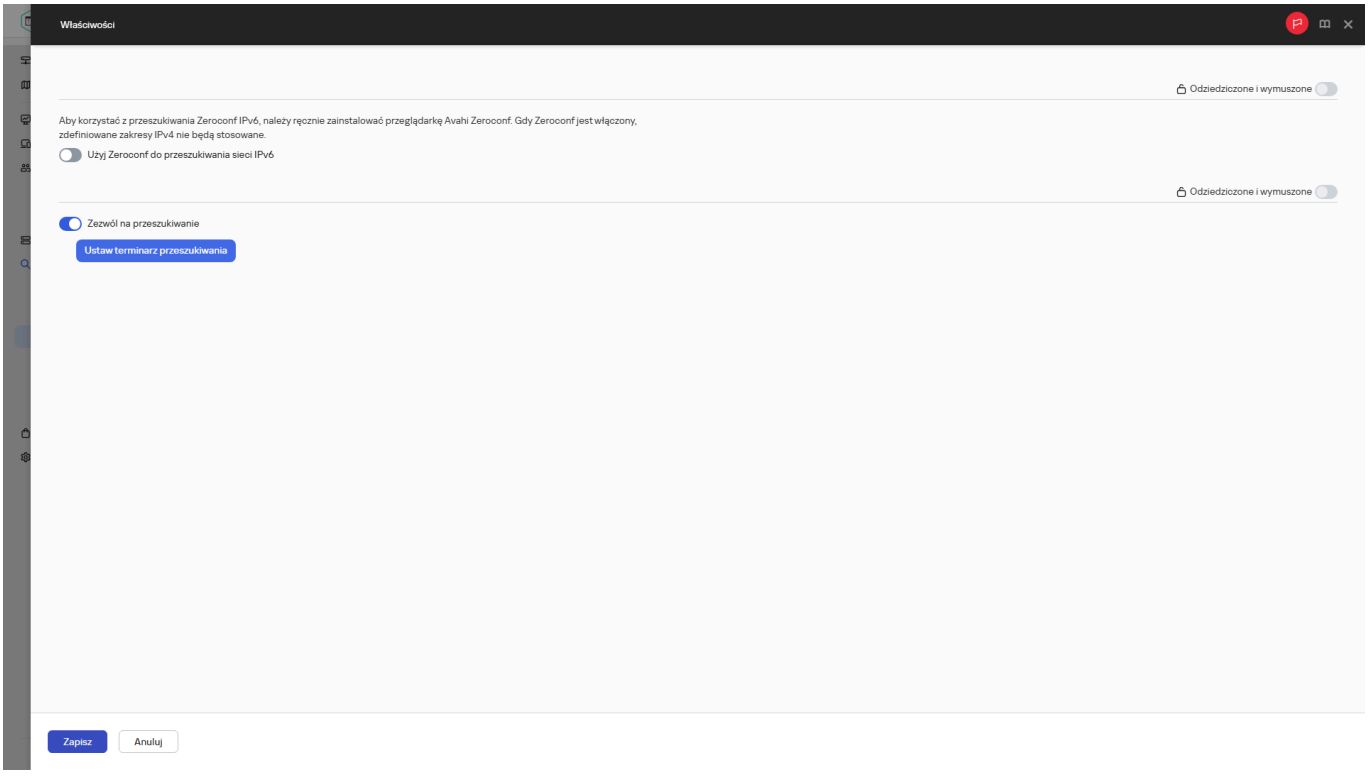
1. W menu głównym przejdź do **Wykrywanie i wdrażanie** → **Wykrywanie** → **Zakresy IP**.



Lista zakresu IP

2. Kliknij przycisk **Właściwości**.

   Zostanie otwarte okno właściwości przeszukiwania IP.



Właściwości przeszukiwania IP

3. Włącz lub wyłącz przeszukiwanie IP przy użyciu przycisku przełącznika **Zezwól na przeszukiwanie**.

4. Skonfiguruj terminarz przeszukiwania. Domyślnie, przeszukiwanie IP jest uruchamiane co 420 minut (siedem godzin).

   Podczas określania przedziału czasu przeszukiwania upewnij się, że to ustawienie nie przekracza wartości Parametr czasu dzierżawy adresu IP. Jeśli adres IP nie został zweryfikowany przez przeszukiwanie w trakcie czasu dzierżawy adresu IP, ten adres IP jest automatycznie usuwany z wyników przeszukiwania. Domyślnie, wyniki przeszukiwania są ważne 24 godziny, ponieważ dynamiczne adresy IP (przypisane przy użyciu Protokołu dynamicznej konfiguracji hosta (DHCP)) zmieniają się co 24 godziny.

   Dostępne są następujące opcje terminarza przeszukiwania:

   - **Co N dni**

     Przeszukiwanie odbywa się regularnie, w określonych przedziałach czasu, począwszy od określonego dnia i godziny.

     Domyślnie, przeszukiwanie jest uruchamiane codziennie, począwszy od bieżącej daty i godziny systemowej.

   - **Co N minut**

     Przeszukiwanie odbywa się regularnie, w określonych przedziałach czasu, począwszy od określonego czasu.

   - **Według dni tygodnia**

     Przeszukiwanie odbywa się regularnie, w określone dni tygodnia i o określonej godzinie.

   - **Miesięcznie wybranego dnia tygodnia**

     Przeszukiwanie odbywa się regularnie, w określone dni miesiąca i o określonej godzinie.

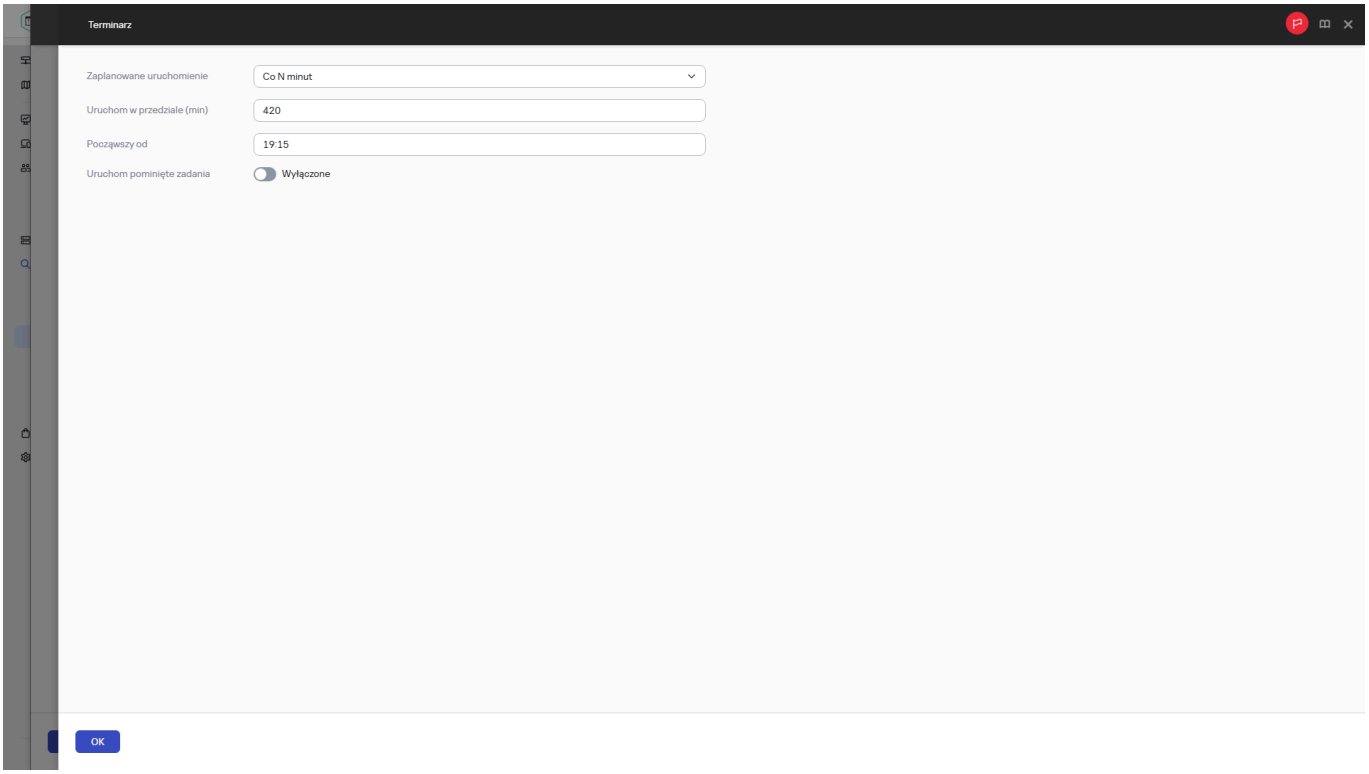
   - **Uruchom pominięte zadania**

     Jeśli Serwer administracyjny jest wyłączony lub niedostępny w czasie, dla którego zaplanowane jest przeszukiwanie, Serwer administracyjny może uruchomić przeszukiwanie od razu po jego włączeniu lub odczekać do następnego zaplanowanego przeszukiwania.

     Jeśli ta opcja jest włączona, Serwer administracyjny rozpoczyna przeszukiwanie od razu po jego włączeniu.

     Jeśli ta opcja jest wyłączona, Serwer administracyjny odczekuje do następnego zaplanowanego przeszukiwania.

Domyślnie opcja ta jest wyłączona.



Konfigurowanie terminarza przeszukiwania

5. Kliknij przycisk **Zapisz**.

   Właściwości zostaną zapisane i zastosowane do wszystkich zakresów IP.

Ręczne uruchamianie przeszukiwania

W celu natychmiastowego uruchomienia przeszukiwania:

Kliknij **Uruchom przeszukiwanie**.

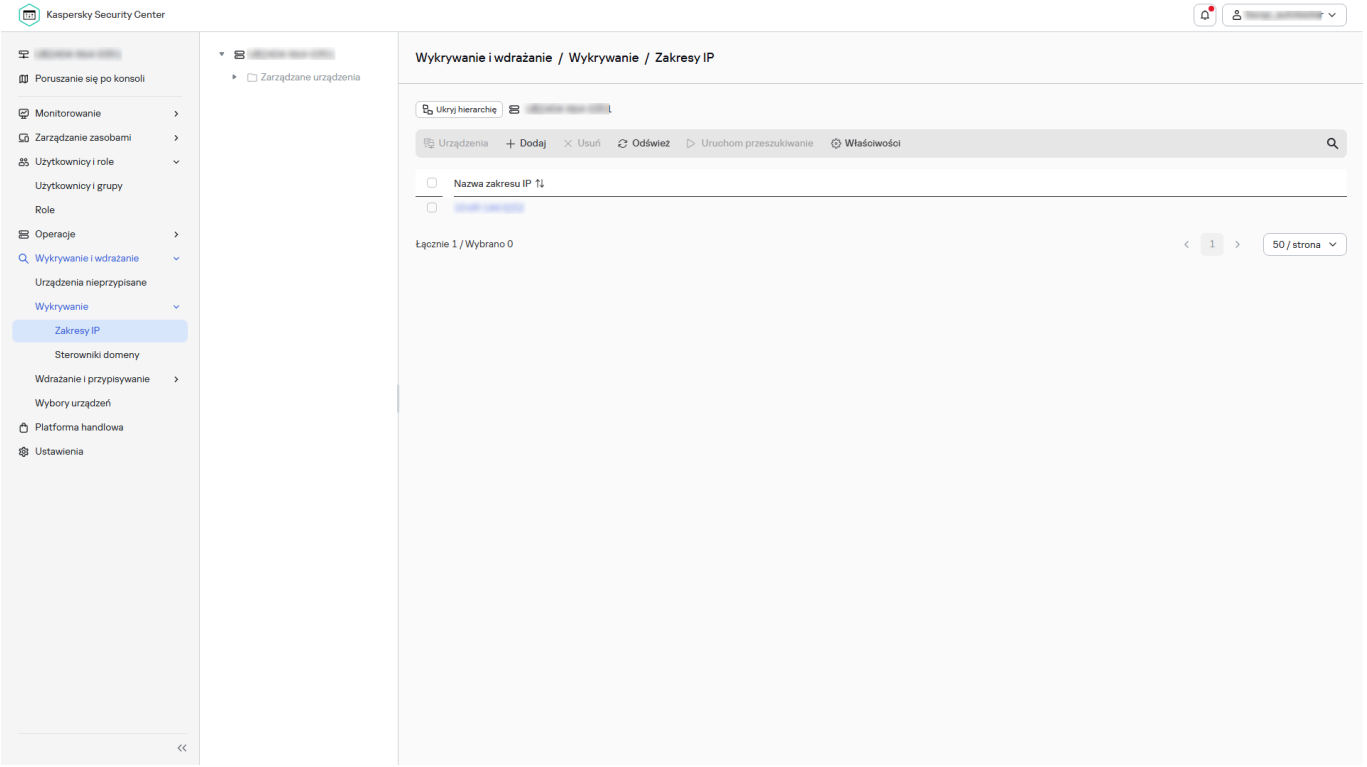
Dodawanie i modyfikowanie zakresu IP

Na początku program Kaspersky Security Center Linux uzyskuje zakresy adresów IP dla przeszukiwania z ustawień sieciowych urządzenia, na którym jest zainstalowany. Jeśli adres urządzenia to 192.168.0.1, a maska podsieci to 255.255.255.0, Kaspersky Security Center Linux uwzględnia sieć 192.168.0.0/24 na liście automatycznego przeszukiwania adresów. Kaspersky Security Center Linux przeszukuje wszystkie adresy od 192.168.0.1 do 192.168.0.254. Możesz zmodyfikować automatycznie definiowany zakres adresów IP lub dodać niestandardowe zakresy adresów IP.

Możesz utworzyć zakres tylko dla adresów IPv4. Jeśli włączysz Przeszukiwanie Zeroconf, Kaspersky Security Center Linux przeszuka całą sieć.

W celu dodania nowego zakresu IP:

1. W menu głównym przejdź do **Wykrywanie i wdrażanie** → **Wykrywanie** → **Zakresy IP**.



Lista zakresu IP

2. Aby dodać nowy zakres IP, kliknij przycisk **Dodaj**.

3. W otwartym oknie określ następujące ustawienia:

   - **Nazwa zakresu IP**

     Nazwa zakresu IP. Możesz określić sam zakres IP jako nazwę, na przykład: „192.168.0.0/24".

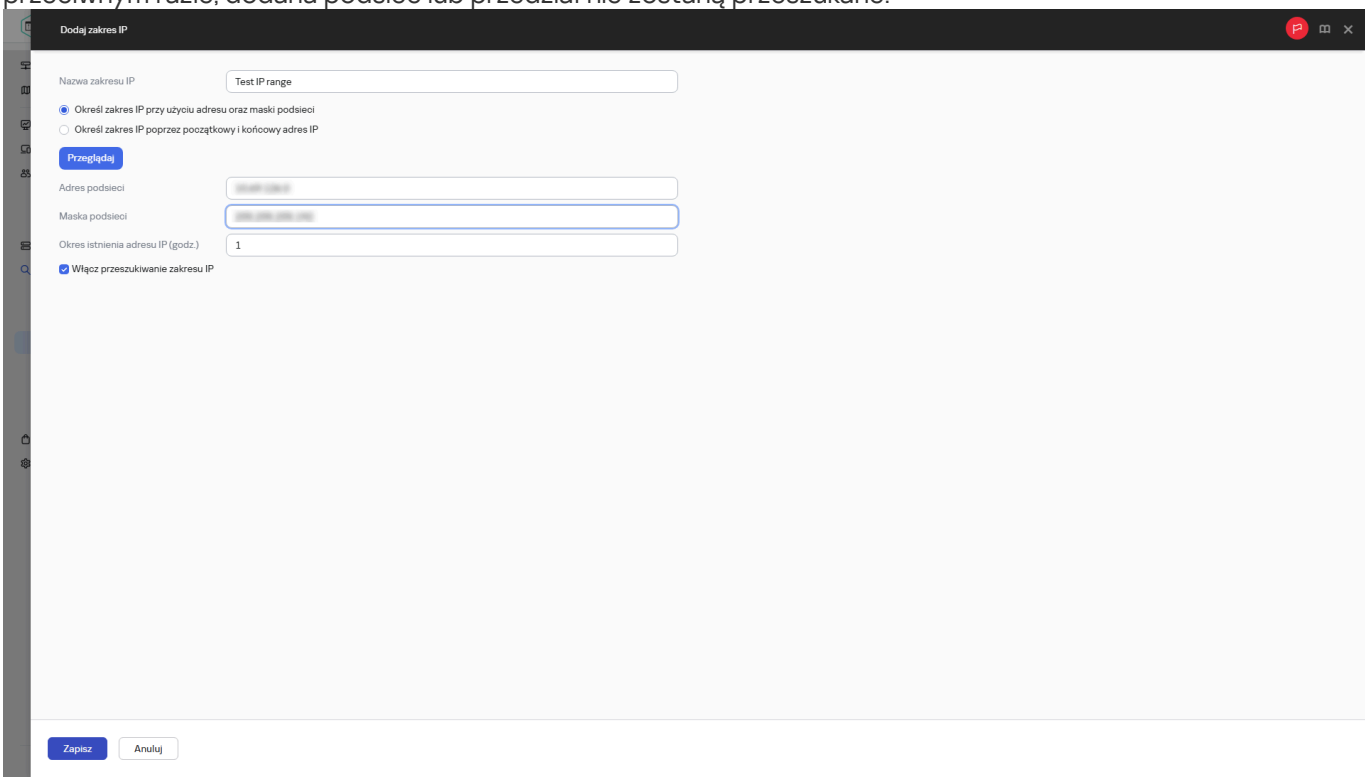
   - **Zakres IP lub adres podsieci i maska**

     Ustaw zakres IP, określając początkowy i końcowy adres IP lub adres podsieci i maskę podsieci. Możesz także wybrać jeden z już istniejących zakresów IP, klikając przycisk **Przeglądaj**.

   - **Okres istnienia adresu IP (godz.)**

     Podczas określania tego parametru upewnij się, że przekracza on czas przeszukiwania ustawiony w terminarzu przeszukiwania. Jeśli adres IP nie został zweryfikowany przez przeszukiwanie w trakcie czasu dzierżawy adresu IP, ten adres IP jest automatycznie usuwany z wyników przeszukiwania. Domyślnie, wyniki przeszukiwania są ważne 24 godziny, ponieważ dynamiczne adresy IP (przypisane przy użyciu Protokołu dynamicznej konfiguracji hosta (DHCP)) zmieniają się co 24 godziny.

4. Wybierz **Włącz przeszukiwanie zakresu IP**, jeśli chcesz przeszukać podsieć lub przedział, które dodałeś. W przeciwnym razie, dodana podsieć lub przedział nie zostaną przeszukane.



Określanie ustawień zakresu IP

5. Kliknij przycisk **Zapisz**.

   Nowy zakres IP jest dodawany do listy zakresów IP.

Możesz uruchomić przeszukiwanie każdego zakresu IP oddzielnie, korzystając z przycisku **Uruchom przeszukiwanie**. Domyślnie, wyniki przeszukiwania są ważne 24 godziny, co jest równe ustawieniu czasu dzierżawy adresu IP.

W celu dodania podsieci do istniejącego zakresu IP:

1. W menu głównym przejdź do **Wykrywanie i wdrażanie** → **Wykrywanie** → **Zakresy IP**.

2. Kliknij nazwę zakresu IP, do którego chcesz dodać podsieć.

3. W otwartym oknie kliknij przycisk **Dodaj**.

4. Określ podsieć, używając jej adresu i maski lub używając pierwszego i ostatniego adresu IP w zakresie IP. Lub dodaj istniejącą podsieć, klikając przycisk **Przeglądaj**.

5. Kliknij przycisk **Zapisz**.

   Nowa podsieć zostanie dodana do zakresu IP.

6. Kliknij przycisk **Zapisz**.

   Zostaną zapisane nowe ustawienia zakresu IP.

Możesz dodać tyle podsieci, ile potrzebujesz. Nazwane zakresy IP nie mogą się nakładać, ale nienazwane podsieci wewnątrz zakresu IP nie posiadają takich ograniczeń. Możesz włączać i wyłączać przeszukiwanie niezależnie dla każdego zakresu IP.

Przeszukiwanie Zeroconf

Ten typ przeszukiwania jest obsługiwany tylko w przypadku punktów dystrybucji opartych na systemie Linux.

Kaspersky Security Center Linux może przeszukiwać sieci, które mają urządzenia z adresami IPv6. W takim przypadku zakresy adresów IP nie są określone, a Kaspersky Security Center Linux przeszukuje całą sieć za pomocą zero-configuration networking (zwany również *Zeroconf*). Aby rozpocząć korzystanie z Zeroconf, musisz zainstalować narzędzie avahi-browse na urządzeniu z systemem Linux, które odpytuje sieci — Serwer administracyjny lub punkt dystrybucji.

W celu włączenia przeszukiwania Zeroconf:

1. W menu głównym przejdź do **Wykrywanie i wdrażanie** → **Wykrywanie** → **Zakresy IP**.
2. Kliknij przycisk **Właściwości**.
3. W otwartym oknie przełącz przycisk przełącznika **Użyj Zeroconf do przeszukania sieci IPv6**.

Następnie Kaspersky Security Center Linux zaczyna przeszukiwać sieć. W takim przypadku określone zakresy adresów IP są ignorowane.

Przeszukiwanie kontrolera domeny

Kaspersky Security Center Linux obsługuje przeszukiwanie następujących typów kontrolerów domeny:

- Microsoft Active Directory
- Samba
- FreeIPA
- ALD Pro

W przypadku kontrolera domeny Samba kontroler Samba 4 jest używany jako kontroler domeny Active Directory.

Kiedy przeszukujesz kontroler domeny, Serwer administracyjny lub punkt dystrybucji pobiera informacje o strukturze domeny, kontach użytkowników, grupach zabezpieczeń i nazwach DNS urządzeń znajdujących się w domenie.

Zalecamy korzystanie z przeszukiwania kontrolera domeny, jeśli wszystkie urządzenia sieciowe są członkami domeny. Jeśli niektóre urządzenia sieciowe nie znajdują się w domenie, nie można ich wykryć przez przeszukiwanie kontrolera domeny.

Wymagania wstępne

Przed odpytywaniem kontrolera domeny upewnij się, że zezwalasz na połączenia z kontrolerem domeny przez zaporę lub serwer proxy. Upewnij się także, że na kontrolerze domeny włączone są następujące protokoły:

- Lightweight Directory Access Protocol (LDAP)
- Simple Authentication and Security Layer (SASL)

  Protokół ten jest używany, jeśli połączenie z kontrolerem domeny jest nawiązywane przy użyciu uwierzytelniania SASL. Serwer administracyjny i punkty dystrybucji obsługują jedynie mechanizm DIGEST-MD5.
- Lightweight Directory Access Protocol over Secure Sockets Layer (LDAPS)

  Ten protokół jest używany, jeśli chcesz połączyć się z kontrolerem domeny za pomocą połączenia szyfrowanego.

Upewnij się, że na urządzeniu kontrolera domeny są dostępne następujące porty:

- 389 dla protokołu LDAP i prostego uwierzytelniania (w tym SASL)
- 636 w przypadku protokołu LDAPS

W przypadku systemów FreeIPA i ALD Pro protokoły LDAP i LDAPS są używane wyłącznie do przeszukiwania domeny. Kaspersky Security Center Linux nie obsługuje uwierzytelniania kont FreeIPA za pośrednictwem LDAP(S). Aby umożliwić użytkownikom FreeIPA i ALD Pro logowanie się do Web Console, należy skonfigurować uwierzytelnianie Kerberos za pośrednictwem usługi IAM.

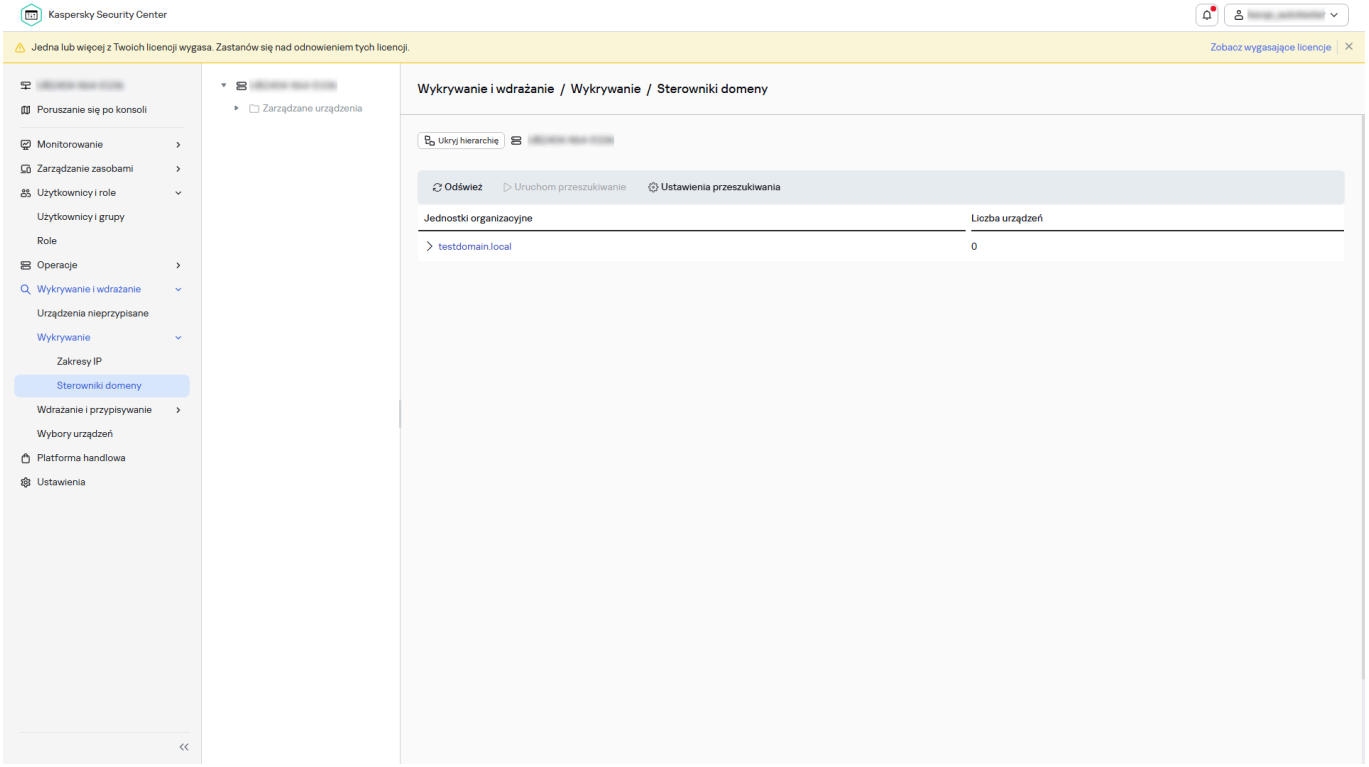
Dla wszystkich hostów z systemem Linux w ramach kontrolera domeny Microsoft Active Directory, Samba, FreeIPA, lub ALD Pro określ parametry `netbios name` i `workgroup` w pliku `/etc/samba/smb.conf`. W przeciwnym razie wyniki przeszukiwania mogą zawierać zduplikowane hosty.

Jeśli domena Microsoft Active Directory zawiera wiele kontrolerów domeny, wybór konkretnego kontrolera podczas przeszukiwania domeny nie jest obsługiwany. Połączenie jest nawiązywane z pierwszym wykrytym kontrolerem domeny. Aby zapewnić prawidłowe uwierzytelnianie w domenie Microsoft Active Directory, pole Alternatywna nazwa podmiotu (SAN) certyfikatu musi zawierać wszystkie adresy kontrolerów domeny należących do tej domeny, a także nazwę NetBIOS domeny Microsoft Active Directory.

Przeszukiwanie kontrolera domeny przy użyciu Serwera administracyjnego

Aby przeszukać kontroler domeny przy użyciu Serwera administracyjnego:

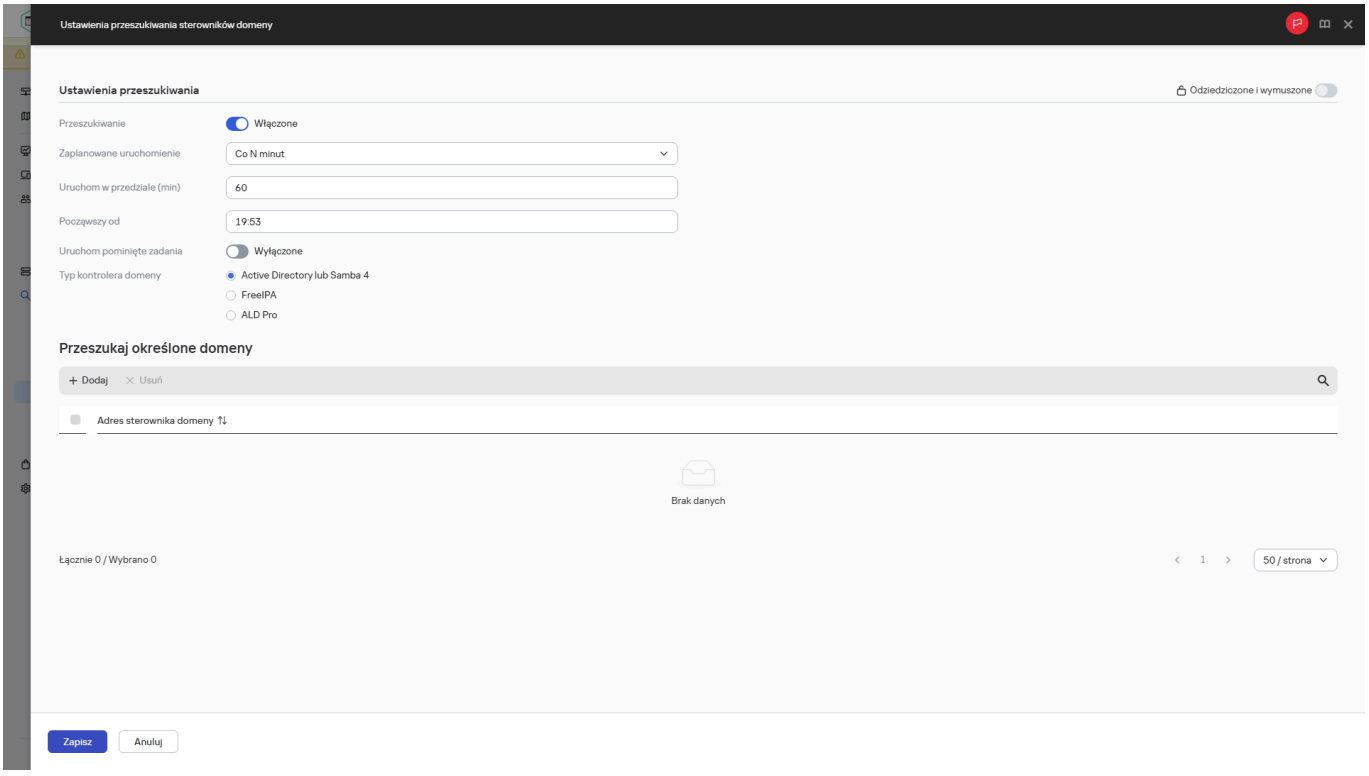
1. W menu głównym przejdź do **Wykrywanie i wdrażanie** → **Wykrywanie** → **Sterowniki domeny**.



Okno przeszukiwania kontrolera domeny

2. Kliknij **Konfiguruj ustawienia przeszukiwania**.

   Zostanie otwarte okno **Ustawienia przeszukiwania sterowników domeny**.



Ustawienia przeszukiwania kontrolera domeny

3. W polu **Przeszukiwanie** przełącz przycisk przełącznika na pozycję **Włączone**.

4. W polu **Przeszukaj określone domeny** kliknij przycisk **Dodaj**, a następnie określ adres i dane uwierzytelniające użytkownika kontrolera domeny.

5. W oknie **Ustawienia przeszukiwania sterowników domeny** wykonaj następujące czynności:

   - Wybierz typ kontrolera domeny, który ma zostać przeszukany: **Active Directory lub Samba 4**, **FreeIPA**, **ALD Pro**.

   - Jeśli to konieczne, określ harmonogram przeszukiwania. Domyślny przedział czasu wynosi jedną godzinę. Dane otrzymane przy kolejnym przeszukiwaniu całkowicie zastępują starsze dane.

     Dostępne są następujące opcje terminarza przeszukiwania:

     - **Co N dni**

       Przeszukiwanie odbywa się regularnie, w określonych przedziałach czasu, począwszy od określonego dnia i godziny.

       Domyślnie, przeszukiwanie jest uruchamiane codziennie, począwszy od bieżącej daty i godziny systemowej.

     - **Co N minut**

       Przeszukiwanie odbywa się regularnie, w określonych przedziałach czasu, począwszy od określonego czasu.

     - **Według dni tygodnia**

       Przeszukiwanie odbywa się regularnie, w określone dni tygodnia i o określonej godzinie.

     - **Miesięcznie wybranego dnia tygodnia**

       Przeszukiwanie odbywa się regularnie, w określone dni miesiąca i o określonej godzinie.

     - **Uruchom pominięte zadania**

       Jeśli Serwer administracyjny jest wyłączony lub niedostępny w czasie, dla którego zaplanowane jest przeszukiwanie, Serwer administracyjny może uruchomić przeszukiwanie od razu po jego włączeniu lub odczekać do następnego zaplanowanego przeszukiwania.

       Jeśli ta opcja jest włączona, Serwer administracyjny rozpoczyna przeszukiwanie od razu po jego włączeniu.

       Jeśli ta opcja jest wyłączona, Serwer administracyjny odczekuje do następnego zaplanowanego przeszukiwania.

       Domyślnie opcja ta jest wyłączona.

Jeśli zmienisz konta użytkowników w grupie zabezpieczeń domeny, zmiany te zostaną wyświetlone w Kaspersky Security Center Linux godzinę po przeszukiwaniu kontrolera domeny.

6. Kliknij **Zapisz**, aby zastosować zmiany.

7. Jeśli chcesz przeprowadzić przeszukiwanie natychmiast, kliknij przycisk **Uruchom przeszukiwanie**.

Przeszukiwanie kontrolera domeny przy użyciu punktu dystrybucji

Można również przeszukiwać kontroler domeny, korzystając z punktu dystrybucji. Zarządzane urządzenie z systemem Windows lub Linux może działać jako punkt dystrybucji.

W przypadku punktu dystrybucji z systemem Linux obsługiwane jest przeszukiwanie wszystkich typów kontrolerów domeny.
W przypadku punktu dystrybucji z systemem Windows obsługiwane jest tylko przeszukiwanie kontrolera domeny Microsoft Active Directory.
Przeszukiwanie przy użyciu punktu dystrybucji na komputerze Mac nie jest obsługiwane.

Aby skonfigurować przeszukiwanie kontrolera domeny przy użyciu punktu dystrybucji:

1. Otwórz właściwości punktu dystrybucji.
2. Wybierz sekcję **Przeszukiwanie sterowników domeny**.
3. W polu **Przeszukiwanie** przełącz przycisk przełącznika na pozycję **Włączone**.
4. Jeżeli używasz punktu dystrybucji Linux, wybierz typ kontrolera domeny, który ma zostać przeszukany: **Active Directory lub Samba 4**, **FreeIPA**, **ALD Pro**.

   Nie jest konieczne określanie tego samego typu kontrolera domeny podczas konfigurowania przeszukiwania za pomocą punktu dystrybucji i za pomocą Serwera administracyjnego.
5. Wybierz kontroler domeny, który chcesz przeszukać.

   Jeśli korzystasz z punktu dystrybucji systemu Linux, w sekcji **Przeszukaj określone domeny** kliknij opcję **Dodaj**, a następnie określ adres i dane uwierzytelniające użytkownika kontrolera domeny.

   Jeśli korzystasz z punktu dystrybucji systemu Windows, możesz wybrać jedną z następujących opcji:

   - **Przeszukaj bieżącą domenę**
   - **Przeszukaj cały las domeny**
   - **Przeszukaj określone domeny**
6. Kliknij przycisk **Ustaw terminarz przeszukiwania**, aby w razie potrzeby określić opcje terminarza przeszukiwania.

   Przeszukiwanie rozpoczyna się wyłącznie zgodnie z określonym terminarzem. Ręczne rozpoczęcie przeszukiwania nie jest dostępne.

Po zakończeniu przeszukiwania struktura domeny zostanie wyświetlona w sekcji **Sterowniki domeny**.

Jeśli skonfigurowałeś i włączyłeś reguły przenoszenia urządzeń, nowo wykryte urządzenia są automatycznie umieszczane w grupie **Zarządzane urządzenia**. Jeśli nie włączono żadnych reguł przenoszenia, nowo wykryte urządzenia zostają automatycznie uwzględnione w grupie **Urządzenia nieprzypisane**.

Wykryte konta użytkowników można wykorzystać do uwierzytelnienia domeny w Kaspersky Security Center Web Console.

Uwierzytelnianie i połączenie z kontrolerem domeny

Uwierzytelnianie i połączenie z kontrolerem domeny podczas przeszukiwania domeny

Podczas przeszukiwania kontrolera domeny Serwer administracyjny lub punkt dystrybucji identyfikuje protokół połączenia w celu nawiązania początkowego połączenia z kontrolerem domeny. Protokół ten będzie używany do wszystkich przyszłych połączeń z kontrolerem domeny. Podczas nawiązywania początkowego połączenia z kontrolerem domeny można zmienić opcje połączenia, korzystając z flag Agenta sieciowego (`KLNAG_LDAP_TLS_REQCERT` i `KLNAG_LDAP_SSL_CACERT`). Flagi Agenta sieciowego można skonfigurować za pomocą polecenia klscflag, zgodnie z opisem w tym artykule.

Początkowe połączenie z kontrolerem domeny przebiega w następujący sposób:

1. Serwer administracyjny lub punkt dystrybucji próbuje połączyć się z kontrolerem domeny poprzez protokół LDAPS.

   Domyślnie weryfikacja certyfikatu nie jest wymagana. Ustaw flagę `KLNAG_LDAP_TLS_REQCERT` na 1, aby wymusić weryfikację certyfikatu.

   Możliwe wartości flagi `KLNAG_LDAP_TLS_REQCERT`:

   - `0`—Żądano certyfikatu, ale jeśli nie został on dostarczony lub weryfikacja certyfikatu nie powiodła się, połączenie TLS nadal uważa się za pomyślnie utworzone (wartość domyślna).
   - `1`—Wymagana jest ścisła weryfikacja certyfikatu serwera LDAP.

   Domyślnie, w przypadku gdy flaga `KLNAG_LDAP_SSL_CACERT` nie jest określona, do uzyskania dostępu do łańcucha certyfikatów używana jest ścieżka do urzędu certyfikacji (CA) zależna od systemu operacyjnego. Użyj flagi `KLNAG_LDAP_SSL_CACERT`, aby określić ścieżkę niestandardową.

2. Jeżeli połączenie LDAPS nie powiedzie się, Serwer administracyjny lub punkt dystrybucji podejmie próbę połączenia się z kontrolerem domeny poprzez nieszyfrowane połączenie TCP przy użyciu protokołu SASL (DIGEST-MD5).

Uwierzytelnianie i połączenie z kontrolerem domeny podczas uwierzytelniania użytkownika domeny na Serwerze administracyjnym

Kiedy użytkownik domeny uwierzytelnia się na Serwerze administracyjnym, Serwer administracyjny identyfikuje protokół w celu nawiązania połączenia z kontrolerem domeny.

W przypadku systemów FreeIPA i ALD Pro protokoły LDAP i LDAPS są używane wyłącznie do przeszukiwania domeny. Kaspersky Security Center Linux nie obsługuje uwierzytelniania kont FreeIPA za pośrednictwem LDAP(S). Aby umożliwić użytkownikom FreeIPA i ALD Pro logowanie się do Web Console, należy skonfigurować uwierzytelnianie Kerberos za pośrednictwem usługi IAM.

Połączenie z kontrolerem domeny przebiega w następujący sposób:

1. Serwer administracyjny próbuje połączyć się z kontrolerem domeny poprzez protokół LDAPS.

   Wymagana jest ścisła weryfikacja certyfikatu serwera LDAP.

   Domyślnie, w przypadku gdy flaga `KLNAG_LDAP_SSL_CACERT` nie jest określona, do uzyskania dostępu do łańcucha certyfikatów używana jest ścieżka do urzędu certyfikacji (CA) zależna od systemu operacyjnego. Użyj flagi `KLNAG_LDAP_SSL_CACERT`, aby określić ścieżkę niestandardową.

2. Jeśli połączenie LDAPS nie powiedzie się, wystąpi błąd podczas łączenia z kontrolerem domeny i inne protokoły połączenia nie będą używane.

Konfiguracja flag

Do konfigurowania flag można użyć narzędzia klscflag.

Uruchom wiersz poleceń, a następnie zmień bieżący katalog na katalog z narzędziem klscflag. Na urządzeniu Serwera administracyjnego narzędzie klscflag znajduje się w katalogu instalacyjnym. Domyślna ścieżka instalacji to /opt/kaspersky/ksc64/sbin.

Na przykład następujące polecenie wymusza weryfikację certyfikatu:

```
klscflag -fset -pv klnagent -n KLNAG_LDAP_TLS_REQCERT -t d -v 1
```

Konfigurowanie kontrolera domeny Samba

Kaspersky Security Center Linux obsługuje kontroler domeny Linux działający tylko w systemie Samba 4.

Kontroler domeny Samba obsługuje te same rozszerzenia schematu, co kontroler domeny Microsoft Active Directory. Można włączyć pełną kompatybilność kontrolera domeny Samba z kontrolerem domeny Microsoft Active Directory, używając rozszerzenia schematu Samba 4. Jest to akcja opcjonalna.

> Zalecamy włączenie pełnej kompatybilności kontrolera domeny Samba z kontrolerem domeny Microsoft Active Directory. Zapewni to poprawną interakcję pomiędzy Kaspersky Security Center Linux a kontrolerem domeny Samba.

Aby włączyć pełną kompatybilność kontrolera domeny Samba z kontrolerem domeny Microsoft Active Directory:

1. Wykonaj następujące polecenie, aby użyć rozszerzenia schematu RFC2307:

   ```
   samba-tool domain provision --use-rfc2307 --interactive
   ```

2. Włącz aktualizację schematu w kontrolerze domeny Samba. W tym celu, do pliku `/etc/samba/smb.conf` dodaj następujący wiersz:

   ```
   dsdb:schema update allowed = true
   ```

   > Jeśli aktualizacja schematu zakończy się błędem, należy wykonać pełne przywrócenie kontrolera domeny pełniącego funkcję głównego schematu.

Dla wszystkich hostów z systemem Linux w ramach kontrolera domeny Samba określ parametry `netbios name` i `workgroup` w pliku `/etc/samba/smb.conf`. W przeciwnym razie wyniki przeszukiwania mogą zawierać zduplikowane hosty.

Inwentaryzacja sprzętu

Lista sprzętu (**Zarządzanie zasobami** → **Sprzęt**), której używasz do przeprowadzenia inwentaryzacji sprzętu, jest uzupełniana na dwa sposoby: automatycznie i ręcznie. Po każdym przeszukaniu sieci, wszystkie wykryte urządzenia zostają dodane do listy automatycznie; jednakże możesz także ręcznie dodać urządzenia, jeśli nie chcesz przeszukiwać sieci. Możesz ręcznie dodać inne urządzenia do listy, na przykład, routery, drukarki lub sprzęt komputerowy.

We właściwościach urządzenia możesz wyświetlić i zmodyfikować szczegółowe informacje o tym urządzeniu.

Lista sprzętu może zawierać następujące typy urządzeń:

- Komputery
- Urządzenia mobilne
- Urządzenia sieciowe
- Urządzenia wirtualne
- Składniki OEM
- Peryferia komputerowe
- Podłączone urządzenia
- Telefony VoIP
- Repozytoria sieciowe

Administrator może przypisać atrybut *Sprzęt firmowy* do wykrytych urządzeń. Ten atrybut jest przypisywany ręcznie we właściwościach urządzenia, administrator może również określić kryteria automatycznego przypisywania dla tego atrybutu. W takim przypadku atrybut *Sprzęt firmowy* jest przypisywany zgodnie z typem urządzenia.

Kaspersky Security Center Linux pozwala na wyrejestrowywanie sprzętu. W tym celu wybierz opcję **Wyrejestrowane** we właściwościach urządzenia. Takie urządzenie nie jest wyświetlane na liście sprzętu.

Administrator może zarządzać listą programowalnych sterowników logicznych (PLC) w folderze **Sprzęt**. Szczegółowe informacje na temat zarządzania listą PLC można znaleźć w *podręczniku użytkownika dla Kaspersky Industrial CyberSecurity for Nodes*.

Dodawanie informacji o nowych urządzeniach

W celu dodania informacji o nowych urządzeniach w sieci:

1. W menu głównym przejdź do **Zarządzanie zasobami** → **Sprzęt**.
2. Kliknij przycisk **Dodaj**, aby otworzyć okno **Nowe urządzenie**.
3. W oknie **Nowe urządzenie**, na liście rozwijalnej **Typ urządzenia** wybierz typ urządzenia, które chcesz dodać.
4. Kliknij **OK**.

   Okno właściwości urządzenia zostanie otwarte na sekcji **Ogólne**.
5. W sekcji **Ogólne** wypełnij pola wejściowe danymi urządzenia. Sekcja **Ogólne** wyświetla następujące ustawienia:
   - **Urządzenie firmowe**. Zaznacz to pole, jeśli chcesz przypisać atrybut *Firmowy* do urządzenia. Przy użyciu tego atrybutu można wyszukiwać urządzenia w folderze **Sprzęt**.
   - **Wyrejestrowane**. Zaznacz pole, jeśli nie chcesz, aby urządzenie było wyświetlane na liście urządzeń w folderze **Sprzęt**.
6. Kliknij **Zastosuj**.

Nowe urządzenie będzie wyświetlane w obszarze roboczym strony **Sprzęt**.

Konfigurowanie kryteriów wykorzystywanych do określania urządzeń firmowych

W celu skonfigurowania kryteriów wykrywania dla urządzeń firmowych:

1. W menu głównym przejdź do **Zarządzanie zasobami** → **Sprzęt**.
2. Na górze strony **Sprzęt** kliknij łącze **Ustaw regułę dla urządzeń firmowych**.

   Wywołany zostanie panel **Ustaw regułę dla urządzeń firmowych**.
3. W panelu **Ustaw regułę dla urządzeń firmowych** włącz opcję **Ustaw dla urządzenia atrybut urządzenie firmowego automatycznie**. Określ typy urządzeń, do których atrybut *firmowy* jest przypisywany automatycznie.

   > Ta opcja dotyczy tylko urządzeń, które zostały dodane przez przeszukiwanie sieci. W przypadku urządzeń dodanych ręcznie ustaw atrybut *Firmowy* ręcznie.
4. Kliknij **OK**.

Skonfigurowano kryteria wykrywania dla urządzeń firmowych.

Używanie dynamicznego trybu VDI na urządzeniach klienckich

Wirtualna infrastruktura może zostać wdrożona w sieci firmowej z użyciem tymczasowych maszyn wirtualnych. Kaspersky Security Center Linux wykrywa tymczasowe maszyny wirtualne i dodaje o nich informacje do bazy danych Serwera administracyjnego. Gdy użytkownik zakończy korzystanie z tymczasowej maszyny wirtualnej, maszyna ta jest usuwana z wirtualnej infrastruktury. Wpis dotyczący usuniętej maszyny wirtualnej może być zapisany w bazie danych Serwera administracyjnego. W Kaspersky Security Center Web Console mogą być również wyświetlane nieistniejące maszyny wirtualne.

Aby informacje o nieistniejących maszynach wirtualnych nie były zapisywane, Kaspersky Security Center Linux obsługuje tryb dynamiczny obsługi Virtual Desktop Infrastructure (VDI). Administrator może włączyć obsługę trybu dynamicznego dla VDI we właściwościach pakietu instalacyjnego Agenta sieciowego instalowanego na tymczasowej maszynie wirtualnej.

Jeśli tymczasowa maszyna wirtualna jest wyłączona, Agent sieciowy informuje Serwer administracyjny o jej wyłączeniu. Po pomyślnym wyłączeniu maszyny wirtualnej jest ona usuwana z listy urządzeń podłączonych do Serwera administracyjnego. Jeśli wyłączenie maszyny wirtualnej zakończyło się błędami, a Agent sieciowy nie wysłał do Serwera administracyjnego powiadomienia o wyłączonej maszynie wirtualnej, wdrażany jest scenariusz kopii zapasowej. W tym scenariuszu maszyna wirtualna jest usuwana z listy urządzeń podłączonych do Serwera administracyjnego po trzech niepomyślnych próbach synchronizacji z Serwerem administracyjnym.

Włączanie dynamicznego trybu VDI we właściwościach pakietu instalacyjnego Agenta sieciowego

W celu włączenia dynamicznego trybu VDI:

1. W menu głównym przejdź do **Zarządzanie oprogramowaniem** → **Pakiety instalacyjne**.
2. Z menu kontekstowego pakietu instalacyjnego Agenta sieciowego wybierz **Właściwości**.
   Zostanie otwarte okno **Właściwości**.
3. W oknie **Właściwości** wybierz sekcję **Zaawansowane**.
4. W sekcji **Zaawansowane** wybierz opcję **Włącz tryb dynamiczny VDI**.

Urządzenie, na którym ma zostać zainstalowany Agent sieciowy, staje się częścią VDI.

Przenoszenie urządzeń z VDI do grupy administracyjnej

W celu przeniesienia urządzeń będących częścią VDI do grupy administracyjnej:

1. Przejdź do opcji **Zarządzanie zasobami** → **Reguły przenoszenia**.
2. Kliknij **Dodaj**.
3. Na karcie **Warunki reguły** wybierz kartę **Maszyny wirtualne**.

4. Ustaw regułę **Jest maszyną wirtualną** na **Tak** oraz **Część Virtual Desktop Infrastructure** na **Tak.**

5. Kliknij **Zapisz**.

Zarządzanie urządzeniami klienckimi

Kaspersky Security Center Linux umożliwia zarządzanie urządzeniami klienckimi:

- Przeglądaj ustawienia i stany zarządzanych urządzeń, w tym klastrów i macierzy serwerów.
- Konfiguruj punkty dystrybucji.
- Zarządzaj zadaniami.

Za pomocą grup administracyjnych można łączyć urządzenia klienckie w zestaw, którym można zarządzać jak pojedynczą jednostką. Urządzenie klienckie może należeć tylko do jednej grupy administracyjnej. Urządzenia mogą być automatycznie przydzielane do grupy na podstawie **Warunki reguły**:

- Tworzenie reguł przenoszenia urządzeń.
- Kopiowanie reguł przenoszenia urządzeń.
- Warunki dla reguły przenoszenia urządzeń.

Możesz użyć opcji wyboru urządzeń, aby filtrować urządzenia na podstawie określonego warunku. Można również oznaczać urządzenia znacznikami w celu tworzenia selekcji, wyszukiwania urządzeń i przydzielania urządzeń grupom administracyjnym.

Ustawienia zarządzanego urządzenia

W celu sprawdzenia ustawień zarządzanego urządzenia:

1. W menu głównym przejdź do **Zarządzanie zasobami** → **Zasoby (urządzenia)**.

   Zostanie wyświetlona lista zarządzanych urządzeń.

2. Na liście zarządzanych urządzeń, kliknij odnośnik z nazwą żądanego urządzenia.

Zostanie wyświetlone okno właściwości wybranego urządzenia.

W górnej części okna właściwości wyświetlane są następujące zakładki reprezentujące główne grupy ustawień:

- **Ogólne**

  Ta zakładka zawiera następujące sekcje:

  - Sekcja **Ogólne** wyświetla ogólne informacje o urządzeniu klienckim. Informacje są dostarczane w oparciu o dane otrzymane podczas ostatniej synchronizacji urządzenia klienckiego z Serwerem administracyjnym:

    - **Nazwa**

      W tym polu możesz wyświetlić i zmodyfikować nazwę urządzenia klienckiego w grupie administracyjnej.

    - **Opis**

      W tym polu możesz wprowadzić dodatkowy opis urządzenia klienckiego.

- **Stan urządzenia**

  Stan urządzenia klienckiego przypisany w oparciu o kryteria zdefiniowane przez administratora dla stanu ochrony antywirusowej na urządzeniu i aktywności urządzenia w sieci.

- **Właściciel urządzenia**

  Nazwa właściciela urządzenia. Możesz przypisać lub usunąć użytkownika jako właściciela urządzenia, klikając łącze **Zarządzaj właścicielem urządzenia**.

- **Pełna nazwa grupy**

  Grupa administracyjna zawierająca urządzenie klienckie.

- **Ostatnia aktualizacja antywirusowych baz danych**

  Data ostatniej aktualizacji antywirusowych baz danych lub aplikacji na urządzeniu.

- **Połączono z Serwerem administracyjnym**

  Data i godzina ostatniego połączenia Agenta sieciowego, zainstalowanego na urządzeniu klienckim, z Serwerem administracyjnym.

- **Ostatnio dostępny**

  Data i godzina, gdy urządzenie było ostatnio widoczne w sieci.

- **Wersja Agenta sieciowego**

  Wersja zainstalowanego Agenta sieciowego.

- **Utworzono**

  Data utworzenia urządzenia w Kaspersky Security Center Linux.

- **Nie odłączaj od Serwera administracyjnego**

  Jeśli ta opcja jest włączona, utrzymywana jest ciągła łączność pomiędzy zarządzanym urządzeniem a Serwerem administracyjnym. Możesz użyć tej opcji, jeśli nie używasz serwerów push, które zapewniają taką łączność.

  Jeśli ta opcja jest wyłączona, a serwery push nie są używane, zarządzane urządzenie będzie nawiązywało połączenie z Serwerem administracyjnym jedynie w celu synchronizacji danych lub przesłania informacji.

  Maksymalna całkowita liczba urządzeń z wybraną opcją **Nie odłączaj od Serwera administracyjnego** to 300.

  Ta opcja jest wyłączona domyślnie na zarządzanych urządzeniach. Ta opcja jest włączona domyślnie na urządzeniu, na którym jest zainstalowany Serwer administracyjny i pozostaje włączona nawet w przypadku próby jej wyłączenia.

- **Sesje**

  W tej sekcji znajduje się tabela z informacjami o użytkownikach aktualnie zalogowanych na urządzeniu. Tabela wyświetla następujące dane w odpowiednich kolumnach:

  - Nazwa użytkownika
  - Nazwa konta SAM

- Nazwa główna użytkownika
- Adres e-mail

Aby poprawnie wyświetlić informacje o sesjach użytkowników domeny, należy skorzystać z funkcji przeszukiwania kontrolera domeny.

- Sekcja **Sieć** wyświetla następujące informacje o właściwościach sieci urządzenia klienckiego:
  - **Adres IP**

    Adres IP urządzenia.
  - **Domena Windows**

    Grupa robocza zawierająca urządzenie.
  - **Nazwa DNS**

    Nazwa domeny DNS urządzenia klienckiego.
  - **Nazwa NetBIOS**

    Nazwa urządzenia klienckiego.
  - **Adres IPv6**
- Sekcja **System** zawiera informacje o systemie operacyjnym zainstalowanym na urządzeniu klienckim:
  - **System operacyjny**
  - **Architektura procesora**
  - **Nazwa urządzenia**
  - **Typ maszyny wirtualnej**

    Producent maszyny wirtualnej.
  - **Dynamiczna maszyna wirtualna jako część VDI**

    Ten wiersz pokazuje, czy urządzenie klienckie jest dynamiczną maszyną wirtualną w ramach VDI.
- Sekcja **Ochrona** zawiera informacje o bieżącym stanie ochrony antywirusowej na urządzeniu klienckim:
  - **Widoczny**

    Stan widoczności urządzenia klienckiego.
  - **Stan urządzenia**

    Stan urządzenia klienckiego przypisany w oparciu o kryteria zdefiniowane przez administratora dla stanu ochrony antywirusowej na urządzeniu i aktywności urządzenia w sieci.
  - **Opis stanu**

    Stan ochrony urządzenia klienckiego i połączenia z Serwerem administracyjnym.

- **Stan ochrony**

  To pole wyświetla bieżący stan ochrony urządzenia klienckiego w czasie rzeczywistym.

  Jeśli stan zmieni się na urządzeniu, nowy stan zostanie wyświetlony w oknie właściwości urządzenia dopiero po zsynchronizowaniu urządzenia klienckiego z Serwerem administracyjnym.

- **Ostatnie pełne skanowanie**

  Data i godzina ostatniego skanowania w poszukiwaniu szkodliwego oprogramowania przeprowadzonego na urządzeniu klienckim.

- **Wykryto wirusa**

  Całkowita liczba zagrożeń wykrytych na urządzeniu klienckim od momentu zainstalowania aplikacji zabezpieczającej (pierwsze skanowanie) lub od momentu ostatniego zresetowania licznika zagrożeń.

- **Obiekty, których leczenie nie powiodło się**

  Liczba nieprzetworzonych plików na urządzeniu klienckim.

  To pole ignoruje liczbę nieprzetworzonych plików na urządzeniach mobilnych.

- **Stan szyfrowania dysku**

  Bieżący stan szyfrowania plików na lokalnych dyskach urządzenia. Opis statusów znajduje się w pomocy Kaspersky Endpoint Security for Windows.

  Pliki mogą być szyfrowane tylko na zarządzanych urządzeniach, na których jest zainstalowany Kaspersky Endpoint Security for Windows.

- Sekcja **Stan urządzenia zdefiniowany przez aplikację** zawiera informacje o stanie urządzenia zdefiniowanym przez zarządzaną aplikację zainstalowaną na urządzeniu. Ten stan urządzenia może różnić się od stanu zdefiniowanego przez Kaspersky Security Center Linux.

- **Aplikacje**

  Na tej karcie znajdują się wszystkie aplikacje Kaspersky zainstalowane na urządzeniu klienckim. Ta karta zawiera przyciski **Uruchom** i **Zatrzymaj** umożliwiające uruchomienie i zatrzymanie wybranej aplikacji Kaspersky (z wyłączeniem Agenta sieciowego). Można użyć tych przycisków, jeśli na zarządzanym urządzeniu dostępny jest port UDP o numerze 15000 do odbierania powiadomień push z Serwera administracyjnego. Jeśli zarządzane urządzenie nie jest dostępne dla powiadomień push, ale włączony jest tryb ciągłego połączenia z Serwerem administracyjnym (włączona jest opcja **Nie odłączaj od Serwera administracyjnego** w sekcji **Ogólne**), dostępne są również przyciski **Uruchom** i **Zatrzymaj**. W przeciwnym wypadku podczas próby uruchomienia lub zatrzymania aplikacji wyświetlany jest komunikat o błędzie. Możesz kliknąć nazwę aplikacji, aby wyświetlić ogólne informacje o aplikacji, listę zdarzeń, które wystąpiły na urządzeniu oraz ustawienia aplikacji.

- **Aktywne zasady i profile zasad**

  Ta karta zawiera listę zasad i profili zasad, które są aktualnie przypisane do zarządzanego urządzeniu.

- **Zadania**

  W zakładce **Zadania** możesz zarządzać zadaniami urządzenia klienckiego: przeglądać listę istniejących zadań, tworzyć nowe zadania, usuwać, uruchamiać i zatrzymywać zadania, a także modyfikować ustawienia zadań i przeglądać wyniki ich wykonania. Lista zadań jest tworzona w oparciu o dane otrzymane w czasie ostatniej synchronizacji komputera klienckiego z Serwerem administracyjnym. Serwer administracyjny żąda od urządzenia klienckiego szczegółów dotyczących stanu zadania. Jeżeli na zarządzanym urządzeniu dostępny jest port UDP o numerze 15000 do odbierania powiadomień push o otrzymaniu danych z Serwera administracyjnego, wyświetlany jest status zadania i włączane są przyciski umożliwiające zarządzanie zadaniem. Jeśli serwer push nie może uzyskać dostępu do zarządzanego urządzenia, ale włączony jest tryb ciągłego połączenia z Serwerem administracyjnym (włączona jest opcja **Nie odłączaj od Serwera administracyjnego** w sekcji **Ogólne**), dostępne są również akcje z zadaniami.

  Jeśli połączenie nie zostanie nawiązane, stan nie będzie wyświetlany.

- **Zdarzenia**

  Zakładka **Zdarzenia** wyświetla zdarzenia zarejestrowane na Serwerze administracyjnym dla wybranego urządzenia klienckiego.

  Możesz eksportować, kopiować i usuwać zdarzenia urządzenia.

- **Incydenty związane z bezpieczeństwem**

  Na zakładce **Incydenty związane z bezpieczeństwem** możesz przejrzeć, zmodyfikować i utworzyć incydenty związane z bezpieczeństwem dla urządzenia klienckiego. Problemy bezpieczeństwa mogą być tworzone automatycznie poprzez zarządzane aplikacje firmy Kaspersky zainstalowane na urządzeniu klienckim, a także ręcznie przez administratora. Na przykład, jeśli niektórzy użytkownicy regularnie przenoszą szkodliwe oprogramowanie ze swoich nośników wymiennych na urządzenia, administrator może utworzyć problem bezpieczeństwa. W treści problemu bezpieczeństwa administrator może dostarczyć krótki opis przypadku oraz zalecane działania (na przykład działania dyscyplinarne wobec użytkownika), a także dodać odsyłacz.

  Problem bezpieczeństwa, dla którego zostały wykonane wszystkie wymagane działania, nazywane jest *przetworzonym*. Obecność nieprzetworzonych problemów bezpieczeństwa może zostać wybrana jako warunek zmiany stanu urządzenia na *Krytyczny* lub *Ostrzeżenie*.

  Ta sekcja zawiera listę problemów bezpieczeństwa, które zostały utworzone dla urządzenia. Problemy bezpieczeństwa są klasyfikowane według priorytetu i typu. Typ incydentu związanego z bezpieczeństwem jest definiowany przez aplikację Kaspersky, która utworzyła incydent związany z bezpieczeństwem. Możesz podświetlić przetworzone zdarzenia na liście, zaznaczając pole w kolumnie **Przetworzone**.

- **Znaczniki**

  W zakładce **Znaczniki** możesz zarządzać listą słów kluczowych, które są używane podczas wyszukiwania urządzeń klienckich: przejrzeć listę istniejących znaczników, przypisać znaczniki z listy, skonfigurować reguły automatycznego oznaczania oraz dodać nowe znaczniki i zmienić nazwy starszych znaczników, a także usunąć znaczniki.

- **Zaawansowane**

  Ta zakładka zawiera następujące sekcje:

  - **Rejestr aplikacji**. W tej sekcji możesz przejrzeć rejestr aplikacji zainstalowanych na urządzeniu klienckim i ich uaktualnień, a także możesz skonfigurować wyświetlanie rejestru aplikacji.

    Informacje o zainstalowanych aplikacjach są dostępne, jeśli Agent sieciowy zainstalowany na urządzeniu klienckim prześle żądane informacje do Serwera administracyjnego. Możesz skonfigurować przesyłanie informacji do Serwera administracyjnego w oknie właściwości Agenta sieciowego lub jego zasady, w sekcji **Repozytoria**.

    Kliknięcie nazwy aplikacji powoduje otwarcie okna zawierającego szczegółowe informacje o aplikacji oraz listę pakietów aktualizacji zainstalowanych dla aplikacji.

- **Pliki wykonywalne**. Ta sekcja wyświetla pliki wykonywalne wykryte na urządzeniu klienckim.
- **Punkty dystrybucji**. Ta sekcja zawiera listę punktów dystrybucji, z którymi urządzenie komunikuje się.
  - **Eksportuj do pliku**

    Kliknij przycisk **Eksportuj do pliku**, aby zapisać do pliku listę punktów dystrybucji, z którymi urządzenie komunikuje się. Domyślnie aplikacja eksportuje listę urządzeń do pliku CSV.
  - **Właściwości**

    Kliknij przycisk **Właściwości**, aby przejrzeć i skonfigurować punkt dystrybucji, z którym urządzenie komunikuje się.
- **Rejestr sprzętu**. W tej sekcji możesz wyświetlić informacje o sprzęcie zainstalowanym na urządzeniu klienckim.

  Jeżeli Agent sieciowy jest zainstalowany na urządzeniu z systemem Windows, wysyła on do Serwera administracyjnego następujące informacje o sprzęcie urządzenia:

  - Pamięć RAM
  - Urządzenia pamięci masowej
  - Płyta główna
  - Procesor
  - Karty sieciowe
  - Monitory
  - Karta graficzna
  - Karta dźwiękowa

  Jeżeli Agent sieciowy jest zainstalowany na urządzeniu z systemem Linux lub macOS, wysyła on do Serwera administracyjnego następujące informacje o sprzęcie urządzenia, jeżeli informacje te są dostarczane przez system operacyjny:

  - Całkowita ilość pamięci RAM
  - Całkowita pojemność urządzeń pamięci masowej
  - Płyta główna
  - Procesor
  - Karty sieciowe
- **Dostępne aktualizacje**. Sekcja ta wyświetla listę aktualizacji oprogramowania znajdujących się na tym urządzeniu, ale jeszcze nie zainstalowanych.
- **Luki w oprogramowaniu**. Ta sekcja zawiera informacje o lukach w aplikacjach firm trzecich zainstalowanych na urządzeniach klienckich.

  Aby zapisać luki w pliku, zaznacz pola wyboru obok luk, które chcesz zapisać, a następnie kliknij przycisk **Eksportuj do pliku CSV** lub przycisk **Eksportuj do pliku TXT**.

Ta sekcja zawiera następujące ustawienia:

- **Pokaż tylko luki, które można naprawić**

  Jeśli ta opcja jest włączona, sekcja wyświetla luki, które można naprawić przy użyciu poprawki.

  Jeśli ta opcja jest wyłączona, sekcja wyświetla luki, które można wyeliminować przy użyciu poprawki, oraz luki, dla których nie opublikowano poprawki.

  Domyślnie opcja ta jest włączona.

- **Właściwości luki**

  Na liście kliknij nazwę luki w oprogramowaniu, aby przejrzeć właściwości wybranej luki w oprogramowaniu w oddzielnym oknie. W oknie możesz wykonać następujące czynności:

  - Zignoruj lukę w oprogramowaniu na tym zarządzanym urządzeniu (w Kaspersky Security Center Web Console).
  - Przejrzyj listę zalecanych poprawek dla luki.
  - Ręcznie określ aktualizacje oprogramowania, aby naprawić lukę (w Kaspersky Security Center Web Console).
  - Przejrzyj instancje luki.
  - Przejrzyj listę istniejących zadań, aby naprawić lukę i utworzyć nowe zadania w celu wyeliminowania luki.

- **Zdalna diagnostyka** W tej sekcji możesz przeprowadzić zdalną diagnostykę urządzeń klienckich.

Jeśli używasz systemu PostgreSQL, MariaDB lub MySQL DBMS, karta **Zdarzenia** może wyświetlać niekompletną listę zdarzeń dla wybranego urządzenia klienckiego. Dzieje się tak, gdy system DBMS przechowuje bardzo dużą liczbę zdarzeń. Liczbę wyświetlanych zdarzeń można zwiększyć, wykonując jedną z następujących czynności:

- Usuwanie niepotrzebnych zdarzeń.
- Skrócenie okresu przechowywania niepotrzebnych zdarzeń.

Aby zobaczyć pełną listę zdarzeń zarejestrowanych na Serwerze administracyjnym dla danego urządzenia, należy użyć opcji Raporty.

Ręczne sprawdzanie połączenia pomiędzy urządzeniem klienckim a Serwerem administracyjnym. Narzędzie klnagchk

Możesz sprawdzić połączenie oraz uzyskać szczegółowe informacje o ustawieniach połączenia pomiędzy urządzeniem klienckim a Serwerem administracyjnym, korzystając z narzędzia klnagchk. Narzędzie klnagchk znajduje się w folderze instalacyjnym Agenta sieciowego.

Po uruchomieniu narzędzia klnagchk z poziomu wiersza poleceń będzie ono mogło wykonać następujące akcje (w zależności od używanych parametrów):

- Wyświetla na ekranie lub zapisuje w raporcie wartości ustawień używanych do łączenia Agenta sieciowego, zainstalowanego na urządzeniu, z Serwerem administracyjnym.
- Rejestruje w pliku dziennika zdarzeń statystyki Agenta sieciowego (od jego ostatniego uruchomienia) oraz wyniki działania narzędzia lub wyświetlić informacje na ekranie.
- Podejmij próbę nawiązania połączenia pomiędzy Agentem sieciowym a Serwerem administracyjnym.

  Jeżeli próba nawiązania połączenia nie powiedzie się, narzędzie wyśle pakiet ICMP w celu sprawdzenia stanu urządzenia, na którym zainstalowany jest Serwer administracyjny.

W celu sprawdzenia połączenia pomiędzy urządzeniem klienckim a Serwerem administracyjnym, korzystając z narzędzia klnagchk,

Na urządzeniu z zainstalowanym Agentem sieciowym uruchom narzędzie klnagchk z wiersza poleceń, korzystając z konta administratora lokalnego.

Składnia wiersza poleceń narzędzia:

```
klnagchk [-logfile <nazwa pliku>] [-sp] [-savecert <ścieżka do pliku certyfikatu>] [-restart][-sendhb]
```

Opisy przełączników:

- `-logfile <nazwa pliku>`—Zapisuje do pliku raportu wartości ustawień połączenia pomiędzy Agentem sieciowym a Serwerem administracyjnym oraz wyniki działania narzędzia.

  Domyślnie informacje są zapisywane w standardowym strumieniu wyjścia (stdout). Jeżeli parametr ten nie zostanie użyty, na ekranie zostaną wyświetlane wiadomości: o błędzie, z wynikami oraz ustawieniami.
- `-sp`—Wyświetla hasło używane do autoryzacji użytkownika na serwerze proxy.

  Klucz jest używany, jeśli połączenie z Serwerem administracyjnym jest nawiązywane za pośrednictwem serwera proxy.
- `-savecert <nazwa pliku>`—Zapisuje w określonym pliku certyfikat używany do uzyskiwania dostępu do Serwera administracyjnego.
- `-restart`—Ponowne uruchamia Agenta sieciowego po zakończeniu działania narzędzia.
- `-sendhb`—Rozpoczyna synchronizację Agenta sieciowego z Serwerem administracyjnym.

Po uruchomieniu narzędzie klnagchk uzyskuje dostęp do plików konfiguracyjnych Agenta sieciowego i wyświetla parametry połączenia. Parametry te są określane podczas instalacji Agenta sieciowego oraz w ustawieniach zasady Agenta sieciowego:

- `Current device`—Nazwa urządzenia klienckiego w sieci Windows.
- `Network Agent version`—Pełny numer wersji Agenta sieciowego (z poprawkami) zainstalowanego na urządzeniu.
- `Administration Server address`—Adres Serwera administracyjnego.

- `Use SSL`—Parametr wskazujący, czy podczas łączenia się z Serwerem administracyjnym używane jest bezpieczne połączenie.

  Możliwe wartości:

  - 0 — bezpieczne połączenie nie jest używane.
  - 1 — używane jest bezpieczne połączenie.

- `Compress traffic`—Parametr wskazujący, czy ruch pomiędzy urządzeniem klienckim a Serwerem administracyjnym jest kompresowany.

- `Numbers of the Administration Server SSL ports`—Liczba prawidłowych portów do komunikacji z Serwerem administracyjnym podczas korzystania z bezpiecznego połączenia.

- `Numbers of the Administration Server ports`—Numery prawidłowych portów do komunikacji z Serwerem administracyjnym podczas korzystania ze zwykłego połączenia.

- `Use proxy server`—Parametr wskazujący, czy używany jest serwer proxy.

  Możliwe wartości:

  - 0 — serwer proxy nie jest używany.
  - 1 — używany jest serwer proxy.

- `Address`—Adres i port serwera proxy oddzielone dwukropkiem. Ten parametr jest wyświetlany tylko wtedy, gdy używany jest serwer proxy.

- `User name`—Nazwa użytkownika umożliwiająca dostęp do serwera proxy. Ten parametr jest wyświetlany tylko wtedy, gdy używany jest serwer proxy.

- `Password`—Hasło dostępu do serwera proxy. Ten parametr jest wyświetlany tylko wtedy, gdy używany jest serwer proxy. Aby wyświetlić hasło serwera proxy, musisz użyć klucza `sp` w poleceniu.

- `Administration Server certificate`—Parametr wskazujący, czy urządzenie klienckie posiada certyfikat Serwera administracyjnego. Certyfikat może nie istnieć, jeśli Agent sieciowy nigdy nie nawiązał pomyślnego połączenia z Serwerem administracyjnym.

  Możliwe wartości:

  - `not installed`—Urządzenie klienckie nie posiada certyfikatu Serwera administracyjnego.
  - `available`— Urządzenie klienckie posiada certyfikat Serwera administracyjnego.

- `Open UDP port`—Parametr wskazujący, czy Agent sieciowy używa portu UDP do odbierania żądań synchronizacji z Serwera administracyjnego.

  Możliwe wartości:

  - 0 — Port UDP jest zamknięty dla odbierania żądań synchronizacji z Serwera administracyjnego.
  - 1 — Port UDP jest otwarty do odbierania żądań synchronizacji z Serwera administracyjnego.

- `Numbers of UDP ports`—Numery portów UDP, z których może korzystać Agent sieciowy.

- `Location name`—Lokalizacja sieciowa urządzenia.

- `State of network location`—Parametr wskazujący, czy urządzenie klienckie może zostać przełączone z jednego profilu połączenia Serwera administracyjnego na inny.

  Możliwe wartości:

  - `Enabled`—Profil połączenia Serwera administracyjnego można przełączyć dla urządzenia klienckiego.
  - `Disabled`—Nie można przełączyć profilu połączenia Serwera administracyjnego dla urządzenia klienckiego.

- `Profile to use`—Profil połączenia dla Serwera administracyjnego.
- `Condition`—Adres IP i maska podsieci, do której podłączone jest urządzenie klienckie.
- `Synchronization interval (min)`—Standardowy odstęp między synchronizacjami.
- `Connection timeout (in seconds)`—Limit czasu połączenia.
- `Send / receive timeout (in seconds)`—Limit czasu połączenia dla operacji odczytu i zapisu.
- `Device ID`—Identyfikator urządzenia w sieci. `Device ID` jest unikalny wśród urządzeń klienckich zarządzanych przez konkretny Serwer administracyjny.
- `Locations of connection gateways`—Parametry łączenia urządzenia klienckiego z Serwerem administracyjnym poprzez bramę połączeń.
- `Location of distribution points`—Parametry łączenia urządzenia klienckiego z Serwerem administracyjnym poprzez punkt dystrybucji.
- `Connection with server`—Parametr wskazujący, czy brama połączenia ma ciągłe połączenie z Serwerem administracyjnym. Parametr wyświetlany tylko wtedy, gdy urządzenie klienckie pełni funkcję bramy połączenia.

  Możliwe wartości:

  - `active`—Brama połączenia ma ciągłe połączenie z Serwerem administracyjnym.
  - `inactive`—Brama połączenia nie ma ciągłego połączenia z Serwerem administracyjnym.

- `Connection with server through connection gateway`—Parametr wskazujący, czy połączenie z Serwerem administracyjnym przez bramę połączenia zostało nawiązane prawidłowo. Parametr wyświetlany tylko wtedy, gdy urządzenie klienckie pełni funkcję bramy połączenia.

  Możliwe wartości:

  - `active`—Połączenie z Serwerem administracyjnym poprzez bramę połączenia jest nawiązane prawidłowo.
  - `inactive`—Połączenie z Serwerem administracyjnym przez bramę połączenia jest nawiązane nieprawidłowo.

Ponadto dane wyjściowe narzędzia klnagchk mogą zawierać jeden z następujących wierszy:

- `Administration Server is installed on this device`—Narzędzie klnagchk jest uruchomione na urządzeniu Serwera administracyjnego.
- `This device has been assigned a connection gateway but is not yet registered on Administration Server`—Narzędzie klnagchk jest uruchamiane na urządzeniu, na którym jest zainstalowany Agent sieciowy, w trybie bramy połączenia. Skonfigurowana brama połączenia czeka na połączenie z Serwerem administracyjnym, ale Serwer administracyjny nie wyświetla urządzenia wśród zarządzanych urządzeń. Należy zapewnić, że Serwer administracyjny zainicjuje połączenie z bramą połączenia.

- `This device is a connection gateway`—Narzędzie klnagchk jest uruchamiane na urządzeniu pełniącym rolę bramy połączenia.

- `Acts as a distribution point`—Narzędzie klnagchk jest uruchamiane na urządzeniu pełniącym funkcję punktu dystrybucji.

Narzędzie klnagchk sprawdza stan usługi Agenta sieciowego. Jeśli usługa nie jest uruchomiona, narzędzie zostanie zatrzymane. Jeśli usługa jest uruchomiona, narzędzie wyświetla następujące statystyki połączeń:

- `Total number of synchronization requests`—Liczba prób połączenia urządzenia klienckiego z Serwerem administracyjnym.

- `The number of successful synchronization request`—Liczba pomyślnych prób połączenia urządzenia klienckiego z Serwerem administracyjnym.

- `Total number of synchronizations`—Liczba prób synchronizacji ustawień urządzenia klienckiego z ustawieniami Serwera administracyjnego.

- `The number of successful synchronizations`—Liczba udanych prób synchronizacji ustawień urządzenia klienckiego z Serwerem administracyjnym.

- `Date/time of the last request for synchronization`—Data i godzina ostatniego połączenia.

Podczas analizowania połączenia pomiędzy Serwerem administracyjnym a Agentem sieciowym należy użyć parametrów `Total number of synchronization requests` i `The number of successful synchronization request`. Ustawienia urządzenia klienckiego synchronizują się z ustawieniami Serwera administracyjnego tylko wtedy, gdy ustawienia Serwera administracyjnego zostały zmienione (na przykład, jeśli dodano nowe zadania lub zmodyfikowano ustawienia zasady). W przeciwnym razie wartości parametrów `Total number of synchronizations` i `The number of successful synchronizations` pozostają niezmienione.

Aby uzyskać więcej informacji na temat rozwiązywania problemów z połączeniem agenta sieciowego z Serwerem administracyjnym, zapoznaj się z sekcją Często zadawane pytania dotyczące Kaspersky Security Center Linux.

Reguły przenoszenia urządzeń

Zalecane jest automatyczne przydzielanie urządzeń do grup administracyjnych za pośrednictwem *reguł przenoszenia urządzeń*. Reguła przenoszenia urządzeń składa się z trzech głównych części: nazwy, warunku wykonania (wyrażenie logiczne z atrybutami urządzenia) oraz docelowej grupy administracyjnej. Reguła przenosi urządzenie do docelowej grupy administracyjnej, jeśli atrybuty urządzenia spełniają warunek wykonania reguły.

Wszystkie reguły przenoszenia urządzeń posiadają priorytety. Serwer administracyjny sprawdza, czy atrybuty urządzenia spełniają warunek wykonania każdej reguły, w rosnącej kolejności priorytetów. Jeśli atrybuty urządzenia spełniają warunek wykonania reguły, urządzenie zostaje przeniesione do grupy docelowej, a przetwarzanie reguły zostanie zakończone dla tego urządzenia. Jeśli atrybuty urządzenia spełniają warunki kilku reguł, urządzenie zostanie przeniesione do grupy docelowej reguły z najwyższym priorytetem (czyli tej, która znajduje się najwyżej na liście).

Reguły przenoszenia urządzeń mogą być tworzone pośrednio. Na przykład, we właściwościach pakietu instalacyjnego lub zadania zdalnej instalacji możesz określić grupę administracyjną, do której urządzenie musi zostać przeniesione po zainstalowaniu na nim Agenta sieciowego. Również reguły przenoszenia urządzeń mogą być tworzone także bezpośrednio przez administratora Kaspersky Security Center Linux w sekcji **Zarządzanie zasobami** → **Reguły przenoszenia**.

Domyślnie reguła przenoszenia urządzeń jest przeznaczona do jednorazowego, wstępnego przydzielenia urządzeń do grup administracyjnych. Reguła przenosi urządzenia z grupy Urządzenia nieprzypisane tylko raz. Jeśli urządzenie było już raz przeniesione przy użyciu tej reguły, reguła ta nie przeniesie go już nawet wtedy, gdy ręcznie przeniesiesz urządzenie z powrotem do grupy Urządzenia nieprzypisane. Jest to zalecany sposób stosowania reguł przenoszenia.

Możesz przenieść urządzenia, które już zostały przydzielone do niektórych grup administracyjnych. Aby to zrobić, we właściwościach reguły odznacz pole **Przenoś tylko urządzenia, które nie są przypisane do grup administracyjnych**.

Stosowanie reguł przenoszenia do urządzeń, które już zostały przydzielone do niektórych grup administracyjnych, znacząco zwiększa obciążenie na Serwerze administracyjnym.

Pole wyboru **Przenoś tylko urządzenia, które nie są przypisane do grup administracyjnych** jest zablokowane we właściwościach automatycznie tworzonych reguł przenoszenia. Takie reguły są tworzone podczas dodawania zadania *Zdalna instalacja aplikacji* lub tworzenia autonomicznego pakietu instalacyjnego.

Możesz utworzyć regułę przenoszenia, która będzie nieprzerwanie oddziaływać na jedno urządzenie.

Szczególnie zalecane jest unikanie ciągłego przenoszenia jednego urządzenia z jednej grupy do drugiej (na przykład, w celu zastosowania specjalnej zasady do tego urządzenia, uruchomienia specjalnego zadania grupowego lub zaktualizowania urządzenia poprzez punkt dystrybucji).

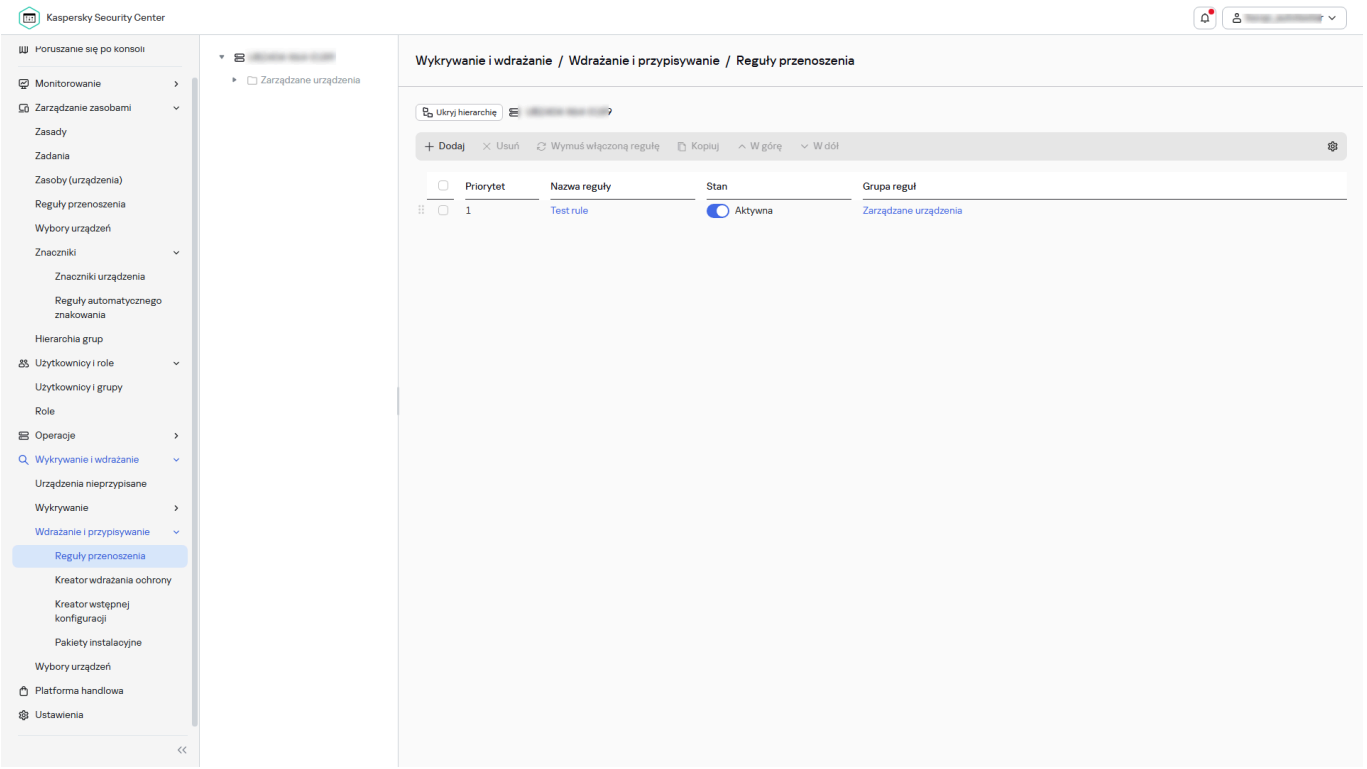
Takie scenariusze nie są obsługiwane, ponieważ w bardzo dużym stopniu zwiększają obciążenie na Serwerze administracyjnym oraz ruch sieciowy. Te scenariusze doprowadzają też do konfliktu z zasadami działania Kaspersky Security Center Linux (szczególnie w obszarze uprawnień dostępu, zdarzeń i raportów). Należy znaleźć inne rozwiązanie, na przykład, poprzez użycie profili zasad, zadań dla wyborów urządzeń, przydzielania Agentów sieciowych zgodnie ze standardowym scenariuszem.

Tworzenie reguł przenoszenia urządzeń

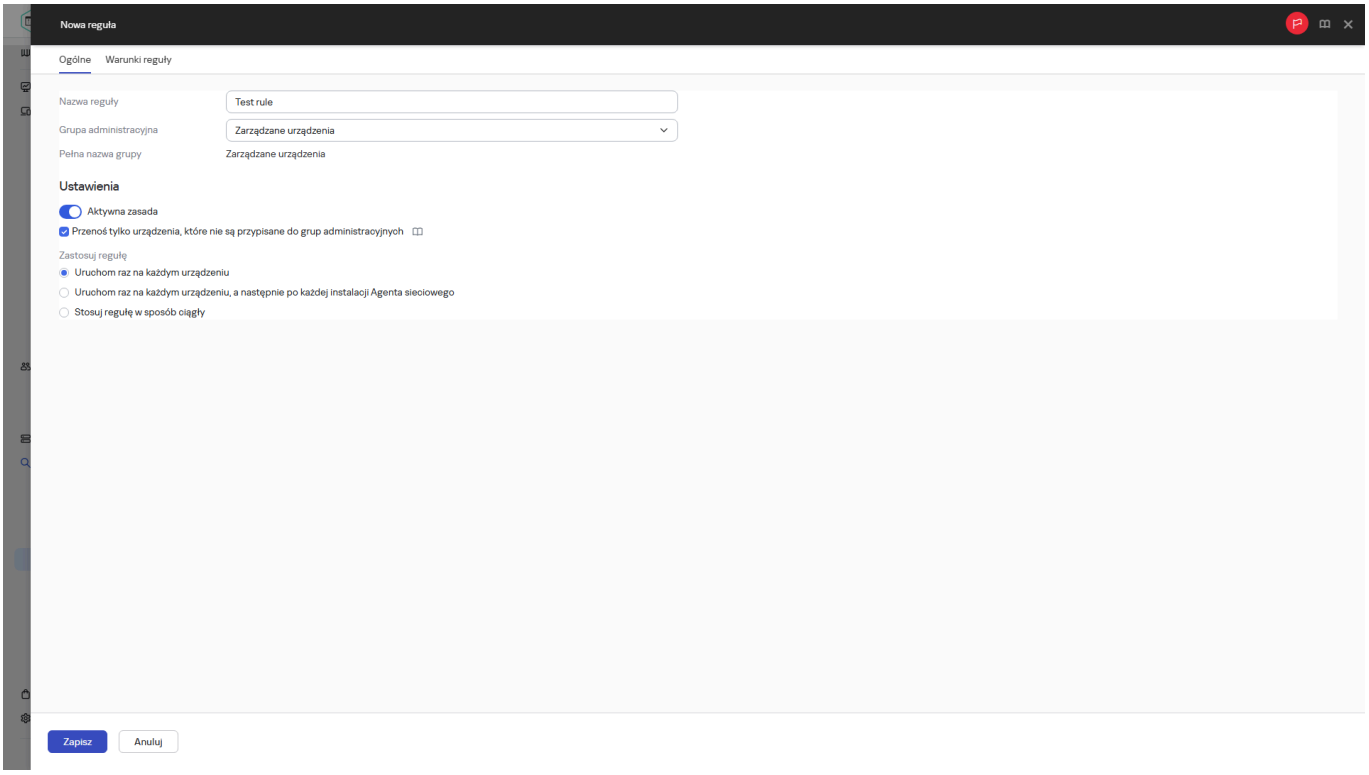
Możesz skonfigurować reguły przenoszenia urządzeń, czyli reguły, które automatycznie przypisują urządzenia do grup administracyjnych.

W celu utworzenia reguły przenoszenia:

1. W menu głównym przejdź na **Zarządzanie zasobami** → **Reguły przenoszenia**.



2. Kliknij **Dodaj**. Zostanie otwarte okno **Nowa reguła**.



3. W otwartym oknie, na zakładce **Ogólne** określ następujące informacje:

- **Nazwa reguły**

  Wprowadź nazwę nowej reguły.

  Jeśli kopiujesz regułę, nowa reguła otrzyma tę samą nazwę co reguła źródłowa, ale do nazwy zostanie dodany indeks w formacie (), na przykład: (1).

- **Grupa administracyjna**

  Wybierz grupę administracyjną, do której urządzenia są przenoszone automatycznie.

- **Stan reguły**

  Jeśli ta opcja jest włączona, reguła jest włączona i zaczyna działać po jej zapisaniu.

  Jeśli ta opcja jest wyłączona, reguła zostaje utworzona, ale nie jest włączona. Nie będzie działać, dopóki nie włączysz tej opcji.

- **Priorytet**

  Możesz określić priorytet przenoszonej reguły. Najwyższy priorytet to 1. Im większa wartość **Priorytet**, tym niższy priorytet reguły i jej pozycja na liście.

  Jeśli nie przypisano żadnego priorytetu, regule przypisywany jest najniższy priorytet.

  Podczas kopiowania reguły, jej kopii przypisywany jest priorytet reguły oryginalnej. Priorytet reguły oryginalnej jest następnie zwiększany o 1.

- **Przenoś tylko urządzenia, które nie są przypisane do grup administracyjnych**

  Jeśli ta opcja jest włączona, do wybranej grupy zostaną przeniesione tylko urządzenia nieprzypisane.

  Jeśli ta opcja jest wyłączona, urządzenia, które już należą do innych grup administracyjnych, a także urządzenia nieprzypisane, zostaną przeniesione do wybranej grupy.

- **Zastosuj regułę**

  Możesz wybrać jedną z następujących opcji:

  - **Uruchom raz na każdym urządzeniu**

    Reguła jest stosowana raz dla każdego urządzenia, które odpowiada Twoim kryteriom.

  - **Uruchom raz na każdym urządzeniu, a następnie po każdej instalacji Agenta sieciowego**

    Reguła jest stosowana raz dla każdego urządzenia, które odpowiada Twoim kryteriom, a następnie tylko wtedy, gdy Agent sieciowy jest ponownie instalowany na tych urządzeniach.

  - **Stosuj regułę w sposób ciągły**

    Reguła jest stosowana zgodnie z terminarzem, który Serwer administracyjny konfiguruje automatycznie (zazwyczaj co kilka godzin).

4. Na karcie **Warunki reguły** określ co najmniej jedno kryterium, według którego urządzenia są przenoszone do grupy administracyjnej.

5. Kliknij **Zapisz**.

Reguła przenoszenia została utworzona. Jest wyświetlana na liście reguł przenoszenia.

Im wyższa pozycja na liście, tym wyższy priorytet reguły.

Aby zmienić priorytet:

1. Zaznacz pole wyboru reguły przenoszenia.
2. Wykonaj jedną z poniższych czynności:
   - Kliknij przycisk **Zmień priorytet** i określ nowy priorytet.
   - Przenieś regułę w górę lub w dół na liście, odpowiednio, klikając przyciski **W górę** lub **W dół**.
3. Kliknij przycisk **Zapisz**.

> Jeśli zaznaczona jest opcja **Stosuj regułę w sposób ciągły**, reguła przenoszenia zostanie zastosowana niezależnie od ustawień priorytetu. Reguły takie są stosowane zgodnie z harmonogramem konfigurowanym automatycznie przez Serwer administracyjny.

Jeśli atrybuty urządzenia spełniają warunki kilku reguł, urządzenie zostanie przeniesione do grupy docelowej reguły z najwyższym priorytetem (czyli tej, która znajduje się najwyżej na liście).

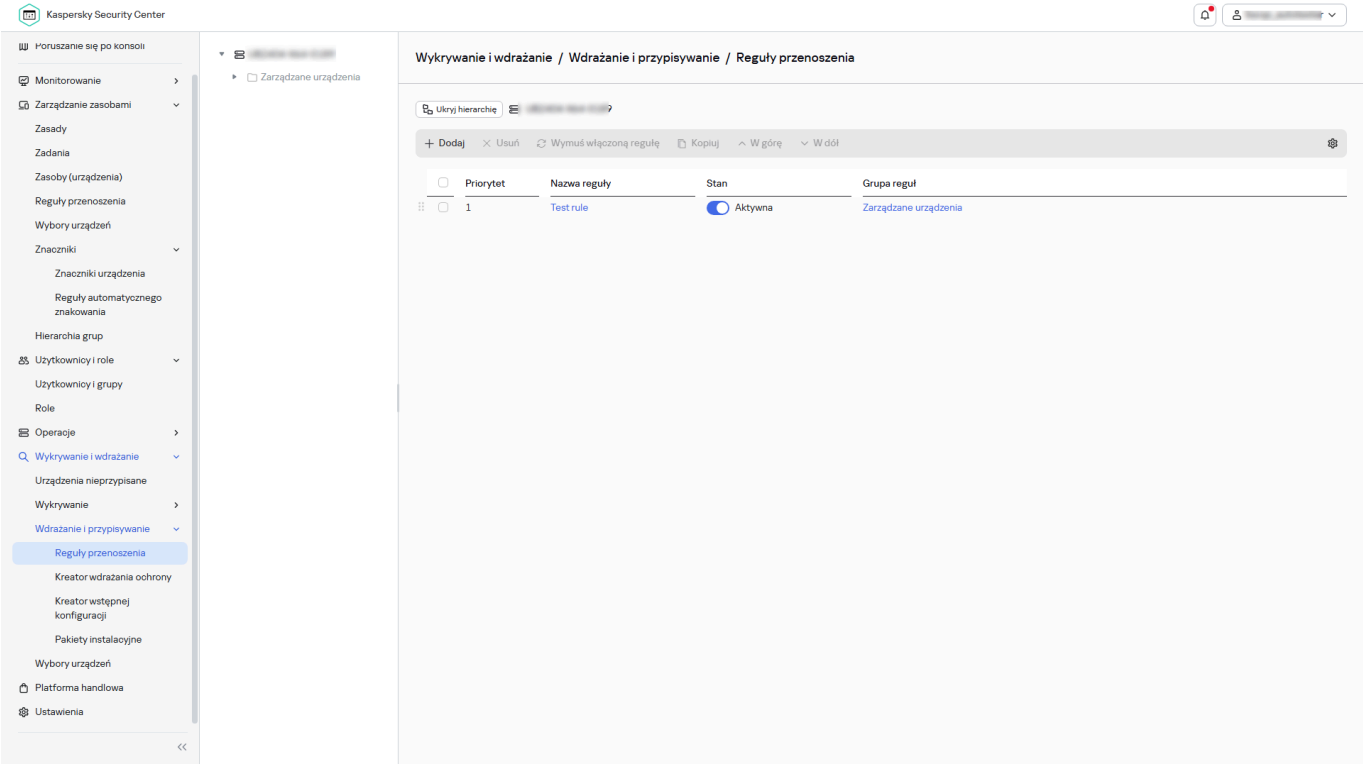
Kopiowanie reguł przenoszenia urządzeń

Możesz kopiować reguły przenoszenia, na przykład, jeśli chcesz mieć kilka identycznych reguł dla różnych docelowych grup administracyjnych.

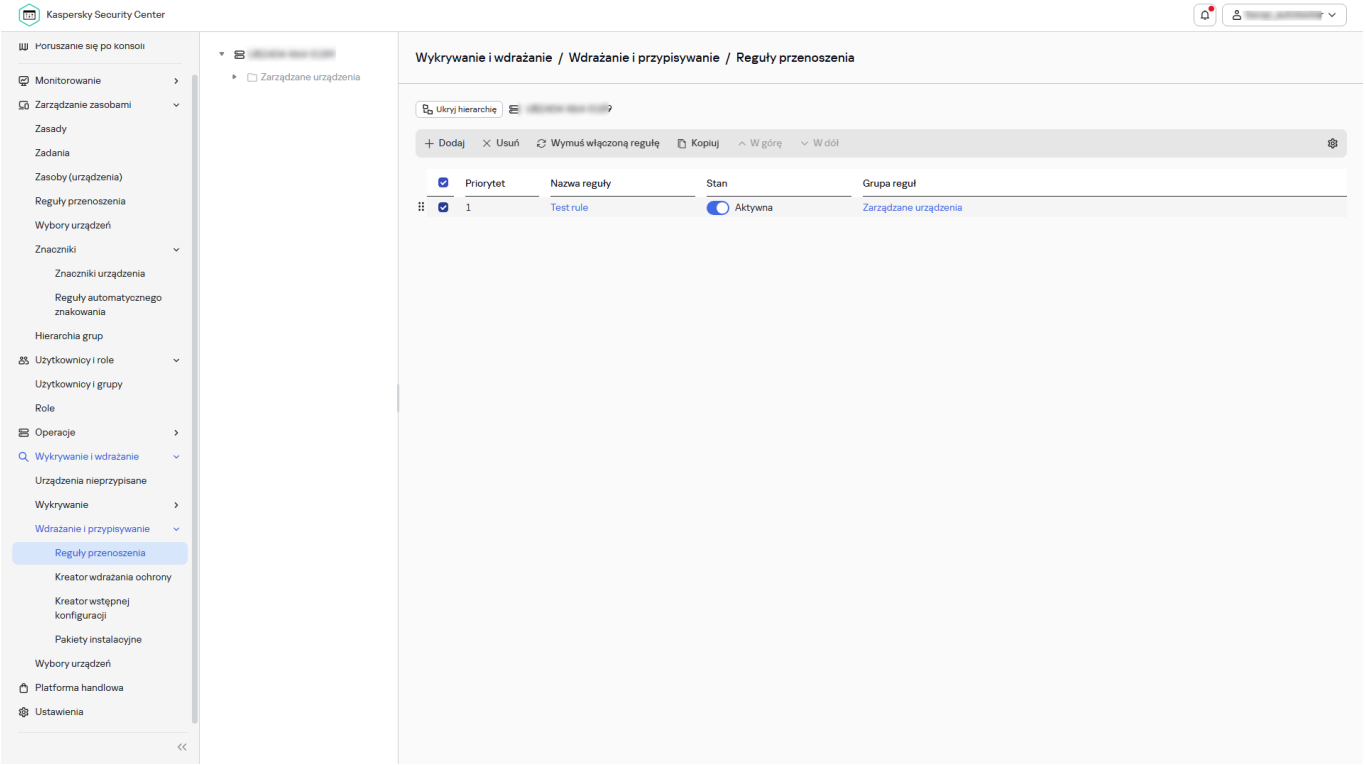
W celu skopiowania istniejącej reguły przenoszenia:

1. Wykonaj jedną z poniższych czynności:
   - W menu głównym przejdź na **Zarządzanie zasobami** → **Reguły przenoszenia**.
   - W menu głównym przejdź do **Wykrywanie i wdrażanie** → **Wdrażanie i przypisywanie** → **Reguły przenoszenia**.

   Zostanie wyświetlona lista reguł przenoszenia.



2. Zaznacz pole obok reguły, którą chcesz skopiować.



3. Kliknij **Kopiuj**.

4. W otwartym oknie zmień następujące informacje na zakładce **Ogólne** lub nie wprowadzaj żadnych zmian, jeśli chcesz tylko skopiować regułę bez zmiany jej ustawień:

   - **Nazwa reguły**

     Wprowadź nazwę nowej reguły.

     Jeśli kopiujesz regułę, nowa reguła otrzyma tę samą nazwę co reguła źródłowa, ale do nazwy zostanie dodany indeks w formacie (), na przykład: (1).

- **Grupa administracyjna**

  Wybierz grupę administracyjną, do której urządzenia są przenoszone automatycznie.

- **Stan reguły**

  Jeśli ta opcja jest włączona, reguła jest włączona i zaczyna działać po jej zapisaniu.

  Jeśli ta opcja jest wyłączona, reguła zostaje utworzona, ale nie jest włączona. Nie będzie działać, dopóki nie włączysz tej opcji.

- **Priorytet**

  Możesz określić priorytet przenoszonej reguły. Najwyższy priorytet to 1. Im większa wartość **Priorytet**, tym niższy priorytet reguły i jej pozycja na liście.

  Jeśli nie przypisano żadnego priorytetu, regule przypisywany jest najniższy priorytet.

  Podczas kopiowania reguły, jej kopii przypisywany jest priorytet reguły oryginalnej. Priorytet reguły oryginalnej jest następnie zwiększany o 1.

- **Przenoś tylko urządzenia, które nie są przypisane do grup administracyjnych**

  Jeśli ta opcja jest włączona, do wybranej grupy zostaną przeniesione tylko urządzenia nieprzypisane.

  Jeśli ta opcja jest wyłączona, urządzenia, które już należą do innych grup administracyjnych, a także urządzenia nieprzypisane, zostaną przeniesione do wybranej grupy.

- **Zastosuj regułę**

  Możesz wybrać jedną z następujących opcji:

  - **Uruchom raz na każdym urządzeniu**

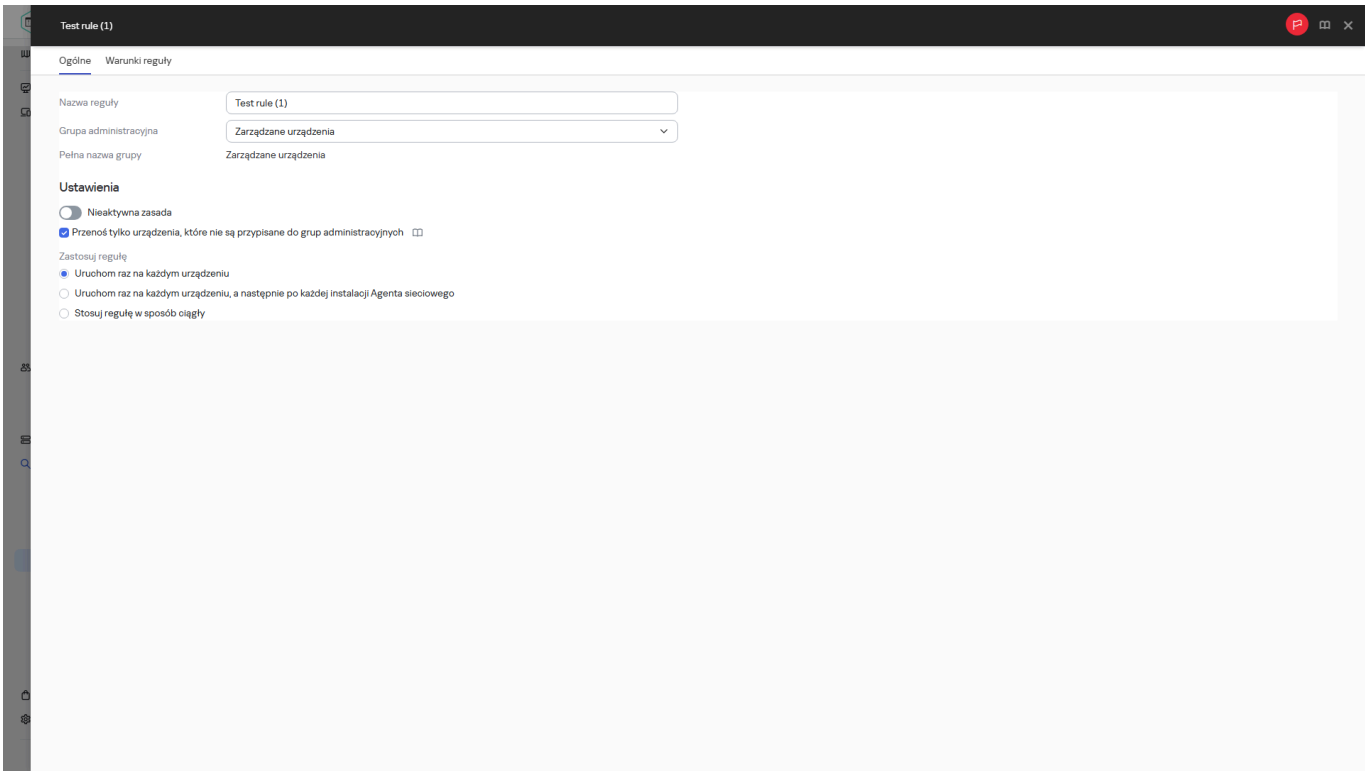
    Reguła jest stosowana raz dla każdego urządzenia, które odpowiada Twoim kryteriom.

  - **Uruchom raz na każdym urządzeniu, a następnie po każdej instalacji Agenta sieciowego**

    Reguła jest stosowana raz dla każdego urządzenia, które odpowiada Twoim kryteriom, a następnie tylko wtedy, gdy Agent sieciowy jest ponownie instalowany na tych urządzeniach.

  - **Stosuj regułę w sposób ciągły**

    Reguła jest stosowana zgodnie z terminarzem, który Serwer administracyjny konfiguruje automatycznie (zazwyczaj co kilka godzin).



5. Na karcie **Warunki reguły** określ co najmniej jedno kryterium dla urządzeń, które mają być przenoszone automatycznie.

6. Kliknij **Zapisz**.

Nowa reguła przenoszenia została utworzona. Jest wyświetlana na liście reguł przenoszenia.

Warunki dla reguły przenoszenia urządzenia

Gdy tworzysz lub kopiujesz regułę przenoszenia urządzeń klienckich do grup administracyjnych, na karcie **Warunki reguły** ustawiasz warunki przenoszenia urządzeń. Aby określić, które urządzenia przenieść, możesz skorzystać z następujących kryteriów:

- Tagi przypisane do urządzeń klienckich.
- Parametry sieciowe. Na przykład możesz przenieść urządzenia z adresami IP z określonego zakresu.
- Właściciel urządzenia, jego rola i przynależność do grupy zabezpieczeń.
- Aplikacje zarządzane zainstalowane na urządzeniach klienckich, na przykład Agent sieciowy lub Serwer administracyjny.
- Maszyny wirtualne, które są urządzeniami klienckimi.
- Jednostki organizacyjne kontrolera domeny.
- Segmenty chmury.

Poniżej znajdziesz opis, jak określić te informacje w regule przenoszenia urządzeń.

Jeśli określisz kilka warunków w regule, operator logiczny AND działa i wszystkie warunki mają zastosowanie w tym samym czasie. Jeśli nie zaznaczysz żadnych opcji lub pozostawisz niektóre pola puste, takie warunki nie mają zastosowania.

Zakładka Znaczniki

Na tej zakładce można skonfigurować regułę przenoszenia urządzeń na podstawie znaczników urządzenia, które zostały wcześniej dodane do opisów urządzeń klienckich. Aby to zrobić, wybierz wymagane tagi. Możesz także włączyć następujące opcje:

- **Zastosuj do urządzeń bez określonych znaczników**

  Jeśli ta opcja jest włączona, wszystkie urządzenia z określonymi tagami są wykluczane z reguły przenoszenia urządzeń. Jeśli ta opcja jest wyłączona, reguła przenoszenia urządzeń dotyczy urządzeń ze wszystkimi wybranymi tagami.

  Domyślnie opcja ta jest wyłączona.

- **Zastosuj, jeśli co najmniej jeden określony znacznik jest zgodny**

  Jeśli ta opcja jest włączona, reguła przenoszenia urządzeń dotyczy urządzeń klienckich z co najmniej jednym z wybranych tagów. Jeśli ta opcja jest wyłączona, reguła przenoszenia urządzeń dotyczy urządzeń ze wszystkimi wybranymi tagami.

  Domyślnie opcja ta jest wyłączona.

Karta Sieć

Na tej karcie możesz określić dane sieciowe urządzeń, które uwzględnia reguła przenoszenia urządzeń:

- **Nazwa urządzenia w sieci Windows**

  Nazwa sieciowa systemu Windows (nazwa NetBIOS) urządzenia lub adres IPv4 lub IPv6.

- **Domena Windows**

  Reguła przenoszenia urządzeń dotyczy wszystkich urządzeń znajdujących się w określonej domenie Windows.

- **Nazwa DNS urządzenia**

  Nazwa domeny DNS urządzenia klienckiego, które chcesz przenieść. Wypełnij to pole, jeśli Twoja sieć zawiera serwer DNS.

  > Jeśli dla bazy danych używanej z Kaspersky Security Center Linux ustawione jest sortowanie z rozróżnianiem wielkości liter, zachowaj wielkość liter podczas określania nazwy DNS urządzenia. W przeciwnym razie reguła przenoszenia urządzenia nie będzie działać.

- **Domena DNS**

  Reguła przenoszenia urządzeń dotyczy wszystkich urządzeń zawartych w określonym głównym sufiksie DNS. Wypełnij to pole, jeśli Twoja sieć zawiera serwer DNS.

- **Zakres IP**

  Jeśli ta opcja jest włączona, możesz wprowadzić początkowy i końcowy adres IP z zakresu adresów IP, do którego muszą zostać włączone odpowiednie urządzenia.

  Domyślnie opcja ta jest wyłączona.

- **Adres IP do łączenia z Serwerem administracyjnym**

  Jeżeli ta opcja jest włączona, możesz ustawić adresy IP, za pomocą których urządzenia klienckie będą połączone z Serwerem administracyjnym. W tym celu określ zakres adresów IP, który zawiera wszystkie niezbędne adresy IP.

  Domyślnie opcja ta jest wyłączona.

- **Urządzenie znajduje się w grupie podrzędnej grupy Domeny**

  Jeżeli ta opcja jest włączona, możesz wybrać podgrupę grupy Domeny. Odpowiednie urządzenia muszą znajdować się w wybranej podgrupie.

  Domyślnie opcja ta jest wyłączona.

- **Urządzenie znajduje się w zakresie IP**

  Jeżeli ta opcja jest włączona, możesz wybrać zakres adresów IP, który wcześniej dodałeś w sekcji **Zakresy IP**. Odpowiednie urządzenia muszą znajdować się w wybranym zakresie adresów IP.

  Domyślnie opcja ta jest wyłączona.

- **Zmieniono profil połączenia**

  Wybierz jedną z następujących wartości:

  - **Tak**. Reguła przenoszenia urządzeń dotyczy tylko urządzeń klienckich ze zmienionym profilem połączenia.
  - **Nie**. Reguła przenoszenia urządzeń dotyczy tylko urządzeń klienckich, których profil połączenia nie uległ zmianie.
  - **Nie wybrano wartości**. Warunek nie ma zastosowania.

- **Zarządzane przez inny Serwer administracyjny**

  Wybierz jedną z następujących wartości:

  - **Tak**. Reguła przenoszenia urządzeń dotyczy tylko urządzeń klienckich zarządzanych przez inne Serwery administracyjne. Te serwery różnią się od serwera, na którym konfigurujesz regułę przenoszenia urządzeń.
  - **Nie**. Reguła przenoszenia urządzeń dotyczy tylko urządzeń klienckich zarządzanych przez bieżący Serwer administracyjny.
  - **Nie wybrano wartości**. Warunek nie ma zastosowania.

Zakładka Właściciel urządzenia

Na tej zakładce możesz skonfigurować regułę przenoszenia urządzenia na podstawie właściciela urządzenia, członkostwa w grupie zabezpieczeń i roli:

- **Właściciel urządzenia**

  Wybierz nazwę użytkownika właściciela urządzenia z wewnętrznej grupy zabezpieczeń. Dowiedz się więcej o użytkownikach i rolach użytkowników w tej sekcji.

  > Nie więcej niż jeden użytkownik może być zarejestrowany jako właściciel urządzenia.

- **Członkostwo właściciela urządzenia w grupie zabezpieczeń Active Directory**

  Wybierz zewnętrzną grupę zabezpieczeń Active Directory, do której należy właściciel urządzenia.

  > Użytkownik może należeć do grupy zabezpieczeń Active Directory lub do grupy zawartej w tej grupie zabezpieczeń Active Directory.

- **Rola właściciela urządzenia**

  Wybierz rolę przypisaną właścicielowi urządzenia. Więcej informacji na temat ról użytkowników znajdziesz w tym artykule.

- **Członkostwo właściciela urządzenia w grupie zabezpieczeń Active Directory**

  Wybierz wewnętrzną grupę zabezpieczeń, do której należy właściciel urządzenia.

Karta Aplikacje

Na tej karcie możesz skonfigurować regułę przenoszenia urządzeń na podstawie zarządzanych aplikacji i systemów operacyjnych zainstalowanych na urządzeniach klienckich:

- **Agent sieciowy jest zainstalowany**

  Wybierz jedną z następujących wartości:

  - **Tak**. Reguła przenoszenia urządzeń dotyczy tylko urządzeń klienckich z zainstalowanym Agentem sieciowym.
  - **Nie**. Reguła przenoszenia urządzeń dotyczy tylko urządzeń klienckich, na których nie jest zainstalowany Agent sieciowy.
  - **Nie wybrano wartości**. Warunek nie ma zastosowania.

- **Aplikacje**

  Określ, jakie zarządzane aplikacje powinny być zainstalowane na urządzeniach klienckich, aby reguła przenoszenia urządzeń miała zastosowanie do tych urządzeń. Na przykład możesz wybrać **Agent sieciowy Kaspersky Security Center 16.3** lub **Serwer administracyjny Kaspersky Security Center 16.3**.

Jeśli nie wybierzesz żadnej zarządzanej aplikacji, warunek nie ma zastosowania.

- **Wersja systemu operacyjnego**

  Urządzenia klienckie można usuwać na podstawie wersji systemu operacyjnego. W tym celu określ systemy operacyjne, które powinny być zainstalowane na urządzeniach klienckich. W rezultacie reguła przenoszenia urządzeń dotyczy urządzeń klienckich z wybranymi systemami operacyjnymi.

  Jeśli nie włączysz tej opcji, warunek nie ma zastosowania. Domyślnie opcja ta jest wyłączona.

- **Architektura systemu operacyjnego**

  Urządzenia klienckie można usuwać według rozmiarów bitowych systemu operacyjnego. W polu **Architektura systemu operacyjnego** możesz wybrać jedną z następujących wartości:

  - **Nieznany**
  - **x86**
  - **AMD64**
  - **IA64**

  Aby sprawdzić architekturę systemu operacyjnego urządzeń klienckich:

  1. W menu głównym przejdź do **Zarządzanie zasobami** → **Zasoby (urządzenia)**.
  2. Kliknij przycisk **Ustawienia kolumn** (⚙) po prawej stronie.
  3. Wybierz opcję **Architektura systemu operacyjnego**, a następnie kliknij przycisk **Zapisz**.

     Następnie dla każdego zarządzanego urządzenia zostanie wyświetlona architektura systemu operacyjnego.

- **Menedżer pakietów systemu operacyjnego**

  Urządzenia klienckie można usuwać przez menedżera pakietów systemu operacyjnego. W polu **Menedżer pakietów systemu operacyjnego**, możesz wybrać jedną z następujących wartości:

  - rpm — dla urządzeń z systemami operacyjnymi Red Hat Enterprise Linux, CentOS, Fedora, SUSE, Oracle Linux
  - apt (dpkg) — dla urządzeń z systemami operacyjnymi Debian, Ubuntu, Kali
  - pkg — dla urządzeń z systemami operacyjnymi FreeBSD, OpenBSD

  Aby sprawdzić menedżera pakietów systemu operacyjnego urządzeń klienckich:

  1. W menu głównym przejdź do **Zarządzanie zasobami** → **Zasoby (urządzenia)**.
  2. Kliknij przycisk **Ustawienia kolumn** (⚙) po prawej stronie.
  3. Wybierz opcję **Menedżer pakietów systemu operacyjnego**, a następnie kliknij przycisk **Zapisz**.

     Menedżer pakietów systemu operacyjnego jest wyświetlany dla każdego zarządzanego urządzenia.

- **Wersja dodatku Service Pack systemu operacyjnego**

  W tym polu możesz określić wersję pakietu systemu operacyjnego (w formacie *X.Y*), która będzie określać sposób stosowania reguły przenoszenia do urządzenia. Domyślnie nie jest zdefiniowana żadna wartość.

- **Certyfikat użytkownika**

  Wybierz jedną z następujących wartości:

  - **Zainstalowano**. Reguła przenoszenia urządzeń dotyczy tylko urządzeń mobilnych z certyfikatem mobilnym.
  - **Nie zainstalowano**. Reguła przenoszenia urządzeń dotyczy tylko urządzeń mobilnych bez certyfikatu mobilnego.
  - **Nie wybrano wartości**. Warunek nie ma zastosowania.

- **Kompilacja systemu operacyjnego**

  To ustawienie jest stosowane tylko w systemach operacyjnych Windows.

  Możesz określić, czy wybrany system operacyjny musi mieć równy, wcześniejszy lub późniejszy numer kompilacji. Możesz także skonfigurować regułę przenoszenia urządzeń dla wszystkich numerów kompilacji z wyjątkiem określonego.

- **Numer wersji systemu operacyjnego**

  To ustawienie jest stosowane tylko w systemach operacyjnych Windows.

  Możesz określić, czy wybrany system operacyjny musi mieć równy, wcześniejszy lub późniejszy numer wydania. Możesz także skonfigurować regułę przenoszenia urządzeń dla wszystkich numerów wersji z wyjątkiem określonego.

Karta Maszyny wirtualne

Na tej karcie możesz skonfigurować regułę przenoszenia urządzeń w zależności od tego, czy urządzenia klienckie są maszynami wirtualnymi, czy częścią Virtual Desktop Infrastructure (VDI):

- **Jest maszyną wirtualną**

  Z listy rozwijalnej możesz wybrać jedną z następujących opcji:

  - **N/D**. Warunek nie ma zastosowania.
  - **Nie**. Przenosi urządzenia, które nie są maszynami wirtualnymi.
  - **Tak**. Przenosi urządzenia, które są maszynami wirtualnymi.

- **Typ maszyny wirtualnej**

- **Część Virtual Desktop Infrastructure**

  Z listy rozwijalnej możesz wybrać jedną z następujących opcji:

  - **N/D**. Warunek nie ma zastosowania.
  - **Nie**. Przenieś urządzenia, które nie są częścią VDI.
  - **Tak**. Przenieś urządzenia, które są częścią VDI.

Karta Sterownik domeny

Na tej karcie możesz określić, że konieczne jest przeniesienie urządzeń znajdujących się w jednostce organizacyjnej domeny. Możesz także przenieść urządzenia ze wszystkich podrzędnych jednostek organizacyjnych określonej jednostki organizacyjnej domeny:

- **Urządzenie wchodzi w skład następującej jednostki organizacyjnej**

  Jeśli ta opcja jest włączona, reguła przenoszenia urządzeń dotyczy urządzeń z jednostki organizacyjnej kontrolera Active Directory określonej na liście pod opcją.

  Domyślnie opcja ta jest wyłączona.

- **Uwzględnij podrzędne jednostki organizacyjne**

  Jeśli ta opcja jest włączona, wybór zawiera urządzenia ze wszystkich podrzędnych jednostek organizacyjnych określonej jednostki organizacyjnej kontroler domeny.

  Domyślnie opcja ta jest wyłączona.

- **Przenieś urządzenia z podrzędnych jednostek do odpowiednich podgrup**
- **Utwórz podgrupy odpowiadające kontenerom nowo wykrytych urządzeń**
- **Usuń podgrupy, które nie są obecne w domenie**
- **Urządzenie należy do następującej grupy zabezpieczeń domeny**

  Jeśli ta opcja jest włączona, reguła przenoszenia urządzeń dotyczy urządzeń z grupy bezpieczeństwa domeny określonej na liście pod opcją.

  Domyślnie opcja ta jest wyłączona.

Zakładka Segmenty chmury

Na tej karcie można określić, że konieczne jest przeniesienie urządzeń należących do segmentu chmury. Możesz także przenieść urządzenia ze wszystkich podrzędnych jednostek organizacyjnych określonej jednostki organizacyjnej domeny:

- **Urządzenie znajduje się w segmencie chmury**

  Jeśli wybierzesz tę opcję, reguła przenoszenia urządzeń zostanie zastosowana do urządzeń klienckich należących do segmentu chmury. Możesz wybrać żądany segment chmury aż do podsieci na liście pod opcją.

  Domyślnie opcja ta jest wyłączona.

- **Włączając obiekty potomne**

  Jeśli ta opcja jest włączona, wybór obejmuje urządzenia ze wszystkich podrzędnych jednostek organizacyjnych określonego segmentu chmury.

  Domyślnie opcja ta jest wyłączona.

- **Przenieś urządzenia z obiektów zagnieżdżonych do odpowiednich podgrup**
- **Utwórz podgrupy odpowiadające kontenerom nowo wykrytych urządzeń**
- **Usuń podgrupy, dla których nie odnaleziono odpowiednika w segmentach chmury**
- **Urządzenie wykryte przy pomocy API**

  Z listy rozwijalnej możesz wybrać jedną z następujących opcji:

  - Nie wybrano wartości. Warunek nie ma zastosowania.
  - **Nie**. Przenieś urządzenia, które nie zostały wykryte przy użyciu interfejsu API.
  - **AWS**. Przenieś urządzenia wykryte przy użyciu interfejsu API AWS.
  - **Azure**. Przenieś urządzenia wykryte przy użyciu interfejsu API platformy Azure.
  - **Google Cloud**. Przenieś urządzenia wykryte przy użyciu interfejsu API Google Cloud.

  Następnie, w zależności od wybranej wartości, możesz wypełnić następujące pola:

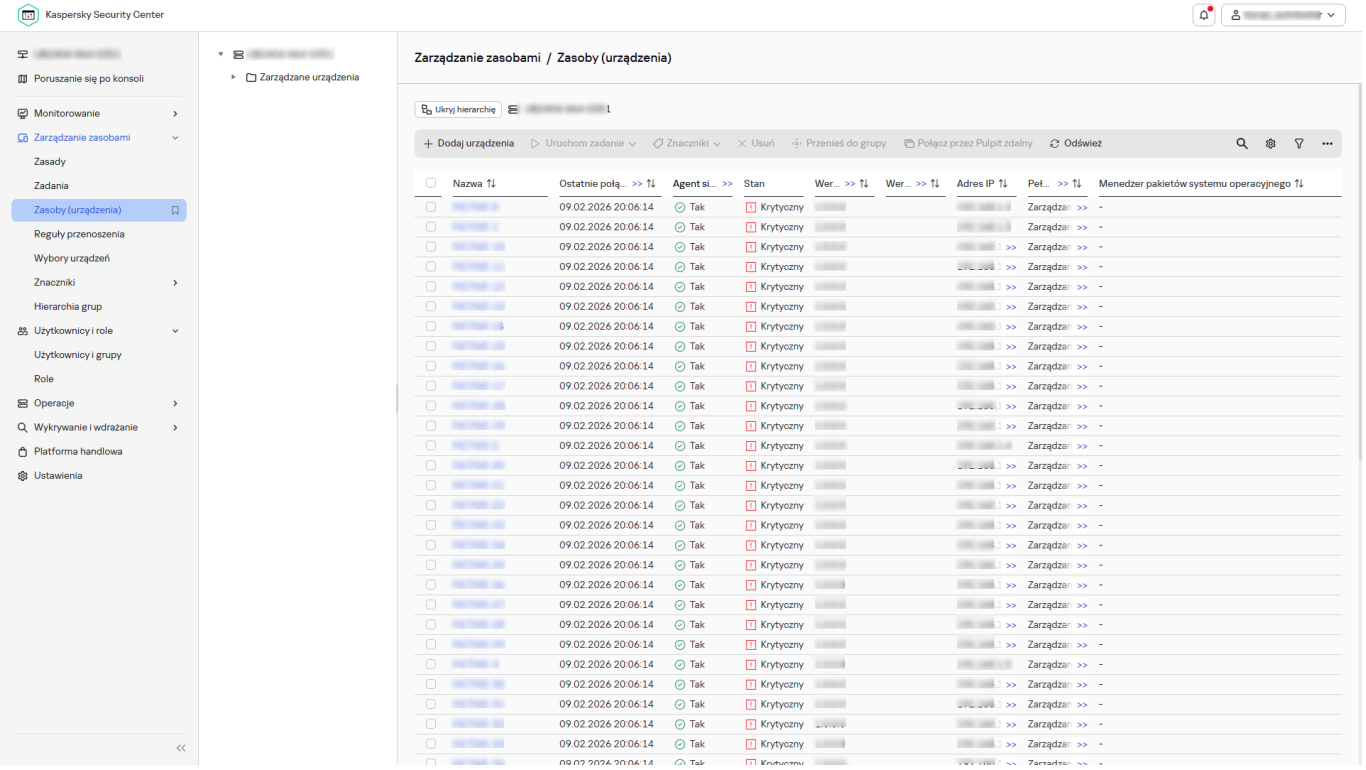
  - **Podsieć urządzenia w chmurze**.
  - **Strefa dostępności urządzenia w chmurze**.
  - **Grupa umiejscowienia urządzeń w chmurze**.

Ręczne dodawanie urządzeń do grupy administracyjnej

Możesz automatycznie przenieść urządzenia do grup administracyjnych, tworząc reguły przenoszenia urządzeń, lub ręcznie, przenosząc urządzenia z jednej grupy administracyjnej do innej lub dodając urządzenia do wybranej grupy administracyjnej. Ta sekcja opisuje sposób ręcznego dodawania urządzeń do grupy administracyjnej.

W celu ręcznego dodania jednego lub kilku urządzeń do wybranej grupy administracyjnej:

1. W menu głównym przejdź do **Zarządzanie zasobami** → **Zasoby (urządzenia)**.



Lista zarządzanych urządzeń

2. Wybierz grupę administracyjną, do której chcesz dodać urządzenia:

   - Dla grupy głównej:

     W takim przypadku możesz przejść do następnego kroku.

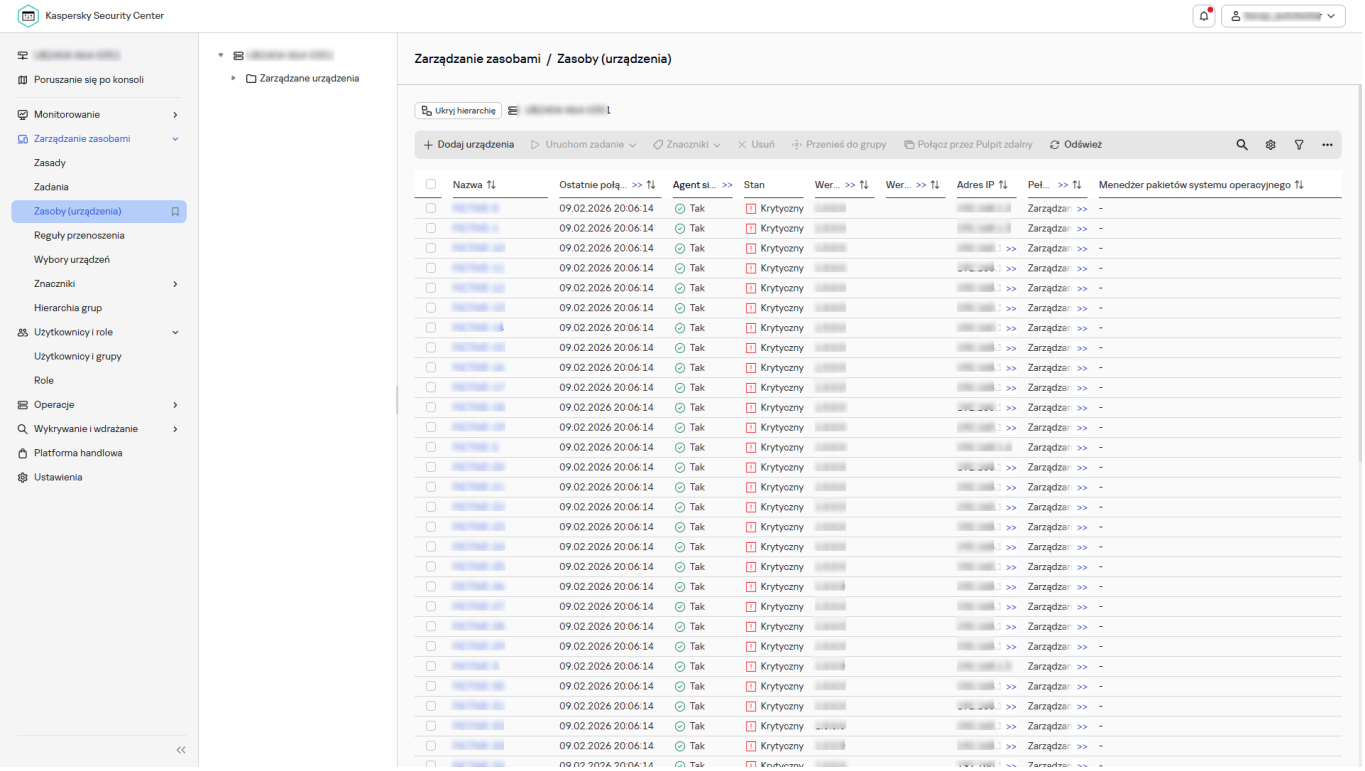
   - Dla grupy podrzędnej:

     a. Kliknij przycisk **Pokaż hierarchię** znajdujący się na górze strony.

     Nazwa przycisku zmieni się na **Ukryj hierarchię**.

     b. W otwartym oknie kliknij odnośnik z nazwą podgrupy.

Ścieżka do wybranej grupy jest wyświetlana na górze strony. W razie potrzeby możesz kliknąć odnośnik z nazwą grupy administracyjnej, aby do niej przejść. Domyślnie ostatni odnośnik na ścieżce jest nieaktywny. Można również zamknąć okno hierarchii, klikając przycisk **Ukryj hierarchię**.



Wybieranie grupy administracyjnej

3. Kliknij przycisk **Dodaj urządzenia**.

   Zostanie uruchomiony Kreator przenoszenia urządzeń.

4. Utwórz listę urządzeń, które chcesz dodać do grupy administracyjnej.

   Możesz dodać tylko urządzenia, dla których informacje zostały już dodane do bazy danych Serwera administracyjnego przy podłączeniu urządzenia lub po wykrywaniu urządzeń.

   Wybierz sposób dodawania urządzeń do listy:

   - Kliknij przycisk **Dodaj urządzenia**, a następnie określ urządzenia w jeden z następujących sposobów:
     - Wybierz urządzenia z listy urządzeń wykrytych przez Serwer administracyjny.
     - Określ adres IP urządzenia lub zakres IP.

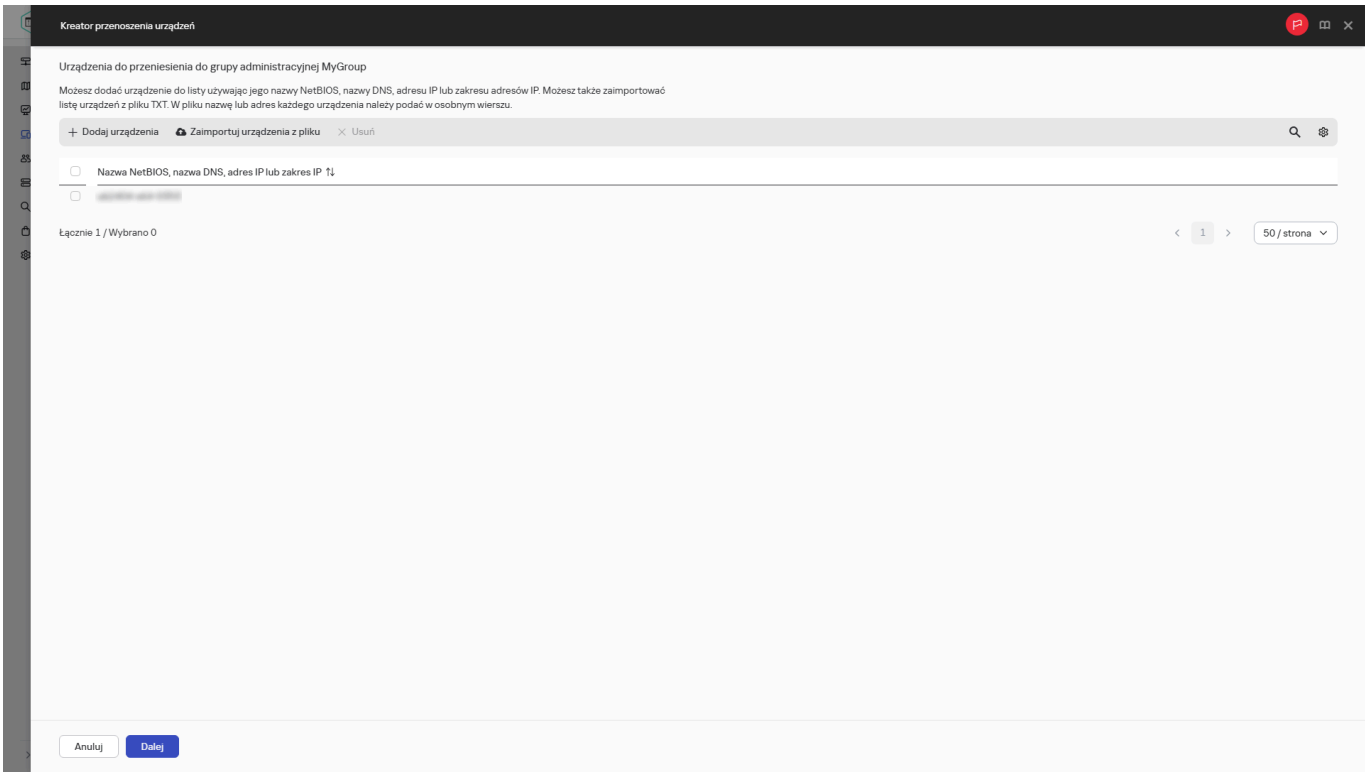
       Zakres adresów IP nie może zawierać więcej niż 1 048 576 adresów.

     - Podaj nazwę DNS urządzenia.

       Pole nazwy urządzenia nie może zawierać spacji, znaków backspace, a także następujących zakazanych znaków: , \ / * ' " ; : & ` ~ ! @ # $ ^ ( ) = + [ ] { } | < > %

- Kliknij przycisk **Zaimportuj urządzenia z pliku**, aby zaimportować listę urządzeń z pliku .txt. Adres lub nazwa każdego urządzenia musi znajdować się w oddzielnym wierszu.

  Plik nie może zawierać spacji, znaków backspace, a także następujących zakazanych znaków: , \ / * ' " ; : & ` ~ ! @ # $ ^ ( ) = + [ ] { } | < > %



Wybieranie urządzeń w celu przeniesienia do grupy administracyjnej.

5. Przejrzyj listę urządzeń, które mają zostać dodane do grupy administracyjnej. Możesz edytować listę, dodając lub usuwając urządzenia.

6. Jeśli upewnisz się, że lista jest poprawna, kliknij przycisk **Dalej**.

   Kreator przetwarza listę urządzeń i wyświetla wynik. Pomyślnie przetworzone urządzenia zostaną dodane do grupy administracyjnej i będą wyświetlane na liście urządzeń pod nazwami wygenerowanymi przez Serwer administracyjny.

Ręczne przenoszenie urządzeń lub klastrów do grupy administracyjnej

Możesz przenieść urządzenia z jednej grupy administracyjnej do innej lub z grupy nieprzypisanych urządzeń do grupy administracyjnej.

Możesz także przenosić klastry lub macierze serwerowe z jednej grupy administracyjnej do drugiej. Kiedy przenosisz klaster lub macierz serwerową do innej grupy, wszystkie jego węzły są przenoszone razem z nim, ponieważ klaster i dowolny z jego węzłów zawsze należą do tej samej grupy administracyjnej. Po wybraniu pojedynczego węzła klastra na karcie **Urządzenia** przycisk **Przenieś do grupy** staje się niedostępny.

W celu przeniesienia jednego lub kilku urządzeń lub klastrów do wybranej grupy administracyjnej:

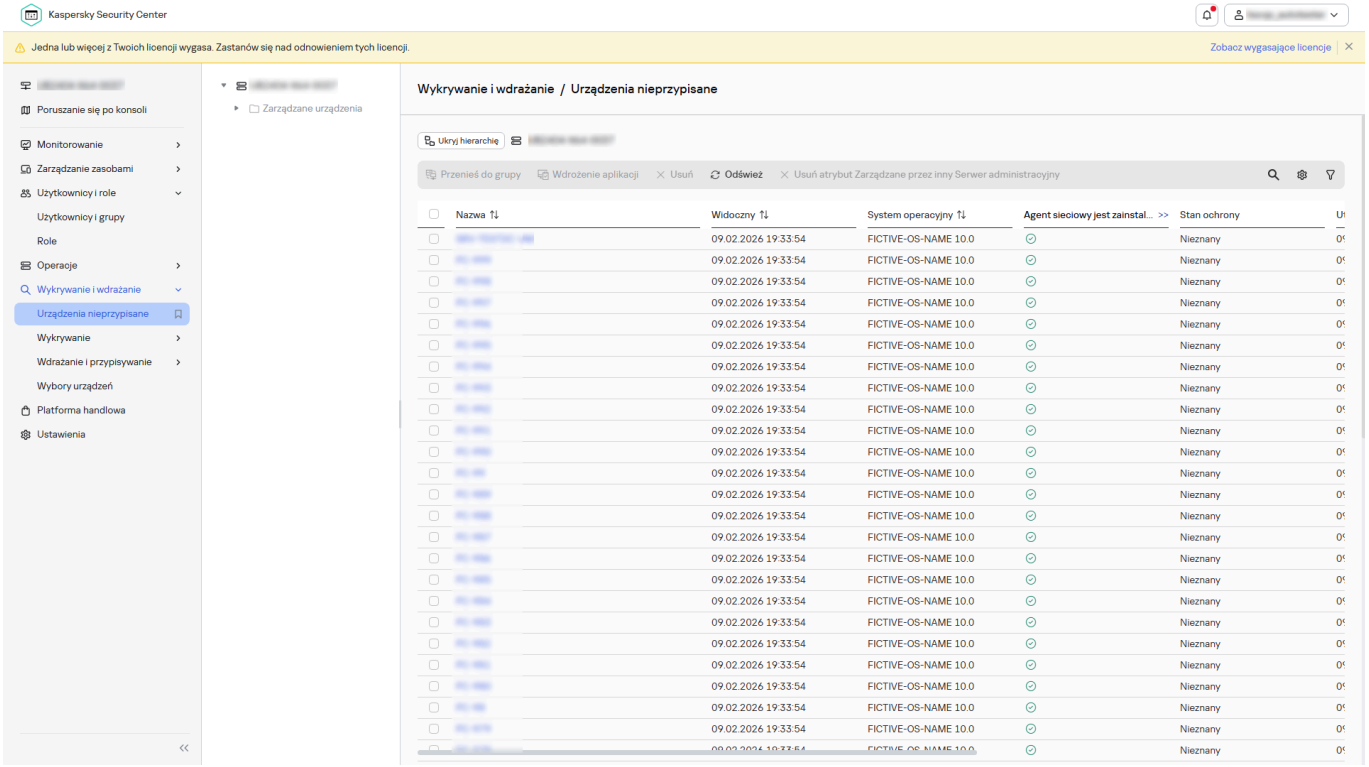
1. Otwórz grupę administracyjną, z której chcesz przenieść urządzenia. W tym celu wykonaj jedną z następujących czynności:

   - Aby otworzyć grupę administracyjną, w menu głównym przejdź do **Zarządzanie zasobami** → **Zasoby (urządzenia)**, a następnie wybierz żądaną grupę administracyjną.

     - W przypadku grupy głównej możesz przejść do następnego kroku.

     - Aby utworzyć podgrupę, kliknij przycisk **Pokaż hierarchię** na górze strony, a następnie w otwartym oknie wybierz żądaną grupę administracyjną.

   - Aby otworzyć grupę **Urządzenia nieprzypisane**, w menu głównym przejdź do **Zarządzanie zasobami** → **Urządzenia nieprzypisane**.



Lista nieprzypisanych urządzeń

2. Jeżeli grupa administracyjna zawiera klastry lub macierze serwerowe, sekcja **Zasoby (urządzenia)** jest podzielona na dwie karty — kartę **Urządzenia** oraz kartę **Klastry i grupy serwerów**. Otwórz kartę obiektu, który chcesz przenieść.

3. Zaznacz pola obok urządzeń lub klastrów, które chcesz przenieść do innej grupy.

4. Kliknij przycisk **Przenieś do grupy**.

5. W hierarchii grup administracyjnych zaznacz pole obok grupy administracyjnej, do której chcesz przenieść wybrane urządzenia lub klastry.

6. Kliknij przycisk **Przenieś**.

Wybrane urządzenia lub klastry są przenoszone do wybranej grupy administracyjnej.

Informacje o klastrach i macierzach serwerowych

Kaspersky Security Center Linux obsługuje technologię klastra. Jeśli Agent sieciowy wyśle na Serwer administracyjny informacje potwierdzające, że aplikacja zainstalowana na urządzeniu klienckim jest częścią grupy serwerów, to urządzenie klienckie staje się węzłem klastra.

Jeśli grupa administracyjna zawiera klastry lub macierze serwerowe, na stronie **Zasoby (urządzenia)** są wyświetlane dwie zakładki — jedna dla poszczególnych urządzeń, a druga dla klastrów i macierzy serwerowych. Po wykryciu zarządzanych urządzeń jako węzłów klastra, klaster jest dodawany jako pojedynczy obiekt na karcie **Klastry i grupy serwerów**.

Węzły klastra lub macierzy serwerowej są wymienione na karcie **Urządzenia** wraz z innymi zarządzanymi urządzeniami. Możesz przeglądać właściwości węzłów jako pojedynczych urządzeń i wykonywać inne operacje, ale nie możesz usunąć węzła klastra ani przenieść go do innej grupy administracyjnej niezależnie od jego klastra. Możesz usunąć lub przenieść tylko cały klaster.

Na klastrach lub macierzach serwerowych można wykonywać następujące operacje:

- Wyświetl właściwości
- Przenieś klaster lub macierz serwerową do innej grupy administracyjnej

  Kiedy przenosisz klaster lub macierz serwerową do innej grupy, wszystkie jego węzły są przenoszone razem z nim, ponieważ klaster i dowolny z jego węzłów zawsze należą do tej samej grupy administracyjnej.
- Delete

  Usunięcie klastra lub macierzy serwerowej jest zasadne tylko wtedy, gdy klaster lub macierz serwerowa nie istnieją już w sieci organizacji. Jeśli klaster jest nadal widoczny w Twojej sieci, a Agent sieciowy i aplikacja zabezpieczająca Kaspersky są nadal zainstalowane na węzłach klastra, Kaspersky Security Center Linux automatycznie przywraca usunięty klaster i jego węzły z powrotem na listę zarządzanych urządzeń.

Właściwości klastra lub macierzy serwerowej

Aby wyświetlić ustawienia klastra lub macierzy serwerów:

1. W menu głównym przejdź do **Zarządzanie zasobami** → **Zasoby (urządzenia)** → **Klastry i grupy serwerów**.

   Zostanie wyświetlona lista klastrów i macierzy serwerowych.
2. Kliknij nazwę wymaganego klastra lub macierzy serwerowej.

Zostanie wyświetlone okno właściwości wybranego klastra lub macierzy serwerowej.

Ogólne

W sekcji **Ogólne** wyświetlane są ogólne informacje dotyczące klastra lub macierzy serwerowej. Informacje są dostarczane w oparciu o dane otrzymane podczas ostatniej synchronizacji węzłów klastra z Serwerem administracyjnym:

- **Nazwa**
- **Opis**
- **Domena Windows**

  Domena lub grupa robocza systemu Windows, która zawiera klaster lub macierz serwerową.
- **Nazwa NetBIOS**

  Nazwa sieciowa systemu Windows klastra lub macierzy serwerowej.
- **Nazwa DNS**

  Nazwa domeny DNS klastra lub macierzy serwerowej.

Zadania

Na karcie **Zadania** możesz zarządzać zadaniami przydzielonymi do klastra lub macierzy serwerowej: przeglądać listę istniejących zadań; tworzyć nowe zadania; usuwać, uruchamiać i zatrzymywać zadania; modyfikować ustawienia zadań; oraz przeglądać wyniki ich wykonania. Wymienione zadania dotyczą aplikacji zabezpieczającej Kaspersky zainstalowanej na węzłach klastra. Kaspersky Security Center Linux otrzymuje listę zadań i szczegóły stanu zadań z węzłów klastra. Jeśli połączenie nie jest nawiązane, stan nie jest wyświetlany.

Węzły

Na tej karcie wyświetlana jest lista węzłów wchodzących w skład klastra lub macierzy serwerowej. Możesz kliknąć nazwę węzła, aby wyświetlić okno właściwości urządzenia.

Aplikacja Kaspersky

Okno właściwości może również zawierać dodatkowe karty z informacjami i ustawieniami związanymi z aplikacją zabezpieczającą Kaspersky zainstalowaną na węzłach klastra.

Dostosowanie punktów dystrybucji i bram połączenia

Struktura grup administracyjnych w Kaspersky Security Center Linux pełni następujące funkcje:

- Tworzy zakres zasad

  Istnieje alternatywny sposób stosowania odpowiednich ustawień na urządzeniach przy użyciu *profili zasad*.

- Tworzy zakres zadań grupowych

  Istnieje sposób określania zakresu zadań grupowych, który nie jest oparty na hierarchii grup administracyjnych: korzystanie z zadań dla wyboru urządzeń oraz z zadań dla określonych urządzeń.

- Nadaje urządzeniom, wirtualnym Serwerom administracyjnym oraz podrzędnym Serwerom administracyjnym prawa dostępu

- Przypisuje punkty dystrybucji

Podczas tworzenia struktury grup administracyjnych należy wziąć pod uwagę topologię sieci organizacji dla optymalnego przydzielenia punktów dystrybucji. Optymalne przydzielenie punktów dystrybucji pozwala na zmniejszenie ruchu w sieci organizacji.

W zależności od schematu organizacyjnego oraz topologii sieci, w strukturze grup administracyjnych można zastosować następujące standardowe konfiguracje:

- Jedno biuro

- Wiele małych, zdalnych biur

Urządzenia pełniące rolę punktów dystrybucji muszą być chronione, włączając w to ochronę fizyczną, przed wszelkim nieautoryzowanym dostępem.

Informacje o punktach dystrybucji

Urządzenie z zainstalowanym Agentem sieciowym może być używane jako punkt dystrybucji. W tym trybie Agent sieciowy może dystrybuować aktualizacje, które można pobrać z Serwera administracyjnego lub z serwerów Kaspersky. W tym drugim przypadku skonfiguruj pobieranie aktualizacji dla danego punktu dystrybucji.

Wdrożenie punktów dystrybucji w sieci organizacji realizuje następujące cele:

- Zmniejszanie obciążenia na Serwerze administracyjnym.

- Optymalizowanie ruchu sieciowego.

- Zapewnienie Serwerowi administracyjnemu dostępu do urządzeń w ciężko dostępnych miejscach sieci organizacji. Dostępność punktu dystrybucji w sieci poza NAT (w powiązaniu z Serwerem administracyjnym) umożliwia Serwerowi administracyjnemu wykonywanie następujących działań:

  - Wysyłanie powiadomień do urządzeń przez UDP w sieci IPv4 lub IPv6

  - Przeszukiwanie sieci IPv4 lub IPv6

- Przeprowadzanie wstępnego wdrożenia
- Pełnienie funkcji serwera push

Punkt dystrybucji jest przydzielony do grupy administracyjnej. W tym przypadku zakres działania punktu dystrybucji obejmuje wszystkie urządzenia w grupie administracyjnej i jej podgrupach. Jednakże urządzenie pełniące funkcję punktu dystrybucji może nie znajdować się w grupie administracyjnej, do której zostało przydzielone.

Możesz sprawić, że punkt dystrybucji będzie działał jako brama połączenia. W tym przypadku urządzenia objęte zakresem działania punktu dystrybucji będą łączyły się z Serwerem administracyjnym poprzez bramę, a nie bezpośrednio. Ten tryb może być przydatny w scenariuszach, które nie zezwalają na nawiązywanie bezpośredniego połączenia między Serwerem administracyjnym a zarządzanymi urządzeniami.

Jeśli używasz urządzenia opartego na systemie Linux jako punktu dystrybucji, zdecydowanie zalecamy zwiększenie limitu deskryptorów plików dla usługi klnagent, ponieważ jeśli zakres punktu dystrybucji obejmuje wiele urządzeń, domyślna maksymalna liczba plików, które można otworzyć, może być niewystarczająca.

Standardowa konfiguracja punktów dystrybucji: Jedno biuro

W standardowej konfiguracji „jedno biuro” wszystkie urządzenia znajdują się w obrębie sieci organizacji i są dla siebie widoczne. Sieć organizacji może zawierać kilka oddzielnych części (sieci lub fragmentów sieci) połączonych ze sobą wąskimi kanałami.

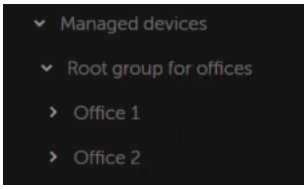
Dostępne są następujące metody tworzenia struktury grup administracyjnych:

- Tworzenie struktury grup administracyjnych z uwzględnieniem topologii sieci. Struktura grup administracyjnych nie musi odzwierciedlać topologii sieci z absolutną dokładnością. Wystarczy dopasowanie oddzielnych części sieci i pewnych grup administracyjnych. Możesz skorzystać z automatycznego przydzielenia punktów dystrybucji lub zrobić to ręcznie.
- Tworzenie struktury grup administracyjnych bez uwzględnienia topologii sieci. W tym przypadku należy wyłączyć automatyczne przydzielanie punktów dystrybucji, a następnie wskazać jedno lub kilka urządzeń jako punkty dystrybucji dla głównej grupy administracyjnej w każdej z oddzielnych części sieci, na przykład dla grupy **Zarządzane urządzenia**. Wszystkie punkty dystrybucji będą na tym samym poziomie i będą obejmować ten sam obszar, uwzględniając wszystkie urządzenia w sieci organizacji. W takim przypadku każdy z Agentów sieciowych połączy się z punktem dystrybucji o najkrótszej trasie. Trasę do punktu dystrybucji można ustalić za pomocą narzędzia tracert.

Standardowa konfiguracja punktów dystrybucji: Małe zdalne biura

Ta standardowa konfiguracja została utworzona z myślą o małych zdalnych biurach, które mogą kontaktować się z główną siedzibą za pośrednictwem internetu. Każde zdalne biuro znajduje się poza NAT, czyli połączenie jednego zdalnego biura z innym jest niemożliwe, gdyż biura są od siebie odizolowane.

Konfiguracja musi być odzwierciedlona w strukturze grup administracyjnych: dla każdego zdalnego biura musi zostać utworzona oddzielna grupa administracyjna (grupy **Office 1** i **Office 2** na rysunku poniżej).



Zdalne biura uwzględnione w strukturze grupy administracyjnej

Do każdej grupy administracyjnej odpowiadającej biuru należy przydzielić jeden lub kilka punktów dystrybucji. Punktami dystrybucji muszą być urządzenia w zdalnym biurze, które posiadają wystarczającą ilość wolnego miejsca na dysku. Urządzenia z grupy **Office 1** będą, na przykład, łączyć się z punktami dystrybucji przydzielonymi do grupy administracyjnej **Office 1**.

Jeśli niektórzy użytkownicy poruszają się między biurami ze swoimi laptopami, w każdym zdalnym biurze, dla grupy administracyjnej najwyższego poziomu (**Główna grupa dla biur** na poniższym rysunku) należy wskazać dwa lub więcej urządzeń jako punkty dystrybucji (oprócz już istniejących punktów dystrybucji).

Na przykład: Laptop znajduje się w grupie administracyjnej **Office 1**, a następnie zostaje fizycznie przeniesiony do biura, które odpowiada grupie administracyjnej **Office 2**. Po przeniesieniu laptopa, Agent sieciowy spróbuje połączyć się z punktami dystrybucji przypisanymi do grupy **Office 1**, ale te punkty dystrybucji są niedostępne. Następnie Agent sieciowy próbuje połączyć się z punktami dystrybucji, które zostały przypisane do **Głównej grupy dla biur**. Ponieważ zdalne biura są odizolowane od siebie, próby nawiązania połączenia z punktami dystrybucji przypisanymi do grupy administracyjnej **Główna grupa dla biur** zakończą się pomyślnie tylko wtedy, gdy Agent sieciowy spróbuje połączyć się z punktami dystrybucji w grupie **Office 2**. Oznacza to, że laptop pozostanie w grupie administracyjnej, która odpowiada pierwszemu biuru, ale będzie korzystał z punktu dystrybucji biura, w którym aktualnie się znajduje.

Obliczanie liczby i konfigurowanie punktów dystrybucji

Im więcej urządzeń klienckich zawiera sieć, tym więcej punktów dystrybucji wymaga. Nie jest zalecane wyłączanie automatycznego przypisywania punktów dystrybucji. Jeśli automatyczne przypisywanie punktów dystrybucji jest włączone, Serwer administracyjny przypisuje punkty dystrybucji, gdy liczba urządzeń klienckich jest dosyć duża, oraz definiuje ich konfigurację.

Używanie specjalnie przypisanych punktów dystrybucji

Jeśli planujesz używać określonych urządzeń jako punktów dystrybucji (na przykład, specjalnie wybranych serwerów), możesz zrezygnować z automatycznego przypisywania punktów dystrybucji. W tym przypadku upewnij się, że na urządzeniach, które mają pełnić rolę punktów dystrybucji, jest wystarczająca ilość wolnego miejsca, nie są regularnie wyłączane, a tryb uśpienia jest na nich wyłączony.

Liczba specjalnie przypisanych punktów dystrybucji w sieci, która zawiera pojedynczy segment sieci w oparciu o liczbę urządzeń w sieci

Liczba urządzeń klienckich w segmencie sieci	Liczba punktów dystrybucji
Mniej niż 300	0 (nie przypisuj punktów dystrybucji)
Więcej niż 300	Dopuszczalne: (N/10 000 + 1), zalecane: (N/5000 + 2), gdzie N to liczba urządzeń w sieci

Liczba specjalnie przypisanych punktów dystrybucji w sieci, która zawiera kilka segmentów sieci w oparciu o liczbę urządzeń w sieci

Liczba urządzeń klienckich na segment sieci	Liczba punktów dystrybucji
Mniej niż 10	0 (nie przypisuj punktów dystrybucji)
10–100	1
Więcej niż 100	Dopuszczalne: (N/10 000 + 1), zalecane: (N/5000 + 2), gdzie N to liczba urządzeń w sieci

Korzystanie ze standardowych urządzeń klienckich (stacji roboczych) jako punktów dystrybucji

Jeśli planujesz używać standardowych urządzeń klienckich (czyli stacji roboczych) jako punktów dystrybucji, zalecane jest przypisanie punktów dystrybucji w sposób pokazany w tabelach poniżej, aby uniknąć nadmiernego obciążenia kanałów komunikacji i Serwera administracyjnego:

Liczba stacji roboczych działających jako punkty dystrybucji w sieci, która zawiera pojedynczy segment sieci w oparciu o liczbę urządzeń w sieci

Liczba urządzeń klienckich w segmencie sieci	Liczba punktów dystrybucji
Mniej niż 300	0 (nie przypisuj punktów dystrybucji)
Więcej niż 300	(N/300 + 1), gdzie N oznacza liczbę urządzeń w sieci; muszą być przynajmniej 3 punkty dystrybucji

Liczba stacji roboczych działających jako punkty dystrybucji w sieci, która zawiera kilka segmentów sieci w oparciu o liczbę urządzeń w sieci

Liczba urządzeń klienckich na segment sieci	Liczba punktów dystrybucji
Mniej niż 10	0 (nie przypisuj punktów dystrybucji)
10–30	1
31–300	2
Więcej niż 300	(N/300 + 1), gdzie N oznacza liczbę urządzeń w sieci; muszą być przynajmniej 3 punkty dystrybucji

Jeśli punkt dystrybucji jest wyłączony (lub z jakiegoś powodu niedostępny), zarządzane urządzenia w tym obszarze mogą uzyskać dostęp do Serwera administracyjnego w celu pobrania uaktualnień.

Automatyczne przypisywanie punktów dystrybucji

Zalecane jest automatyczne przypisywanie punktów dystrybucji. W tym przypadku, Kaspersky Security Center Linux sam wybierze urządzenia, które mają być punktami dystrybucji.

Urządzenia z systemem Microsoft Windows oparte na architekturze Arm nie mogą pełnić funkcji punktów dystrybucji.

Aby automatycznie przypisać punkty dystrybucji:

1. W menu głównym kliknij nazwę Serwera administracyjnego.

   Zostanie otwarte okno właściwości Serwera administracyjnego.

2. Na zakładce **Ogólne** wybierz sekcję **Punkty dystrybucji**.

3. Wybierz opcję **Automatycznie przypisz punkty dystrybucji**.

> Jeśli włączone jest automatyczne wskazywanie urządzeń jako punktów dystrybucji, nie można ręcznie skonfigurować punktów dystrybucji, ani też zmodyfikować listy punktów dystrybucji.

4. Kliknij przycisk **Zapisz**.

Serwer administracyjny automatycznie przypisze i skonfiguruje punkty dystrybucji.

Ręczne przypisywanie punktów dystrybucji

Kaspersky Security Center Linux umożliwia ręczne wskazanie urządzeń do pełnienia roli punktów dystrybucji.

Zalecane jest automatyczne przypisywanie punktów dystrybucji. W tym przypadku, Kaspersky Security Center Linux sam wybierze urządzenia, które mają być punktami dystrybucji. Jednakże, jeśli z jakiegoś powodu musisz zrezygnować z automatycznego przypisywania punktów dystrybucji (na przykład, jeśli chcesz korzystać ze specjalnie wybranych serwerów), możesz ręcznie przypisać punkty dystrybucji po obliczeniu liczby i konfiguracji punktów dystrybucji.

> Urządzenia pełniące rolę punktów dystrybucji muszą być chronione, włączając w to ochronę fizyczną, przed wszelkim nieautoryzowanym dostępem.

> Urządzenia z systemem Microsoft Windows oparte na architekturze Arm nie mogą pełnić funkcji punktów dystrybucji.

W celu ręcznego wskazania urządzenia jako punktu dystrybucji:

1. W menu głównym kliknij nazwę Serwera administracyjnego.

   Zostanie otwarte okno właściwości Serwera administracyjnego.

2. Na zakładce **Ogólne** wybierz sekcję **Punkty dystrybucji**.

3. Wybierz opcję **Ręcznie przypisz punkty dystrybucji**.

4. Kliknij przycisk **Przypisz**.

5. Wybierz urządzenie, które ma być punktem dystrybucji.

   Podczas wybierania urządzenia pamiętaj o zasadach działania punktów dystrybucji i wymaganiach ustawionych dla urządzenia pełniącego rolę punktu dystrybucji.

6. Wybierz grupę administracyjną, którą chcesz uwzględnić w obszarze wybranego punktu dystrybucji.

7. Kliknij przycisk **OK**.

   Dodany punkt dystrybucji będzie wyświetlany na liście punktów dystrybucji, w sekcji **Punkty dystrybucji**.

8. Na liście kliknij nowo dodany punkt dystrybucji, aby otworzyć jego okno właściwości.

9. Skonfiguruj punkt dystrybucji w oknie właściwości:

- Sekcja **Ogólne** zawiera ustawienia interakcji pomiędzy punktem dystrybucji a urządzeniami klienckimi.

  - **Port SSL**

    Numer portu SSL do nawiązywania zaszyfrowanych połączeń między urządzeniami klienckimi a punktem dystrybucji przy użyciu SSL.

    Domyślnie wykorzystywany jest port 13000.

  - **Włączone**

    Jeśli ta opcja jest włączona, multicasting IP będzie używany do automatycznego rozsyłania pakietów instalacyjnych na urządzenia klienckie w obrębie grupy.

    Multiemisja IP zmniejsza czas wymagany do zainstalowania aplikacji z pakietu instalacyjnego w grupie urządzeń klienckich, ale zwiększa czas instalacji, gdy instalujesz aplikację na jednym urządzeniu klienckim.

  - **Adres multiemisji IP**

    Adres IP, który będzie używany do multiemisji. Możesz zdefiniować adres IP z zakresu 224.0.0.0 – 239.255.255.255

    Domyślnie, Kaspersky Security Center Linux automatycznie przypisze unikatowy adres IP multiemisji w obrębie danego zakresu.

  - **Numer portu multiemisji IP**

    Numer portu do multiemisji IP.

    Domyślnym numerem portu jest 15001. Jeśli jako punkt dystrybucji określono urządzenie, na którym działa Serwer administracyjny, domyślnie dla połączenia SSL używany jest port 13001.

  - **Adres punktu dystrybucji dla urządzeń zdalnych**

    Adres sieciowy, za pośrednictwem którego urządzenia zdalne łączą się z punktem dystrybucji.

  - **Włączone**

    Aktualizacje są dystrybuowane na zarządzane urządzenia z następujących źródeł:

    - Ten punkt dystrybucji, jeśli ta opcja jest włączona.
    - Inne punkty dystrybucji, Serwer administracyjny lub serwery aktualizacji Kaspersky, jeśli ta opcja jest wyłączona.

    Jeśli używasz punktów dystrybucji do wdrażania aktualizacji, możesz zmniejszyć ruch, ponieważ zmniejszasz liczbę pobrań. Możesz także odciążyć Serwer administracyjny i przenieść obciążenie między punktami dystrybucji. Możesz obliczyć liczbę punktów dystrybucji w Twojej sieci w celu optymalizacji ruchu i obciążenia.

    Jeśli wyłączysz tę opcję, liczba pobrań aktualizacji i obciążenia Serwera administracyjnego mogą wzrosnąć. Domyślnie opcja ta jest włączona.

  - **Włączone**

    Pakiety instalacyjne są dystrybuowane na zarządzane urządzenia z następujących źródeł:

    - Ten punkt dystrybucji, jeśli ta opcja jest włączona.
    - Inne punkty dystrybucji, Serwer administracyjny lub serwery aktualizacji Kaspersky, jeśli ta opcja jest wyłączona.

Jeśli używasz punktów dystrybucji do wdrażania pakietów instalacyjnych, możesz zmniejszyć ruch, ponieważ zmniejszasz liczbę pobrań. Możesz także odciążyć Serwer administracyjny i przenieść obciążenie między punktami dystrybucji. Możesz obliczyć liczbę punktów dystrybucji w Twojej sieci w celu optymalizacji ruchu i obciążenia.

Jeśli wyłączysz tę opcję, liczba pobrań pakietów instalacyjnych i obciążenie Serwera administracyjnego może wzrosnąć. Domyślnie opcja ta jest włączona.

- **Włączone**

  W Kaspersky Security Center Linux punkt dystrybucji może działać jako serwer push dla urządzeń zarządzanych za pośrednictwem protokołu mobilnego oraz zarządzanych za pośrednictwem agenta sieciowego. Na przykład, serwer push musi być włączony, jeśli chcesz mieć możliwość wymuszenia synchronizacji urządzeń KasperskyOS z Serwerem administracyjnym. Serwer push posiada ten sam obszar zarządzanych urządzeń jako punkt dystrybucji, na którym włączono serwer push. Jeśli posiadasz kilka punktów dystrybucji przypisanych dla tej samej grupy administracyjnej, możesz włączyć serwer push na każdym punkcie dystrybucji. W tym przypadku Serwer administracyjny rozkłada obciążenie między punkty dystrybucji.

- **Port serwera push**

  Numer portu serwera push. Możesz określić numer dowolnego zajętego portu.

- W sekcji **Zakres** określ grupy administracyjne, do których punkt dystrybucji będzie dystrybuować aktualizacje.

- W sekcji **Źródło aktualizacji** możesz wybrać źródło aktualizacji dla punktu dystrybucji:

  - **Źródło aktualizacji**

    Wybierz źródło aktualizacji dla punktu dystrybucji:

    - Aby zezwolić punktowi dystrybucji na pobieranie uaktualnień z Serwera administracyjnego, zaznacz opcję **Pobierz z Serwera administracyjnego**.

    - Aby umożliwić punktowi dystrybucji otrzymywanie aktualizacji za pomocą zadania, wybierz **Użyj zadania pobierania aktualizacji**, a następnie określ zadanie *Pobierz aktualizacje do repozytoriów punktów dystrybucji*:

      - Jeśli takie zadanie już istnieje na urządzeniu, wybierz zadanie z listy.

      - Jeśli takie zadanie jeszcze nie istnieje na urządzeniu, kliknij łącze **Utwórz zadanie**, aby utworzyć zadanie. Zostanie uruchomiony Kreator tworzenia nowego zadania. Postępuj zgodnie z instrukcjami kreatora.

  - **Pobierz pliki diff**

    Ta opcja włącza funkcję pobierania plików diff.

    Domyślnie opcja ta jest włączona.

- Jeśli Twoje punkty dystrybucji korzystają z serwera proxy podczas łączenia się z Internetem, w podsekcji **Ustawienia połączenia internetowego** możesz określić następujące ustawienia:

  - **Użyj serwera proxy**

    Jeśli to pole wyboru jest zaznaczone, do łączenia punktów dystrybucji z serwerami aktualizacji Kaspersky używany jest internetowy serwer proxy. W polach można skonfigurować połączenie z serwerem proxy.

    Domyślnie pole to nie jest zaznaczone.

- **Adres serwera proxy**

  Adres serwera proxy.

- **Numer portu**

  Numer portu używanego do nawiązywania połączenia.

- **Pomiń serwer proxy dla adresów lokalnych**

  Jeśli ta opcja jest włączona, żaden serwer proxy nie będzie używany do nawiązywania połączenia z urządzeniami w sieci lokalnej.

  Domyślnie opcja ta jest wyłączona.

- **Uwierzytelnianie na serwerze proxy**

  Jeśli to pole jest zaznaczone, w polach wejściowych możesz określić dane uwierzytelniające do autoryzacji na serwerze proxy.

  Domyślnie pole to nie jest zaznaczone.

- **Nazwa użytkownika**

  Konto użytkownika, z poziomu którego nawiązywane jest połączenie z serwerem proxy.

- **Hasło**

  Hasło do konta, z poziomu którego zadanie będzie uruchamiane.

- W sekcji **KSN Proxy** możesz skonfigurować aplikację, aby używała punktu dystrybucji do przesyłania żądań KSN z zarządzanych urządzeń:

  - **Włącz KSN Proxy po stronie punktu dystrybucji**

    Usługa KSN proxy jest uruchamiana na urządzeniu, które jest używane jako punkt dystrybucji. Użyj tej funkcji do redystrybucji i optymalizacji ruchu w sieci.

    Punkt dystrybucji wysyła statystyki KSN, które zostały wymienione w Oświadczeniu Kaspersky Security Network, do Kaspersky.

    Domyślnie opcja ta jest wyłączona. Włączenie tej opcji działa, jeśli opcje **Użyj Serwera administracyjnego jako serwera proxy** i **Zgadzam się na korzystanie z Kaspersky Security Network** zostały włączone w oknie właściwości Serwera administracyjnego.

    Możesz przypisać węzeł klastra aktywny-pasywny do punktu dystrybucji i włączyć serwer proxy KSN na tym węźle.

  - **Przesyłaj żądania KSN do Serwera administracyjnego**

    Punkt dystrybucji przesyła żądania KSN z zarządzanych urządzeń do Serwera administracyjnego.

    Domyślnie opcja ta jest włączona.

  - **Dostęp do KSN Cloud/KPSN bezpośrednio przez Internet**

    Punkt dystrybucji przesyła żądania KSN z zarządzanych urządzeń do chmury KSN lub KPSN. Żądania KSN wygenerowane na samym punkcie dystrybucji są także wysyłane bezpośrednio do chmury KSN lub KPSN.

- **Ignoruj ustawienia serwera proxy w przypadku łączenia z KPSN**

  Włącz tę opcję, jeśli skonfigurowałeś ustawienia serwera proxy we właściwościach punktu dystrybucji lub w zasadzie Agenta sieciowego, ale architektura Twojej sieci wymaga bezpośredniego korzystania z KPSN. W przeciwnym razie, żądania z zarządzanych aplikacji nie będą mogły dotrzeć do KPSN.

  Ta opcja jest dostępna, jeśli wybierzesz opcję **Dostęp do KSN Cloud/KPSN bezpośrednio przez Internet**.

- **Port**

  Numer portu TCP, którego zarządzane urządzenia będą używały do nawiązywania połączenia z serwerem KSN proxy. Domyślny numer portu to 13111.

- **Użyj portu UDP**

  Jeśli chcesz, żeby zarządzane urządzenia nawiązywały połączenie z serwerem KSN proxy poprzez port UDP, włącz opcję **Użyj portu UDP** i określ numer portu UDP. Domyślnie opcja ta jest włączona.

- **Port UDP**

  Numer portu UDP, którego zarządzane urządzenia będą używały do nawiązywania połączenia z serwerem KSN proxy. Domyślny port UDP do nawiązywania połączenia z serwerem KSN Proxy to 15111.

- **Użyj HTTPS**

  Jeśli chcesz, aby zarządzane urządzenia nawiązywały połączenie z serwerem KSN Proxy poprzez port HTTPS, włącz opcję **Użyj HTTPS** i określ numer **HTTPS przez port**. Domyślny port HTTPS do nawiązywania połączenia z serwerem KSN Proxy to 17111.

- **Port HTTPS**

  Numer portu HTTPS, którego zarządzane urządzenia będą używały do nawiązywania połączenia z serwerem KSN Proxy. Domyślny port HTTPS do nawiązywania połączenia z serwerem KSN Proxy to 17111.

- W sekcji **Brama połączenia** możesz skonfigurować punkt dystrybucyjny tak, aby działał jako brama połączenia między instancjami Agenta sieciowego a Serwerem administracyjnym:

  - **Brama połączenia**

    Jeżeli bezpośrednie połączenie między Serwerem administracyjnym a Agentami sieciowymi nie może zostać nawiązane z powodu organizacji Twojej sieci, możesz użyć punktu dystrybucji, aby działał jako brama połączenia między Serwerem administracyjnym a Agentami sieciowymi.

    Włącz tę opcję, jeśli chcesz, aby punkt dystrybucji działał jako brama połączenia między Agentami sieciowymi a Serwerem administracyjnym. Domyślnie opcja ta jest wyłączona.

  - **Nawiąż połączenie z bramą z poziomu Serwera administracyjnego (jeśli brama znajduje się w DMZ)**

    Jeżeli Serwer administracyjny znajduje się poza strefą zdemilitaryzowaną (DMZ), w sieci lokalnej, Agenty sieciowe zainstalowane na zdalnych urządzeniach nie mogą łączyć się z Serwerem administracyjnym. Możesz użyć punktu dystrybucji jako bramy połączenia z odwrotną łącznością (Serwer administracyjny nawiązuje połączenie z punktem dystrybucji).

    Włącz tę opcję, jeśli chcesz połączyć Serwer administracyjny z bramą połączenia w strefie DMZ.

  - **Otwórz lokalny port dla Kaspersky Security Center Web Console**

    Włącz tę opcję, jeśli chcesz, aby brama połączenia w strefie DMZ otwierała port dla Web Console znajdujący się w strefie DMZ lub w Internecie. Określ numer portu, który będzie używany do połączenia z Web Console do punktu dystrybucji. Domyślny numer portu to 13299.

Ta opcja jest dostępna, jeśli włączysz opcję **Nawiąż połączenie z bramą z poziomu Serwera administracyjnego (jeśli brama znajduje się w DMZ)**.

Podczas podłączania urządzeń mobilnych do Serwera administracyjnego za pośrednictwem punktu dystrybucji pełniącego funkcję bramy połączenia można włączyć następujące opcje:

- **Otwórz port dla urządzeń mobilnych (tylko uwierzytelnianie SSL Serwera administracyjnego)**

  Włącz tę opcję, jeśli potrzebujesz, aby brama połączenia otwierała port dla urządzeń mobilnych i określała numer portu, którego będą używać urządzenia mobilne do łączenia się z punktem dystrybucji. Domyślny numer portu to 13292. Urządzenie mobilne sprawdzi certyfikat Serwera administracyjnego. Podczas nawiązywania połączenia uwierzytelniany jest tylko Serwer administracyjny.

- **Otwórz port dla urządzeń mobilnych (wzajemne uwierzytelnianie SSL)**

  Włącz tę opcję, jeśli potrzebujesz bramy połączenia, aby otworzyć port, który będzie używany do dwukierunkowej autoryzacji Serwera administracyjnego i urządzeń mobilnych. Urządzenie mobilne sprawdzi certyfikat Serwera administracyjnego, a Serwer administracyjny sprawdzi certyfikat urządzenia mobilnego. Określ następujące parametry:

  - Numer portu, którego urządzenia mobilne będą używać do łączenia się z punktem dystrybucji. Domyślny numer portu to 13293.

  - Nazwy domen DNS bramy połączenia, które będą używane przez urządzenia mobilne. Oddziel nazwy domen przecinkami. Określone nazwy domen zostaną uwzględnione w certyfikacie punktu dystrybucji. Jeśli nazwy domen używane przez urządzenia mobilne nie są zgodne z nazwą wspólną w certyfikacie punktu dystrybucji, urządzenia mobilne nie łączą się z punktem dystrybucji.

    Domyślną nazwą domeny DNS jest nazwa FQDN bramy połączenia.

W obu przypadkach certyfikaty są sprawdzane wyłącznie podczas nawiązywania sesji TLS w punkcie dystrybucji. Certyfikaty nie są przesyłane do sprawdzenia przez Serwer administracyjny. Po nawiązaniu sesji TLS z urządzeniem mobilnym punkt dystrybucji używa certyfikatu serwera administracyjnego w celu utworzenia tunelu umożliwiającego synchronizację między urządzeniem mobilnym a Serwerem administracyjnym. Jeśli otworzysz port dla dwukierunkowego uwierzytelniania SSL, jedynym sposobem na dystrybucję certyfikatu urządzenia mobilnego będzie użycie pakietu instalacyjnego.

- Skonfiguruj przeszukiwania sieci Windows przez punkt dystrybucji oparty na systemie Windows.

  - **Domeny Windows**

    Możesz włączyć wykrywanie urządzeń dla domen Windows i ustawić terminarz dla wyszukiwania.

- Skonfiguruj przeszukiwanie kontrolera domeny przez punkt dystrybucji.

  - **Przeszukiwanie sterowników domeny**

    Możesz włączyć wykrywanie urządzeń dla kontrolerów domeny.

    W polu **Przeszukiwanie** po przełączeniu przycisku przełącznika na pozycję **Włączone** możesz wybrać kontrolery domeny, które chcesz przeszukiwać, a także określić dla nich harmonogram przeszukiwania.

    Jeśli korzystasz z punktu dystrybucji systemu Linux, w sekcji **Przeszukaj określone domeny** kliknij opcję **Dodaj**, a następnie określ adres i dane uwierzytelniające użytkownika kontrolera domeny. Można również określić typ domeny, która ma być przeszukiwana: Active Directory lub Samba, FreeIPA, ALD Pro.

Jeśli korzystasz z punktu dystrybucji systemu Windows, możesz wybrać jedną z następujących opcji:

- **Przeszukaj bieżącą domenę**
- **Przeszukaj cały las domeny**
- **Przeszukaj określone domeny**

- Skonfiguruj przeszukiwanie zakresów adresów IP przez punkt dystrybucji.
  - **Przeszukiwanie zakresów IP**

    Możesz włączyć wykrywanie urządzeń dla zakresów IPv4 i sieci IPv6.

    Jeśli włączysz opcję **Włącz przeszukiwanie zakresów**, możesz dodać skanowane zakresy i skonfigurować dla nich terminarz. Możesz dodać zakresy IP do listy skanowanych zakresów.

    Jeśli włączysz opcję **Użyj Zeroconf do przeszukania sieci IPv6**, punkt dystrybucji automatycznie odpytuje sieć IPv6 za pomocą zero-configuration networking (zwany również *Zeroconf*). W takim przypadku określone zakresy adresów IP są ignorowane, ponieważ punkt dystrybucji przeszukuje całą sieć. Opcja **Użyj Zeroconf do przeszukania sieci IPv6** jest dostępna, jeśli w punkcie dystrybucji działa system Linux. Aby korzystać z odpytywania Zeroconf IPv6, musisz zainstalować narzędzie avahi-browse w punkcie dystrybucji.

- W sekcji **Zaawansowane** określ folder, którego punkt dystrybucji musi używać do przechowywania rozsyłanych danych.
  - **Użyj folderu domyślnego**

    Jeśli wybierzesz tę opcję, aplikacja użyje folderu instalacyjnego Agenta sieciowego na urządzeniu działającym jako punkt dystrybucji.

  - **Użyj określonego folderu**

    Jeśli wybierzesz tę opcję, w polu poniżej możesz określić ścieżkę dostępu do wybranego folderu. Może to być folder lokalny na urządzeniu działającym jako punkt dystrybucji lub folder na dowolnym urządzeniu w obrębie sieci korporacyjnej.

    Konto użytkownika używane na urządzeniu działającym jako punkt dystrybucji do uruchamiania Agenta sieciowego musi mieć uprawnienia do odczytu/zapisu określonego folderu.

10. Kliknij przycisk **OK**.

Wybrane urządzenia będą pełnić rolę punktów dystrybucji.

Dodawanie bramy połączenia w strefie DMZ jako punktu dystrybucji

Jeśli Serwer administracyjny znajduje się poza strefą zdemilitaryzowaną (DMZ), Agenty sieciowe zainstalowane na urządzeniach zewnętrznych nie mogą nawiązać połączenia z Serwerem administracyjnym. W tym przypadku możesz użyć punktu dystrybucji jako bramy połączenia w strefie DMZ. Punkt dystrybucji otwiera port dla Serwera administracyjnego w celu nawiązania połączenia. Po uruchomieniu Serwera administracyjnego połączy się on z punktem dystrybucji i utrzyma to połączenie podczas całej sesji.

Jeśli konieczne jest nawiązanie połączenia między Serwerem administracyjnym a zarządzanymi urządzeniami poza okresem synchronizacji między Agentem sieciowym a Serwerem administracyjnym, należy włączyć serwer push i otworzyć port 13295 po stronie punktu dystrybucji.

Zalecamy użycie specjalnie przypisanego urządzenia jako bramy połączenia. Informacje na temat maksymalnej liczby urządzeń klienckich (w tym urządzeń mobilnych) można znaleźć w poradniku dotyczącym rozmiarów.

> Brama połączenia oczekuje na połączenia z Serwerem administracyjnym bardziej niż nawiązuje te połączenia z Serwerem administracyjnym. To oznacza, że od razu po zainstalowaniu bramy połączenia na urządzeniu w DMZ, Serwer administracyjny nie wyświetla urządzenia wśród zarządzanych urządzeń. Dlatego też należy przeprowadzić specjalną procedurę w celu zapewnienia, że Serwer administracyjny zainicjuje połączenie z bramą połączenia.

W celu dodania urządzenia z bramą połączenia jako punktu dystrybucji:

1. W menu głównym kliknij nazwę Serwera administracyjnego.

   Zostanie otwarte okno właściwości Serwera administracyjnego.

2. Na zakładce **Ogólne** wybierz sekcję **Punkty dystrybucji**.

3. Wybierz opcję **Ręcznie przypisz punkty dystrybucji**.

4. Na pasku narzędzi kliknij przycisk **Przypisz**.

5. W prawej części okna wykonaj jedną z następujących czynności:

   a. Wybierz opcję **Użyj bramy połączenia DMZ przy użyciu adresu**.

   b. W polu **Adres bramy połączenia** określ adres IP urządzenia lub nazwę DNS.

   c. Kliknij przycisk **Przypisz**.

   d. Panel zostanie zamknięty, a punkt dystrybucji zostanie wyświetlony z **Wpis tymczasowy dla bramy połączenia**.

6. Kliknij przycisk **Zapisz**.

   Serwer administracyjny próbuje nawiązać połączenie z bramą połączenia pod podanym adresem. Jeśli się powiedzie, nazwa wpisu zmieni się na nazwę urządzenia bramy połączenia. Ten proces trwa do pięciu minut.

Jeśli otworzysz właściwości punktu dystrybucji, klikając **Wpis tymczasowy dla bramy połączenia**, wszystkie opcje będą wyszarzone. Możesz wyświetlić tylko zakładkę Ogólne, która wyświetla nazwę punktu dystrybucji. Domyślnie wykorzystywany jest port (13000). Możesz skonfigurować punkt dystrybucji dopiero po połączeniu się z nim przez Serwer administracyjny. Podczas gdy tymczasowy wpis dla bramy połączenia jest konwertowany na nazwany wpis, brama połączenia pojawia się również w grupie Nieprzypisane urządzenia.

Aby dodać bramę połączenia do wcześniej skonfigurowanej sieci:

1. Zainstaluj Agenta sieciowego w trybie bramy połączenia.

2. Ponownie zainstaluj Agenta sieciowego na urządzeniach, które chcesz połączyć z nowo dodaną bramą połączenia.

Modyfikowanie listy punktów dystrybucji dla grupy administracyjnej

Możesz wyświetlić listę punktów dystrybucji przypisanych do określonej grupy administracyjnej oraz zmodyfikować listę, dodając lub usuwając punkty dystrybucji.

W celu przejrzenia i zmodyfikowania listy punktów dystrybucji przypisanych do grupy administracyjnej:

1. W menu głównym przejdź do **Zarządzanie zasobami** → **Zasoby (urządzenia)**.

2. Wybierz grupę administracyjną, dla której chcesz wyświetlić przypisane punkty dystrybucji, klikając przycisk **Pokaż hierarchię** znajdujący się na górze strony, a następnie w otwartym oknie kliknij nazwę żądanej grupy.

   Spowoduje to włączenie pozycji menu **Punkty dystrybucji**.

   Ścieżka do wybranej grupy jest wyświetlana na górze strony. W razie potrzeby, w tej ścieżce możesz kliknąć odnośnik z nazwą grupy administracyjnej, aby do niej przejść. Domyślnie ostatni odnośnik na ścieżce jest nieaktywny.

3. W menu głównym przejdź do **Zarządzanie zasobami** → **Punkty dystrybucji**.

4. Aby dodać nowe punkty dystrybucji dla grupy administracyjnej, kliknij przycisk **Przypisz**.

5. Aby usunąć przypisane punkty dystrybucji, wybierz urządzenia z listy i kliknij przycisk **Cofnij przypisanie**.

W zależności od Twoich modyfikacji, nowe punkty dystrybucji są dodawane do listy lub istniejące punkty dystrybucji zostają usunięte z listy.

Włączanie serwera push

W Kaspersky Security Center Linux punkt dystrybucji może działać jako serwer push dla urządzeń zarządzanych za pośrednictwem protokołu mobilnego oraz zarządzanych za pośrednictwem agenta sieciowego. Na przykład, serwer push musi być włączony, jeśli chcesz mieć możliwość wymuszenia synchronizacji urządzeń KasperskyOS z Serwerem administracyjnym. Serwer push posiada ten sam obszar zarządzanych urządzeń jako punkt dystrybucji, na którym włączono serwer push. Jeśli posiadasz kilka punktów dystrybucji przypisanych dla tej samej grupy administracyjnej, możesz włączyć serwer push na każdym punkcie dystrybucji. W tym przypadku Serwer administracyjny rozkłada obciążenie między punkty dystrybucji.

Punktów dystrybucji można używać jako serwerów push, aby zapewnić ciągłą łączność między zarządzanym urządzeniem a Serwerem administracyjnym. W przypadku niektórych operacji, takich jak uruchamianie i zatrzymywanie zadań lokalnych, odbieranie statystyk dla zarządzanej aplikacji lub tworzenie tunelu, wymagana jest ciągła łączność. Jeśli używasz punktu dystrybucji jako serwera push, nie musisz używać opcji **Nie odłączaj od Serwera administracyjnego** na zarządzanych urządzeniach lub wysyłaj pakiety do portu UDP Agenta sieciowego.

Serwer push obsługuje do 50 000 jednoczesnych połączeń.

W celu włączenia serwera push na punkcie dystrybucji:

1. W menu głównym kliknij nazwę Serwera administracyjnego.

   Zostanie otwarte okno właściwości Serwera administracyjnego.

2. Na zakładce **Ogólne** wybierz sekcję **Punkty dystrybucji**.

3. Kliknij nazwę punktu dystrybucji, na którym chcesz włączyć serwer push.

   Spowoduje to otwarcie okna właściwości punktu dystrybucji.

4. W sekcji **Ogólne** włącz opcję **Włączone**.

5. W polu **Port serwera push** wpisz numer portu. Możesz określić numer dowolnego zajętego portu.

6. W polu **Adres zdalnych hostów** określ adres IP lub nazwę urządzenia punktu dystrybucyjnego.

7. Kliknij przycisk **OK**.

Serwer push jest włączony na wybranym punkcie dystrybucyjnym.

Zwiększenie limitu deskryptorów plików dla usługi klnagent

Jeśli zakres punktu dystrybucji opartego na systemie Linux obejmuje wiele urządzeń, domyślny limit plików, które można otworzyć (deskryptory plików) może nie być wystarczający. Aby tego uniknąć, możesz zwiększyć limit deskryptorów plików dla usługi klnagent.

Aby zwiększyć limit deskryptorów plików dla usługi klnagent:

1. Na urządzeniu opartym na systemie Linux, które działa jako punkt dystrybucji, wykonaj następujące polecenie:

   ```
   systemctl edit klnagent64.service
   ```

2. Określ miękkie i twarde limity deskryptorów plików w parametrze `LimitNOFILE` w sekcji `[Service]`:

   ```
   LimitNOFILE=<miękki limit zasobów>:<twardy limit zasobów>
   ```

   Na przykład, `LimitNOFILE=32768:131072`. Należy pamiętać, że miękki limit deskryptorów plików musi być mniejszy lub równy twardemu limitowi.

3. Uruchom następujące polecenie, aby upewnić się, że parametry zostały określone poprawnie:

   ```
   systemd-analyze verify klnagent64.service
   ```

   Jeśli parametry zostaną określone niepoprawnie, to polecenie może wyświetlić jeden z następujących błędów:

   - `/lib/systemd/system/klnagent64.service:11: Failed to parse resource value, ignoring: 32768:13107`

     Jeśli wystąpi ten błąd, oznacza to, że symbole w wierszu `LimitNOFILE` zostały określone niepoprawnie. Należy sprawdzić i poprawić wprowadzony wiersz.

   - `/lib/systemd/system/klnagent64.service:11: Soft resource limit chosen higher than hard limit, ignoring: 32768:13107`

     Jeśli wystąpi ten błąd, miękki limit wprowadzonych deskryptorów plików jest większy niż twardy limit. Musisz sprawdzić wprowadzony wiersz i upewnić się, że miękki limit deskryptorów plików jest mniejszy lub równy twardemu limitowi.

4. Uruchom następujące polecenie, aby ponownie załadować proces systemowy:

   ```
   systemctl daemon-reload
   ```

5. Uruchom następujące polecenie, aby ponownie uruchomić usługę Agenta sieciowego:

```
systemctl restart klnagent
```

6. Uruchom następujące polecenie, aby upewnić się, że określone parametry zostały zastosowane poprawnie:

```
less /proc/< ID procesu nagent >/limits
```

gdzie parametr `< ID procesu nagent >` jest identyfikatorem procesu Agenta sieciowego. Aby uzyskać identyfikator, możesz uruchomić następujące polecenie:

```
ps -ax | grep klnagent
```

W przypadku punktu dystrybucji opartego na systemie Linux zwiększa się limit plików, które można otworzyć.

Informacje o stanach urządzeń

Kaspersky Security Center Linux przypisze stan do każdego zarządzanego urządzenia. Określony stan zależy od tego, czy spełnione są warunki zdefiniowane przez użytkownika. W niektórych przypadkach, podczas przypisywania stanu do urządzenia, Kaspersky Security Center Linux bierze pod uwagę flagę widoczności urządzenia w sieci (patrz tabela poniżej). Na przykład, jeśli do zarządzanego urządzenia został przypisany stan *Krytyczny*, ponieważ spełniony był warunek *Bazy danych są nieaktualne*, a później flaga widoczności została ustawiona dla urządzenia, wówczas do urządzenia zostanie przypisany stan *OK*. Jeśli Kaspersky Security Center Linux nie znajdzie urządzenia w sieci w ciągu dwóch godzin, flaga widoczności urządzenia zostanie ustawiona na *Nie jest widoczne*.

Stany są następujące:

- *Krytyczny* lub *Krytyczny / Widoczny*
- *Ostrzeżenie* lub *Ostrzeżenie / Widoczne*
- *OK* lub *OK/Widoczne*

Poniższa tabela wyświetla domyślne warunki, które muszą być spełnione, aby przypisać stan *Krytyczny* lub *Ostrzeżenie* do urządzenia, wraz ze wszystkimi możliwymi wartościami.

Warunki przypisania stanu do urządzenia

Warunek	Opis warunku	Dostępne wartości
Aplikacja zabezpieczająca nie jest zainstalowana	Agent sieciowy jest zainstalowany na urządzeniu, ale aplikacja zabezpieczająca nie jest zainstalowana.	• Przycisk przełącznika jest ustawiony w pozycji włączenia. • Przycisk przełącznika jest ustawiony w pozycji wyłączenia.
Wykryto zbyt wiele wirusów	Niektóre wirusy zostały wykryte na urządzeniu przez zadanie wykrywania wirusów, na przykład, zadanie Skanowanie w poszukiwaniu szkodliwego oprogramowania oraz liczba wykrytych wirusów przekraczają określoną wartość.	Większe niż 0.
Poziom ochrony w czasie rzeczywistym jest inny niż poziom zdefiniowany przez administratora	Urządzenie jest widoczne w sieci, ale poziom ochrony w czasie rzeczywistym różni się od poziomu ustawionego (w warunku) przez administratora dla stanu urządzenia.	• Zatrzymane. • Wstrzymane. • Uruchomione.
Skanowanie w poszukiwaniu złośliwego oprogramowania nie było wykonywane od dłuższego czasu	Urządzenie jest widoczne w sieci, a aplikacja zabezpieczająca jest zainstalowana na urządzeniu, ale zadanie *Skanowanie w poszukiwaniu szkodliwego oprogramowania* ani zadanie lokalnego skanowania nie było uruchamiane w określonym przedziale czasu. Warunek jest stosowany tylko do urządzeń, które zostały dodane do bazy danych Serwera administracyjnego 7 dni temu lub wcześniej.	Więcej niż 1 dzień.

Warunek	Opis warunku	Dostępne wartości
Bazy danych są nieaktualne	Urządzenie jest widoczne w sieci, a aplikacja zabezpieczająca jest zainstalowana na urządzeniu, ale antywirusowe bazy danych nie były aktualizowane na tym urządzeniu w określonym przedziale czasu. Warunek jest stosowany tylko do urządzeń, które zostały dodane do bazy danych Serwera administracyjnego dzień wcześniej lub jeszcze wcześniej.	Więcej niż 1 dzień.
Niepołączony od dłuższego czasu	Agent sieciowy jest zainstalowany na urządzeniu, ale urządzenie nie było połączone z Serwerem administracyjnym w określonym przedziale czasu, ponieważ urządzenie było wyłączone.	Więcej niż 1 dzień.
Wykryto aktywne zagrożenia	Liczba nieprzetworzonych obiektów w folderze **Aktywne zagrożenia** przekracza określoną wartość.	Więcej niż 0 elementów.
Czas od momentu zażądania restartu	Urządzenie jest widoczne w sieci, ale aplikacja wymaga ponownego uruchomienia urządzenia dłużej niż określony przedział czasu.	Więcej niż 0 minut.
Przyczyna restartu	Urządzenie jest widoczne w sieci, ale aplikacja wymaga ponownego uruchomienia urządzenia z jednego z wybranych powodów.	• Nieznana przyczyna • Aplikacja nie będzie działała do czasu ponownego uruchomienia • W celu zakończenia aktualizacji wymagane jest ponowne uruchomienie; aplikacja jest uruchomiona • W celu zainicjowania aktualizacji wymagane jest ponowne uruchomienie • W celu zakończenia procesu skanowania lub leczenia wymagane jest ponowne uruchomienie komputera • W celu zakończenia zdalnej instalacji/dezinstalacji wymagane jest ponowne uruchomienie • Kończenie szyfrowania danych na dysku
Zainstalowane są niekompatybilne aplikacje	Urządzenie jest widoczne w sieci, ale inwentaryzacja oprogramowania wykonywana poprzez Agenta sieciowego wykryła niekompatybilne aplikacje zainstalowane na urządzeniu.	• Przycisk przełącznika jest ustawiony w pozycji wyłączenia. • Przycisk przełącznika jest ustawiony w pozycji włączenia.
Wykryto luki w oprogramowaniu	Urządzenie jest widoczne w sieci, a Agent sieciowy jest zainstalowany na urządzeniu, ale zadanie *Wyszukiwania luk i wymaganych aktualizacji* wykryło luki z określonym priorytetem w aplikacjach zainstalowanych na urządzeniu.	• Krytyczny. • Wysoki. • Średni. • Ignoruj, jeśli luka nie może być naprawiona. • Ignoruj, jeśli aktualizacja jest przypisana do instalacji.
Licencja utraciła ważność	Urządzenie jest widoczne w sieci, ale licencja utraciła ważność.	• Przycisk przełącznika jest ustawiony w pozycji wyłączenia. • Przycisk przełącznika jest ustawiony w pozycji włączenia.
Licencja wkrótce utraci ważność	Urządzenie jest widoczne w sieci, ale licencja utraci ważność na urządzeniu za mniej niż określona liczba dni.	Więcej niż 0 dni.

Warunek	Opis warunku	Dostępne wartości
Wyszukiwanie aktualizacji Windows Update nie było przeprowadzane od dłuższego czasu	Urządzenie jest widoczne w sieci, ale zadanie *Wyszukiwania luk i wymaganych aktualizacji* nie było uruchamiane w zdefiniowanym przedziale czasu.	Więcej niż 1 dzień.
Nieprawidłowy stan szyfrowania	Agent sieciowy jest zainstalowany na urządzeniu, ale wynik szyfrowania urządzenia jest równy określonej wartości.	• Nie zgadza się z zasadą w wyniku odmowy użytkownika (tylko dla urządzeń zewnętrznych). • Nie zgadza się z zasadą w wyniku błędu. • Po zastosowaniu zasady wymagane jest ponowne uruchomienie. • Nie określono zasady szyfrowania. • Nieobsługiwany. • Po zastosowaniu zasady.
Ustawienia urządzenia mobilnego nie są zgodne z zasadą	Ustawienia urządzenia mobilnego są inne niż ustawienia, które zostały określone w zasadzie Kaspersky Endpoint Security for Android podczas sprawdzania reguł zgodności.	• Przycisk przełącznika jest ustawiony w pozycji wyłączenia. • Przycisk przełącznika jest ustawiony w pozycji włączenia.
Wykryto nieprzetworzone incydenty związane z bezpieczeństwem	Na urządzeniu zostały wykryte pewne nieprzetworzone problemy bezpieczeństwa. Problemy bezpieczeństwa mogą być tworzone automatycznie poprzez zarządzane aplikacje firmy Kaspersky zainstalowane na urządzeniu klienckim, a także ręcznie przez administratora.	• Przycisk przełącznika jest ustawiony w pozycji wyłączenia. • Przycisk przełącznika jest ustawiony w pozycji włączenia.
Stan urządzenia zdefiniowany przez aplikację	Stan urządzenia jest definiowany przez zarządzaną aplikację. Zarządzane urządzenia mogą mieć stan zdefiniowany przez zarządzane aplikacje, niezależnie od ustawień Kaspersky Security Center Linux. Po zwróceniu przez ten stan jednego ze stanów zdefiniowanych przez Kaspersky Security Center Linux, Serwer administracyjny przypisuje zarządzanemu urządzeniu najbardziej krytyczny stan spośród stanów zwróconych przez zarządzaną aplikację i przypisanych przez Serwer administracyjny. Stany zdefiniowane przez zarządzane aplikacje mają opisy przekazane przez zarządzane aplikacje. Możesz wyświetlić opisy na liście zarządzanych urządzeń, w kolumnie **Opis stanu**.	• Przycisk przełącznika jest ustawiony w pozycji wyłączenia. • Przycisk przełącznika jest ustawiony w pozycji włączenia.
Brakuje miejsca na dysku urządzenia	Wolnego miejsca na dysku jest mniej niż określona wartość lub urządzenie nie mogło zostać zsynchronizowane z Serwerem administracyjnym. Stan *Krytyczny* lub *Ostrzeżenie* zmieniło się na stan *OK*, gdy urządzenie zostało pomyślnie zsynchronizowane z Serwerem administracyjnym, a wolna przestrzeń na urządzeniu jest większa niż lub równa określonej wartości.	Więcej niż 0 MB.
Zarządzanie urządzeniem nie jest możliwe	Podczas wykrywania urządzeń, urządzenie zostało rozpoznane jako widoczne w sieci, ale więcej niż trzy próby synchronizacji z Serwerem administracyjnym nie powiodły się.	• Przycisk przełącznika jest ustawiony w pozycji wyłączenia. • Przycisk przełącznika jest ustawiony w pozycji włączenia.
Ochrona jest wyłączona	Urządzenie jest widoczne w sieci, ale aplikacja zabezpieczająca na urządzeniu została wyłączona na dłużej niż określony przedział czasu. W tym przypadku stan aplikacji zabezpieczającej to *zatrzymany* lub *błąd* i różni się od następujących: *uruchamianie*, *uruchomiony* lub *zawieszony*.	Więcej niż 0 minut.
Aplikacja zabezpieczająca nie jest uruchomiona	Urządzenie jest widoczne w sieci, a aplikacja zabezpieczająca jest zainstalowana na urządzeniu, ale nie jest uruchomiona.	• Przycisk przełącznika jest ustawiony w pozycji wyłączenia. • Przycisk przełącznika jest ustawiony w pozycji włączenia.

Kaspersky Security Center Linux umożliwia skonfigurowanie automatycznego przełączania stanu urządzenia w grupie administracyjnej, gdy spełnione są określone warunki. Jeśli określone warunki są spełnione, do urządzenia klienckiego zostanie przypisany jeden z następujących stanów: *Krytyczny* lub *Ostrzeżenie*. Jeśli określone warunki zostaną spełnione, urządzeniu klienckiemu zostanie przypisany stan *OK*.

Różne stany mogą odpowiadać różnym wartościom jednego warunku. Na przykład, domyślnie, jeśli warunek **Bazy danych są nieaktualne** posiada wartość **Ponad 3 dni**, do urządzenia klienckiego zostaje przypisany stan *Ostrzeżenie*; jeśli wartość to **Ponad 7 dni**, wówczas zostanie przypisany stan *Krytyczny*.

Jeśli aktualizujesz Kaspersky Security Center Linux z poprzedniej wersji, wartości warunku **Bazy danych są nieaktualne** dla przypisania stanu do *Krytyczne* lub *Ostrzeżenie* nie zmienią się.

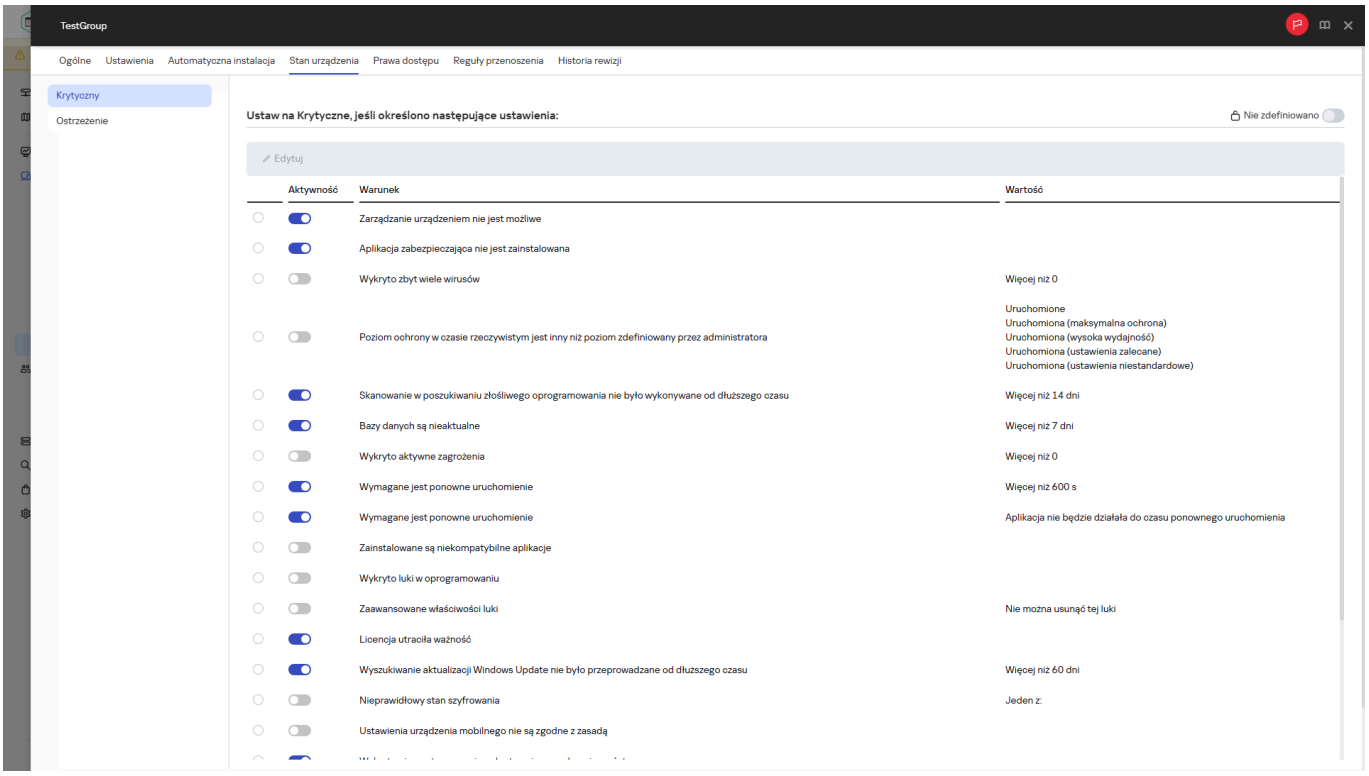
Konfigurowanie przełączania stanów urządzeń

Możesz zmienić warunki, aby przypisać stan *Krytyczny* lub *Ostrzeżenie* do urządzenia.

W celu włączenia zmiany stanu urządzenia na Krytyczny:

1. W menu głównym przejdź do **Zarządzanie zasobami** → **Hierarchia grup**.
2. Przejdź do właściwości grupy administracyjnej, dla której chcesz zmienić przełączanie statusów urządzeń, w jeden z następujących sposobów:
   - Kliknij nazwę żądanej grupy administracyjnej.
   - Kliknij przycisk **Pokaż hierarchię** znajdujący się na górze strony. W otwartym panelu nawigacyjnym najedź kursorem myszy na nazwę wymaganej grupy, a następnie kliknij ikonę ustawień (⚙).

   Zostanie otwarte okno właściwości grupy administracyjnej.
3. W otwartym oknie właściwości wybierz zakładkę **Stan urządzenia**.
4. W lewej części okna wybierz **Krytyczny**.
5. W prawej części okna, w sekcji **Ustaw na Krytyczne, jeśli określono następujące ustawienia** włącz warunek, aby przełączyć urządzenie do stanu *Krytyczny*.



> Możesz zmienić tylko ustawienia, które nie są zablokowane w zasadzie nadrzędnej.

6. Wybierz przycisk radiowy obok warunku na liście.
7. W lewym górnym rogu listy kliknij przycisk **Edytuj**.
8. Dla wybranego warunku ustaw żądaną wartość.

   Nie dla każdego warunku można ustawić wartości.
9. Kliknij **OK**.
10. Kliknij **Zapisz**, aby zachować zmiany.

Jeśli określone warunki zostaną spełnione, zarządzanemu urządzeniu zostanie przypisany stan *Krytyczne*.

W celu włączenia zmiany stanu urządzenia na Ostrzeżenie:

1. W menu głównym przejdź do **Zarządzanie zasobami** → **Hierarchia grup**.
2. Na otwartej liście grup kliknij odnośnik z nazwą grupy, dla której chcesz zmienić przełączanie stanów urządzeń.
3. W otwartym oknie właściwości wybierz zakładkę **Stan urządzenia**.
4. W lewej części okna wybierz **Ostrzeżenie**.
5. W prawej części okna, w sekcji **Ustaw na Ostrzeżenie, jeśli określono następujące ustawienia** włącz warunek, aby przełączyć urządzenie do stanu *Ostrzeżenie*.

> Możesz zmienić tylko ustawienia, które nie są zablokowane w zasadzie nadrzędnej.

6. Wybierz przycisk radiowy obok warunku na liście.

7. W lewym górnym rogu listy kliknij przycisk **Edytuj**.

8. Dla wybranego warunku ustaw żądaną wartość.

   Nie dla każdego warunku można ustawić wartości.

9. Kliknij **OK**.

10. Kliknij **Zapisz**, aby zachować zmiany.

Jeśli określone warunki zostaną spełnione, zarządzanemu urządzeniu zostanie przypisany stan *Ostrzeżenie*.

Wybory urządzeń

Wybory urządzeń to narzędzie do filtrowania urządzeń zgodnie z określonymi warunkami. Możesz użyć wyborów urządzeń do zarządzania kilkoma urządzeniami: na przykład, aby przejrzeć raport dotyczący tylko tych urządzeń lub żeby przenieść wszystkie te urządzenia do innej grupy.

Kaspersky Security Center Linux oferuje szeroki zakres *predefiniowanych wyborów* (na przykład: **Urządzenia ze stanem Krytyczny**, **Ochrona jest wyłączona**, **Wykryto aktywne zagrożenia**). Predefiniowanych wyborów nie można usunąć. Możesz także utworzyć i skonfigurować dodatkowe *wybory zdefiniowane przez użytkownika*.

W wyborach zdefiniowanych przez użytkownika możesz określić obszar wyszukiwania i wybrać wszystkie urządzenia, zarządzane urządzenia lub urządzenia nieprzypisane. Parametry wyszukiwania są określone w warunkach. W wyborze urządzeń możesz utworzyć kilka warunków z różnymi parametrami wyszukiwania. Na przykład, możesz utworzyć dwa warunki i określić różne zakresy IP w każdym z nich. Jeśli określono kilka warunków, wybór wyświetli urządzenia, które spełniają jakikolwiek warunek. Natomiast parametry wyszukiwania w obrębie warunku nakładają się na siebie. Jeśli zakres IP oraz nazwa zainstalowanej aplikacji są określone w warunku, wyświetlane będą tylko te urządzenia, na których jest zainstalowana aplikacja, a adres IP należy do określonego zakresu.

Przeglądanie listy urządzeń z wyboru urządzeń

Kaspersky Security Center Linux umożliwia przeglądanie listy urządzeń z poziomu wyboru urządzenia.

Aby wyświetlić listę urządzeń z poziomu wyboru urządzenia:

1. W menu głównym przejdź do sekcji **Zarządzanie zasobami** → **Wybory urządzeń** lub **Wykrywanie i wdrażanie** → **Wybory urządzeń**.

2. Na liście wyboru kliknij nazwę wybranego urządzenia.

   Na stronie wyświetlana jest tabela z informacjami o urządzeniach uwzględnionych w wyborze.

3. Dane tabeli urządzeń można grupować i filtrować w następujący sposób:

   - Kliknij ikonę ustawień (⚙), a następnie wybierz kolumny, które mają być wyświetlane w tabeli.

   - Kliknij ikonę filtrowania (▽), a następnie określ i zastosuj kryterium filtrowania w wywołanym menu.

     Zostanie wyświetlona przefiltrowana tabela urządzeń.

Można wybrać jedno lub kilka urządzeń i kliknąć przycisk **Nowe zadanie**, aby utworzyć odpowiednie zadanie, które zostanie zastosowane do tychże urządzeń.

Aby przenieść wybrane urządzenia do innej grupy administracyjnej, kliknij przycisk **Przenieś do grupy**, a następnie wybierz docelową grupę administracyjną.

Tworzenie kryteriów wyboru urządzeń

W celu utworzenia kryterium wyboru urządzeń:

1. W menu głównym przejdź do **Zarządzanie zasobami** → **Wybory urządzeń**.

   Zostanie wyświetlona lista wyborów urządzeń.

2. Kliknij przycisk **Dodaj**.

   Zostanie otwarte okno **Ustawienia wyboru urządzeń**.

3. Wprowadź nazwę nowego wyboru.

4. Określ grupę obejmującą urządzenia, które mają zostać uwzględnione w wyborze urządzeń:

   - **Wyszukaj dowolne urządzenia**— Wyszukiwanie urządzeń spełniających kryteria wyboru i uwzględnionych w grupach **Zarządzane urządzenia** lub **Urządzenia nieprzypisane**.

   - **Wyszukaj zarządzane urządzenia**— Wyszukiwanie urządzeń spełniających kryteria wyboru i uwzględnionych w grupie **Zarządzane urządzenia**.

   - **Wyszukaj nieprzypisane urządzenia**— Wyszukiwanie urządzeń spełniających kryteria wyboru i uwzględnionych w grupie **Urządzenia nieprzypisane**.

   Można włączyć pole wyboru **Uwzględnij dane z podrzędnych Serwerów administracyjnych**, aby umożliwić wyszukiwanie urządzeń spełniających kryteria wyboru i zarządzanych przez podrzędne Serwery administracyjne.

5. Kliknij przycisk **Dodaj**.

6. W oknie, które zostanie otwarte, określ warunki, które muszą być spełnione, aby uwzględnić urządzenia w tym wyborze, a następnie kliknij przycisk **OK**.

7. Kliknij przycisk **Zapisz**.

Wybór urządzeń zostanie utworzony i dodany do listy wyborów urządzeń.

Konfigurowanie kryteriów wyboru urządzeń

W celu skonfigurowania kryteriów wyboru urządzeń:

1. W menu głównym przejdź do **Zarządzanie zasobami** → **Wybory urządzeń**.

   Zostanie wyświetlona lista wyborów urządzeń.

2. Wybierz odpowiednie urządzenie zdefiniowane przez użytkownika i kliknij przycisk **Właściwości**.

   Zostanie otwarte okno **Ustawienia wyboru urządzeń**.

3. Na karcie **Ogólne** kliknij łącze **Nowy warunek**.

4. Określ warunki, jakie muszą zostać spełnione do uwzględnienia urządzeń w tym wyborze.

5. Kliknij przycisk **Zapisz**.

   Ustawienia zostaną zastosowane i zapisane.

Poniżej znajdują się opisy warunków przydzielania urządzeń do wyboru. Warunki są łączone przy użyciu operatora logicznego LUB: Wybór będzie zawierał urządzenia odpowiadające przynajmniej jednemu z wymienionych warunków.

Ogólne

W sekcji **Ogólne** możesz zmienić nazwę warunku wyboru oraz określić, czy ten warunek ma być odwrócony:

Odwróć warunek wyboru

Domyślnie opcja ta jest wyłączona.

Jeśli ta opcja jest włączona, określony warunek wyboru zostanie odwrócony. Wybór będzie zawierał wszystkie urządzenia, które nie spełniają warunku.

Poniższy przykład pokazuje logikę działania inwersji:

- **Warunek**: Na Twoim urządzeniu znajduje się system operacyjny z typem Linux i numerem kompilacji 00.0.000.

- **Warunek odwrócony**: Na urządzeniu znajduje się system operacyjny NIE z (typ Linux i numer kompilacji 00.0.000), co jest równoważne z następującym:

  Istnieje system operacyjny z typem NIE Linux LUB numerem kompilacji NIE 00.0.000.

W związku z tym wybór obejmie urządzenia z systemem operacyjnym, na przykład typu Windows i numerem kompilacji 00.0.000 lub typu Linux i dowolnym numerem kompilacji innym niż 00.0.000.

Infrastruktura sieci

W sekcji **Sieć** możesz określić kryteria, które będą wykorzystywane do uwzględniania urządzeń w wyborze zgodnie z ich danymi sieciowymi:

- **Nazwa urządzenia**

  Nazwa sieciowa systemu Windows (nazwa NetBIOS) urządzenia lub adres IPv4 lub IPv6.

- **Domena**

  Wyświetla wszystkie urządzenia znajdujące się w określonej w grupie roboczej.

- **Grupa administracyjna**

  Wyświetla urządzenia znajdujące się w określonej grupie administracyjnej.

- **Opis**

  Tekst wyświetlany w oknie właściwości urządzenia: pole **Opis** sekcji **Ogólne**.

  W celu opisania tekstu w polu **Opis** możesz użyć następujących znaków:

  - W słowie:

    - *****. Zastępuje dowolny wiersz dowolną liczbą znaków.

    Na przykład:

    Aby opisać słowa **Serwer** lub **Serwera**, możesz wpisać **Serwer***.

    - **?.** Zastępuje dowolny pojedynczy znak.

    Na przykład:

    Aby opisać wyrażenia, takie jak **SUSE Linux Enterprise Server 12** lub **SUSE Linux Enterprise Server 15**, możesz wpisać **SUSE Linux Enterprise Server 1?**.

    Gwiazdka (*****) lub znak zapytania (**?**) nie mogą być używane jako pierwsze symbole wyszukiwanego słowa.

  - W celu wyszukania kilku słów użyj:

    - Spacji. Wyświetla wszystkie urządzenia, których opisy zawierają dowolne z wymienionych słów.

    Na przykład:

    Aby odszukać frazę zawierającą słowa **Podrzędny** lub **Wirtualny**, wprowadź **Podrzędny Wirtualny** w tekście wyszukiwania.

    - **+**. Jeśli przed wyrazem wpisano znak „+”, wszystkie wyniki wyszukiwania będą zawierać ten wyraz.

    Na przykład:

    Aby odszukać frazę zawierającą zarówno **Podrzędny**, jak i **Wirtualny**, wprowadź **+Podrzędny+Wirtualny**.

    - **-**. Jeśli przed wyrazem wpisano znak „-”, żaden z wyników wyszukiwania nie będzie zawierać tego wyrazu.

    Na przykład:

    Aby odszukać frazę zawierającą **Podrzędny** i nie zawierającą **Wirtualny**, wprowadź **+Podrzędny-Wirtualny**.

    - **„<jakikolwiek tekst>”**. Tekst w cudzysłowach musi znajdować się w tekście.

    Na przykład:

    Aby odszukać frazę zawierającą kombinację słów **Podrzędny Serwer**, wprowadź **Podrzędny Serwer** w tekście wyszukiwania.

- **Zakres IP**

  Jeśli ta opcja jest włączona, możesz wprowadzić początkowy i końcowy adres IP z zakresu adresów IP, do którego muszą zostać włączone odpowiednie urządzenia.

  Domyślnie opcja ta jest wyłączona.

- **Zarządzane przez inny Serwer administracyjny**

  Wybierz jedną z następujących wartości:

  - **Tak**. Reguła przenoszenia urządzeń dotyczy tylko urządzeń klienckich zarządzanych przez inne Serwery administracyjne. Te serwery różnią się od serwera, na którym konfigurujesz regułę przenoszenia urządzeń.
  - **Nie**. Reguła przenoszenia urządzeń dotyczy tylko urządzeń klienckich zarządzanych przez bieżący Serwer administracyjny.
  - **Nie wybrano wartości**. Warunek nie ma zastosowania.

W podsekcji **Sterownik domeny** możesz skonfigurować kryteria uwzględniania urządzeń w wyborze na podstawie przynależności do domeny:

- **Urządzenie znajduje się w jednostce organizacyjnej domeny**

  Jeśli ta opcja jest włączona, wybór będzie zawierał urządzenia z jednostki organizacyjnej domeny określonej w polu wejściowym.

  Domyślnie opcja ta jest wyłączona.

- **Urządzenie to należy do grupy zabezpieczeń domeny**

  Jeśli ta opcja jest włączona, wybór będzie zawierał urządzenia z grupy bezpieczeństwa domeny określonej w polu wejściowym.

  Domyślnie opcja ta jest wyłączona.

W sekcji **Aktywność sieciowa** możesz określić kryteria, które będą używane do uwzględniania urządzeń w wyborze zgodnie z ich aktywnością sieciową:

- **Działa jako punkt dystrybucji**

  Na liście rozwijalnej możesz ustawić kryterium uwzględniania urządzeń w wyborze podczas wyszukiwania:

  - **Tak**. Wybór zawiera urządzenia pełniące role punktów dystrybucji.
  - **Nie**. Urządzenia pełniące role punktów dystrybucji nie będą uwzględniane w wyborze.
  - **Nie wybrano wartości**. Kryterium nie będzie stosowane.

- **Nie odłączaj od Serwera administracyjnego**

  Na liście rozwijalnej możesz ustawić kryterium uwzględniania urządzeń w wyborze podczas wyszukiwania:

  - **Włączona**. Wybór będzie zawierał urządzenia, na których zaznaczono pole **Nie odłączaj od Serwera administracyjnego**.
  - **Wyłączona**. Wybór będzie zawierał urządzenia, na których odznaczono pole **Nie odłączaj od Serwera administracyjnego**.
  - **Nie wybrano wartości**. Kryterium nie będzie stosowane.

- **Przełączanie profilu połączenia**

  Na liście rozwijalnej możesz ustawić kryterium uwzględniania urządzeń w wyborze podczas wyszukiwania:

  - **Tak**. Wybór będzie zawierał urządzenia, które zostały podłączone do Serwera administracyjnego po przełączeniu profilu połączenia.
  - **Nie**. Wybór nie będzie zawierał urządzeń, które zostały podłączone do Serwera administracyjnego po przełączeniu profilu połączenia.
  - **Nie wybrano wartości**. Kryterium nie będzie stosowane.

- **Ostatnie połączenie z Serwerem administracyjnym**

  To pole ustawia kryterium wyszukiwania urządzeń według godziny ostatniego połączenia z Serwerem administracyjnym.

  Jeśli to pole jest zaznaczone, w polach wejściowych możesz określić przedział czasu (datę i godzinę), w trakcie którego zostało nawiązane ostatnie połączenie pomiędzy Agentem sieciowym zainstalowanym na urządzeniu klienckim a Serwerem administracyjnym. Wybór będzie zawierał urządzenia mieszczące się w określonym przedziale czasu.

  Jeśli to pole nie jest zaznaczone, kryterium nie będzie stosowane.

  Domyślnie pole to nie jest zaznaczone.

- **Nowe urządzenia odnalezione podczas skanowania sieci**

  Wyszukiwanie nowych urządzeń, które zostały wykryte podczas przeszukiwania sieci w przeciągu kilku ostatnich dni.

  Jeśli ta opcja jest włączona, wybór będzie zawierał nowe urządzenia wykryte podczas wykrywania urządzeń w czasie określonym w polu **Okres wykrywania (dni)**.

  Jeśli ta opcja jest wyłączona, wybór będzie zawierał wszystkie urządzenia wykryte podczas wykrywania urządzeń.

  Domyślnie opcja ta jest wyłączona.

- **Dostępność urządzenia**

  Na liście rozwijalnej możesz ustawić kryterium uwzględniania urządzeń w wyborze podczas wyszukiwania:

  - **Tak**. Aplikacja uwzględnia w wyborze urządzenia, które są aktualnie widoczne w sieci.
  - **Nie**. Aplikacja uwzględnia w wyborze urządzenia, które są aktualnie niewidoczne w sieci.
  - **Nie wybrano wartości**. Kryterium nie będzie stosowane.

Stany urządzenia

W sekcji **Stan zarządzanego urządzenia** możesz skonfigurować kryteria uwzględniania urządzeń w oparciu o opis stanu urządzeń z zarządzanej aplikacji:

- **Stan urządzenia**

  Lista rozwijalna, z której możesz wybrać jeden ze stanów urządzenia: *OK*, *Krytyczny*, or *Ostrzeżenie*.

- **Stan ochrony w czasie rzeczywistym**

  Lista rozwijalna, z której możesz wybrać stan ochrony w czasie rzeczywistym. Urządzenia z określonymi stanami ochrony w czasie rzeczywistym są uwzględniane w wyborze.

- **Opis stanu urządzenia**

  W tym polu możesz zaznaczyć pola obok warunków, które, jeśli są spełnione, spowodują przypisanie do urządzenia jednego z następujących stanów: *OK, Krytyczny* lub *Ostrzeżenie*.

W sekcji **Stan komponentów w zarządzanych aplikacjach** możesz skonfigurować kryteria uwzględniania urządzeń w oparciu o stan składników w zarządzanych aplikacjach:

- **Stan ochrony przed wyciekiem danych**

  Wyszukiwanie urządzeń według stanu Ochrona przed wyciekaniem danych (*Nieznany, Zatrzymano, Uruchamianie, Wstrzymana, Uruchomiona, Niepowodzenie*).

- **Stan ochrony serwerów współpracy**

  Wyszukiwanie urządzeń według stanu ochrony serwerów współpracy (*Nieznany*, *Zatrzymano*, *Uruchamianie, Wstrzymana*, *Uruchomiona*, *Niepowodzenie*).

- **Stan ochrony antywirusowej serwerów pocztowych**

  Wyszukiwanie urządzeń według stanu ochrony dla serwerów pocztowych (*Nieznany, Zatrzymano, Uruchamianie, Wstrzymana, Uruchomiona, Niepowodzenie*).

- **Stan czujnika Endpoint Sensor**

  Wyszukiwanie urządzeń według stanu komponentu Endpoint Sensor (*Nieznany, Zatrzymano, Uruchamianie, Wstrzymana, Uruchomiona, Niepowodzenie*).

W sekcji **Problemy mające wpływ na stan zarządzanych aplikacji** możesz określić kryteria, które będą używane do uwzględniania urządzeń do wyboru według listy możliwych problemów wykrytych przez zarządzaną aplikację. Jeśli przynajmniej jeden problem, który wybrałeś, istnieje na urządzeniu, urządzenie zostanie uwzględnione w wyborze. Jeśli wybierzesz problem wymieniony dla kilku aplikacji, masz opcję automatycznego wyboru tego problemu na wszystkich listach.

Możesz zaznaczyć opcje dla opisów stanów z zarządzanej aplikacji. Po odebraniu tych stanów, urządzenia zostaną uwzględnione w wyborze. Jeśli wybierzesz stan wymieniony dla kilku aplikacji, masz opcję automatycznego wyboru tego stanu na wszystkich listach.

Informacje o systemie

W sekcji **System operacyjny** możesz określić kryteria, które będą używane do uwzględniania urządzeń w wyborze zgodnie z typem systemu operacyjnego.

- **Typ platformy**

  Jeśli pole jest zaznaczone, możesz wybrać system operacyjny z listy. Urządzenia, na których zainstalowany jest określony system operacyjny, są uwzględniane w wynikach wyszukiwania.

- **Wersja dodatku Service Pack systemu operacyjnego**

  W tym polu możesz określić wersję pakietu systemu operacyjnego (w formacie *X.Y*), która będzie określać sposób stosowania reguły przenoszenia do urządzenia. Domyślnie nie jest zdefiniowana żadna wartość.

- **Architektura systemu operacyjnego**

  Z listy rozwijalnej możesz wybrać architekturę swojego systemu operacyjnego, która określi sposób stosowania reguły przenoszenia do urządzenia (**Nieznany**, **x86**, **AMD64**, or **IA64**). Domyślnie, na liście nie wybrano żadnej opcji i tym samym nie zdefiniowano architektury systemu operacyjnego.

- **Kompilacja systemu operacyjnego**

  > To ustawienie jest stosowane tylko w systemach operacyjnych Windows.

  Numer kompilacji systemu operacyjnego. Możesz określić, czy wybrany system operacyjny musi mieć równy, wcześniejszy lub późniejszy numer kompilacji. Możesz także skonfigurować wyszukiwanie wszystkich numerów kompilacji, za wyjątkiem określonego.

- **Numer wersji systemu operacyjnego**

  > To ustawienie jest stosowane tylko w systemach operacyjnych Windows.

  Identyfikator wydania systemu operacyjnego. Możesz określić, czy wybrany system operacyjny musi mieć równy, wcześniejszy lub późniejszy identyfikator wydania. Możesz także skonfigurować wyszukiwanie wszystkich numerów identyfikatorów wydania, za wyjątkiem określonego.

W sekcji **Maszyny wirtualne** możesz skonfigurować kryteria uwzględniania urządzeń w wyborze w zależności od tego, czy są to maszyny wirtualne lub czy są one częścią Virtual Desktop Infrastructure (VDI):

- **Jest maszyną wirtualną**

  Z listy rozwijalnej możesz wybrać następujące opcje:

  - **Nie zdefiniowano**.
  - **Nie**. Wyszukuje urządzenia, które nie są maszynami wirtualnymi.
  - **Tak**. Wyszukuje urządzenia, które są maszynami wirtualnymi.

- **Typ maszyny wirtualnej**

  Z listy rozwijalnej możesz wybrać producenta maszyny wirtualnej.

  Ta lista rozwijalna jest dostępna, jeśli wartość **Tak** lub **Nieważne** została wybrana na liście rozwijalnej **Jest maszyną wirtualną**.

- **Część Virtual Desktop Infrastructure**

  Z listy rozwijalnej możesz wybrać następujące opcje:

  - **Nie zdefiniowano**.
  - **Nie**. Wyszukuje urządzenia, które nie są częścią Virtual Desktop Infrastructure.
  - **Tak**. Wyszukuje urządzenia, które są częścią Virtual Desktop Infrastructure (VDI).

W sekcji **Rejestr sprzętu** możesz skonfigurować kryteria uwzględniania urządzeń w oparciu o sprzęt na nich zainstalowany:

> Upewnij się, że narzędzie lshw jest zainstalowane na urządzeniach z systemem Linux, z których chcesz pobrać szczegółowe informacje o sprzęcie. Szczegóły dot. sprzętu przechwycone z maszyn wirtualnych mogą być niekompletne, w zależności od używanego hiperwizora.

- **Urządzenie**

  Z listy rozwijalnej możesz wybrać typ jednostki. Wszystkie urządzenia z tą jednostką zostają uwzględnione w wynikach wyszukiwania.

  Pole obsługuje wyszukiwanie pełnotekstowe.

- **Producent**

  Z listy rozwijalnej możesz wybrać nazwę producenta jednostki. Wszystkie urządzenia z tą jednostką zostają uwzględnione w wynikach wyszukiwania.

  Pole obsługuje wyszukiwanie pełnotekstowe.

- **Nazwa urządzenia**

  Urządzenie z określoną nazwą zostanie uwzględniony w wyborze.

- **Opis**

  Opis urządzenia lub sprzętu. Urządzenia z opisem określonym w tym polu zostaną uwzględnione w wyborze.

  Opis urządzenia w dowolnym formacie może zostać wprowadzony w oknie właściwości tego urządzenia. Pole obsługuje wyszukiwanie pełnotekstowe.

- **Producent urządzenia**

  Nazwa producenta urządzenia. Urządzenia, które zostały wyprodukowane przez producenta określonego w tym polu, zostaną uwzględnione w wyborze.

  Nazwę producenta można wprowadzić w oknie właściwości urządzenia.

- **Numer seryjny**

  Cały sprzęt o numerze seryjnym określonym w tym polu zostanie uwzględniony w wyborze.

- **Numer ewidencyjny**

  Sprzęt o numerze inwentarzowym podanym w tym polu zostanie uwzględniony w wyborze.

- **Użytkownik**

  Cały sprzęt użytkownika określonego w tym polu zostanie uwzględniony w wyborze.

- **Lokalizacja**

  Lokalizacja urządzenia lub sprzętu (na przykład: w kwaterze głównej lub w oddziale firmy). Komputery lub inne urządzenia zainstalowane w lokalizacji określonej w tym polu zostaną uwzględnione w wyborze.

  Możesz opisać lokalizację urządzenia w dowolnym formacie w oknie właściwości tego urządzenia.

- **Częstotliwość taktowania procesora, w MHz, od**

  Minimalna częstotliwość taktowania procesora. Urządzenia z procesorem pasującym do zakresu częstotliwości taktowania określonego w polach wejściowych (włącznie) zostaną uwzględnione w wyborze.

- **Częstotliwość taktowania procesora, w MHz, do**

  Maksymalna częstotliwość taktowania procesora. Urządzenia z procesorem pasującym do zakresu częstotliwości taktowania określonego w polach wejściowych (włącznie) zostaną uwzględnione w wyborze.

- **Liczba rdzeni procesora wirtualnego, od**

  Minimalna liczba wirtualnych rdzeni CPU. Urządzenia z procesorem odpowiadającym zakresowi liczby wirtualnych rdzeni wg definicji w polach wejściowych (włącznie) zostaną uwzględnione w wyborze.

- **Liczba rdzeni procesora wirtualnego, do**

  Maksymalna liczba wirtualnych rdzeni CPU. Urządzenia z procesorem odpowiadającym zakresowi liczby wirtualnych rdzeni wg definicji w polach wejściowych (włącznie) zostaną uwzględnione w wyborze.

- **Pojemność dysku twardego, w GB, od**

  Minimalna pojemność dysku twardego w urządzeniu. Urządzenia z dyskami twardymi odpowiadającymi zakresowi określonemu w polach wejściowych (włącznie) zostaną uwzględnione w wyborze.

- **Pojemność dysku twardego, w GB, do**

  Maksymalna pojemność dysku twardego w urządzeniu. Urządzenia z dyskami twardymi odpowiadającymi zakresowi określonemu w polach wejściowych (włącznie) zostaną uwzględnione w wyborze.

- **Rozmiar pamięci RAM, w MB, od**

  Minimalny rozmiar pamięci RAM urządzenia. Urządzenia z pamięcią RAM o rozmiarze odpowiadającym zakresowi podanemu w polach wejściowych (włącznie) zostaną uwzględnione w wyborze.

- **Rozmiar pamięci RAM, w MB, do**

  Maksymalny rozmiar pamięci RAM urządzenia. Urządzenia z pamięcią RAM o rozmiarze odpowiadającym zakresowi podanemu w polach wejściowych (włącznie) zostaną uwzględnione w wyborze.

Informacje o oprogramowaniu innych firm

W sekcji **Rejestr aplikacji** możesz skonfigurować kryteria wyszukiwania urządzeń na podstawie aplikacji na nich zainstalowanych:

- **Nazwa aplikacji**

  Lista rozwijalna, z której możesz wybrać aplikację. Urządzenia, na których jest zainstalowana określona aplikacja, są uwzględnione w wyborze.

- **Wersja aplikacji**

  Pole, w którym możesz określić wersję wybranej aplikacji.

- **Producent**

  Lista rozwijalna, z której możesz wybrać producenta aplikacji zainstalowanej na urządzeniu.

- **Stan aplikacji**

  Lista rozwijalna, z której możesz wybrać stan aplikacji (*Zainstalowana*, *Nie zainstalowana*). Urządzenia, na których określona aplikacja została zainstalowana lub nie została zainstalowana, w zależności od wybranego stanu, zostaną uwzględnione w wyborze.

- **Wyszukaj według aktualizacji**

  Jeśli ta opcja jest włączona, wyszukiwanie będzie się odbywać z użyciem szczegółów aktualizacji dla aplikacji zainstalowanych na odpowiednich urządzeniach. Po zaznaczeniu pola, pola **Nazwa aplikacji**, **Wersja aplikacji** i **Stan aplikacji** zostaną zmienione na **Nazwa aktualizacji**, **Wersja aktualizacji** i **Stan**.

  Domyślnie opcja ta jest wyłączona.

- **Nazwa niekompatybilnej aplikacji zabezpieczającej**

  Lista rozwijalna, z której możesz wybrać aplikacje zabezpieczające firm trzecich. Podczas wyszukiwania, urządzenia, na których jest zainstalowana określona aplikacja, są uwzględnione w wyborze.

- **Znacznik aplikacji**

  Z listy rozwijalnej możesz wybrać znacznik aplikacji. Wszystkie urządzenia, na których są zainstalowane aplikacje z wybranym znacznikiem w opisie, zostają uwzględnione w wyborze urządzeń.

- **Zastosuj do urządzeń bez określonych znaczników**

  Jeśli ta opcja jest włączona, wybór obejmuje urządzenia z opisami, które nie zawierają żadnego z wybranych znaczników.

  Jeśli ta opcja jest wyłączona, kryterium nie zostanie zastosowane.

  Domyślnie opcja ta jest wyłączona.

W sekcji **Luki oraz aktualizacje** możesz określić kryteria, które będą wykorzystywane do uwzględniania urządzeń w wyborze zgodnie z ich źródłem Windows Update:

WUA został przełączony na Serwer administracyjny

Z listy rozwijalnej można wybrać jedną z następujących opcji wyszukiwania:

- **Tak**. Jeśli wybrano tę opcję, wyniki wyszukiwania będą uwzględniać urządzenia, które uzyskały aktualizacje poprzez Windows Update z Serwera administracyjnego.

- **Nie**. Jeśli wybrano tę opcję, wyniki będą uwzględniać urządzenia, które uzyskały aktualizacje za pośrednictwem Windows Update z innych źródeł.

Szczegóły aplikacji Kaspersky

W sekcji **Aplikacje Kaspersky** możesz skonfigurować kryteria uwzględniania urządzeń w oparciu o wybraną zarządzaną aplikację:

- **Nazwa aplikacji**

  Na liście rozwijalnej możesz ustawić kryterium uwzględniania urządzeń w wyborze podczas wyszukiwania według nazwy aplikacji Kaspersky.

  Lista zawiera tylko nazwy aplikacji z wtyczkami administracyjnymi zainstalowanych na stacji roboczej administratora.

Jeśli żadna aplikacja nie została wybrana, kryterium nie będzie stosowane.

- **Wersja aplikacji**

  W polu wejściowym możesz ustawić kryterium uwzględniania urządzeń w wyborze podczas wyszukiwania według numeru wersji aplikacji Kaspersky.

  Jeśli żaden numer wersji nie został określony, kryterium nie będzie stosowane.

- **Nazwa aktualizacji krytycznej**

  W polu wejściowym możesz ustawić kryterium uwzględniania urządzeń w wyborze podczas wyszukiwania według nazwy aplikacji lub numeru pakietu aktualizacyjnego.

  Jeśli pole będzie puste, kryterium nie będzie stosowane.

- **Stan aplikacji**

  Lista rozwijalna, z której możesz wybrać stan aplikacji (*Zainstalowana*, *Nie zainstalowana*). Urządzenia, na których określona aplikacja została zainstalowana lub nie została zainstalowana, w zależności od wybranego stanu, zostaną uwzględnione w wyborze.

- **Wybierz okres ostatniej aktualizacji modułów**

  Ta opcja może zostać użyta do ustawienia kryterium wyszukiwania urządzeń według godziny ostatniej aktualizacji modułów aplikacji zainstalowanych na tych urządzeniach.

  Jeśli to pole jest zaznaczone, w polach wejściowych możesz określić przedział czasu (datę i godzinę), w trakcie którego została wykonana ostatnia aktualizacja modułów aplikacji zainstalowanych na tych urządzeniach.

  Jeśli to pole nie jest zaznaczone, kryterium nie będzie stosowane.

  Domyślnie pole to nie jest zaznaczone.

- **Urządzenie jest zarządzane przez Serwer administracyjny**

  Korzystając z tej listy rozwijalnej, w wyborze możesz uwzględnić urządzenia zarządzane poprzez Kaspersky Security Center Linux:

  - **Tak**. Aplikacja uwzględni w wyborze urządzenia zarządzane poprzez Kaspersky Security Center Linux.
  - **Nie**. Aplikacja uwzględni w wyborze urządzenia, jeśli nie są one zarządzane przez Kaspersky Security Center Linux.
  - **Nie wybrano wartości**. Kryterium nie będzie stosowane.

- **Aplikacja zabezpieczająca jest zainstalowana**

  Korzystając z tej listy rozwijalnej, w wyborze możesz uwzględnić wszystkie urządzenia z zainstalowaną aplikacją zabezpieczającą:

  - **Tak**. Aplikacja uwzględni w wyborze wszystkie urządzenia z zainstalowaną aplikacją zabezpieczającą.
  - **Nie**. Aplikacja uwzględni w wyborze wszystkie urządzenia bez zainstalowanej aplikacji zabezpieczającej.
  - **Nie wybrano wartości**. Kryterium nie będzie stosowane.

W sekcji **Ochrona antywirusowa** możesz skonfigurować kryteria uwzględniania urządzeń w oparciu o ich stan ochrony:

- **Data opublikowania baz danych**

  Jeśli ta opcja jest włączona, możesz wyszukiwać urządzenia klienckie według daty opublikowania antywirusowej bazy danych. W polach do wprowadzania danych możesz określić przedział czasu, na podstawie którego wykonywane jest wyszukiwanie.

  Domyślnie opcja ta jest wyłączona.

- **Liczba wpisów w bazie danych**

  Jeśli ta opcja jest włączona, możesz wyszukiwać urządzenia klienckie według liczby wpisów w bazie danych. W polach wejściowych możesz określić niższe i wyższe wartości progowe wpisów w antywirusowej bazie danych.

  Domyślnie opcja ta jest wyłączona.

- **Ostatnie skanowanie**

  Jeśli ta opcja jest włączona, możesz wyszukiwać urządzenia klienckie według czasu ostatniego skanowania w poszukiwaniu złośliwego oprogramowania. W polach wejściowych możesz określić przedział czasu, w trakcie którego zostało wykonane ostatnie skanowanie w poszukiwaniu złośliwego oprogramowania.

  Domyślnie opcja ta jest wyłączona.

- **Wykryte zagrożenia**

  Jeśli ta opcja jest włączona, możesz wyszukiwać urządzenia klienckie według liczby wykrytych wirusów. W polach wejściowych możesz określić niższe i wyższe wartości progowe liczby wykrytych wirusów.

  Domyślnie opcja ta jest wyłączona.

W sekcji **Szyfrowanie** możesz skonfigurować kryteria uwzględniania urządzeń w oparciu o wybrany algorytm szyfrowania:

Algorytm szyfrowania

Algorytm blokowego szyfru symetrycznego AES (Advanced Encryption Standard). Z listy rozwijalnej możesz wybrać długość klucza szyfrowania (56-bitowy, 128-bitowy, 192-bitowy lub 256-bitowy).

Dostępne wartości: *AES56*, *AES128*, *AES192* i *AES256*.

Podsekcja **Składniki aplikacji** obejmuje listę składników tych aplikacji, które mają odpowiednie wtyczki administracyjne zainstalowane w Kaspersky Security Center Web Console.

W sekcji **Składniki aplikacji** możesz określić kryteria uwzględniania urządzeń – zgodnie ze statusami i numerami wersji komponentów, które odpowiadają wybieranej przez ciebie aplikacji:

- **Stan**

  Wyszukiwanie urządzeń zgodnie ze stanem komponentu wysłanym przez aplikację do Serwera administracyjnego. Możesz wybrać jeden z następujących stanów: *Nie dotyczy, Zatrzymane*, *Wstrzymane*, *Uruchamianie*, *Uruchomione, Niepowodzenie, Nie zainstalowane, Nie obsługiwane na podstawie licencji*. Jeśli wybrany komponent aplikacji zainstalowanej na zarządzanym urządzeniu posiada określony stan, urządzenie jest uwzględniane w wyborze urządzeń.

Stany wysłane przez aplikacje:

- *Zatrzymane*—komponent jest wyłączony i nie działa w tym momencie.
- *Wstrzymane*—komponent został zawieszony, na przykład, po wstrzymaniu przez użytkownika ochrony w zarządzanej aplikacji.
- *Uruchamianie*—komponent jest właśnie w procesie inicjalizacji.
- *Uruchomione*—komponent jest włączony i działa poprawnie.
- *Niepowodzenie* — Podczas działania składnika wystąpił błąd.
- *Nie zainstalowano*—użytkownik nie wybrał komponentu do zainstalowania podczas konfigurowania niestandardowej instalacji aplikacji.
- *Nie obsługiwany na podstawie licencji* — Licencja nie obejmuje wybranego składnika.

W przeciwieństwie do pozostałych stanów, stan *Nie dotyczy* nie jest przekazywany poprzez aplikacje. Ta opcja pokazuje, że aplikacje nie posiadają informacji o wybranym stanie komponentu. Na przykład, to może mieć miejsce, gdy wybrany komponent nie należy do żadnej z aplikacji zainstalowanych na urządzeniu lub gdy urządzenie jest wyłączone.

- **Wersja**

  Wyszukiwanie urządzeń zgodnie z numerem wersji komponentu, który wybierasz na liście. Możesz wpisać numer wersji, na przykład `3.4.1.0`, a następnie określić, czy wybrany komponent musi posiadać równą, wcześniejszą lub nowszą wersję. Możesz także skonfigurować wyszukiwanie wszystkich wersji, za wyjątkiem określonej.

Znaczniki

W sekcji **Znaczniki** możesz skonfigurować kryteria uwzględniania urządzeń w wyborze w oparciu o słowa kluczowe (znaczniki), które wcześniej zostały dodane do opisów zarządzanych urządzeń:

Zastosuj, jeśli co najmniej jeden określony znacznik jest zgodny

Jeśli ta opcja jest włączona, w wynikach wyszukiwania będą wyświetlane urządzenia z opisami, które zawierają przynajmniej jeden z wybranych znaczników.

Jeśli ta opcja jest wyłączona, w wynikach wyszukiwania będą wyświetlane tylko urządzeni z opisami, które zawierają wszystkie wybrane znaczniki.

Domyślnie opcja ta jest wyłączona.

Aby dodać tagi do kryterium, kliknij przycisk **Dodaj** i wybierz tagi, klikając pole wejściowe **Znacznik**. Określanie, czy urządzenia z wybranymi tagami mają być uwzględniane w wyborze urządzeń, czy też wykluczane.

- **Wszystkie urządzenia posiadające ten znacznik**

  Jeśli ta opcja jest zaznaczona, w wynikach wyszukiwania będą wyświetlane urządzenia, których opisy zawierają wybrany znacznik. Aby odszukać urządzenia, możesz użyć gwiazdki, która oznacza dowolny wiersz z dowolną liczbą znaków.

  Domyślnie opcja ta jest zaznaczona.

- **Wszystkie urządzenia nieposiadające tego znacznika**

  Jeśli ta opcja jest zaznaczona, w wynikach wyszukiwania będą wyświetlane urządzenia, których opisy nie zawierają wybranego znacznika. Aby odszukać urządzenia, możesz użyć gwiazdki, która oznacza dowolny wiersz z dowolną liczbą znaków.

Użytkownicy

W sekcji **Użytkownicy** możesz skonfigurować kryteria uwzględniania urządzeń w wyborze według kont użytkowników, którzy logowali się do systemu operacyjnego.

- **Ostatni użytkownik zalogowany do systemu**

  Jeśli ta opcja jest włączona, można wybrać konto użytkownika do konfiguracji kryterium. Wyniki wyszukiwania obejmują urządzenia, na których określony użytkownik ostatnio logował się do systemu.

- **Użytkownik zalogowany do systemu co najmniej raz**

  Jeśli ta opcja jest włączona, kliknij przycisk **Przeglądaj**, aby określić konto użytkownika. Wyniki wyszukiwania zawierają urządzenia, na których określony użytkownik przynajmniej raz logował się do systemu.

Właściciel urządzenia

W sekcji **Właściciel urządzenia** możesz ustawić kryteria uwzględniania urządzeń przy wyborze według zarejestrowanych właścicieli urządzenia, ich ról i członkostwa w grupach zabezpieczeń:

- **Właściciel urządzenia**

  Wybierz nazwę użytkownika właściciela urządzenia z wewnętrznej grupy zabezpieczeń. Dowiedz się więcej o użytkownikach i rolach użytkowników w tej sekcji.

  > Nie więcej niż jeden użytkownik może być zarejestrowany jako właściciel urządzenia.

- **Członkostwo właściciela urządzenia w grupie zabezpieczeń Active Directory**

  Wybierz zewnętrzną grupę zabezpieczeń Active Directory, do której należy właściciel urządzenia.

  > Użytkownik może należeć do grupy zabezpieczeń Active Directory lub do grupy zawartej w tej grupie zabezpieczeń Active Directory.

- **Rola właściciela urządzenia**

  Wybierz rolę przypisaną właścicielowi urządzenia. Więcej informacji na temat ról użytkowników znajdziesz w tym artykule.

- **Członkostwo właściciela urządzenia w grupie zabezpieczeń Active Directory**

  Wybierz wewnętrzną grupę zabezpieczeń, do której należy właściciel urządzenia.

Eksportowanie listy urządzeń z wyboru urządzeń

Kaspersky Security Center Linux umożliwia zapisywanie informacji o urządzeniach z zakresu urządzeń i wyeksportowanie ich do pliku CSV lub TXT.

Aby wyeksportować listę urządzeń z poziomu wyboru urządzenia:

1. Otwórz tabelę z urządzeniami z wyboru urządzeń.
2. Użyj jednego z poniższych sposobów, aby wybrać urządzenia, które chcesz wyeksportować:
   - Aby wybrać określone urządzenia, zaznacz pola wyboru obok nich.
   - Aby wybrać wszystkie urządzenia z bieżącej strony tabeli, zaznacz pole wyboru w nagłówku tabeli urządzeń, a następnie zaznacz pole wyboru **Wybierz wszystko na bieżącej stronie**.
   - Aby wybrać wszystkie urządzenia z tabeli, zaznacz pole wyboru w nagłówku tabeli urządzeń, a następnie zaznacz pole wyboru **Wybierz wszystko**.
3. Kliknij przycisk **Eksportuj do pliku CSV** lub **Eksportuj do pliku TXT**. Wszystkie informacje o wybranych urządzeniach zawarte w tabeli zostaną wyeksportowane.

Należy pamiętać, że jeśli do tabeli urządzeń zastosowano kryterium filtrowania, zostaną wyeksportowane tylko przefiltrowane dane z wyświetlonych kolumn.

Usuwanie urządzeń z grup administracyjnych w wyborze

Podczas pracy z wyborami urządzeń możesz usunąć urządzenia z grup administracyjnych bezpośrednio w tym wyborze, bez przełączania do grup administracyjnych, z których te urządzenia mają być usunięte.

W celu usunięcia urządzeń z grup administracyjnych:

1. W menu głównym przejdź do sekcji **Zarządzanie zasobami** → **Wybory urządzeń** lub **Wykrywanie i wdrażanie** → **Wybory urządzeń**.
2. Na liście wyboru kliknij nazwę wybranego urządzenia.

   Na stronie wyświetlana jest tabela z informacjami o urządzeniach uwzględnionych w wyborze.
3. Wybierz urządzenia, które chcesz usunąć, a następnie kliknij **Usuń**.

   Wybrane urządzenia zostaną usunięte z odpowiednich grup administracyjnych.

Znaczniki urządzeń

Kaspersky Security Center Linux umożliwia *znakowanie* urządzeń. Znacznik to wartość ciągu, która może zostać użyta do grupowania, opisywania lub wyszukiwania urządzeń. Znaczniki przydzielone do urządzeń mogą być użyte do tworzenia wyborów, wyszukiwania urządzeń i rozdzielania urządzeń pomiędzy grupami administracyjnymi.

Urządzenia można znakować ręcznie lub automatycznie. Jeśli chcesz oznakować pojedyncze urządzenie, możesz użyć oznaczania ręcznego. Automatyczne znakowanie jest wykonywane przez Kaspersky Security Center Linux na jeden z następujących sposobów:

- Zgodnie z określonymi regułami znakowania.
- Przez aplikację.

> Nie zalecamy używania różnych sposobów znakowania w celu przypisania tego samego znacznika. Przykładowo, jeśli znacznik jest przypisany przez regułę, nie zaleca się ręcznego przypisywania tego znacznika do urządzeń.

Jeśli znaczniki są przypisane przez reguły, urządzenia zostaną automatycznie oznakowane po spełnieniu określonych reguł. Każdemu znacznikowi odpowiada pojedyncza reguła. Reguły są stosowane do właściwości sieciowych urządzenia, systemu operacyjnego, aplikacji zainstalowanych na urządzeniu i innych właściwości urządzenia. Na przykład, możesz skonfigurować regułę, która przypisze znacznik `[CentOS]` do wszystkich urządzeń działających pod kontrolą systemu operacyjnego CentOS. Następnie możesz użyć tego znacznika podczas tworzenia wyboru urządzeń; pomoże to w sortowaniu wszystkich urządzeń z systemem CentOS i przypisaniu do nich zadania.

> Można dodać tylko jedną regułę automatycznego znakowania na znacznik. Jeśli utworzysz nową regułę dla tego samego znacznika, poprzednia zostanie zastąpiona.

Znacznik jest automatycznie usuwany z urządzenia w następujących przypadkach:

- Jeśli urządzenie przestanie spełniać warunki reguły, która przypisuje znacznik.
- Jeśli reguła, która przypisuje znacznik, jest wyłączona lub została usunięta.

Lista znaczników oraz lista reguł na każdym Serwerze administracyjnym są niezależne od wszystkich pozostałych Serwerów administracyjnych, w tym głównego Serwera administracyjnego lub podległych wirtualnych Serwerów administracyjnych. Reguła jest stosowana tylko do urządzeń z tego samego Serwera administracyjnego, na którym reguła jest tworzona.

Tworzenie znacznika urządzenia

W celu utworzenia znacznika urządzenia:

1. W menu głównym przejdź do **Zarządzanie zasobami** → **Znaczniki** → **Znaczniki urządzenia**.
2. Kliknij **Dodaj**.
   Zostanie otwarte okno nowego znacznika.
3. W polu **Znacznik** wprowadź nazwę znacznika.
4. Kliknij **Zapisz**, aby zachować zmiany.

Nowy znacznik pojawi się na liście znaczników urządzenia.

Zmienianie nazwy znacznika urządzenia

W celu zmiany nazwy znacznika urządzenia:

1. W menu głównym przejdź do **Zarządzanie zasobami** → **Znaczniki** → **Znaczniki urządzenia**.
2. Kliknij nazwę znacznika, którego nazwę chcesz zmienić.
   Zostanie otwarte okno właściwości znacznika.
3. W polu **Znacznik** zmień nazwę znacznika.
4. Kliknij **Zapisz**, aby zachować zmiany.

Zaktualizowany znacznik pojawi się na liście znaczników urządzenia.

Usuwanie znacznika urządzenia

Możesz usunąć tylko znaczniki przypisane ręcznie.

W celu usunięcia przypisanego znacznika urządzenia:

1. W menu głównym przejdź do **Zarządzanie zasobami** → **Znaczniki** → **Znaczniki urządzenia**.
   Zostanie wyświetlona lista znaczników.
2. Wybierz znacznik urządzenia, który chcesz usunąć.

3. Kliknij przycisk **Usuń**.

4. W otwartym oknie kliknij **Tak**.

   Znacznik urządzenia zostanie usunięty. Usunięty znacznik jest automatycznie usuwany ze wszystkich urządzeń, do których został przypisany.

Gdy usuniesz znacznik przypisany do urządzenia przez regułę automatycznego znakowania, reguła nie zostanie usunięta, a znacznik zostanie przypisany do nowego urządzenia, gdy urządzenie po raz pierwszy spełni warunki reguły. Jeśli usuniesz regułę automatycznego znakowania, znacznik określony w warunkach reguły zostanie usunięty ze wszystkich urządzeń, do których został przypisany, ale nie zostanie usunięty z listy znaczników. W razie potrzeby możesz ręcznie usunąć znacznik z listy.

Usunięty tag nie jest automatycznie usuwany z urządzenia, jeśli ten tag jest przypisany do urządzenia przez aplikację lub Agenta sieciowego. Aby zarządzać tymi znacznikami, użyj narzędzia klscflag.

Przeglądanie urządzeń, do których przypisano znacznik

W celu przejrzenia urządzeń, do których przypisywany jest znacznik:

1. W menu głównym przejdź do **Zarządzanie zasobami** → **Znaczniki** → **Znaczniki urządzenia**.

2. Kliknij odnośnik **Wyświetl urządzenia** obok znacznika, dla którego chcesz wyświetlić przypisane urządzenia.

   Zostaniesz przekierowany do sekcji **Zasoby (urządzenia)** w menu głównym, gdzie urządzenia zostaną odfiltrowane według tagu, dla którego kliknąłeś odnośnik **Wyświetl urządzenia**.

3. Jeśli chcesz wrócić do listy znaczników urządzenia, kliknij przycisk **Wstecz** w swojej przeglądarce.

Po przejrzeniu urządzeń, do których przypisany jest znacznik, możesz utworzyć i przypisać nowy znacznik lub przypisać istniejący znacznik do innych urządzeń. W takim przypadku należy usunąć filtr według znacznika, wybrać urządzenia, a następnie przypisać znacznik.

Przeglądanie znaczników przydzielonych do urządzenia

W celu przejrzenia znaczników przydzielonych do urządzenia:

1. W menu głównym przejdź do **Zarządzanie zasobami** → **Zasoby (urządzenia)**.

2. Kliknij nazwę urządzenia, którego znaczniki chcesz przejrzeć.

3. W otwartym oknie właściwości urządzenia wybierz zakładkę **Znaczniki**.

   Zostanie wyświetlona lista znaczników przypisanych do wybranego urządzenia. W kolumnie **Przypisany znacznik** możesz zobaczyć, w jaki sposób znacznik został przypisany.

W pasku narzędzi możesz wykonać następujące czynności:

- Przypisz inny znacznik do urządzenia.
- Usuń już przypisany znacznik.
- Wyświetl wszystkie znaczniki urządzenia, które znajdują się na Serwerze administracyjnym.

Nie można przeglądać przypisanych znaczników lokalnie na urządzeniu.

Ręczne oznaczanie urządzenia

W celu ręcznego przypisania znacznika do urządzenia:

1. Przejrzyj znaczniki przypisane do urządzenia, do którego chcesz przypisać inny znacznik.
2. Kliknij **Dodaj**.
3. W otwartym oknie wykonaj jedną z następujących czynności:
   - Aby utworzyć i przypisać nowy znacznik, wybierz **Utwórz nowy znacznik**, a następnie określ nazwę nowego znacznika.
   - Aby wybrać istniejący znacznik, wybierz **Przypisz istniejący znacznik**, a następnie, z listy rozwijalnej wybierz potrzebny znacznik.
4. Kliknij **OK**, aby zastosować zmiany.
5. Kliknij **Zapisz**, aby zachować zmiany.

Wybrany znacznik zostanie przypisany do urządzenia.

Usuwanie przydzielonego znacznika z urządzenia

W celu usunięcia znacznika z urządzenia:

1. W menu głównym przejdź do **Zarządzanie zasobami** → **Zasoby (urządzenia)**.
2. Kliknij nazwę urządzenia, którego znaczniki chcesz przejrzeć.
3. W otwartym oknie właściwości urządzenia wybierz zakładkę **Znaczniki**.
4. Zaznacz pole obok znacznika, który chcesz usunąć.

5. U góry listy kliknij przycisk **Wycofaj przypisanie znacznika**.

6. W otwartym oknie potwierdzenia kliknij **OK**.

   Znacznik zostanie usunięty z urządzenia.

Znacznik urządzenia nieprzypisanego został usunięty. Jeśli chcesz, możesz usunąć go ręcznie.

Nie możesz ręcznie usunąć znaczników przypisanych do urządzenia przez aplikacje lub Agenta sieciowego. Aby zarządzać tymi znacznikami, użyj narzędzia klscflag.

Wyświetlanie reguł automatycznego oznaczania urządzeń

W celu wyświetlenia reguł automatycznego znakowania urządzeń:

Wykonaj jedną z poniższych czynności:

- W menu głównym przejdź do **Zarządzanie zasobami** → **Znaczniki** → **Reguły automatycznego znakowania**.
- W menu głównym przejdź do **Zarządzanie zasobami** → **Znaczniki** → **Znaczniki urządzenia**, and then click the **Ustaw reguły automatycznego znakowania**.
- Wyświetl tagi przypisane do urządzenia, a następnie kliknij przycisk **Ustaw reguły automatycznego znakowania**.

Zostanie wyświetlona lista reguł automatycznego znakowania urządzeń.

Edytowanie reguły automatycznego znakowania urządzeń

W celu edytowania reguły automatycznego znakowania urządzeń:

1. Wyświetl reguły automatycznego oznaczania urządzeń.
2. Kliknij nazwę reguły, którą chcesz edytować.

   Zostanie otwarte okno ustawień reguły.
3. Edytuj ogólne właściwości reguły:

   a. W polu **Nazwa reguły** zmień nazwę reguły.

      Nazwa nie może zawierać więcej niż 256 znaków.

   b. Wykonaj jedną z poniższych czynności:

      - Włącz regułę, ustawiając przełącznik w pozycji **Reguła włączona**.
      - Wyłącz regułę, ustawiając przełącznik w pozycji **Reguła wyłączona**.

4. Wykonaj jedną z poniższych czynności:

   - Jeśli chcesz dodać nowy warunek, kliknij przycisk **Dodaj** i w otwartym oknie określ ustawienia nowego warunku.
   - Jeśli chcesz edytować istniejący warunek, kliknij nazwę warunku, który chcesz edytować, a następnie edytuj ustawienia warunku.
   - Jeśli chcesz usunąć warunek, zaznacz pole obok nazwy warunku, który chcesz usunąć, a następnie kliknij **Usuń**.

5. Kliknij przycisk **OK** w oknie ustawień warunków.

6. Kliknij **Zapisz**, aby zachować zmiany.

Edytowana reguła zostanie wyświetlona na liście.

Tworzenie reguły automatycznego znakowania urządzeń

W celu utworzenia reguły automatycznego znakowania urządzeń:

1. Wyświetl reguły automatycznego oznaczania urządzeń.

2. Kliknij **Dodaj**.

   Zostanie otwarte okno ustawień nowej reguły.

3. Skonfiguruj ogólne właściwości reguły:

   a. W polu **Nazwa reguły** wprowadź nazwę reguły.

      Długość nazwy nie może wynosić więcej niż 256 znaków.

   b. Wykonaj jedną z poniższych czynności:

      - Włącz regułę, ustawiając przełącznik w pozycji **Reguła włączona**.
      - Wyłącz regułę, ustawiając przełącznik w pozycji **Reguła wyłączona**.

   c. W polu **Znacznik** wprowadź nazwę nowego znacznika urządzenia lub wybierz istniejące znaczniki urządzeń z listy.

      Długość nazwy nie może wynosić więcej niż 256 znaków.

4. W sekcji warunków kliknij przycisk **Dodaj**, aby dodać nowy warunek.

   Zostanie otwarte okno ustawień nowego warunku.

5. Wprowadź nazwę warunku.

   Długość nazwy nie może wynosić więcej niż 256 znaków. Nazwa musi być unikatowa w obrębie reguły.

6. Skonfiguruj wyzwalanie reguły zgodnie z następującymi warunkami. Możesz określić kilka warunków.

   - **Sieć** — właściwości sieciowe urządzenia, takie jak nazwa DNS urządzenia lub włączenie urządzenia do podsieci IP.

     Jeśli dla bazy danych używanej z Kaspersky Security Center Linux ustawione jest sortowanie z rozróżnianiem wielkości liter, zachowaj wielkość liter podczas określania nazwy DNS urządzenia. W przeciwnym razie reguła automatycznego tagowania nie będzie działać.

   - **Aplikacje**—obecność Agenta sieciowego na urządzeniu oraz typ, wersja i architektura systemu operacyjnego.
   - **Maszyny wirtualne**—urządzenie należy do określonego typu maszyny wirtualnej.
   - **Rejestr aplikacji**—obecność aplikacji różnych producentów na urządzeniu.

7. Kliknij **OK**, aby zachować zmiany.

   Jeśli to konieczne, dla jednej reguły możesz ustawić kilka warunków. W tej sytuacji znacznik zostanie przypisany do urządzenia, jeśli spełnia przynajmniej jeden warunek.

8. Kliknij **Zapisz**, aby zachować zmiany.

Nowo utworzona reguła jest wymuszona na urządzeniach zarządzanych przez wybrany Serwer administracyjny. Jeśli ustawienia urządzenia spełniają warunki reguły, do urządzenia zostanie przydzielony znacznik.

Później reguła będzie stosowana w następujących przypadkach:

- Automatycznie i okresowo, w zależności od obciążenia na serwerze
- Po edytowaniu reguły
- Jeśli ręcznie uruchamiasz regułę
- Po wykryciu przez Serwer administracyjny zmian w ustawieniach urządzenia, które spełnia warunki reguły lub w ustawieniach grupy, która zawiera to urządzenie

Możesz utworzyć kilka reguł znakowania. Do jednego urządzenia może zostać przypisanych kilka znaczników, jeśli utworzyłeś kilka reguł znakowania i jeśli odpowiednie warunki tych reguł są spełnione w tym samym czasie. Listę wszystkich przydzielonych znaczników można przejrzeć we właściwościach urządzenia.

Uruchamianie reguł automatycznego znakowania urządzeń

Jeśli reguła jest uruchomiona, znacznik określony we właściwościach tej reguły zostanie przypisany do urządzeń, które spełniają warunki określone we właściwościach tej samej reguły. Możesz uruchamiać tylko aktywne reguły.

W celu uruchomienia reguł automatycznego znakowania urządzeń:

1. Wyświetl reguły automatycznego oznaczania urządzeń.
2. Zaznacz pola obok aktywnych reguł, które chcesz uruchomić.
3. Kliknij przycisk **Uruchom regułę**.

   Wybrane reguły zostały uruchomione.

Usuwanie reguły automatycznego oznaczania urządzeń

W celu usunięcia reguły automatycznego oznaczania urządzeń:

1. Wyświetl reguły automatycznego oznaczania urządzeń.
2. Zaznacz pole obok reguły, którą chcesz usunąć.
3. Kliknij **Usuń**.
4. W otwartym oknie potwierdzenia kliknij **OK**.

   Wybrana reguła została usunięta. Znacznik, który został określony we właściwościach tej reguły, został wypisany ze wszystkich urządzeń, do których został przypisany.

   Znacznik urządzenia nieprzypisanego został usunięty. Jeśli chcesz, możesz usunąć go ręcznie.

Zarządzanie znacznikami urządzeń za pomocą narzędzia klscflag

Aby przypisać zestaw znaczników do urządzenia, należy uruchomić narzędzie klscflag na urządzeniu klienta, do którego mają zostać przypisane znaczniki.

Narzędzie klscflag nadpisuje istniejące znaczniki przypisane do urządzenia. Oznacza to, że możesz dodawać lub usuwać znaczniki, określając w poleceniu żądany zestaw znaczników. Narzędzie nie posiada osobnych poleceń do dodawania lub usuwania poszczególnych znaczników. Zamiast tego modyfikujesz cały zestaw znaczników.

Podczas określania nazw znaczników w poleceniach typu klscflag zaleca się stosowanie spójnego podejścia polegającego na przykład na pisaniu wielkimi literami. Używanie samych wielkich liter może pomóc uniknąć potencjalnych problemów ze znacznikami, które różnią się jedynie wielkością liter, w zależności od konfiguracji systemu DBMS.

Aby przypisać jeden lub kilka znaczników do swojego urządzenia za pomocą narzędzia klscflag:

1. Uruchom wiersz poleceń na koncie z uprawnieniami administratora, a następnie zmień bieżący katalog na katalog, w którym znajduje się narzędzie klscflag. Narzędzie klscflag znajduje się w katalogu, w którym zainstalowany jest Agent sieciowy. Domyślny katalog instalacyjny to /opt/kaspersky/klnagent64/sbin/.

2. Uruchom jedno z następujących poleceń:

   - Aby przypisać zestaw znaczników:

     `/opt/kaspersky/klnagent64/sbin/klscflag -ssvset -pv 1103/1.0.0.0 -s KLNAG_SECTION_TAGS_INFO -n KLCONN_HOST_TAGS -sv "[\"NAZWA ZNACZNIKA 1\",\"NAZWA ZNACZNIKA 2\",\"NAZWA ZNACZNIKA 3\"]" -svt ARRAY_T -ss "|ss_type = \"SS_PRODINFO\";"`

     gdzie `[\"NAZWA ZNACZNIKA 1\",\"NAZWA ZNACZNIKA 2\",\"NAZWA ZNACZNIKA 3\"]` to lista znaczników, które chcesz przypisać do swojego urządzenia.

     Jeżeli pozostawisz nawiasy kwadratowe puste, spowoduje to usunięcie wszystkich znaczników z urządzenia:

     `/opt/kaspersky/klnagent64/sbin/klscflag -ssvset -pv 1103/1.0.0.0 -s KLNAG_SECTION_TAGS_INFO -n KLCONN_HOST_TAGS -sv "[]" -svt ARRAY_T -ss "|ss_type = \"SS_PRODINFO\";"`

   - Aby przypisać nowy znacznik do istniejącego zestawu znaczników:

     `/opt/kaspersky/klnagent64/sbin/klscflag -ssvset -pv 1103/1.0.0.0 -s KLNAG_SECTION_TAGS_INFO -n KLCONN_HOST_TAGS -sv "[\"NAZWA NOWEGO ZNACZNIKA\",\"NAZWA ZNACZNIKA 1\",\"NAZWA ZNACZNIKA 2\",\"NAZWA ZNACZNIKA 3\"]" -svt ARRAY_T -ss "|ss_type = \"SS_PRODINFO\";"`

     gdzie `NAZWA NOWEGO ZNACZNIKA` to nazwa znacznika, który chcesz przypisać do swojego urządzenia, a `NAZWA ZNACZNIKA 1`, `NAZWA ZNACZNIKA 2`, `NAZWA ZNACZNIKA 3` to nazwy znaczników już przypisanych do urządzenia.

   - Aby usunąć konkretny znacznik bez usuwania innych znaczników już przypisanych do urządzenia, uruchom polecenie ze zaktualizowanym zestawem znaczników.

     Na przykład, jeśli Twoje obecne znaczniki to `NAZWA ZNACZNIKA 1`, `NAZWA ZNACZNIKA 2`, `NAZWA ZNACZNIKA 3` i chcesz usunąć `NAZWA ZNACZNIKA 2`, uruchom następujące polecenie:

     `/opt/kaspersky/klnagent64/sbin/klscflag -ssvset -pv 1103/1.0.0.0 -s KLNAG_SECTION_TAGS_INFO -n KLCONN_HOST_TAGS -sv "[\"NAZWA ZNACZNIKA 1\",\"NAZWA ZNACZNIKA 3\"]" -svt ARRAY_T -ss "|ss_type = \"SS_PRODINFO\";"`

3. Uruchom następujące polecenie, aby ponownie uruchomić usługę Agenta sieciowego:

   ```
   systemctl restart klnagent
   ```

   Narzędzie klscflag przypisuje określone znaczniki do Twojego urządzenia.

4. Aby mieć pewność, że narzędzie klscflag pomyślnie przypisało określone znaczniki, wyświetl znaczniki przypisane do urządzenia.

Alternatywnie możesz ręcznie przypisać znaczniki urządzeń.

Szyfrowanie i ochrona danych

Szyfrowanie danych zmniejsza ryzyko niezamierzonego wycieku poufnych i firmowych danych w przypadku kradzieży lub zagubienia laptopa lub dysku twardego. Ponadto szyfrowanie danych pozwala uniemożliwić dostęp nieautoryzowanym użytkownikom i aplikacjom.

Możesz użyć funkcji szyfrowania danych, jeśli Twoja sieć zawiera zarządzane urządzenia z systemem Windows z zainstalowanym Kaspersky Endpoint Security for Windows. W takim przypadku na urządzeniach z systemem operacyjnym Windows można zarządzać następującymi rodzajami szyfrowania:

- Szyfrowanie dysków funkcją BitLocker
- Kaspersky Disk Encryption

Nie zalecamy włączania szyfrowania w VDI.

Korzystając z tych komponentów Kaspersky Endpoint Security for Windows, możesz na przykład włączyć lub wyłączyć szyfrowanie, przeglądać listę zaszyfrowanych dysków lub generować i przeglądać raporty dotyczące szyfrowania.

Aby skonfigurować szyfrowanie, zdefiniuj zasadę Kaspersky Endpoint Security for Windows w Kaspersky Security Center Linux. Kaspersky Endpoint Security for Windows wykonuje szyfrowanie i odszyfrowywanie zgodnie z aktywną zasadą. Szczegółowe instrukcje dotyczące konfigurowania reguł oraz opis funkcji szyfrowania są dostępne w Pomocy Kaspersky Endpoint Security for Windows.

Zarządzanie szyfrowaniem dla hierarchii Serwerów administracyjnych nie jest obecnie dostępne w Web Console. Użyj głównego Serwera administracyjnego do zarządzania zaszyfrowanymi urządzeniami.

Za pomocą ustawień interfejsu użytkownika można wyświetlić lub ukryć niektóre elementy interfejsu związane z funkcją zarządzania szyfrowaniem.

Przeglądanie listy zaszyfrowanych dysków

W Kaspersky Security Center Linux możesz przeglądać szczegółowe informacje o zaszyfrowanych dyskach i urządzeniach zaszyfrowanych na poziomie dysku. Po odszyfrowaniu informacji na dysku, dysk jest automatycznie usuwane z listy.

W celu przejrzenia listy zaszyfrowanych dysków:

W menu głównym przejdź do **Operacje** → **Ochrona i szyfrowanie danych** → **Zaszyfrowane dyski**.

Jeśli sekcji nie ma w menu, oznacza to, że jest ukryta. W ustawieniach interfejsu użytkownika włącz opcję **Pokaż ochronę i szyfrowanie danych**, aby wyświetlić sekcję.

Możesz wyeksportować listę zaszyfrowanych dysków do pliku CSV lub pliku TXT. W tym celu kliknij przycisk **Eksportuj do pliku CSV** lub **Eksportuj do pliku TXT**.

Wyświetlanie listy zdarzeń szyfrowania

Podczas wykonywania zadań szyfrowania lub odszyfrowywania danych na urządzeniach, Kaspersky Endpoint Security for Windows wysyła do Kaspersky Security Center Linux informacje o zdarzeniach następujących typów:

- Nie można zaszyfrować ani odszyfrować pliku lub utworzyć zaszyfrowanego archiwum ze względu na brak wolnego miejsca na dysku.
- Nie można zaszyfrować ani odszyfrować pliku lub utworzyć zaszyfrowanego archiwum ze względu na problemy z licencją.
- Nie można zaszyfrować ani odszyfrować pliku lub utworzyć zaszyfrowanego archiwum ze względu na brak praw dostępu.
- Dla aplikacji zablokowano dostęp do zaszyfrowanego pliku.
- Nieznane błędy.

W celu wyświetlenia listy zdarzeń, które wystąpiły w trakcie szyfrowania danych na urządzeniach:

W menu głównym przejdź do **Operacje** → **Ochrona i szyfrowanie danych** → **Zdarzenia szyfrowania**.

Jeśli sekcji nie ma w menu, oznacza to, że jest ukryta. W ustawieniach interfejsu użytkownika włącz opcję **Pokaż ochronę i szyfrowanie danych**, aby wyświetlić sekcję.

Możesz wyeksportować listę zaszyfrowanych dysków do pliku CSV lub pliku TXT. W tym celu kliknij przycisk **Eksportuj do pliku CSV** lub **Eksportuj do pliku TXT**.

Alternatywnie możesz przejrzeć listę zdarzeń szyfrowania dla każdego zarządzanego urządzenia.

Aby wyświetlić zdarzenia szyfrowania dla zarządzanego urządzenia:

1. W menu głównym przejdź do **Zarządzanie zasobami** → **Zasoby (urządzenia)**.
2. Kliknij nazwę zarządzanego urządzenia.
3. Na karcie **Ogólne** przejdź do sekcji **Ochrona**.
4. Kliknij łącze **Wyświetl błędy szyfrowania danych**.

Tworzenie i przeglądanie raportów z szyfrowania

Możesz wygenerować następujące raporty:

- Raport o stanie szyfrowania zarządzanych urządzeń. Ten raport zawiera szczegółowe informacje na temat szyfrowania danych na różnych zarządzanych urządzeniach. Na przykład raport pokazuje liczbę urządzeń, do których ma zastosowanie zasada ze skonfigurowanymi regułami szyfrowania. Możesz także dowiedzieć się, na przykład, ile urządzeń wymaga ponownego uruchomienia. Raport zawiera również informacje o technologii i algorytmie szyfrowania dla każdego urządzenia.

- Raport o stanie szyfrowania urządzeń pamięci masowej. Ten raport zawiera podobne informacje jak raport o stanie szyfrowania zarządzanych urządzeń, ale zawiera dane tylko dla urządzeń pamięci masowej i dysków wymiennych.

- Raport o prawach dostępu do zaszyfrowanych dysków. Ten raport pokazuje, które konta użytkowników mają dostęp do zaszyfrowanych dysków.

- Raport o błędach podczas szyfrowania plików. Ten raport zawiera informacje o błędach, które wystąpiły podczas uruchamiania zadań szyfrowania lub odszyfrowywania danych na urządzeniach.

- Raport o zablokowanym dostępie do zaszyfrowanych plików. Ten raport zawiera informacje o blokowaniu dostępu aplikacji do zaszyfrowanych plików. Ten raport jest pomocny, jeśli nieautoryzowany użytkownik lub aplikacja próbuje uzyskać dostęp do zaszyfrowanych plików lub dysków.

Możesz wygenerować dowolny raport w sekcji **Monitorowanie** → **Raporty**. Alternatywnie w sekcji **Operacje** → **Ochrona i szyfrowanie danych** możesz wygenerować następujące raporty dotyczące szyfrowania:

- Raport o stanie szyfrowania urządzeń pamięci masowej

- Raport o prawach dostępu do zaszyfrowanych dysków

- Raport o błędach podczas szyfrowania plików

*Aby wygenerować raport szyfrowania w sekcji **Ochrona i szyfrowanie danych**:*

1. Upewnij się, że włączyłeś opcję **Pokaż ochronę i szyfrowanie danych** w opcjach interfejsu.

2. We właściwościach zasady otwórz zakładkę **Konfiguracja zdarzenia**.

3. W sekcji **Krytyczny** kliknij **Dodaj zdarzenie** i zaznacz pole wyboru obok zdarzenia *Błąd podczas stosowania reguł szyfrowania/odszyfrowywania pliku*.

4. Kliknij **OK**.

5. W menu głównym przejdź do **Operacje** → **Ochrona i szyfrowanie danych**.

6. Wybierz jedną z następujących sekcji:

   - **Zaszyfrowane dyski** generuje raport o stanie szyfrowania urządzeń pamięci masowej lub raport o prawach dostępu do zaszyfrowanych dysków.

   - **Zdarzenia szyfrowania** generuje raport o błędach szyfrowania plików.

7. Kliknij nazwę raportu, który chcesz wygenerować.

Zostanie rozpoczęte tworzenie raportu.

Udzielanie dostępu do zaszyfrowanego dysku w trybie offline

Użytkownik może poprosić o dostęp do zaszyfrowanego urządzenia, na przykład, gdy Kaspersky Endpoint Security nie jest zainstalowany na zarządzanym urządzeniu. Po otrzymaniu żądania możesz utworzyć plik klucza dostępu i wysłać go do użytkownika. Wszystkie przypadki użycia i szczegółowe instrukcje znajdują się w Pomocy Kaspersky Endpoint Security dla wymaganej platformy.

Aby przyznać dostęp do zaszyfrowanego dysku w trybie offline w Kaspersky Endpoint Security for Windows:

1. Uzyskaj plik żądania dostępu od użytkownika (plik z rozszerzeniem FDERTC). Postępuj zgodnie z instrukcjami zawartymi w Pomocy Kaspersky Endpoint Security for Windows aby wygenerować plik w Kaspersky Endpoint Security for Windows.

2. W menu głównym przejdź do **Operacje** → **Ochrona i szyfrowanie danych** → **Zaszyfrowane dyski**.

   Zostanie wyświetlona lista zaszyfrowanych dysków.

3. Wybierz dysk, do którego użytkownik zażądał dostępu.

4. Kliknij przycisk **Udziel dostępu do urządzenia w trybie offline**.

5. W oknie, które zostanie otwarte, wybierz wtyczkę Kaspersky Endpoint Security for Windows.

6. Postępuj zgodnie z instrukcjami podanymi w Pomocy Kaspersky Endpoint Security for Windows (zobacz instrukcje dla Kaspersky Security Center Web Console na końcu tej sekcji).

Następnie użytkownik stosuje otrzymany plik, aby uzyskać dostęp do zaszyfrowanego dysku i odczytać dane zapisane na dysku.

Przesyłanie kluczy szyfrowania między Serwerami administracyjnymi

Jeśli funkcja szyfrowania danych jest włączona na zarządzanym urządzeniu, klucz szyfrowania jest przechowywany na Serwerze administracyjnym. Klucz szyfrowania służy do uzyskiwania dostępu do zaszyfrowanych danych i zarządzania zasadą szyfrowania.

Klucz szyfrowania musi zostać przesłany do innego Serwera administracyjnego w następujących przypadkach:

- Ponowna konfiguracja Agenta sieciowego na zarządzanym urządzeniu, aby przypisać urządzenie do innego Serwera administracyjnego. Jeśli to urządzenie zawiera zaszyfrowane dane, klucz szyfrowania musi zostać przesłany do docelowego Serwera administracyjnego. W przeciwnym razie dane nie mogą zostać odszyfrowane.

- Szyfrowanie dysku wymiennego podłączonego do urządzenia D1 zarządzanego przez Serwer administracyjny S1, a następnie podłączenie tego dysku wymiennego do urządzenia D2 zarządzanego przez Serwer administracyjny S2. Aby uzyskać dostęp do danych na dysku wymiennym, klucz szyfrowania musi zostać przesłany z Serwera administracyjnego S1 do Serwera administracyjnego S2.

- Zaszyfrowanie pliku na urządzeniu D1 zarządzanym przez Serwer administracyjny S1, a następnie próba uzyskania dostępu do pliku na urządzeniu D2 zarządzanym przez Serwer administracyjny S2. Aby uzyskać dostęp do pliku, klucz szyfrowania musi zostać przesłany z Serwera administracyjnego S1 do Serwera administracyjnego S2.

Możesz przesłać klucze szyfrowania na następujące sposoby:

- Automatycznie, włączając opcję **Użyj hierarchii Serwerów administracyjnych, aby uzyskać klucze szyfrowania** we właściwościach dwóch Serwerów administracyjnych, między którymi należy przesłać klucz szyfrowania. Jeśli ta opcja jest wyłączona dla jednego z Serwerów administracyjnych, automatyczne przesyłanie kluczy szyfrowania nie jest możliwe.

  Jeśli włączysz opcję **Użyj hierarchii Serwerów administracyjnych, aby uzyskać klucze szyfrowania** we właściwościach Serwera administracyjnego, Serwer administracyjny wyśle wszystkie klucze szyfrowania przechowywane w swoim repozytorium do głównego Serwera administracyjnego (jeśli istnieje) o jeden poziom wyżej w hierarchii.

  Podczas próby uzyskania dostępu do zaszyfrowanych danych Serwer administracyjny najpierw wyszukuje klucz szyfrowania we własnym repozytorium. Jeśli opcja **Użyj hierarchii Serwerów administracyjnych, aby uzyskać klucze szyfrowania** jest włączona, a żądany klucz szyfrowania nie został znaleziony w repozytorium, Serwer administracyjny dodatkowo wyśle żądanie do głównych Serwerów administracyjnych (jeśli istnieją) w celu dostarczenia żądanego klucza szyfrowania. Żądanie zostanie wysłane na wszystkie główne Serwery administracyjne, aż do serwera na najwyższym poziomie hierarchii.

- Ręcznie z jednego Serwera administracyjnego na inny, eksportując i importując plik zawierający klucze szyfrowania.

  Eksportowanie i importowanie kluczy szyfrowania to czynności uwzględnione w funkcji zarządzania kluczami szyfrowania. Aby wykonać te akcje, skonfiguruj prawa dostępu do funkcji dla użytkowników Kaspersky Security Center Linux w następujący sposób:

  - Przyznaj prawo dostępu **Odczyt** do funkcji zarządzania kluczami szyfrowania użytkownikowi, który eksportuje klucze szyfrowania z pomocniczego Serwera administracyjnego.

  - Przyznaj prawo dostępu **Wpisz** do funkcji zarządzania kluczami szyfrowania użytkownikowi, który importuje klucze szyfrowania na docelowy Serwer administracyjny.

W celu włączenia automatycznego przesyłania kluczy szyfrowania między Serwerami administracyjnymi w obrębie hierarchii:

1. Przejdź do właściwości wymaganego Serwera administracyjnego:

   a. W menu głównym wybierz dowolną sekcję (z wyjątkiem **Platforma handlowa**, **Poruszanie się po konsoli** i **Ustawień**), a następnie na górze strony kliknij przycisk **Pokaż hierarchię**.

   b. W otwartym panelu nawigacyjnym najedź kursorem myszy na nazwę żądanego Serwera administracyjnego, a następnie kliknij ikonę ustawień (⚙).

   Alternatywnie możesz kliknąć nazwę Serwera administracyjnego, a następnie, po wyświetleniu nazwy w menu głównym, kliknąć ją w menu głównym, aby otworzyć okno właściwości serwera.

2. W otwartym oknie właściwości wybierz sekcję **Algorytm szyfrowania**.

3. Włącz opcję **Użyj hierarchii Serwerów administracyjnych, aby uzyskać klucze szyfrowania**.

4. Kliknij **OK**, aby zastosować zmiany.

Klucze szyfrowania zostaną przesłane na główne Serwery administracyjne (jeśli istnieją) przy kolejnej synchronizacji (puls). Ten Serwer administracyjny dostarczy również, na żądanie, klucz szyfrowania ze swojego repozytorium do podrzędnego Serwera administracyjnego.

W celu ręcznego przesyłania kluczy szyfrowania między Serwerami administracyjnymi:

1. Przejdź do właściwości Serwera administracyjnego, z którego chcesz wyeksportować klucze szyfrowania:

   a. W menu głównym wybierz dowolną sekcję (z wyjątkiem **Platforma handlowa**, **Poruszanie się po konsoli** i **Ustawień**), a następnie na górze strony kliknij przycisk **Pokaż hierarchię**.

   b. W otwartym panelu nawigacyjnym najedź kursorem myszy na nazwę żądanego Serwera administracyjnego, a następnie kliknij ikonę ustawień (⚙).

   Alternatywnie możesz kliknąć nazwę Serwera administracyjnego, a następnie, po wyświetleniu nazwy w menu głównym, kliknąć ją w menu głównym, aby otworzyć okno właściwości serwera.

2. W otwartym oknie właściwości wybierz sekcję **Algorytm szyfrowania**.

3. Kliknij **Wyeksportuj klucze szyfrowania z Serwera administracyjnego**.

   Upewnij się, że użytkownik, który eksportuje klucze szyfrowania z serwera, ma przyznane prawo dostępu **Odczyt** do funkcji zarządzania kluczami szyfrowania.

4. W oknie **Eksportuj klucze szyfrowania**:

   - Kliknij przycisk **Przeglądaj**, a następnie określ, gdzie należy zapisać plik.
   - Określ hasło do ochrony pliku przed nieautoryzowanym dostępem.

   > Zapamiętaj hasło. Utraconego hasła nie można odzyskać. Jeśli hasło zostanie utracone, należy powtórzyć procedurę eksportowania. Dlatego zanotuj hasło i miej je pod ręką.

5. Prześlij plik na inny Serwer administracyjny, na przykład, poprzez folder współdzielony lub nośnik wymienny.

6. Przejdź do właściwości Serwera administracyjnego, do którego chcesz zaimportować klucze szyfrowania.

7. W oknie właściwości wybierz sekcję **Algorytm szyfrowania**.

8. Kliknij **Zaimportuj klucze szyfrowania do Serwera administracyjnego**.

   Upewnij się, że użytkownik, który eksportuje klucze szyfrowania z serwera, ma przyznane prawo dostępu **Wpisz** do funkcji zarządzania kluczami szyfrowania.

9. W oknie **Importuj klucze szyfrowania**:

   - Kliknij przycisk **Przeglądaj**, a następnie wybierz plik zawierający klucze szyfrowania.
   - Określ hasło.

10. Kliknij **OK**.

Klucze szyfrowania są przesyłane na docelowy Serwer administracyjny.

Zmienianie Serwera administracyjnego dla urządzeń klienckich

Możesz zmienić Serwer administracyjny na inny dla określonych urządzeń klienckich. W tym celu użyj zadania *Zmiana Serwera administracyjnego*.

W celu zmiany Serwera administracyjnego zarządzającego urządzeniami klienckimi na inny Serwer:

1. Nawiąż połączenie z Serwerem administracyjnym, który zarządza urządzeniami.

2. Utwórz zadanie zmiany Serwera administracyjnego.

   Zostanie uruchomiony Kreator tworzenia nowego zadania. Postępuj zgodnie z instrukcjami kreatora. W oknie **Nowe zadanie** kreatora tworzenia nowego zadania wybierz aplikację **Kaspersky Security Center 16.3** oraz typ zadania **Zmiana Serwera administracyjnego**. Następnie określ urządzenia, dla których chcesz zmienić Serwer administracyjny:

   - **Przypisz zadanie do grupy administracyjnej**

     Zadanie jest przypisywane do urządzeń znajdujących się w grupie administracyjnej. Możesz określić jedną z istniejących grup lub utworzyć nową grupę.

     Na przykład, możesz chcieć użyć tej opcji do uruchomienia zadania wysyłania wiadomości do użytkowników, jeśli wiadomość jest specyficzna dla urządzeń znajdujących się w określonej grupie administracyjnej.

     Jeśli zadanie jest przypisane do grupy administracyjnej, zakładka **Zabezpieczenia** nie jest wyświetlana w oknie właściwości zadania, ponieważ zadania grupowe podlegają ustawieniom zabezpieczeń grup, do których się odnoszą.

   - **Określ adresy urządzeń ręcznie lub zaimportuj adresy z listy**

     Możesz określić nazwy NetBIOS, nazwy DNS, adresy IP oraz podsieci IP urządzeń, do których chcesz przydzielić zadanie.

     Możesz użyć tej opcji do wykonania zadania dla określonej podsieci. Na przykład, możesz chcieć zainstalować pewną aplikację na urządzeniach księgowych lub przeskanować urządzenia w podsieci, która jest prawdopodobnie zainfekowana.

- **Przypisz zadanie do wyboru urządzeń**

  Zadanie jest przypisywane do urządzeń znajdujących się w wyborze urządzeń. Możesz określić jeden z istniejących wyborów.

  Na przykład, możesz chcieć użyć tej opcji do uruchomienia zadania na urządzeniach z określoną wersją systemu operacyjnego.

3. Uruchom utworzone zadanie.

Po zakończeniu wykonywania zadania, urządzenia klienckie, dla których zostało ono utworzone, zostaną przekazane Serwerowi administracyjnemu określonemu w ustawieniach zadania.

Jeśli Serwer administracyjny obsługuje szyfrowanie i ochronę danych, a Ty tworzysz zadanie *Zmiana Serwera administracyjnego*, zostanie wyświetlone ostrzeżenie. Ostrzeżenie informuje, że jeśli jakiekolwiek zaszyfrowane dane są przechowywane na urządzeniach, po rozpoczęciu przez nowy Serwer zarządzania urządzeniami, użytkownicy będą mieli dostęp tylko do zaszyfrowanych danych, z którymi wcześniej pracowali. W innych przypadkach dostęp do zaszyfrowanych danych będzie niemożliwy. Szczegółowe opisy scenariuszy, w których dostęp do zaszyfrowanych danych nie jest zapewniany, znajdują się w Pomocy Kaspersky Endpoint Security for Windows.

Unikanie konfliktów między kilkoma Serwerami administracyjnymi

Jeśli w sieci posiadasz więcej niż jeden Serwer administracyjny, mogą one widzieć te same urządzenia klienckie. Może to być na przykład spowodowane zainstalowaniem przez Serwer administracyjny aplikacji, która została już zainstalowana przez inny Serwer administracyjny, a także innymi konfliktami. Aby zapobiec instalacji aplikacji na urządzeniu zarządzanym przez inny Serwer administracyjny, należy włączyć opcję **Zainstaluj tylko na urządzeniach zarządzanych przez ten Serwer administracyjny** we właściwościach zadania *Zdalna instalacja aplikacji*.

Jeśli włączysz opcję **Zainstaluj tylko na urządzeniach zarządzanych przez ten Serwer administracyjny**, a następnie uruchomisz zadanie *Zdalna instalacja aplikacji*, zostanie wykonane sprawdzenie w celu ustalenia, czy urządzenia są zarządzane przez inny Serwer administracyjny. W przypadku urządzeń zarządzanych przez inny Serwer administracyjny wartość atrybutu **Zarządzane przez inny Serwer administracyjny** zostanie ustawiona na `true`. Zadanie *Zdalna instalacja aplikacji* nie zostanie zastosowane do tych urządzeń.

Wartości atrybutu **Zarządzane przez inny Serwer administracyjny** są wyświetlane w kolumnie **Zarządzane przez inny Serwer administracyjny** na liście zarządzanych urządzeń i liście nieprzypisanych urządzeń.

Możesz także użyć właściwości **Zarządzane przez inny Serwer administracyjny** jako kryterium dla:

- Wyświetlanie zarządzanych urządzeń
- Wybory urządzeń
- Reguły przenoszenia urządzeń
- Reguł automatycznego znakowania

Aby zresetować atrybut Zarządzane przez inny Serwer administracyjny:

1. W menu głównym Kaspersky Security Center Web Console przejdź do **Zarządzanie zasobami** → **Urządzenia nieprzypisane**.

2. Wybierz wymagane urządzenie, a następnie kliknij przycisk **Usuń atrybut Zarządzane przez inny Serwer administracyjny**.

Atrybut **Zarządzane przez inny Serwer administracyjny** został zresetowany.

Przenoszenie urządzeń podłączonych do Serwera administracyjnego przez bramy połączeń na inny Serwer administracyjny

Możesz przenieść urządzenia podłączone do Serwera administracyjnego przez bramy połączeń na inny Serwer administracyjny. Może to być na przykład konieczne w przypadku instalacji innej wersji Serwera administracyjnego i braku konieczności ponownej instalacji Agenta sieciowego na urządzeniach, gdyż mogłoby to być czasochłonne.

Polecenia opisane w instrukcji muszą być uruchamiane na urządzeniach klienckich z poziomu konta z uprawnieniami administratora.

Aby przenieść urządzenie podłączone poprzez bramę połączenia do innego Serwera administracyjnego:

1. Uruchom narzędzie klmover z parametrem `-address <adres serwera>`, aby przełączyć się na nowy Serwer administracyjny.

2. Uruchom polecenie `klnagchk -nagwait -tl 4`.

3. Uruchom następujące polecenia, aby ustawić nową bramę połączenia:

   - `klscflag -ssvset -pv klnagent -s FileTransfer -n ft_gateway_mode -sv false -svt BOOL_T -ss "|ss_type = \"SS_SETTINGS\";"`

   - `klscflag -ssvset -pv klnagent -s FileTransfer -n ft_gateway_loc -sv "<ip lub nazwa bramy>" -svt STRING_T -ss "|ss_type = \"SS_SETTINGS\";"`

     Gdzie `<gateway ip or name>` to adres bramy połączenia dostępny z Internetu.

   - `klscflag -ssvset -pv klnagent -s FileTransfer -n ft_gateway_ssl_port -sv 13000 -svt INT_T -ss "|ss_type = \"SS_SETTINGS\";"`

     `13000` to numer portu TCP, na którym nasłuchuje brama połączenia.

4. Uruchom polecenie `klnagchk -restart -tl 4`, aby uruchomić usługę Agenta sieciowego.

Urządzenie zostaje przeniesione na nowy Serwer administracyjny i podłączone poprzez nową podłączoną bramę.

Przeglądanie i konfigurowanie działań, gdy urządzenia wykazują brak aktywności

Jeśli urządzenia klienckie w grupie są nieaktywne, możesz otrzymać informacje na ten temat. Możesz także automatycznie usuwać takie urządzenia.

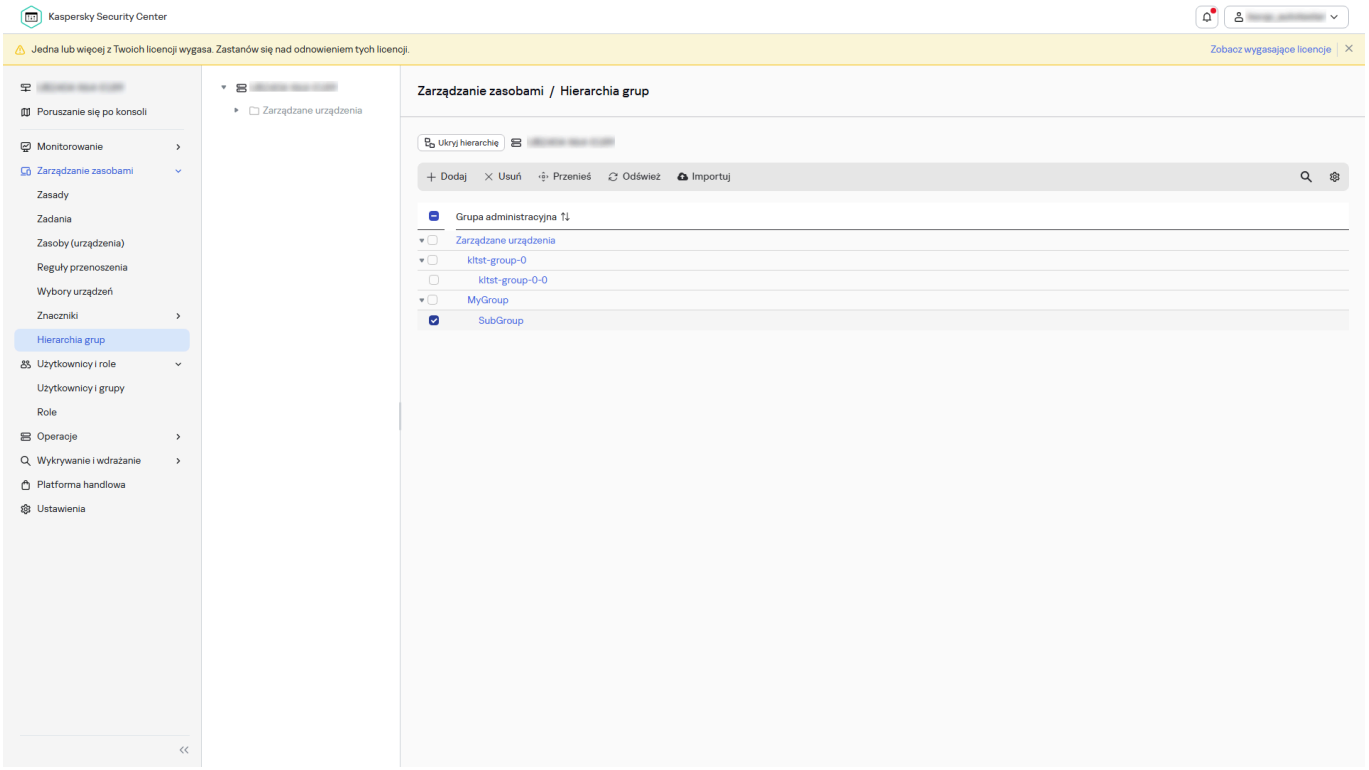
W celu przejrzenia lub skonfigurowania działań, gdy urządzenia w grupie wykazują brak aktywności:

1. W menu głównym przejdź do **Zarządzanie zasobami** → **Hierarchia grup**.

2. Przejdź do właściwości wymaganej grupy administracyjnej w jeden z następujących sposobów:

   - Kliknij nazwę żądanej grupy administracyjnej.

   - Kliknij przycisk **Pokaż hierarchię** znajdujący się na górze strony. W otwartym panelu nawigacyjnym najedź kursorem myszy na nazwę wymaganej grupy, a następnie kliknij ikonę ustawień (⚙).



Hierarchia grup administracyjnych

   Zostanie otwarte okno właściwości grupy administracyjnej.

3. W oknie właściwości przejdź na zakładkę **Ustawienia**.

4. W sekcji **Dziedziczenie** włącz lub wyłącz następujące opcje:

   - **Dziedzicz z grupy nadrzędnej**

     Ustawienia z tej sekcji są dziedziczone od grupy nadrzędnej, w której znajduje się urządzenie klienckie. Jeśli ta opcja jest włączona, ustawienia w sekcji **Aktywność urządzenia w sieci** nie mogą być modyfikowane.

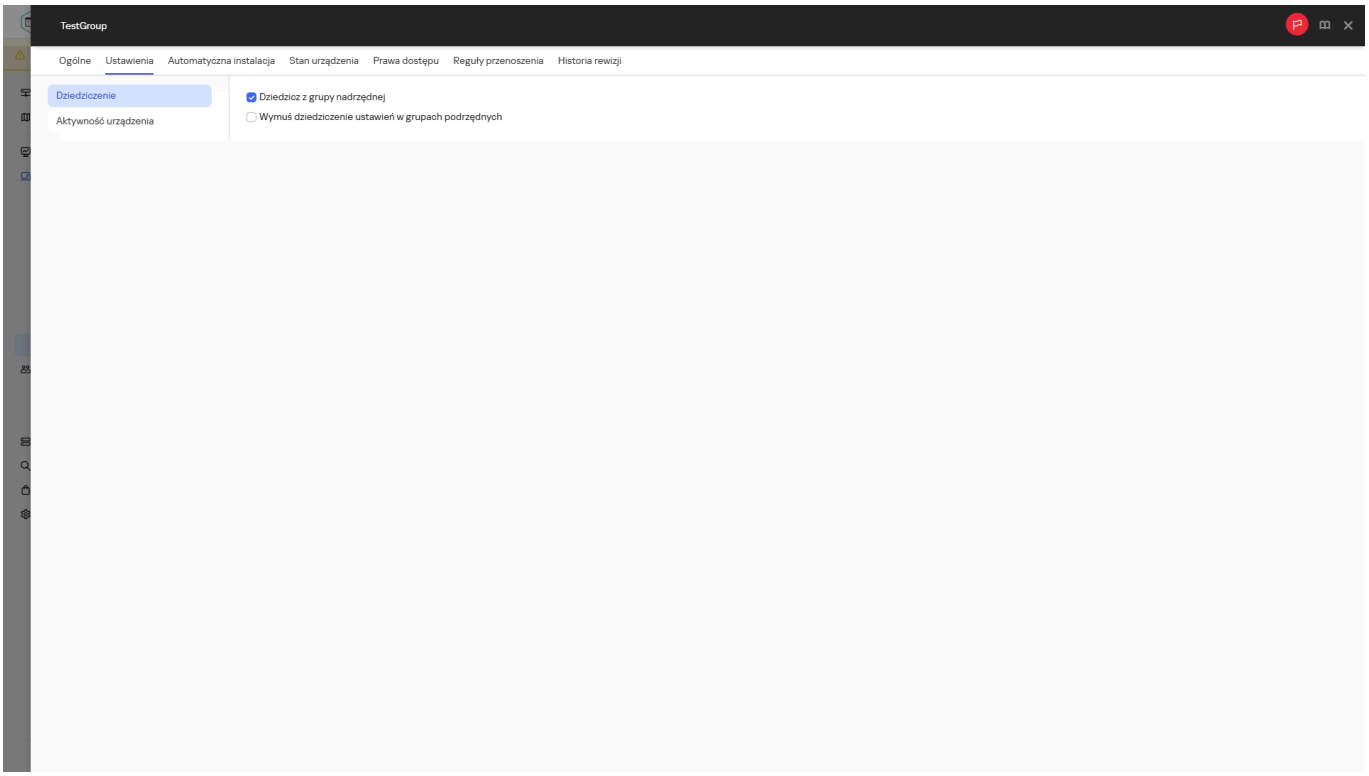
     Ta opcja jest dostępna tylko wtedy, gdy grupa administracyjna posiada grupę nadrzędną.

Domyślnie opcja ta jest włączona.

- **Wymuś dziedziczenie ustawień w grupach podrzędnych**

  Wartości ustawień zostaną rozesłane do grup podrzędnych ale we właściwościach grup podrzędnych te ustawienia są zablokowane.

  Domyślnie opcja ta jest wyłączona.



Właściwości grupy administracyjnej

5. W sekcji **Aktywność urządzenia** włącz lub wyłącz następujące opcje:

   - **Powiadom administratora, jeżeli urządzenie jest nieaktywne dłużej niż (dni)**

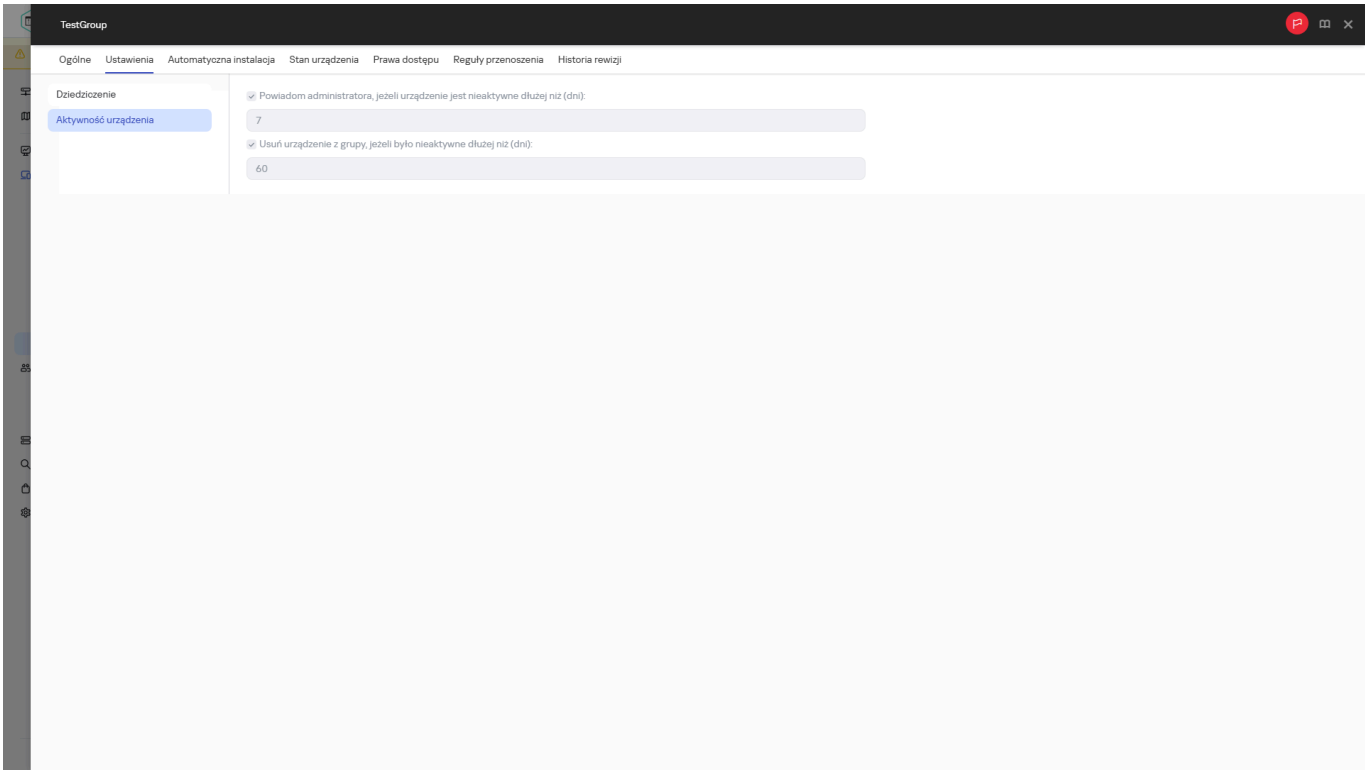
     Jeśli ta opcja jest włączona, administrator otrzyma powiadomienie o nieaktywnych urządzeniach. Możesz określić przedział czasu, po upływie którego tworzone jest zdarzenie **Urządzenie było nieaktywne w sieci od bardzo dawna**. Domyślny przedział czasu wynosi 7 dni.

     Domyślnie opcja ta jest włączona.

   - **Usuń urządzenie z grupy, jeżeli było nieaktywne dłużej niż (dni)**

     Jeśli ta opcja jest włączona, możesz określić przedział czasu, po upływie którego urządzenie zostanie automatycznie usunięte z grupy. Domyślny przedział czasu wynosi 60 dni.

Domyślnie opcja ta jest włączona.



Właściwości grupy administracyjnej

6. Kliknij **Zapisz**.

Twoje zmiany zostaną zapisane i zastosowane.

Wysyłanie wiadomości na urządzenia użytkowników

W celu wysyłania wiadomości do użytkowników urządzeń:

1. W menu głównym przejdź do **Zadania**.
2. Kliknij **Dodaj**.

   Zostanie uruchomiony Kreator tworzenia nowego zadania.
3. Z listy rozwijanej **Typ zadania** wybierz opcję **Wyślij wiadomość do użytkownika**.
4. Wybierz opcję do określenia grupy administracyjnej, wyboru urządzeń lub urządzeń, do których stosowane jest zadanie.
5. Uruchom utworzone zadanie.

Po zakończeniu wykonywania zadania utworzona wiadomość zostanie wysłana do użytkowników wybranych urządzeń. Zadanie **Wyślij wiadomość do użytkownika** jest dostępne tylko dla urządzeń z systemem Windows.

Zdalne włączanie, wyłączanie i ponowne uruchamianie urządzeń klienckich

Kaspersky Security Center Linux pozwala na zdalne zarządzanie urządzeniami klienckimi: włączanie, wyłączanie i ponowne uruchamianie.

W celu zdalnego zarządzania urządzeniami klienckimi:

1. W menu głównym przejdź do **Zadania**.
2. Kliknij **Dodaj**.

   Zostanie uruchomiony Kreator tworzenia nowego zadania.
3. Z listy rozwijalnej **Typ zadania** wybierz **Zarządzaj urządzeniami**.
4. Wybierz opcję do określenia grupy administracyjnej, wyboru urządzeń lub urządzeń, do których stosowane jest zadanie.
5. Wybierz polecenie (włącz, wyłącz lub uruchom ponownie).
6. W razie potrzeby skonfiguruj następujące ustawienia dla poleceń wyłączania i ponownego uruchamiania:
   - Włącz przełącznik **Pytaj użytkownika o potwierdzenie**, aby określić komunikat monitu dla użytkownika oraz odstępy czasu, po których monit ma zostać powtórzony, a urządzenia mają zostać wyłączone lub ponownie uruchomione.
   - Zaznacz pole wyboru **Czas oczekiwania przed wymuszeniem zamknięcia aplikacji dla zablokowanych sesji (min)** i określ czas.

   Ustawienia te dotyczą wyłącznie urządzeń klienckich z systemem Windows. Urządzenia z systemem Linux zostaną ponownie uruchomione lub wyłączone natychmiast po zakończeniu zadania.
7. Uruchom utworzone zadanie.

Po zakończeniu zadania, polecenie (włącz, wyłącz lub uruchom ponownie) zostanie wykonane na wybranych urządzeniach.

Zdalny dostęp do zarządzanych urządzeń

Kaspersky Security Center Linux umożliwia nawiązanie zdalnego połączenia z zarządzanymi urządzeniami. Administrator może uzyskać zdalny dostęp do zarządzanego urządzenia poprzez Agenta sieciowego zainstalowanego na urządzeniu. Zdalne połączenie z urządzeniem poprzez Agenta sieciowego jest możliwe nawet wtedy, gdy porty TCP i UDP urządzenia klienckiego są zamknięte. Po nawiązaniu połączenia z urządzeniem, administrator uzyskuje pełny dostęp do informacji przechowywanych na tym urządzeniu, dzięki czemu może zarządzać aplikacjami, które są na nim zainstalowane.

Metody nawiązywania połączenia zdalnego zależą od platformy używanej na urządzeniu z Kaspersky Security Center Web Console. Kaspersky Security Center Web Console można zainstalować na urządzeniu innym niż Serwer administracyjny, na urządzeniu z systemem Windows lub Linux.

Z poziomu Kaspersky Security Center Web Console zainstalowanej na urządzeniu z systemem Linux możesz nawiązać następujące połączenia:

- Do zarządzanego urządzenia opartego na systemie Linux za pomocą:
  - Połączenia pulpitu zdalnego (RDP)
  - Virtual Network Computing (VNC)
- Do zarządzanego urządzenia opartego na systemie Windows za pomocą:
  - Połączenia pulpitu zdalnego (RDP)
  - Virtual Network Computing (VNC)

Z poziomu Kaspersky Security Center Web Console zainstalowanej na urządzeniu z systemem Windows możesz nawiązać następujące połączenia:

- Do zarządzanego urządzenia opartego na systemie Linux za pomocą:
  - Połączenia pulpitu zdalnego (RDP)
  - Virtual Network Computing (VNC)
- Do zarządzanego urządzenia opartego na systemie Windows za pomocą:
  - Połączenia pulpitu zdalnego (RDP)
  - Windows Desktop Sharing (WDS)

Zdalne połączenie z zarządzanymi urządzeniami nie jest obsługiwane podczas uzyskiwania dostępu do Kaspersky Security Center Web Console z urządzenia z systemem Microsoft Windows opartym na architekturze Arm.

W celu nawiązania zdalnego połączenia z urządzeniem, musisz posiadać następujące:

- narzędzie klsctunnel

  Narzędzie Kaspersky służy do tunelowania połączenia między zarządzanym urządzeniem a Serwerem administracyjnym.

  Kaspersky Security Center Linux umożliwia tunelowanie połączeń TCP z Kaspersky Security Center Web Console poprzez Serwer administracyjny, a następnie poprzez Agenta sieciowego do określonego portu na zarządzanym urządzeniu. Tunelowanie połączeń jest przeznaczone dla połączenia aplikacji klienckiej na urządzeniu z zainstalowaną Kaspersky Security Center Web Console z portem TCP na zarządzanym urządzeniu —jeśli nie jest możliwe bezpośrednie połączenie między Konsolą administracyjną a urządzeniem docelowym.

Tunelowanie połączenia pomiędzy zdalnym urządzeniem klienckim a Serwerem administracyjnym jest wymagane, gdy port używany do nawiązania połączenia z Serwerem administracyjnym nie jest dostępny na urządzeniu. Port może być niedostępny na urządzeniu w następujących przypadkach:

- Zdalne urządzenie jest podłączone do sieci lokalnej, która wykorzystuje mechanizm NAT.
- Zdalne urządzenie jest częścią sieci lokalnej Serwera administracyjnego, ale jego port jest zamknięty przez zaporę sieciową.

Narzędzie można pobrać po nawiązaniu połączenia zdalnego za pośrednictwem Kaspersky Security Center Web Console lub ręcznie ze strony internetowej Kaspersky.

Narzędzie klsctunnel jest instalowane na urządzeniu Serwera administracyjnego i używane do wszystkich typów połączeń zdalnych (RDP, VNC, WDS).

- Klient RDP lub VNC

  Klient RDP lub VNC jest zainstalowany na urządzeniu Serwera administracyjnego. Ten klient umożliwia uzyskanie zdalnego dostępu do zarządzanego urządzenia przy użyciu adresu i portu połączenia lokalnego dostarczonego przez narzędzie klsctunnel.

  Połączenie RDP z bieżącą sesją zdalnego pulpitu użytkownika jest nawiązywane bez zgody użytkownika. Po nawiązaniu przez administratora połączenia z sesją, użytkownik urządzenia zostaje odłączony od sesji bez powiadomienia.

- Windows Desktop Sharing (tylko dla zarządzanych urządzeń z systemem Windows)

  Funkcja ta umożliwia połączenie z istniejącą sesją na urządzeniu klienta bez rozłączania użytkownika w tej sesji. W tym przypadku administrator i użytkownik sesji na urządzeniu klienckim współdzielą dostęp do pulpitu.

  Podczas łączenia się z istniejącą sesją zdalnego pulpitu użytkownik sesji na urządzeniu otrzymuje od administratora żądanie dotyczące połączenia. W raportach utworzonych przez Kaspersky Security Center Linux nie są zapisywane żadne informacje dotyczące zdalnych działań wykonywanych na urządzeniu ani wyniki tych działań.

  Administrator może skonfigurować audyt aktywności użytkownika na zdalnym urządzeniu klienckim. W trakcie audytu aplikacja zapisuje informacje o plikach na urządzeniu klienckim, który został otwarty i/lub zmodyfikowany przez administratora.

Zdalny dostęp z urządzenia opartego na systemie Linux za pomocą Kaspersky Security Center Web Console do urządzenia zarządzanego opartego na systemie Linux

Wymagania wstępne

Przed rozpoczęciem upewnij się, że:

- Na zarządzanym urządzeniu z systemem Linux zainstalowany jest Agent sieciowy w wersji 15.3 lub nowszej.
- Na zarządzanym urządzeniu z systemem Linux zainstalowany jest serwer RDP (jeśli łączysz się z zarządzanym urządzeniem za pomocą Połączenia pulpitu zdalnego).
- Na zarządzanym urządzeniu z systemem Linux zainstalowany jest serwer VNC (jeśli łączysz się z zarządzanym urządzeniem za pomocą VNC).

- Port do tunelowania połączeń RDP jest otwarty (opcja **Otwórz port do tunelowania połączeń RDP** jest włączona w sekcji **Porty połączenia** okna właściwości Serwera administracyjnego).

- Administrator ma prawo do **Uruchom sesje RDP** w celu nawiązywania połączeń RDP (jeśli łączysz się z zarządzanym urządzeniem za pomocą funkcji Podłączanie pulpitu zdalnego).

- Administrator ma prawo do **Rozpocznij tunelowanie** do ustanowienia połączenia tunelowego dla VNC (jeśli łączysz się z zarządzanym urządzeniem za pomocą Virtual Network Computing).

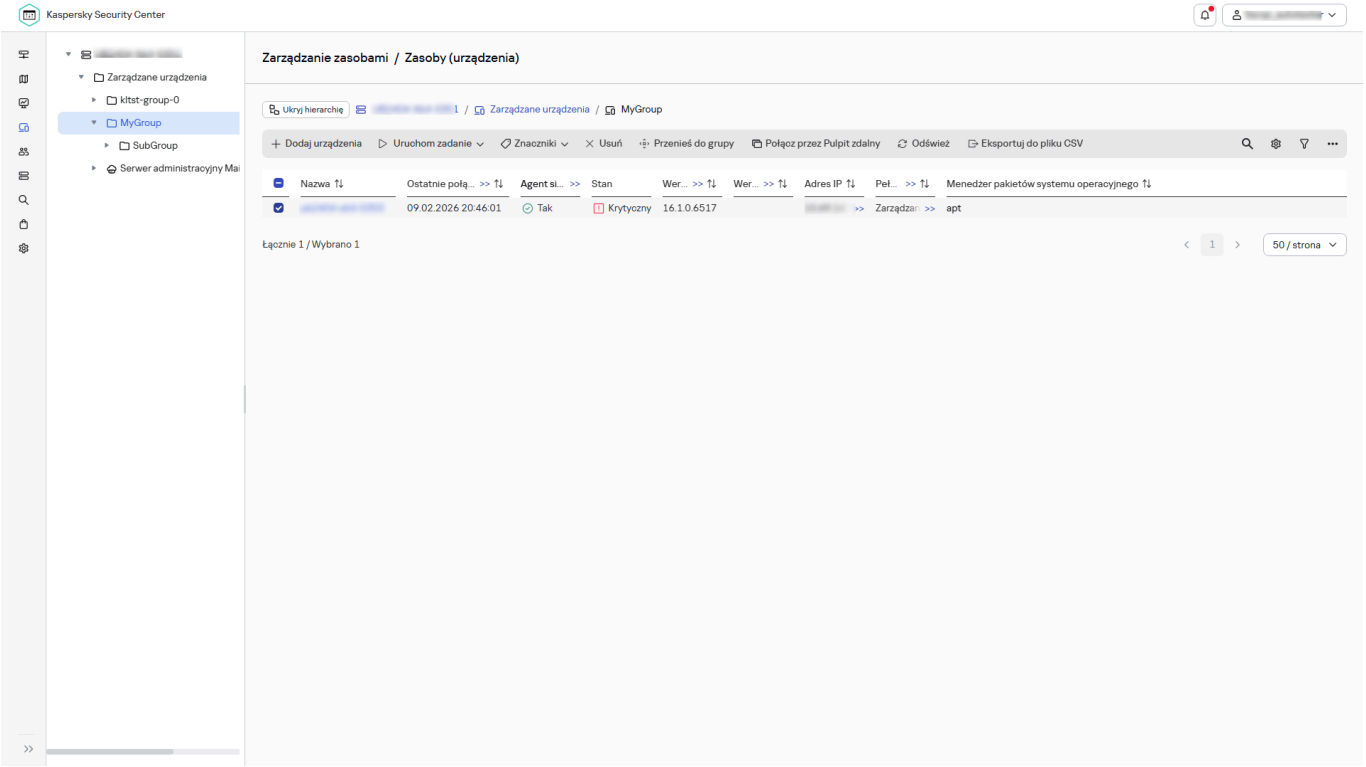
Aby nawiązać połączenie z zarządzanym urządzeniem opartymi na systemie Linux przy użyciu protokołu RDP lub VNC za pośrednictwem Kaspersky Security Center Web Console otwartej na urządzeniu opartym na systemie Linux:

1. W menu głównym przejdź do sekcji **Zarządzanie zasobami** → **Zasoby (urządzenia)** lub otwórz okno wyboru urządzeń.

2. Zaznacz pole wyboru obok zarządzanego urządzenia, z którym chcesz się połączyć zdalnie, a następnie kliknij przycisk **Połącz przez Pulpit zdalny**.

   Otworzy się okno **Połącz przez Pulpit zdalny**.

   Jeśli wybierzesz wiele urządzeń, urządzenie mobilne lub urządzenie z systemem macOS, przycisk **Połącz przez Pulpit zdalny** będzie wyłączony.



Lista zarządzanych urządzeń

3. Pobierz narzędzie klsctunnel, klikając przycisk **Pobierz**, a następnie je uruchom.

Podczas pobierania narzędzia należy wziąć pod uwagę następujące kwestie:

- Aby uzyskać najnowszą wersję narzędzia klsctunnel, upewnij się, że Serwer administracyjny ma dostęp do serwerów aktualizacji Kaspersky.

  Możesz uruchomić zadanie *Pobierz aktualizacje do repozytorium Serwera administracyjnego* i wybrać serwery aktualizacji Kaspersky jako źródło aktualizacji. Jeśli zadanie zakończy się pomyślnie, Serwer administracyjny uzyska dostęp do serwerów aktualizacji Kaspersky.

- Jeśli plik narzędzia nie jest dostępny do pobrania, wyświetlany jest komunikat o błędzie. W takim przypadku pobierz narzędzie ręcznie, a następnie umieść je na urządzeniu Serwera administracyjnego w katalogu /var/opt/kaspersky/klnagent_srv.

4. W oknie **Połącz przez Pulpit zdalny** określ port połączenia. Domyślnie wykorzystywany jest port 3389.

5. Wygeneruj tekstowy obiekt blob z zakodowanymi parametrami połączenia, klikając przycisk **Wygeneruj obiekt blob**, a następnie skopiuj i wklej tekst do odpowiedniego pola w narzędziu klsctunnel.

   Obiekt blob zawiera ustawienia wymagane do nawiązania połączenia pomiędzy Serwerem administracyjnym a zarządzanym urządzeniem. Blob jest ważny przez 3 minuty. Jeśli wygasł, wygeneruj nowy blob.

6. W narzędziu klsctunnel, jeżeli używasz serwera proxy, określ ustawienia połączenia serwera proxy.

   Narzędzie klsctunnel wyświetla adres i port lokalnego połączenia klienta zdalnego dostępu.

   Narzędzie umożliwia administratorowi zamknięcie połączenia tunelowego. Jeżeli połączenie tunelowe zostanie zamknięte, bieżące połączenie ze zdalnym pulpitem zostanie zakończone.

7. Uruchom klienta dostępu zdalnego (RDP lub VNC) i połącz go z zarządzanym urządzeniem, korzystając z adresu i portu dostarczonych przez narzędzie klsctunnel.

Nawiązywane jest połączenie z zarządzanym urządzeniem, a pulpit staje się dostępny w oknie klienta dostępu zdalnego.

Zdalny dostęp z urządzenia opartego na systemie Linux za pomocą Kaspersky Security Center Web Console do urządzenia zarządzanego opartego na systemie Windows

Połączenia pulpitu zdalnego (RDP)

Wymagania wstępne

Przed rozpoczęciem upewnij się, że:

- Zdalne połączenie jest dozwolone w ustawieniach systemu operacyjnego zarządzanego urządzenia.
- Na zarządzanym urządzeniu z systemem Windows zainstalowany jest Agent sieciowy w wersji 13.0 lub nowszej.
- Administrator ma prawo do **Uruchom sesje RDP** w celu nawiązywania połączeń RDP.
- Port do tunelowania połączeń RDP jest otwarty (opcja **Otwórz port do tunelowania połączeń RDP** jest włączona w sekcji **Porty połączenia** okna właściwości Serwera administracyjnego).

Aby nawiązać połączenie z urządzeniem zarządzanym opartym na systemie Windows przy użyciu protokołu RDP za pośrednictwem Kaspersky Security Center Web Console otwartej na urządzeniu opartym na systemie Linux:

1. W menu głównym przejdź do sekcji **Zarządzanie zasobami** → **Zasoby (urządzenia)** lub otwórz okno wyboru urządzeń.

2. Zaznacz pole wyboru obok zarządzanego urządzenia, z którym chcesz się połączyć zdalnie, a następnie kliknij przycisk **Połącz przez Pulpit zdalny**.

   Otworzy się okno **Połącz przez Pulpit zdalny**.

   Jeśli wybierzesz wiele urządzeń, urządzenie mobilne lub urządzenie z systemem macOS, przycisk **Połącz przez Pulpit zdalny** będzie wyłączony.

3. W oknie **Połącz przez Pulpit zdalny** określ typ połączenia **RDP**.

4. Jeśli połączenie zdalne nie jest dozwolone w ustawieniach systemu operacyjnego zarządzanego urządzenia, zezwól na połączenie zdalne centralnie, klikając przycisk **Zmień ustawienia**.

   Jeśli ustawienia zostaną zastosowane prawidłowo, wyświetlone zostanie powiadomienie. Ponadto na zarządzanym urządzeniu, w sekcji **Ustawienia** → **System** → **Pulpit zdalny**, opcja **Włącz pulpit zdalny** jest włączona.

   Jeśli w ustawieniach systemu operacyjnego zarządzanego urządzenia zezwolono na połączenie zdalne, przycisk **Zmień ustawienia** nie będzie wyświetlany.

5. Pobierz narzędzie klsctunnel, klikając przycisk **Pobierz**, a następnie je uruchom.

   Podczas pobierania narzędzia należy wziąć pod uwagę następujące kwestie:

   - Aby uzyskać najnowszą wersję narzędzia klsctunnel, upewnij się, że Serwer administracyjny ma dostęp do serwerów aktualizacji Kaspersky.

     Możesz uruchomić zadanie *Pobierz aktualizacje do repozytorium Serwera administracyjnego* i wybrać serwery aktualizacji Kaspersky jako źródło aktualizacji. Jeśli zadanie zakończy się pomyślnie, Serwer administracyjny uzyska dostęp do serwerów aktualizacji Kaspersky.

   - Jeśli plik narzędzia nie jest dostępny do pobrania, wyświetlany jest komunikat o błędzie. W takim przypadku pobierz narzędzie ręcznie, a następnie umieść je na urządzeniu Serwera administracyjnego w katalogu /var/opt/kaspersky/klnagent_srv.

6. Wygeneruj tekstowy obiekt blob z zakodowanymi parametrami połączenia, klikając przycisk **Wygeneruj obiekt blob**, a następnie skopiuj i wklej tekst do odpowiedniego pola w narzędziu klsctunnel.

   Obiekt blob zawiera ustawienia wymagane do nawiązania połączenia pomiędzy Serwerem administracyjnym a zarządzanym urządzeniem. Blob jest ważny przez 3 minuty. Jeśli wygasł, wygeneruj nowy blob.

7. W narzędziu klsctunnel, jeżeli używasz serwera proxy, określ ustawienia połączenia serwera proxy.

   Narzędzie klsctunnel wyświetla adres i port połączenia ze zdalnym urządzeniem.

   Narzędzie umożliwia administratorowi zamknięcie połączenia tunelowego. Jeżeli połączenie tunelowe zostanie zamknięte, bieżące połączenie ze zdalnym pulpitem zostanie zakończone.

8. Uruchom klienta RDP i połącz go z zarządzanym urządzeniem, korzystając z adresu i portu dostarczonych przez narzędzie klsctunnel.

Nawiązywane jest połączenie z zarządzanym urządzeniem, a pulpit staje się dostępny w oknie klienta RDP.

Połączenie z bieżącą sesją zdalnego pulpitu użytkownika jest nawiązywane bez zgody użytkownika. Po nawiązaniu przez administratora połączenia z sesją, użytkownik urządzenia zostaje odłączony od sesji bez powiadomienia.

System Virtual Network Computing (VNC)

Wymagania wstępne

Przed rozpoczęciem upewnij się, że:

- Na zarządzanym urządzeniu z systemem Windows zainstalowany jest Agent sieciowy w wersji 13.0 lub nowszej.
- Na zarządzanym urządzeniu z systemem Windows zainstalowany jest serwer VNC.
- Administrator ma prawo do **Rozpocznij tunelowanie**, aby ustanowić połączenie tunelowe dla VNC.
- Port do tunelowania połączeń RDP jest otwarty (opcja **Otwórz port do tunelowania połączeń RDP** jest włączona w sekcji **Porty połączenia** okna właściwości Serwera administracyjnego).

Aby nawiązać połączenie z urządzeniem zarządzanym opartym na systemie Windows przy użyciu protokołu VNC za pośrednictwem Kaspersky Security Center Web Console otwartej na urządzeniu opartym na systemie Linux:

1. W menu głównym przejdź do sekcji **Zarządzanie zasobami** → **Zasoby (urządzenia)** lub otwórz okno wyboru urządzeń.
2. Zaznacz pole wyboru obok zarządzanego urządzenia, z którym chcesz się połączyć zdalnie, a następnie kliknij przycisk **Połącz przez Pulpit zdalny**.

   Otworzy się okno **Połącz przez Pulpit zdalny**.

   Jeśli wybierzesz wiele urządzeń, urządzenie mobilne lub urządzenie z systemem macOS, przycisk **Połącz przez Pulpit zdalny** będzie wyłączony.
3. W oknie **Połącz przez Pulpit zdalny** wybierz typ połączenia **VNC**.
4. Pobierz narzędzie klsctunnel, klikając przycisk **Pobierz**, a następnie je uruchom.

   Jeśli plik narzędzia nie jest dostępny do pobrania, wyświetlany jest komunikat o błędzie. W takim przypadku pobierz narzędzie ręcznie.
5. W oknie **Połącz przez Pulpit zdalny** określ port połączenia VNC. Domyślnie wykorzystywany jest port 5900.
6. Wygeneruj tekstowy obiekt blob z zakodowanymi parametrami połączenia, klikając przycisk **Wygeneruj obiekt blob**, a następnie skopiuj i wklej tekst do odpowiedniego pola w narzędziu klsctunnel.

   Obiekt blob zawiera ustawienia wymagane do nawiązania połączenia pomiędzy Serwerem administracyjnym a zarządzanym urządzeniem. Blob jest ważny przez 3 minuty. Jeśli wygasł, wygeneruj nowy blob.
7. W narzędziu klsctunnel, jeżeli używasz serwera proxy, określ ustawienia połączenia serwera proxy.

   Narzędzie klsctunnel wyświetla adres i port lokalnego połączenia klienta VNC.

   Narzędzie umożliwia użytkownikowi zdalnemu zamknięcie połączenia tunelowego. Jeżeli połączenie tunelowe zostanie zamknięte, bieżące połączenie ze zdalnym pulpitem zostanie zakończone.
8. Uruchom klienta VNC i połącz go z zarządzanym urządzeniem, korzystając z adresu i portu dostarczonych przez narzędzie klsctunnel.

Nawiązywane jest połączenie z zarządzanym urządzeniem, a pulpit staje się dostępny w oknie klienta VNC.

Zdalny dostęp z urządzenia opartego na systemie Windows za pomocą Kaspersky Security Center Web Console do urządzenia zarządzanego opartego na systemie Linux

Połączenia pulpitu zdalnego (RDP)

Wymagania wstępne

Przed rozpoczęciem upewnij się, że:

- Na zarządzanym urządzeniu z systemem Linux zainstalowany jest serwer RDP.
- Na zarządzanym urządzeniu z systemem Linux zainstalowany jest Agent sieciowy w wersji 15.3 lub nowszej.
- Administrator ma prawo do **Uruchom sesje RDP** w celu nawiązywania połączeń RDP.
- Port do tunelowania połączeń RDP jest otwarty (opcja **Otwórz port do tunelowania połączeń RDP** jest włączona w sekcji **Porty połączenia** okna właściwości Serwera administracyjnego).

Aby nawiązać połączenie z zarządzanym urządzeniem opartym na systemie Linux przy użyciu protokołu RDP za pośrednictwem Kaspersky Security Center Web Console otwartej na urządzeniu opartym na systemie Windows:

1. W menu głównym przejdź do sekcji **Zarządzanie zasobami** → **Zasoby (urządzenia)** lub otwórz okno wyboru urządzeń.
2. Zaznacz pole wyboru obok zarządzanego urządzenia, z którym chcesz się połączyć zdalnie, a następnie kliknij przycisk **Połącz przez Pulpit zdalny**.

   Otworzy się okno **Połącz przez Pulpit zdalny**.

   Jeśli wybierzesz wiele urządzeń, urządzenie mobilne lub urządzenie z systemem macOS, przycisk **Połącz przez Pulpit zdalny** będzie wyłączony.
3. W oknie **Połącz przez Pulpit zdalny** określ typ połączenia **RDP**.
4. Pobierz narzędzie klsctunnel, klikając przycisk **Pobierz**, a następnie je uruchom.

   Podczas pobierania narzędzia należy wziąć pod uwagę następujące kwestie:

   - Aby uzyskać najnowszą wersję narzędzia klsctunnel, upewnij się, że Serwer administracyjny ma dostęp do serwerów aktualizacji Kaspersky.

     Możesz uruchomić zadanie *Pobierz aktualizacje do repozytorium Serwera administracyjnego* i wybrać serwery aktualizacji Kaspersky jako źródło aktualizacji. Jeśli zadanie zakończy się pomyślnie, Serwer administracyjny uzyska dostęp do serwerów aktualizacji Kaspersky.
   - Jeśli plik narzędzia nie jest dostępny do pobrania, wyświetlany jest komunikat o błędzie. W takim przypadku pobierz narzędzie ręcznie, a następnie umieść je na urządzeniu Serwera administracyjnego w katalogu /var/opt/kaspersky/klnagent_srv.

5. Wygeneruj tekstowy obiekt blob z zakodowanymi parametrami połączenia, klikając przycisk **Wygeneruj obiekt blob**, a następnie skopiuj i wklej tekst do odpowiedniego pola w narzędziu klsctunnel.

   Obiekt blob zawiera ustawienia wymagane do nawiązania połączenia pomiędzy Serwerem administracyjnym a zarządzanym urządzeniem. Blob jest ważny przez 3 minuty. Jeśli wygasł, wygeneruj nowy blob.

6. W narzędziu klsctunnel, jeżeli używasz serwera proxy, określ ustawienia połączenia serwera proxy.

   Aby to zrobić, zaznacz pole wyboru **Użyj serwera proxy**, a następnie określ ustawienia połączenia.

7. Kliknij przycisk **Otwórz port**.

   Zostanie otwarte okno logowania Podłączanie pulpitu zdalnego.

8. Podaj dane uwierzytelniające konta, na którym jesteś aktualnie zalogowany do Kaspersky Security Center Web Console, a następnie połącz się z zarządzanym urządzeniem.

   Narzędzie klsctunnel wyświetla adres i port połączenia ze zdalnym urządzeniem.

   Narzędzie umożliwia administratorowi zamknięcie połączenia tunelowego. Jeżeli połączenie tunelowe zostanie zamknięte, bieżące połączenie ze zdalnym pulpitem zostanie zakończone.

Po nawiązaniu połączenia z urządzeniem, pulpit jest dostępny w oknie Podłączanie pulpitu zdalnego systemu Microsoft Windows.

Połączenie z bieżącą sesją zdalnego pulpitu użytkownika jest nawiązywane bez zgody użytkownika. Po nawiązaniu przez administratora połączenia z sesją, użytkownik urządzenia zostaje odłączony od sesji bez powiadomienia.

System Virtual Network Computing (VNC)

Wymagania wstępne

Przed rozpoczęciem upewnij się, że:

- Na zarządzanym urządzeniu z systemem Linux zainstalowany jest Agent sieciowy w wersji 15.3 lub nowszej.
- Na zarządzanym urządzeniu z systemem Linux zainstalowany jest serwer VNC.
- Administrator ma prawo do **Rozpocznij tunelowanie**, aby ustanowić połączenie tunelowe dla VNC.
- Port do tunelowania połączeń RDP jest otwarty (opcja **Otwórz port do tunelowania połączeń RDP** jest włączona w sekcji **Porty połączenia** okna właściwości Serwera administracyjnego).

Aby nawiązać połączenie z zarządzanym urządzeniem opartym na systemie Linux przy użyciu protokołu VNC za pośrednictwem Kaspersky Security Center Web Console otwartej na urządzeniu opartym na systemie Windows:

1. W menu głównym przejdź do sekcji **Zarządzanie zasobami** → **Zasoby (urządzenia)** lub otwórz okno wyboru urządzeń.

2. Zaznacz pole wyboru obok zarządzanego urządzenia, z którym chcesz się połączyć zdalnie, a następnie kliknij przycisk **Połącz przez Pulpit zdalny**.

   Otworzy się okno **Połącz przez Pulpit zdalny**.

   Jeśli wybierzesz wiele urządzeń, urządzenie mobilne lub urządzenie z systemem macOS, przycisk **Połącz przez Pulpit zdalny** będzie wyłączony.

3. W oknie **Połącz przez Pulpit zdalny** wybierz typ połączenia **VNC**.

4. Pobierz narzędzie klsctunnel, klikając przycisk **Pobierz**, a następnie je uruchom.

   Jeśli plik narzędzia nie jest dostępny do pobrania, wyświetlany jest komunikat o błędzie. W takim przypadku pobierz narzędzie ręcznie.

5. W oknie **Połącz przez Pulpit zdalny** określ port połączenia VNC. Domyślnie wykorzystywany jest port 5900.

6. Wygeneruj tekstowy obiekt blob z zakodowanymi parametrami połączenia, klikając przycisk **Wygeneruj obiekt blob**, a następnie skopiuj i wklej tekst do odpowiedniego pola w narzędziu klsctunnel.

   Obiekt blob zawiera ustawienia wymagane do nawiązania połączenia pomiędzy Serwerem administracyjnym a zarządzanym urządzeniem. Blob jest ważny przez 3 minuty. Jeśli wygasł, wygeneruj nowy blob.

7. W narzędziu klsctunnel, jeżeli używasz serwera proxy, określ ustawienia połączenia serwera proxy.

   Aby to zrobić, zaznacz pole wyboru **Użyj serwera proxy**, a następnie określ ustawienia połączenia.

8. Kliknij przycisk **Otwórz port**.

   Narzędzie klsctunnel wyświetla adres i port lokalnego połączenia klienta VNC.

   Narzędzie umożliwia użytkownikowi zdalnemu zamknięcie połączenia tunelowego. Jeżeli połączenie tunelowe zostanie zamknięte, bieżące połączenie ze zdalnym pulpitem zostanie zakończone.

9. Uruchom klienta VNC i połącz go z zarządzanym urządzeniem, korzystając z adresu i portu dostarczonych przez narzędzie klsctunnel.

Nawiązywane jest połączenie z zarządzanym urządzeniem, a pulpit staje się dostępny w oknie klienta VNC.

Zdalny dostęp z urządzenia opartego na systemie Windows za pomocą Kaspersky Security Center Web Console do urządzenia zarządzanego opartego na systemie Windows

Połączenia pulpitu zdalnego (RDP)

Wymagania wstępne

Przed rozpoczęciem upewnij się, że:

- Na zarządzanym urządzeniu z systemem Windows zainstalowany jest Agent sieciowy w wersji 13.0 lub nowszej.
- Administrator ma prawo do **Uruchom sesje RDP** w celu nawiązywania połączeń RDP.
- Port do tunelowania połączeń RDP jest otwarty (opcja **Otwórz port do tunelowania połączeń RDP** jest włączona w sekcji **Porty połączenia** okna właściwości Serwera administracyjnego).
- Zdalne połączenie jest dozwolone w ustawieniach systemu operacyjnego zarządzanego urządzenia.

Aby nawiązać połączenie z urządzeniem zarządzanym opartym na systemie Windows przy użyciu protokołu RDP za pośrednictwem Kaspersky Security Center Web Console otwartej na urządzeniu opartym na systemie Windows:

1. W menu głównym przejdź do sekcji **Zarządzanie zasobami** → **Zasoby (urządzenia)** lub otwórz okno wyboru urządzeń.

2. Zaznacz pole wyboru obok zarządzanego urządzenia, z którym chcesz się połączyć zdalnie, a następnie kliknij przycisk **Połącz przez Pulpit zdalny**.

   Otworzy się okno **Połącz przez Pulpit zdalny**.

   Jeśli wybierzesz wiele urządzeń, urządzenie mobilne lub urządzenie z systemem macOS, przycisk **Połącz przez Pulpit zdalny** będzie wyłączony.

3. W oknie **Połącz przez Pulpit zdalny** wybierz typ połączenia **Połączenie Pulpitu zdalnego**.

4. Jeśli połączenie zdalne nie jest dozwolone w ustawieniach systemu operacyjnego zarządzanego urządzenia, zezwól na połączenie zdalne centralnie, klikając przycisk **Zmień ustawienia**.

   Jeśli ustawienia zostaną zastosowane prawidłowo, wyświetlone zostanie powiadomienie. Ponadto na zarządzanym urządzeniu, w sekcji **Ustawienia** → **System** → **Pulpit zdalny**, opcja **Włącz pulpit zdalny** jest włączona.

   Jeśli w ustawieniach systemu operacyjnego zarządzanego urządzenia zezwolono na połączenie zdalne, przycisk **Zmień ustawienia** nie będzie wyświetlany.

5. Pobierz narzędzie klsctunnel, klikając przycisk **Pobierz**, a następnie je uruchom.

   Podczas pobierania narzędzia należy wziąć pod uwagę następujące kwestie:

   - Aby uzyskać najnowszą wersję narzędzia klsctunnel, upewnij się, że Serwer administracyjny ma dostęp do serwerów aktualizacji Kaspersky.

     Możesz uruchomić zadanie *Pobierz aktualizacje do repozytorium Serwera administracyjnego* i wybrać serwery aktualizacji Kaspersky jako źródło aktualizacji. Jeśli zadanie zakończy się pomyślnie, Serwer administracyjny uzyska dostęp do serwerów aktualizacji Kaspersky.

   - Jeśli plik narzędzia nie jest dostępny do pobrania, wyświetlany jest komunikat o błędzie. W takim przypadku pobierz narzędzie ręcznie, a następnie umieść je na urządzeniu Serwera administracyjnego w katalogu /var/opt/kaspersky/klnagent_srv.

6. Wygeneruj tekstowy obiekt blob z zakodowanymi parametrami połączenia, klikając przycisk **Wygeneruj obiekt blob**, a następnie skopiuj i wklej tekst do odpowiedniego pola w narzędziu klsctunnel.

   Obiekt blob zawiera ustawienia wymagane do nawiązania połączenia pomiędzy Serwerem administracyjnym a zarządzanym urządzeniem. Blob jest ważny przez 3 minuty. Jeśli wygasł, wygeneruj nowy blob.

7. W narzędziu klsctunnel, jeżeli używasz serwera proxy, określ ustawienia połączenia serwera proxy.

   Aby to zrobić, zaznacz pole wyboru **Użyj serwera proxy**, a następnie określ ustawienia połączenia.

8. Kliknij przycisk **Otwórz port**.

   Zostanie otwarte okno logowania Podłączanie pulpitu zdalnego.

9. Podaj dane uwierzytelniające konta, na którym jesteś aktualnie zalogowany do Kaspersky Security Center Web Console, a następnie połącz się z zarządzanym urządzeniem.

   Narzędzie klsctunnel wyświetla adres i port połączenia ze zdalnym urządzeniem.

Narzędzie umożliwia administratorowi zamknięcie połączenia tunelowego. Jeżeli połączenie tunelowe zostanie zamknięte, bieżące połączenie ze zdalnym pulpitem zostanie zakończone.

Po nawiązaniu połączenia z urządzeniem, pulpit jest dostępny w oknie Podłączanie pulpitu zdalnego systemu Microsoft Windows.

Połączenie z bieżącą sesją zdalnego pulpitu użytkownika jest nawiązywane bez zgody użytkownika. Po nawiązaniu przez administratora połączenia z sesją, użytkownik urządzenia zostaje odłączony od sesji bez powiadomienia.

Windows Desktop Sharing (WDS)

Wymagania wstępne

Przed rozpoczęciem upewnij się, że:

- Na zarządzanym urządzeniu z systemem Windows zainstalowany jest Agent sieciowy w wersji 13.0 lub nowszej.
- Administrator ma prawo **Połączenie z istniejącymi sesjami RDP** w celu ustanowienia połączenia WDS.
- Dostępna jest licencja na Zarządzanie lukami i poprawkami.
- Na stacji roboczej administratora powinien być zainstalowany system operacyjny Microsoft Windows Vista lub nowszy. Typ systemu operacyjnego urządzenia, na którym znajduje się Serwer administracyjny nie nakłada żadnych ograniczeń na łączenie poprzez udostępnianie pulpitu Windows.

  Sprawdź, czy funkcja Windows Desktop Sharing znajduje się w posiadanej przez Ciebie edycji systemu Windows i upewnij się, że klucz CLSID\{32BE5ED2-5C86-480F-A914-0FF8885A1B3F} znajduje się w rejestrze systemu Windows.
- System Microsoft Windows Vista lub nowszy jest zainstalowany na urządzeniu klienckim.

Aby nawiązać połączenie z urządzeniem zarządzanym opartym na systemie Windows przy użyciu protokołu VNC za pośrednictwem Kaspersky Security Center Web Console otwartej na urządzeniu opartym na systemie Windows:

1. W menu głównym przejdź do sekcji **Zarządzanie zasobami** → **Zasoby (urządzenia)** lub otwórz okno wyboru urządzeń.
2. Zaznacz pole wyboru obok zarządzanego urządzenia, z którym chcesz się połączyć zdalnie, a następnie kliknij przycisk **Połącz przez Pulpit zdalny**.

   Otworzy się okno **Połącz przez Pulpit zdalny**.

   Jeśli wybierzesz wiele urządzeń, urządzenie mobilne lub urządzenie z systemem macOS, przycisk **Połącz przez Pulpit zdalny** będzie wyłączony.
3. W oknie **Połącz przez Pulpit zdalny** wybierz typ połączenia **Windows Desktop Sharing**.

   Jeśli licencja na Zarządzanie lukami i poprawkami jest niedostępna, wyświetlany jest komunikat o błędzie.
4. Pobierz narzędzie klsctunnel, klikając przycisk **Pobierz**, a następnie je uruchom.

   Jeśli plik narzędzia nie jest dostępny do pobrania, wyświetlany jest komunikat o błędzie. W takim przypadku pobierz narzędzie ręcznie.

5. Z listy dostępnych sesji użytkownika aktywnych na wybranym urządzeniu wybierz sesję, z którą chcesz się połączyć.

   Zdalny użytkownik musi zezwolić na połączenie. Jeśli użytkownik zdalny odmówi połączenia lub nie zezwoli na połączenie w określonym czasie, zostanie wyświetlony komunikat o błędzie.

6. Wygeneruj tekstowy obiekt blob z zakodowanymi parametrami połączenia, klikając przycisk **Wygeneruj obiekt blob**, a następnie skopiuj i wklej tekst do odpowiedniego pola w narzędziu klsctunnel.

   Obiekt blob zawiera ustawienia wymagane do nawiązania połączenia pomiędzy Serwerem administracyjnym a zarządzanym urządzeniem. Blob jest ważny przez 3 minuty. Jeśli wygasł, wygeneruj nowy blob.

7. W narzędziu klsctunnel, jeżeli używasz serwera proxy, określ ustawienia połączenia serwera proxy.

   Aby to zrobić, zaznacz pole wyboru **Użyj serwera proxy**, a następnie określ ustawienia połączenia.

8. Kliknij przycisk **Otwórz port**.

   Narzędzie klsctunnel wyświetla adres i port lokalnego połączenia klienta VNC.

   Narzędzie umożliwia użytkownikowi zdalnemu zamknięcie połączenia tunelowego. Jeżeli połączenie tunelowe zostanie zamknięte, bieżące połączenie ze zdalnym pulpitem zostanie zakończone.

Udostępnianie pulpitu rozpocznie się w nowym oknie. Jeśli chcesz wejść w interakcję z urządzeniem, kliknij ikonę menu ( ) w lewym górnym rogu okna, a następnie wybierz **Tryb interaktywny**.

Zarządzanie urządzeniami mobilnymi

Zarządzanie ochroną urządzeń mobilnych poprzez Kaspersky Security Center jest realizowane przy użyciu funkcji Zarządzanie urządzeniami mobilnymi, która wymaga dedykowanej licencji. Aby aktywować aplikację zabezpieczającą, należy dodać klucz licencyjny na każdym urządzeniu mobilnym. Jeśli zamierzasz zarządzać urządzeniami mobilnymi należącymi do pracowników Twojej organizacji, włącz i skonfiguruj Zarządzanie urządzeniami mobilnymi.

Zarządzanie urządzeniami mobilnymi umożliwia zarządzanie urządzeniami z systemem Android oraz iOS należącymi do pracowników. Ochronę zapewnia aplikacja Kaspersky Endpoint Security for Android oraz system zarządzania urządzeniami iOS, zainstalowane na urządzeniach mobilnych. Ta aplikacja mobilna zapewnia ochronę urządzeń mobilnych przed zagrożeniami internetowymi, wirusami i innymi programami stanowiącymi zagrożenie. W celu scentralizowanego zarządzania przez konsolę Kaspersky Security Center Web Console musisz zainstalować następujące wtyczki do zarządzania siecią na urządzeniu, na którym jest zainstalowany Kaspersky Security Center Web Console:

- Kaspersky Mobile Devices Protection and Management

  Wtyczka Kaspersky Mobile Devices Protection and Management umożliwia zarządzanie urządzeniami z systemem Android i iOS w Kaspersky Security Center Web Console.

- Ustawienia serwera iOS MDM

  Wtyczka ustawień serwera iOS MDM umożliwia konfigurację ustawień serwera iOS MDM, który służy do łączenia urządzeń iOS z Serwerem administracyjnym i zarządzania urządzeniami iOS.

Aby uzyskać informacje na temat wdrażania ochrony i zarządzania urządzeniami mobilnymi, zapoznaj się z pomocą dla Kaspersky Security for Mobile i pomocą dla Kaspersky Secure Mobility Management.

Korzystanie z Firebase Cloud Messaging

Aby mieć pewność, że polecenia zostaną dostarczone na urządzenia z systemem Android w odpowiednim czasie, Kaspersky Security Center Linux korzysta z mechanizmu powiadomień push. Powiadomienia push są wymieniane pomiędzy urządzeniami z systemem Android a Serwerem administracyjnym za pośrednictwem usługi Firebase Cloud Messaging (zwanej dalej FCM). W Kaspersky Security Center Web Console możesz określić ustawienia Firebase Cloud Messaging do podłączania urządzeń z systemem Android do usługi.

Aby pobrać ustawienia Firebase Cloud Messaging, należy posiadać konto Google.

W celu włączenia korzystania z FCM:

1. W oknie głównym konsoli internetowej Kaspersky Security Center Web Console wybierz **Zarządzanie zasobami** → **Mobile** → **Devices**.
2. Otwórz menu z trzema kropkami (⋮) i wybierz opcję **Forced Android device synchronization**.
3. W polu **Firebase project number** podaj identyfikator nadawcy FCM.
4. W polu **Private key** wybierz plik klucza prywatnego.

   Przy kolejnej synchronizacji z Serwerem administracyjnym, urządzenia z systemem Android zostaną połączone z Firebase Cloud Messaging.

Po przejściu do innego projektu Firebase musisz poczekać 10 minut na wznowienie FCM.

Usługa FCM działa w następujących zakresach adresów:

- Ze strony urządzenia z systemem Android dostęp jest wymagany do portów 443 (HTTPS), 5228 (HTTPS), 5229 (HTTPS) oraz 5230 (HTTPS) dla następujących adresów:
  - google.com
  - fcm.googleapis.com
  - oauth2.googleapis.com
  - android.apis.google.com
  - Wszystkie adresy IP w ASN Google'a dla portu 15169
- Ze strony Serwera administracyjnego dostęp jest wymagany do portu 443 (HTTPS) dla następujących adresów:
  - fcm.googleapis.com
  - Wszystkie adresy IP w ASN Google'a dla portu 15169

Jeśli ustawienia serwera proxy zostały określone we właściwościach Serwera administracyjnego w Kaspersky Security Center Web Console, będą używane do interakcji z FCM.

Konfigurowanie FCM: pobieranie ID nadawcy i pliku klucza prywatnego

W celu skonfigurowania FCM:

1. Zarejestruj się na portalu Google.
2. Przejdź do konsoli Firebase.
3. Wykonaj jedną z poniższych czynności:
   - Aby utworzyć nowy projekt, kliknij **Utwórz projekt** i postępuj zgodnie z instrukcjami wyświetlanymi na ekranie.
   - Otwórz istniejący projekt.
4. Kliknij ikonę koła zębatego i wybierz opcję **Ustawienia projektu**.
   Zostanie otwarte okno **Ustawienia projektu**.
5. Wybierz zakładkę **Cloud Messaging**.
6. Pobierz odpowiedni identyfikator nadawcy z pola **ID nadawcy** w sekcji **Firebase Cloud Messaging API (V1)**.
7. Wybierz zakładkę **Konta usług** i kliknij **Wygeneruj nowy klucz prywatny**.
8. W oknie, które zostanie otwarte, kliknij opcję **Generuj klucz**, aby wygenerować i pobrać plik klucza prywatnego.

Usługa Firebase Cloud Messaging jest teraz skonfigurowana.

Integracja z infrastrukturą kluczy publicznych

Można zintegrować wydawanie certyfikatów z Urzędem Certyfikacji Microsoft (CA) za pośrednictwem infrastruktury klucza publicznego (PKI). Integracja z PKI ma na celu uproszczenie wydawania certyfikatów użytkowników domeny przez Serwer administracyjny. Po przeprowadzeniu integracji certyfikaty są generowane automatycznie.

Szczegółowe informacje na temat konfigurowania integracji z infrastrukturą kluczy publicznych (PKI) w celu wystawiania certyfikatów można znaleźć w pomocy programu Kaspersky Secure Mobility Management.

Można przeprowadzić integrację PKI z określonymi ustawieniami i przypisać PKI jako źródło certyfikatów dla określonych typów certyfikatów. Ustawienia integracji PKI umożliwiają określenie indywidualnego domyślnego szablonu dla wszystkich typów certyfikatów.

Szczegółowe informacje na temat wykorzystania integracji PKI do wydawania certyfikatów:

- Integracja PKI jest domyślnie wyłączona. Szczegółowe informacje na temat włączania infrastruktury klucza publicznego (PKI) i konfigurowania jej ustawień można znaleźć w pomocy programu Kaspersky Secure Mobility Management.

- Wydawanie certyfikatów odbywa się za pośrednictwem Agenta sieciowego Windows, który umożliwia integrację pomiędzy Serwerem administracyjnym a urzędem certyfikacji Microsoft CA. Z uwagi na to, że może być wiele urządzeń z zainstalowanym Agentem sieciowym, w **Issuance rules** można określić urządzenie, które będzie łączyć się z urzędem certyfikacji firmy Microsoft. Na tym urządzeniu musi być zainstalowany certyfikat agenta rejestracji (EA) w repozytorium certyfikatów konta, na którym wykonywana jest integracja z PKI. Certyfikat wydaje administrator urzędu certyfikacji domeny.

- Konto, z którego przeprowadzana jest integracja z PKI, musi być kontem użytkownika domeny i mieć uprawnienie *Logowanie jako usługa*.

- Kaspersky Security Center Linux może współpracować tylko z jedną integracją PKI (Microsoft CA) na raz.

Zarządzanie grupami administracyjnymi

Dostępne są tu informacje o sposobie zarządzania grupami administracyjnymi.

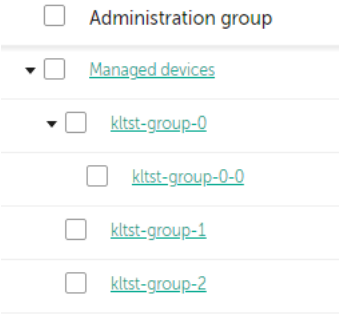
Na grupach administracyjnych możesz wykonać następujące akcje:

- Dodać do grup administracyjnych dowolną liczbę grup zagnieżdżonych z jakiegokolwiek poziomu hierarchii.
- Dodać urządzenia do grup administracyjnych.
- Zmienić hierarchię grup administracyjnych przez przeniesienie pojedynczych urządzeń i całych grup do innych grup.
- Usunąć grupy zagnieżdżone i urządzenia z grup administracyjnych.
- Dodać podrzędne i wirtualne Serwery administracyjne do grup administracyjnych.
- Przenieść urządzenia z grup administracyjnych Serwera administracyjnego do grup innego Serwera.
- Wskazać aplikacje Kaspersky, które będą automatycznie instalowane na urządzeniach znajdujących się w grupie.

Możesz wykonać te działania tylko wtedy, gdy posiadasz uprawnienia **Modyfikacja** w obszarze **Zarządzanie grupami administracyjnymi** dla grup administracyjnych, którymi chcesz zarządzać (lub dla Serwera administracyjnego, do którego te grupy należą).

Tworzenie grup administracyjnych

Od razu po zainstalowaniu Kaspersky Security Center, hierarchia grup administracyjnych zawiera tylko jedną grupę administracyjną, która nosi nazwę **Zarządzane urządzenia**. Podczas tworzenia hierarchii grup administracyjnych możesz dodać urządzenia oraz maszyny wirtualne, do folderu **Zarządzane urządzenia**, a także możesz dodać zagnieżdżone grupy (patrz rysunek poniżej).

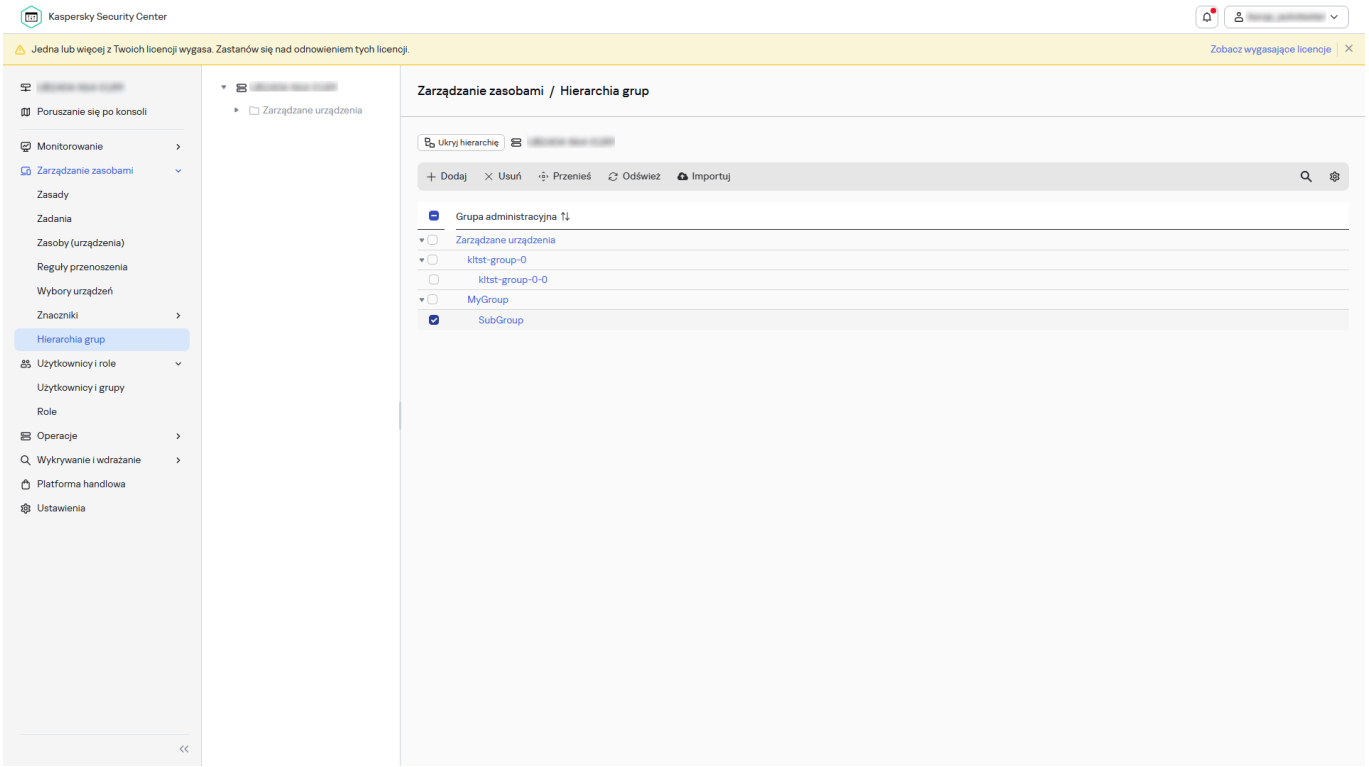


Wyświetlanie hierarchii grup administracyjnych

W celu utworzenia grupy administracyjnej:

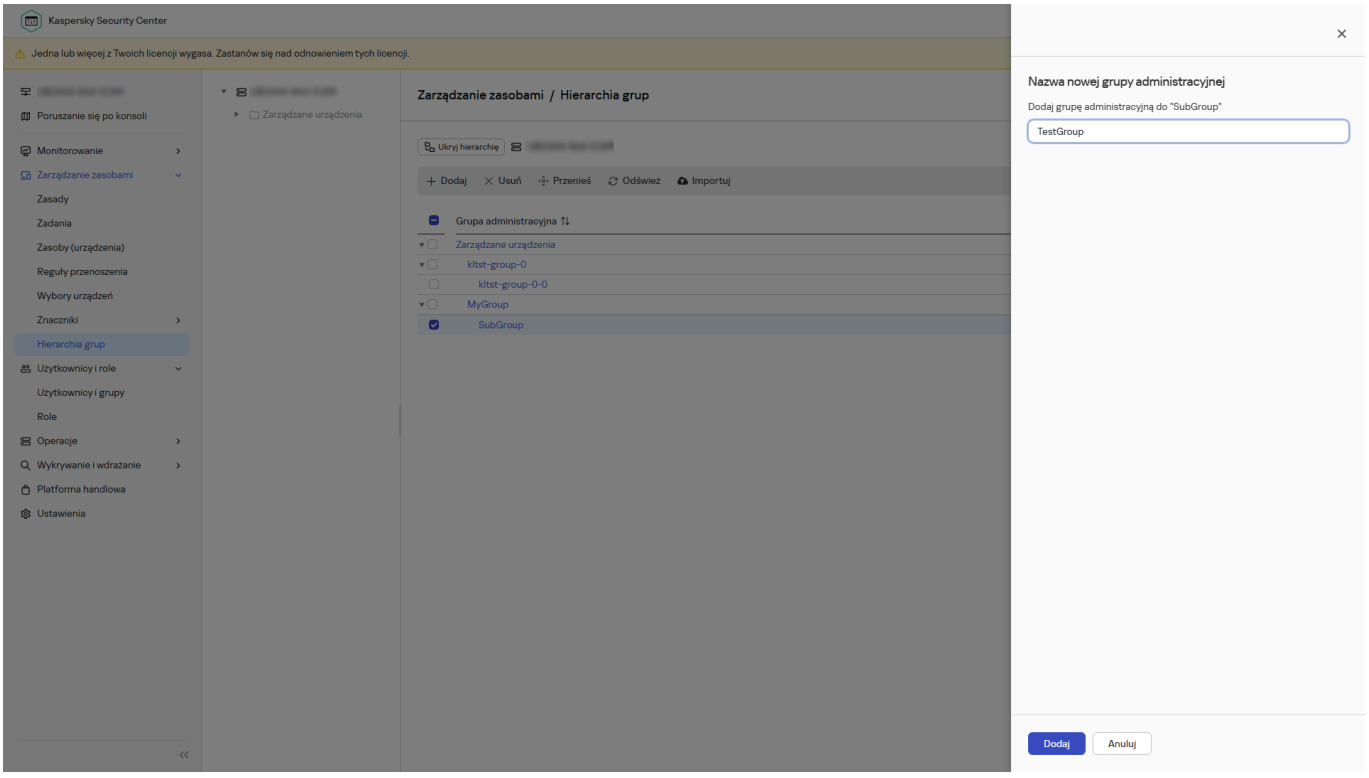
1. W menu głównym przejdź do **Zarządzanie zasobami** → **Hierarchia grup**.

2. W strukturze grupy administracyjnej wybierz grupę administracyjną, aby uwzględnić nową grupę administracyjną.



3. Kliknij przycisk **Dodaj**.

4. W oknie **Nazwa nowej grupy administracyjnej**, które zostanie otwarte, wprowadź nazwę grupy, a następnie kliknij przycisk **Dodaj**.



W nowej grupie administracyjnej z określoną nazwą pojawi się w hierarchii grup administracyjnych.

W celu utworzenia struktury grup administracyjnych:

1. W menu głównym przejdź do **Zarządzanie zasobami** → **Hierarchia grup**.

2. Kliknij przycisk **Importuj**.

   Zostanie uruchomiony Kreator struktury nowej grupy administracyjnej. Postępuj zgodnie z instrukcjami Kreatora.

Automatyczna instalacja aplikacji na urządzeniach w grupie administracyjnej

Możesz określić, które pakiety instalacyjne mają być użyte do automatycznej instalacji zdalnej aplikacji Kaspersky na urządzeniach klienckich w grupie administracyjnej.

W celu skonfigurowania automatycznej instalacji aplikacji na nowych urządzeniach w grupie administracyjnej:

1. W menu głównym przejdź do **Zarządzanie zasobami** → **Hierarchia grup**.

2. Przejdź do właściwości wymaganej grupy administracyjnej w jeden z następujących sposobów:

   - Kliknij nazwę żądanej grupy administracyjnej.

   - Kliknij przycisk **Pokaż hierarchię** znajdujący się na górze strony. W otwartym panelu nawigacyjnym najedź kursorem myszy na nazwę wymaganej grupy, a następnie kliknij ikonę ustawień (⚙).

   Zostanie otwarte okno właściwości grupy administracyjnej.

3. W otwartym oknie przejdź do zakładki **Automatyczna instalacja**.

4. Wybierz pakiety instalacyjne aplikacji, które mają zostać zainstalowane na urządzeniach, a następnie kliknij przycisk **Zapisz**.

   Jeśli wybierzesz kilka pakietów instalacyjnych tej samej aplikacji, które różnią się tylko wersjami, zapisany zostanie pakiet instalacyjny z najnowszą wersją.

Po wybraniu pakietów instalacyjnych dla każdej aplikacji tworzone są zadania grupowe dla instalacji aplikacji na urządzeniach z grupy administracyjnej. Te zadania są uruchamiane na urządzeniach klienckich natychmiast po dodaniu ich do grupy administracyjnej.

Przenoszenie grup administracyjnych

Możliwe jest przenoszenie zagnieżdżonych grup administracyjnych w obrębie hierarchii grup.

Grupa administracyjna jest przenoszona wraz z grupami zagnieżdżonymi, podrzędnymi Serwerami administracyjnymi, urządzeniami, zasadami grupy i zadaniami. System zastosuje do grupy wszystkie ustawienia odpowiadające jej nowej pozycji w hierarchii grup administracyjnych.

Nazwa grupy musi być unikatowa w obrębie tego poziomu hierarchii. Jeżeli w folderze, do którego przenosisz grupę administracyjną, istnieje już grupa o takiej nazwie, powinieneś zmienić nazwę przenoszonej grupy. Jeżeli nie zmienisz nazwy przenoszonej grupy, do jej nazwy zostanie automatycznie dodany przyrostek **(<kolejny numer>)**, na przykład: **(1)**, **(2)**.

Nie można zmienić nazwy ani przenieść grupy **urządzeń zarządzanych**.

Aby przenieść grupę administracyjną na inny poziom hierarchii grup administracyjnych:

1. W menu głównym przejdź do **Zarządzanie zasobami** → **Hierarchia grup**, a następnie zaznacz pole wyboru obok grupy administracyjnej, którą chcesz przenieść.

2. Kliknij przycisk **Przenieś** na pasku narzędzi.

3. W otwartym oknie wybierz miejsce, do którego chcesz przenieść grupę administracyjną, i kliknij przycisk **Przenieś**.

Okno zostanie zamknięte, a grupa administracyjna zostanie przeniesiona na inny poziom hierarchii grup.

Usuwanie grup administracyjnych

Jeśli usuniesz grupę administracyjną zawierającą podrzędne Serwery administracyjne, grupy zagnieżdżone, urządzenia klienckie, zadania grupowe lub zasady utworzone dla tej grupy, wszystkie te elementy również zostaną usunięte.

Przed usunięciem grupy administracyjnej należy usunąć z tej grupy wszystkie podrzędne Serwery administracyjne, grupy zagnieżdżone i urządzenia klienckie.

W celu usunięcia grupy administracyjnej:

1. W menu głównym przejdź do **Zarządzanie zasobami** → **Hierarchia grup**, a następnie zaznacz pole wyboru obok grupy administracyjnej, którą chcesz usunąć.

2. Kliknij przycisk **Usuń** na pasku narzędzi.

Grupa administracyjna została usunięta.

Wdrażanie aplikacji Kaspersky

W tej sekcji opisano sposób wdrażania aplikacji Kaspersky na urządzeniach klienckich w Twojej organizacji przy użyciu Kaspersky Security Center Web Console.

Scenariusz: Wdrażanie aplikacji Kaspersky

Ten scenariusz wyjaśnia sposób wdrażania aplikacji Kaspersky za pośrednictwem Kaspersky Security Center Web Console. Możesz użyć kreatora wstępnej konfiguracji i kreatora wdrażania ochrony lub możesz ręcznie wykonać wszystkie niezbędne kroki.

Do wdrożenia przy użyciu Kaspersky Security Center Web Console dostępne są następujące aplikacje:

- Kaspersky Endpoint Security for Linux
- Kaspersky Endpoint Security for Windows

Etapy

Wdrożenie aplikacji firmy Kaspersky odbywa się w krokach:

1. **Pobieranie webowej wtyczki administracyjnej dla aplikacji**

   Ten krok jest częścią kreatora wstępnej konfiguracji. Jeśli zdecydujesz się nie uruchamiać kreatora, pobierz wtyczki ręcznie.

2. **Pobieranie i tworzenie pakietów instalacyjnych**

   Ten krok jest częścią kreatora wstępnej konfiguracji.

   Kreator wstępnej konfiguracji umożliwia pobranie pakietu instalacyjnego z webową wtyczką administracyjną. Jeśli nie wybrano tej opcji podczas uruchamiania kreatora lub jeśli w ogóle nie uruchomiono kreatora, musisz ręcznie pobrać pakiet.

   Jeśli nie możesz zainstalować aplikacji firmy Kaspersky przy użyciu Kaspersky Security Center Linux na niektórych urządzeniach, na przykład, na zdalnych urządzeniach pracowników, możesz utworzyć autonomiczne pakiety instalacyjne dla aplikacji. Jeśli używasz autonomicznych pakietów do instalacji aplikacji Kaspersky, nie musisz tworzyć i uruchamiać zadania zdalnej instalacji, ani tworzyć i konfigurować zadań dla Kaspersky Endpoint Security for Windows.

   Alternatywnie możesz pobrać pakiety dystrybucyjne dla Agenta sieciowego i aplikacji zabezpieczających ze strony internetowej Kaspersky. Jeśli z jakiegoś powodu zdalna instalacja aplikacji nie jest możliwa, możesz użyć pobranych pakietów dystrybucyjnych, aby zainstalować aplikacje lokalnie.

3. **Tworzenie, konfigurowanie i uruchamianie zadania zdalnej instalacji**

   Ten krok jest częścią kreatora wdrażania ochrony. Jeśli zdecydujesz się nie uruchamiać Kreator wdrażania ochrony, musisz ręcznie utworzyć to zadanie oraz ręcznie je skonfigurować.

   Możesz także ręcznie utworzyć kilka zadań zdalnej instalacji dla różnych grup administracyjnych lub różnych wyborów urządzeń. Możesz wdrożyć różne wersje jednej aplikacji w tych zadaniach.

Upewnij się, że wszystkie urządzenia w Twojej sieci zostały wykryte, a następnie uruchom zadanie zdalnej instalacji (lub zadania).

Jeśli chcesz zainstalować Agenta sieciowego na urządzeniach z systemem operacyjnym SUSE Linux Enterprise Server 15, w pierwszej kolejności zainstaluj pakiet insserv-compat, aby skonfigurować Agenta sieciowego.

Jeśli chcesz zainstalować Agenta sieciowego na urządzeniach z systemem operacyjnym RED OS 7.3.4 lub nowszym albo MSVSPHERE 9.2 lub nowszym, zainstaluj pakiet libxcrypt-compat, aby Agent sieciowy działał prawidłowo.

4. **Tworzenie i konfigurowanie zadań**

   Należy skonfigurować zadanie *Aktualizacja* programu Kaspersky Endpoint Security.

   Ten krok jest częścią kreatora wstępnej konfiguracji: zadanie jest tworzone i konfigurowane automatycznie z domyślnymi ustawieniami. Jeśli nie uruchomiono kreatora, musisz ręcznie utworzyć to zadanie oraz ręcznie je skonfigurować. Jeśli użyjesz kreatora wstępnej konfiguracji, upewnij się, że terminarz zadania spełnia Twoje wymagania (domyślnie, zaplanowane uruchomienie zadania jest ustawione na **Ręcznie**, ale możesz chcieć wybrać inną opcję).

5. **Tworzenie zasad**

   Utwórz zasadę dla Kaspersky Endpoint Security ręcznie lub za pomocą kreatora wstępnej konfiguracji. Możesz użyć domyślnych ustawień zasady; możesz także zmodyfikować domyślne ustawienia zasady zgodnie ze swoimi potrzebami w dowolnym momencie.

6. **Sprawdzanie wyników**

   Upewnij się, że wdrożenie zakończyło się pomyślnie: masz zasady i zadania dla każdej aplikacji, a te aplikacje są instalowane na zarządzanych urządzeniach.

Wyniki

Zakończenie scenariusza powoduje, że:

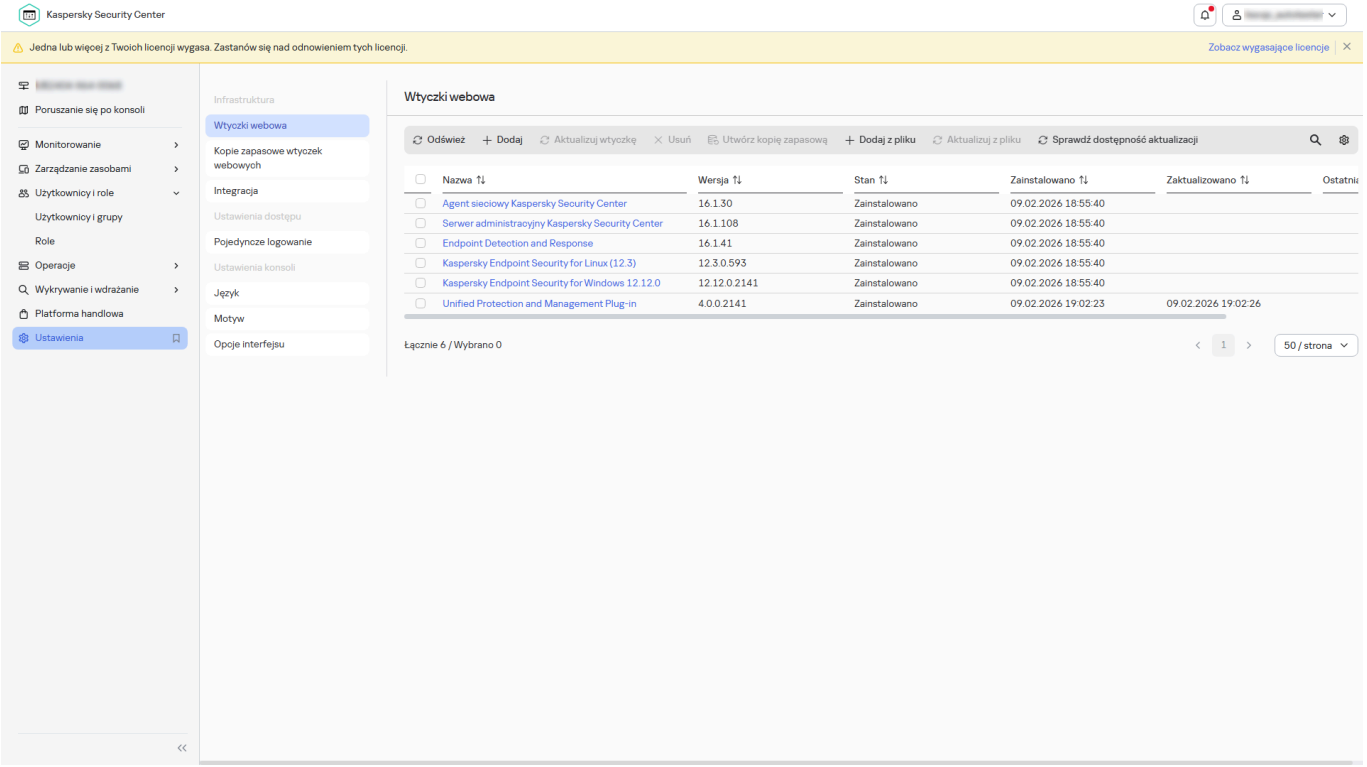
- Zostaną utworzone wszystkie wymagane zasady i zadania dla wybranych aplikacji.
- Terminarze zadań zostaną skonfigurowane według Twoich potrzeb.
- Wybrane aplikacje zostaną zainstalowane lub zostanie zaplanowane ich zainstalowanie na wybranych urządzeniach klienckich.

Dodawanie wtyczek administracyjnych dla aplikacji Kaspersky

Aby wdrożyć aplikację firmy Kaspersky, taką jak Kaspersky Endpoint Security for Linux lub Kaspersky Endpoint Security for Windows, musisz dodać i zainstalować webową wtyczkę administracyjną dla aplikacji.

W celu pobrania webowej wtyczki administracyjnej dla aplikacji Kaspersky:

1. W menu głównym przejdź do **Ustawienia** → **Wtyczki webowa**.



Lista zainstalowanych wtyczek webowych

2. W otwartym oknie kliknij przycisk **Dodaj**.

   Zostanie wyświetlona lista dostępnych wtyczek.

3. Na liście dostępnych wtyczek wybierz wtyczkę, którą chcesz pobrać (na przykład Kaspersky Endpoint Security for Linux), klikając jej nazwę.

   Zostanie wyświetlona strona opisu wtyczki.

4. Na stronie opisu wtyczki kliknij **Zainstaluj wtyczkę**.

5. Po zakończeniu instalacji, kliknij **OK**.

Webowa wtyczka administracyjna zostanie pobrana z domyślną konfiguracją i wyświetlona na liście sieciowych wtyczek administracyjnych.

Możesz dodać wtyczki i zaktualizować pobrane wtyczki z pliku. Webową wtyczkę administracyjna można pobrać ze strony internetowej Kaspersky.

Aby pobrać lub zaktualizować webową wtyczkę administracyjną z pliku:

1. W menu głównym przejdź do **Ustawienia** → **Wtyczki webowa**.

2. Określ plik wtyczki oraz sygnaturę pliku:

   - Kliknij **Dodaj z pliku**, aby pobrać wtyczkę z pliku.

   - Kliknij **Aktualizuj z pliku**, aby pobrać aktualizację wtyczkę z pliku.

3. Określ plik i sygnaturę pliku.

4. Pobierz określone pliki.

   Webowa wtyczka administracyjna zostanie pobrana z pliku i zostanie wyświetlona na liście webowych wtyczek administracyjnych.

Pakiety instalacyjne

Pakiet instalacyjny to zestaw plików utworzonych na potrzeby instalacji zdalnej aplikacji Kaspersky. Pakiet instalacyjny zawiera zakres ustawień potrzebnych do zainstalowania aplikacji i uruchomienia jej natychmiast po zainstalowaniu. Ustawienia odpowiadają domyślnym ustawieniom aplikacji. Pakiet instalacyjny jest tworzony przy użyciu plików z rozszerzeniami KPD i KUD zawartych w pakiecie dystrybucyjnym aplikacji.

Pakiety instalacyjne są generowane przy użyciu następujących metod:

- Automatycznie, z określonych pakietów dystrybucyjnych, na podstawie załączonych *deskryptorów* (pliki z rozszerzeniem .kud, które zawierają reguły dla instalacji, wyniki analizy oraz inne informacje).

- Z pliku archiwum ZIP, CAB, TAR lub TAR.GZ, dla aplikacji standardowych lub obsługiwanych.

Wygenerowane pakiety instalacyjne są zorganizowane hierarchicznie jako foldery z podfolderami i plikami. Oprócz oryginalnego pakietu dystrybucyjnego, pakiet instalacyjny zawiera ustawienia dostępne do modyfikacji (w tym ustawienia instalatora oraz reguły przetwarzania dla takich sytuacji, jak konieczność ponownego uruchomienia systemu operacyjnego w celu zakończenia instalacji), a także drobne moduły pomocnicze.

Wartości ustawień instalacji, które są charakterystyczne dla pojedynczej obsługiwanej aplikacji, można zdefiniować w interfejsie użytkownika konsoli Kaspersky Security Center Web Console podczas tworzenia pakietu instalacyjnego. Podczas zdalnej instalacji aplikacji przy użyciu narzędzi Kaspersky Security Center Linux pakiety instalacyjne są dostarczane na urządzenia, dzięki czemu uruchomienie instalatora aplikacji udostępni dla tej aplikacji wszystkie ustawienia zdefiniowane przez administratora. Jeśli do zainstalowania aplikacji firmy Kaspersky używasz narzędzi firm trzecich, musisz zapewnić dostępność całego pakietu instalacyjnego, czyli pakietu dystrybucyjnego i jego ustawień. Pakiety instalacyjne są tworzone i przechowywane przez Kaspersky Security Center Linux w dedykowanym podfolderze folderu udostępnionego.

W parametrach pakietów instalacyjnych nie należy określać żadnych szczegółów kont użytkowników uprzywilejowanych.

Wdrożenie przy użyciu zasad grupy Microsoft Windows nie jest obsługiwane.

Natychmiast po zainstalowaniu programu Kaspersky Security Center Linux, automatycznie zostaje wygenerowanych kilka pakietów instalacyjnych. Pakiety te są gotowe do zainstalowania i zawierają pakiety Agenta sieciowego oraz pakiety aplikacji zabezpieczających dla Microsoft Windows.

Klucz licencyjny dla aplikacji można ustawić we właściwościach pakietu instalacyjnego, jednakże zalecane jest unikanie tej metody dystrybucji licencji, gdyż w łatwy sposób można uzyskać dostęp do pakietów instalacyjnych. Dla kluczy licencyjnych należy używać zadań automatycznego rozsyłania kluczy licencyjnych lub instalacji.

Pobieranie i tworzenie pakietów instalacyjnych dla aplikacji Kaspersky

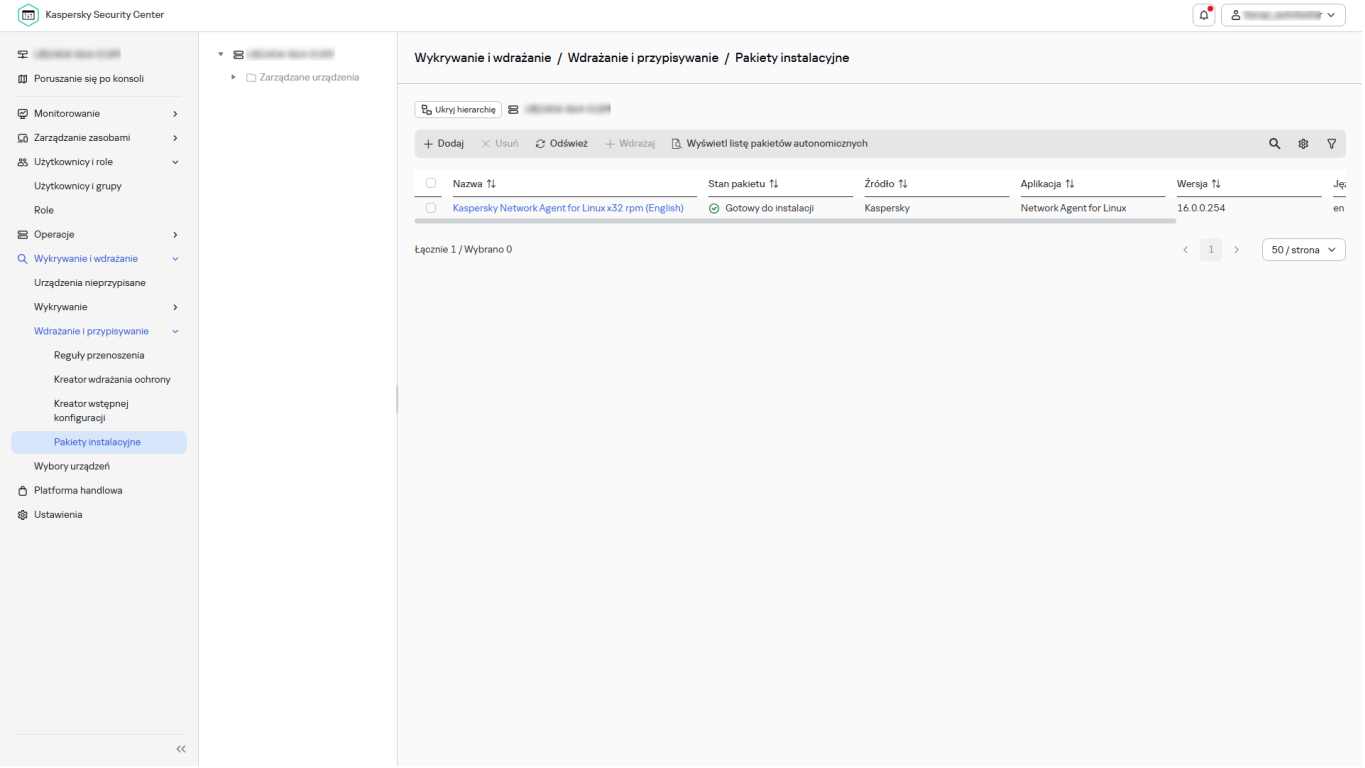
Możesz utworzyć pakiety instalacyjne dla aplikacji firmy Kaspersky z serwerów Kaspersky, jeśli Serwer administracyjny ma dostęp do internetu.

W celu pobrania i utworzenia pakietu instalacyjnego dla aplikacji Kaspersky:

1. W menu głównym przejdź do **Zarządzanie oprogramowaniem** → **Pakiety instalacyjne**.

   Możesz także przejrzeć powiadomienia o nowych pakietach dla aplikacji firmy Kaspersky na liście powiadomień ekranowych. Jeśli istnieją powiadomienia o nowym pakiecie, możesz kliknąć odnośnik obok powiadomienia i przejść do listy dostępnych pakietów instalacyjnych.

   Zostanie wyświetlona lista pakietów instalacyjnych dostępnych na Serwerze administracyjnym.

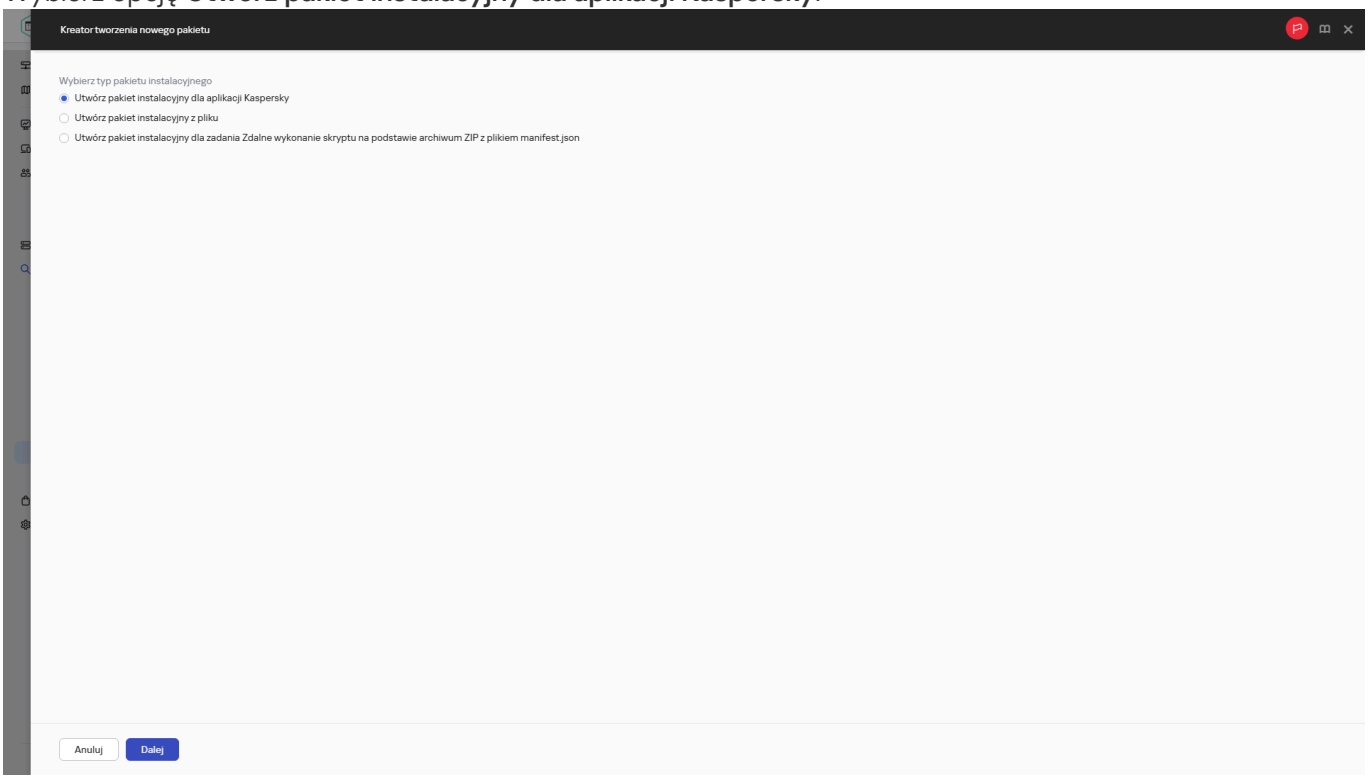


Lista pakietów instalacyjnych

2. Kliknij **Dodaj**.

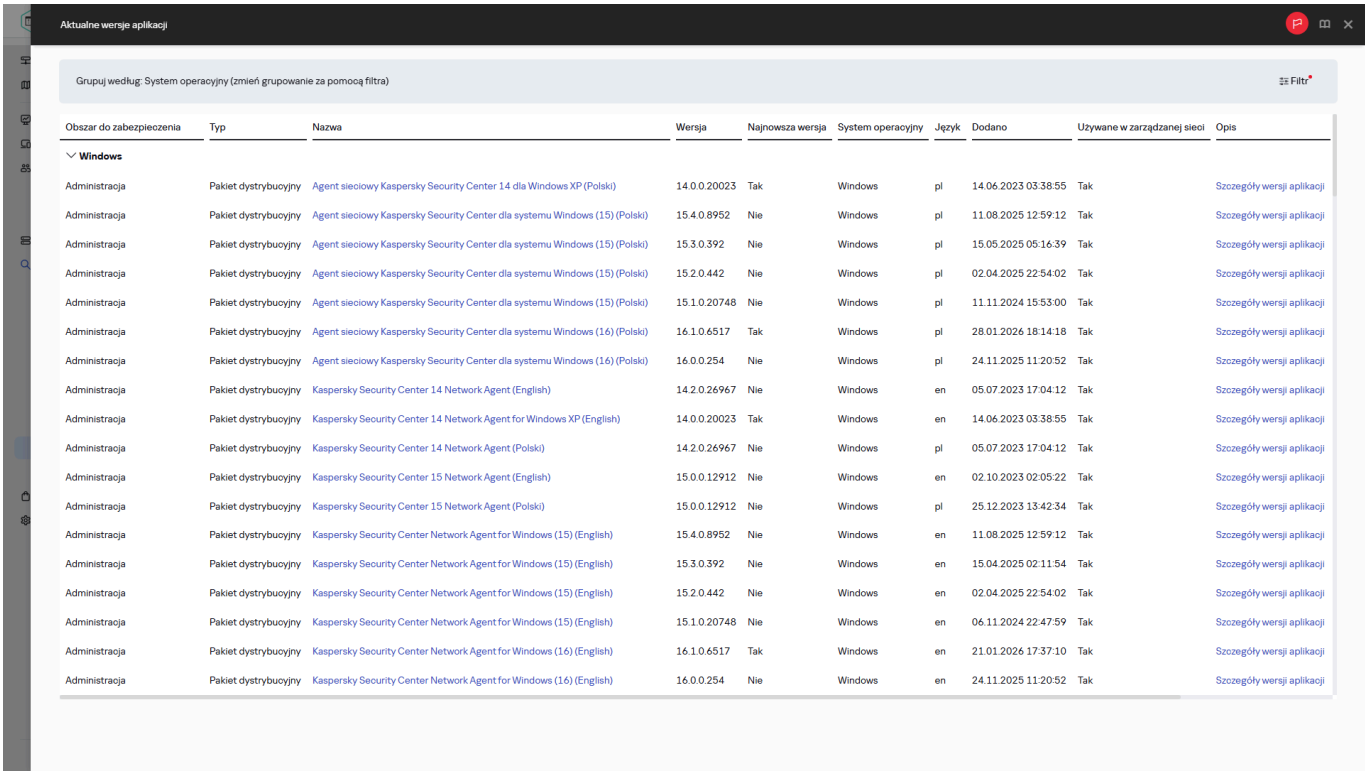
   Zostanie uruchomiony Kreator tworzenia nowego pakietu. Przejdź przez kroki kreatora, korzystając z przycisku **Dalej**.

3. Wybierz opcję **Utwórz pakiet instalacyjny dla aplikacji Kaspersky**.



Wybieranie typu pakietu instalacyjnego

Pojawi się lista pakietów instalacyjnych dostępnych na serwerach sieciowych Kaspersky. Lista zawiera pakiety instalacyjne tylko dla tych aplikacji, które są kompatybilne z bieżącą wersją Kaspersky Security Center Linux. Domyślnie lista pokazuje tylko aplikacje z językiem angielskim oraz językiem odpowiadającym językowi interfejsu. Aby wyświetlić inne języki, kliknij **Filtr** i skonfiguruj ustawienia filtra.



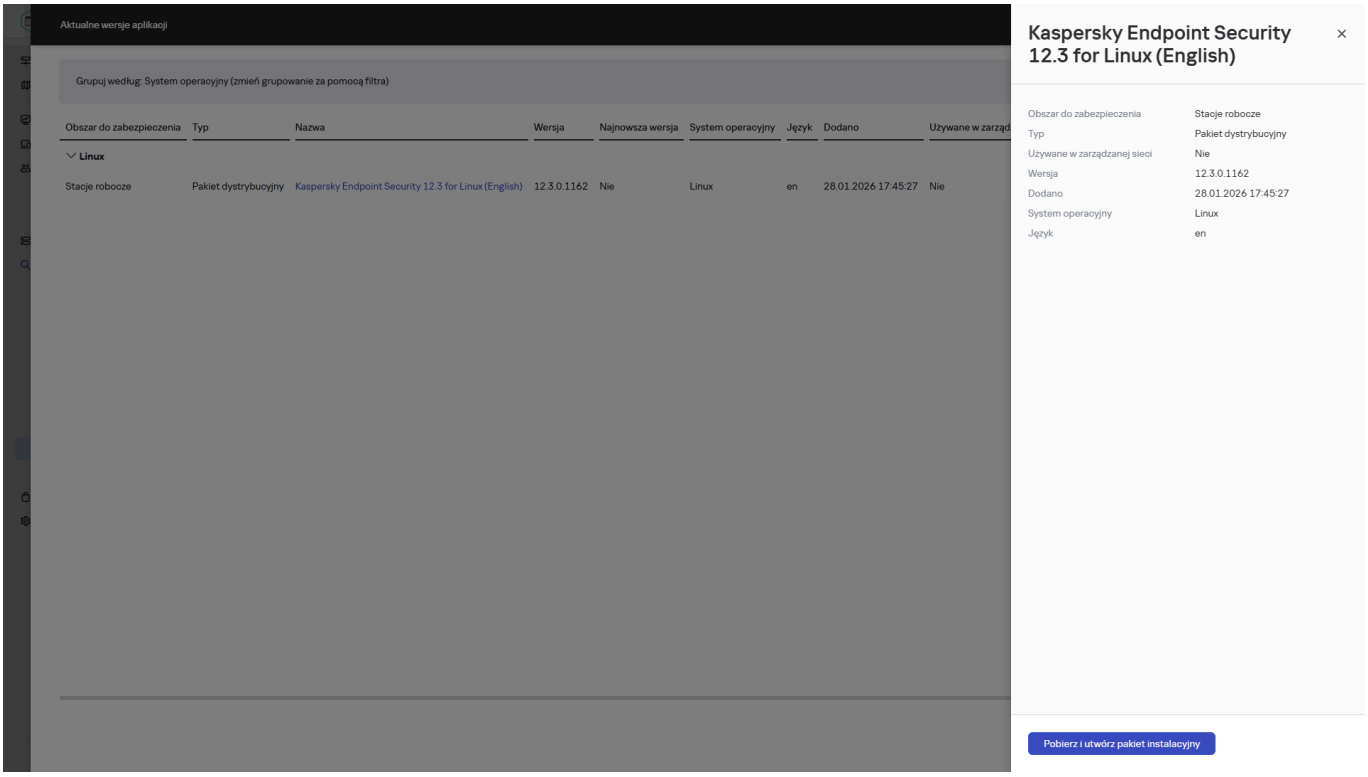
Obszar do zabezpieczenia	Typ	Nazwa	Wersja	Najnowsza wersja	System operacyjny	Język	Dodano	Używane w zarządzanej sieci	Opis
Windows									
Administracja	Pakiet dystrybucyjny	Agent sieciowy Kaspersky Security Center 14 dla Windows XP (Polski)	14.0.0.20023	Tak	Windows	pl	14.06.2023 03:38:55	Tak	Szczegóły wersji aplikacji
Administracja	Pakiet dystrybucyjny	Agent sieciowy Kaspersky Security Center dla systemu Windows (15) (Polski)	15.4.0.8952	Nie	Windows	pl	11.08.2025 12:59:12	Tak	Szczegóły wersji aplikacji
Administracja	Pakiet dystrybucyjny	Agent sieciowy Kaspersky Security Center dla systemu Windows (15) (Polski)	15.3.0.392	Nie	Windows	pl	15.05.2025 05:16:39	Tak	Szczegóły wersji aplikacji
Administracja	Pakiet dystrybucyjny	Agent sieciowy Kaspersky Security Center dla systemu Windows (15) (Polski)	15.2.0.442	Nie	Windows	pl	02.04.2025 22:54:02	Tak	Szczegóły wersji aplikacji
Administracja	Pakiet dystrybucyjny	Agent sieciowy Kaspersky Security Center dla systemu Windows (15) (Polski)	15.1.0.20748	Nie	Windows	pl	11.11.2024 15:53:00	Tak	Szczegóły wersji aplikacji
Administracja	Pakiet dystrybucyjny	Agent sieciowy Kaspersky Security Center dla systemu Windows (16) (Polski)	16.1.0.6517	Tak	Windows	pl	28.01.2026 18:14:18	Tak	Szczegóły wersji aplikacji
Administracja	Pakiet dystrybucyjny	Agent sieciowy Kaspersky Security Center dla systemu Windows (16) (Polski)	16.0.0.254	Nie	Windows	pl	24.11.2025 11:20:52	Tak	Szczegóły wersji aplikacji
Administracja	Pakiet dystrybucyjny	Kaspersky Security Center 14 Network Agent (English)	14.2.0.26967	Nie	Windows	en	05.07.2023 17:04:12	Tak	Szczegóły wersji aplikacji
Administracja	Pakiet dystrybucyjny	Kaspersky Security Center 14 Network Agent for Windows XP (English)	14.0.0.20023	Tak	Windows	en	14.06.2023 03:38:55	Tak	Szczegóły wersji aplikacji
Administracja	Pakiet dystrybucyjny	Kaspersky Security Center 14 Network Agent (Polski)	14.2.0.26967	Nie	Windows	pl	05.07.2023 17:04:12	Tak	Szczegóły wersji aplikacji
Administracja	Pakiet dystrybucyjny	Kaspersky Security Center 15 Network Agent (English)	15.0.0.12912	Nie	Windows	en	02.10.2023 02:05:22	Tak	Szczegóły wersji aplikacji
Administracja	Pakiet dystrybucyjny	Kaspersky Security Center 15 Network Agent (Polski)	15.0.0.12912	Nie	Windows	pl	25.12.2023 13:42:34	Tak	Szczegóły wersji aplikacji
Administracja	Pakiet dystrybucyjny	Kaspersky Security Center Network Agent for Windows (15) (English)	15.4.0.8952	Nie	Windows	en	11.08.2025 12:59:12	Tak	Szczegóły wersji aplikacji
Administracja	Pakiet dystrybucyjny	Kaspersky Security Center Network Agent for Windows (15) (English)	15.3.0.392	Nie	Windows	en	15.04.2025 02:11:54	Tak	Szczegóły wersji aplikacji
Administracja	Pakiet dystrybucyjny	Kaspersky Security Center Network Agent for Windows (15) (English)	15.2.0.442	Nie	Windows	en	02.04.2025 22:54:02	Tak	Szczegóły wersji aplikacji
Administracja	Pakiet dystrybucyjny	Kaspersky Security Center Network Agent for Windows (15) (English)	15.1.0.20748	Nie	Windows	en	06.11.2024 22:47:59	Tak	Szczegóły wersji aplikacji
Administracja	Pakiet dystrybucyjny	Kaspersky Security Center Network Agent for Windows (16) (English)	16.1.0.6517	Tak	Windows	en	21.01.2026 17:37:10	Tak	Szczegóły wersji aplikacji
Administracja	Pakiet dystrybucyjny	Kaspersky Security Center Network Agent for Windows (16) (English)	16.0.0.254	Nie	Windows	en	24.11.2025 11:20:52	Tak	Szczegóły wersji aplikacji

Lista dostępnych pakietów instalacyjnych

4. Kliknij nazwę pakietu instalacyjnego, na przykład Kaspersky Endpoint Security for Linux.

   Zostanie otwarte okno z informacjami o pakiecie instalacyjnym.

Możesz pobrać i używać pakietu instalacyjnego, który zawiera narzędzia kryptograficzne, które implementują silne szyfrowanie, jeśli jest to zgodne z obowiązującymi przepisami i regulacjami. Aby pobrać pakiet instalacyjny Kaspersky Endpoint Security for Windows potrzebny w Twojej organizacji, miej na uwadze ustawodawstwo kraju, w którym znajdują się urządzenia klienckie Twojej organizacji.



Pobieranie pakietu instalacyjnego

5. Przeczytaj informacje i kliknij przycisk **Pobierz i utwórz pakiet instalacyjny**.

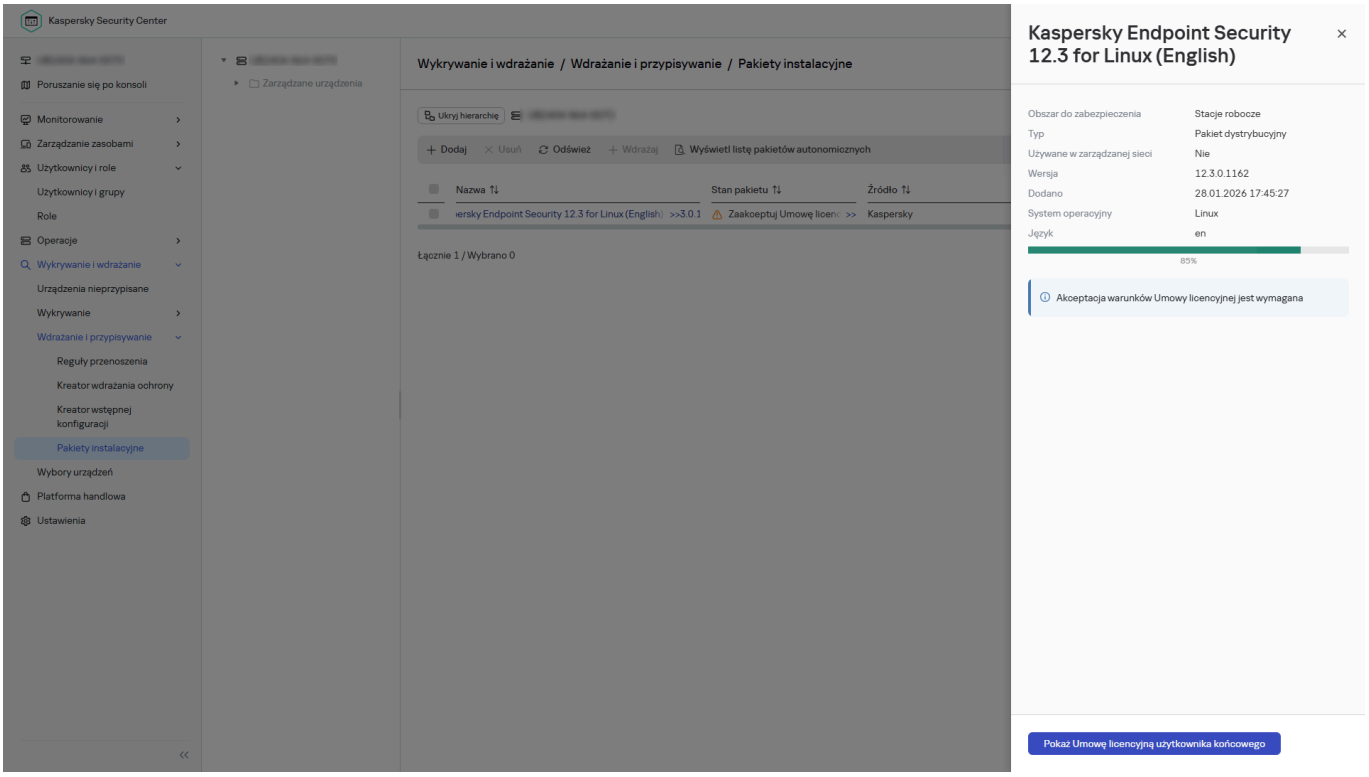
   Jeśli pakiet dystrybucyjny nie może zostać przekonwertowany na pakiet instalacyjny, wyświetlany jest przycisk **Pobierz pakiet dystrybucyjny** zamiast **Pobierz i utwórz pakiet instalacyjny**.

Dla niektórych aplikacji Kaspersky, przed lub podczas pobierania wyświetlany jest przycisk **Pokaż Umowę licencyjną użytkownika końcowego**. Jeśli przycisk jest wyświetlany, wykonaj następujące czynności:

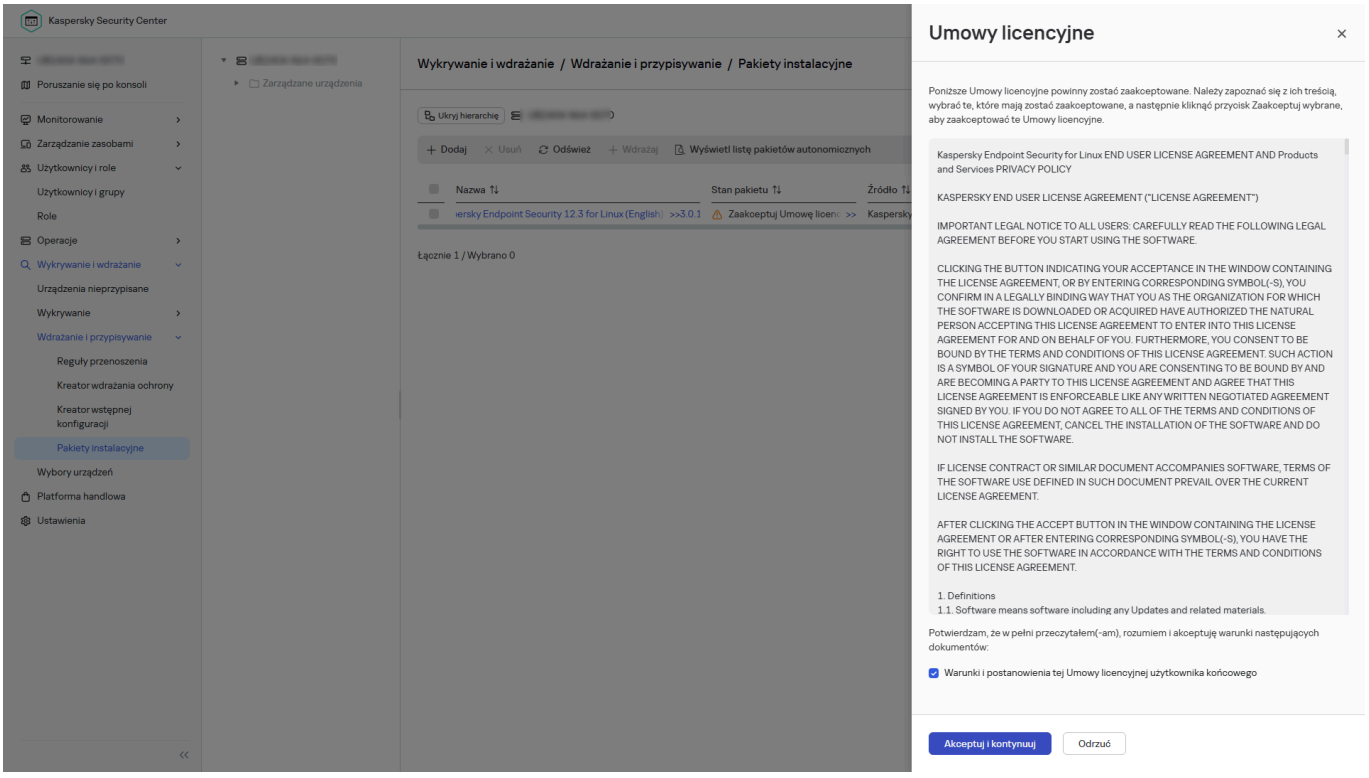
a. Kliknij przycisk **Pokaż Umowę licencyjną użytkownika końcowego**, aby przeczytać Umowę licencyjną użytkownika końcowego (EULA).

b. Przeczytaj Umowę licencyjną użytkownika końcowego, która zostanie wyświetlona na ekranie, i kliknij **Zaakceptuj**.

   Po zaakceptowaniu Umowy licencyjnej użytkownika końcowego, proces pobierania będzie kontynuowany. Jeśli klikniesz **Odrzuć**, proces pobierania zostanie zatrzymany.



Pobieranie pakietu instalacyjnego



Możesz zamknąć okno kreatora. W takim przypadku proces pobierania będzie kontynuowany w tle. Możesz śledzić status pobierania pakietu instalacyjnego, a także filtrować i sortować statusy w kolumnie **Stan pakietu**.

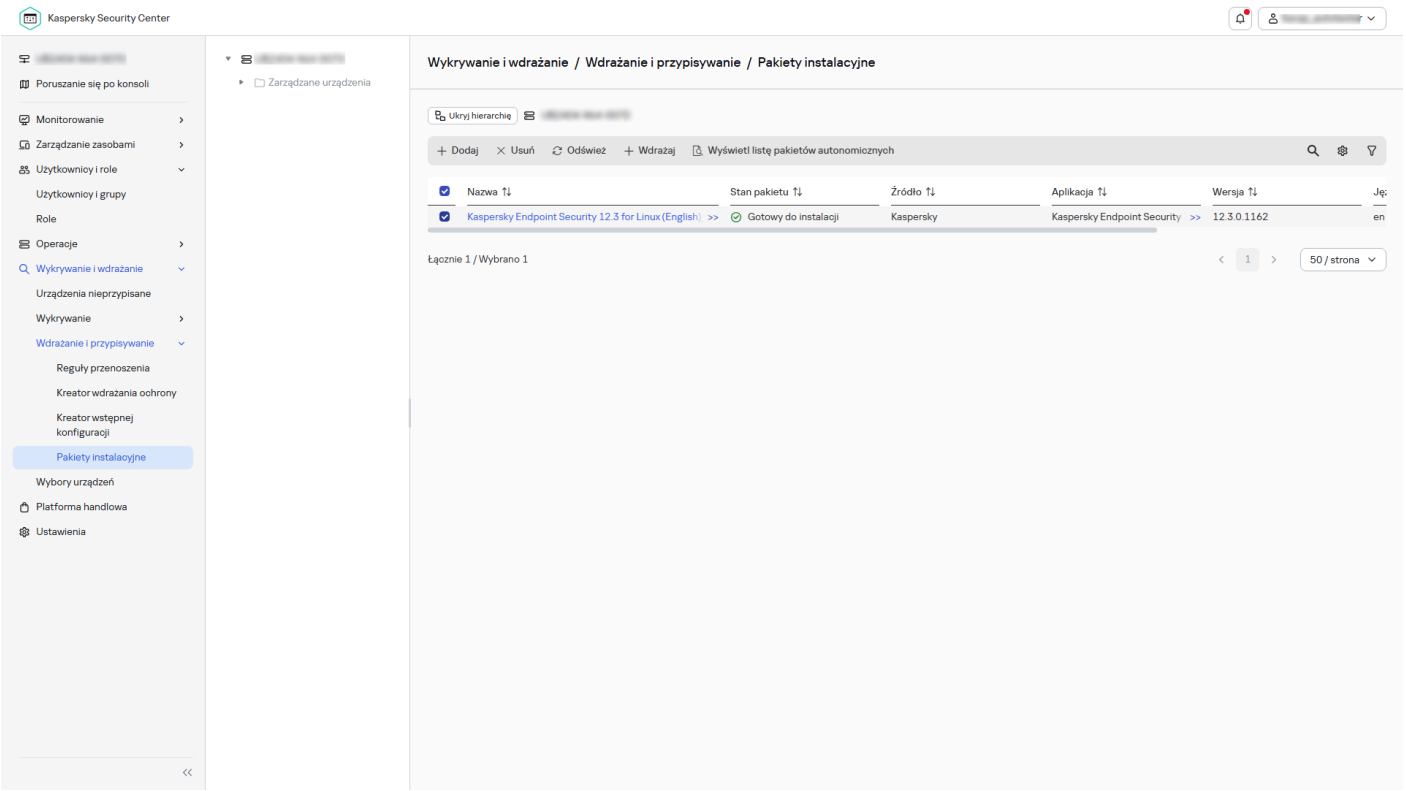
Jeśli proces pobierania zostanie zatrzymany, a stan pobierania przełączy się na **Zaakceptuj Umowę licencyjną użytkownika końcowego**, kliknij nazwę pakietu instalacyjnego, a następnie przejdź do kroku 5.a i 5.b.

Domyślnie pakiety instalacyjne ze statusem **W toku** i **Zaakceptuj Umowę licencyjną użytkownika końcowego** są umieszczane na początku listy.

> Jeśli rozmiar danych znajdujących się w wybranym pakiecie dystrybucyjnym przekracza bieżące ograniczenie, zostanie wyświetlona wiadomość o błędzie. Możesz zmienić ograniczoną wartość, a następnie przejdź do tworzenia pakietu instalacyjnego.

6. Po zakończeniu pobierania kliknij przycisk **Zamknij**.

Wybrany pakiet instalacyjny zostanie pobrany do folderu współdzielonego Serwera administracyjnego, do podfolderu Pakiety. Po pobraniu, pakiet instalacyjny jest wyświetlany na liście pakietów instalacyjnych.



Lista pakietów instalacyjnych

Tworzenie pakietów instalacyjnych z pliku

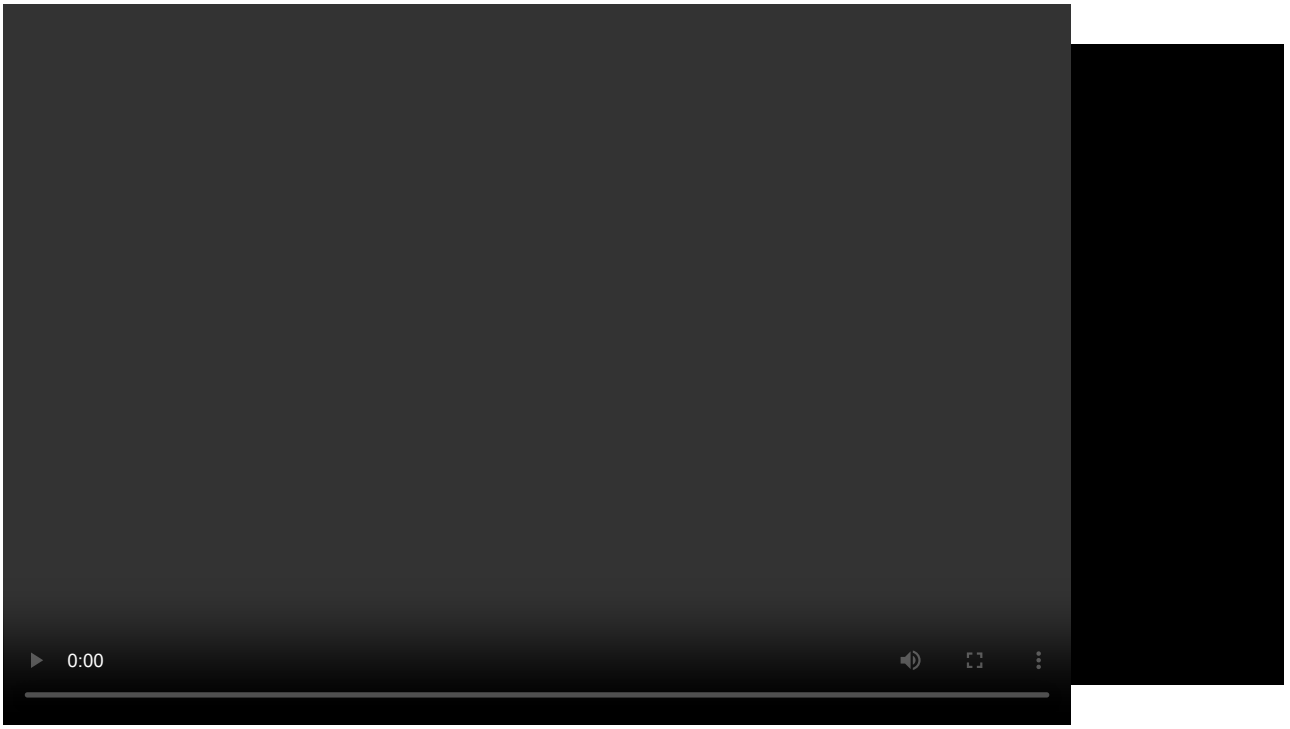
W celu wykonania następujących czynności możesz użyć niestandardowych pakietów instalacyjnych:

- Aby zainstalować dowolną aplikację (taką jak edytor tekstu) na urządzeniu klienckim, na przykład, przy użyciu zadania.
- Aby utworzyć autonomiczny pakiet instalacyjny.

Niestandardowy pakiet instalacyjny to folder z zestawem plików. Źródło utworzenia niestandardowego pakietu instalacyjnego to *plik archiwum*. Plik archiwum zawiera plik lub pliki, które muszą znajdować się w niestandardowym pakiecie instalacyjnym.

Podczas tworzenia niestandardowego pakietu instalacyjnego możesz określić parametry wiersza poleceń, na przykład, aby zainstalować aplikację w trybie cichym.

Obejrzyj film, aby dowiedzieć się, jak utworzyć i wdrożyć niestandardowy pakiet instalacyjny dla systemu Windows. Wersja tekstowa tego samouczka dla urządzeń z systemem Windows i Linux jest dostępna poniżej.

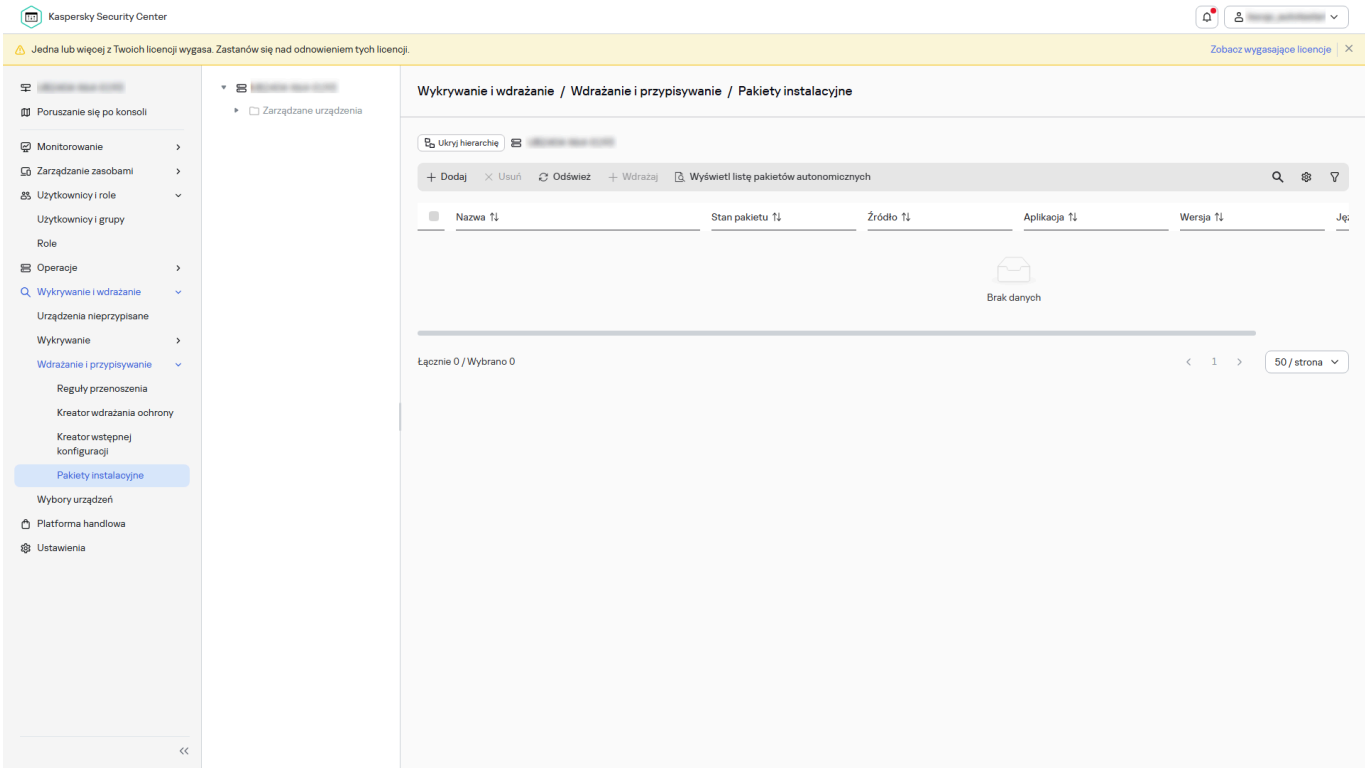


Tworzenie i wdrażanie niestandardowego pakietu instalacyjnego z pliku dla systemu Windows. Film wideo

W celu utworzenia niestandardowego pakietu instalacyjnego:

1. W menu głównym przejdź do **Zarządzanie oprogramowaniem** → **Pakiety instalacyjne**.

Zostanie wyświetlona lista pakietów instalacyjnych dostępnych na Serwerze administracyjnym.

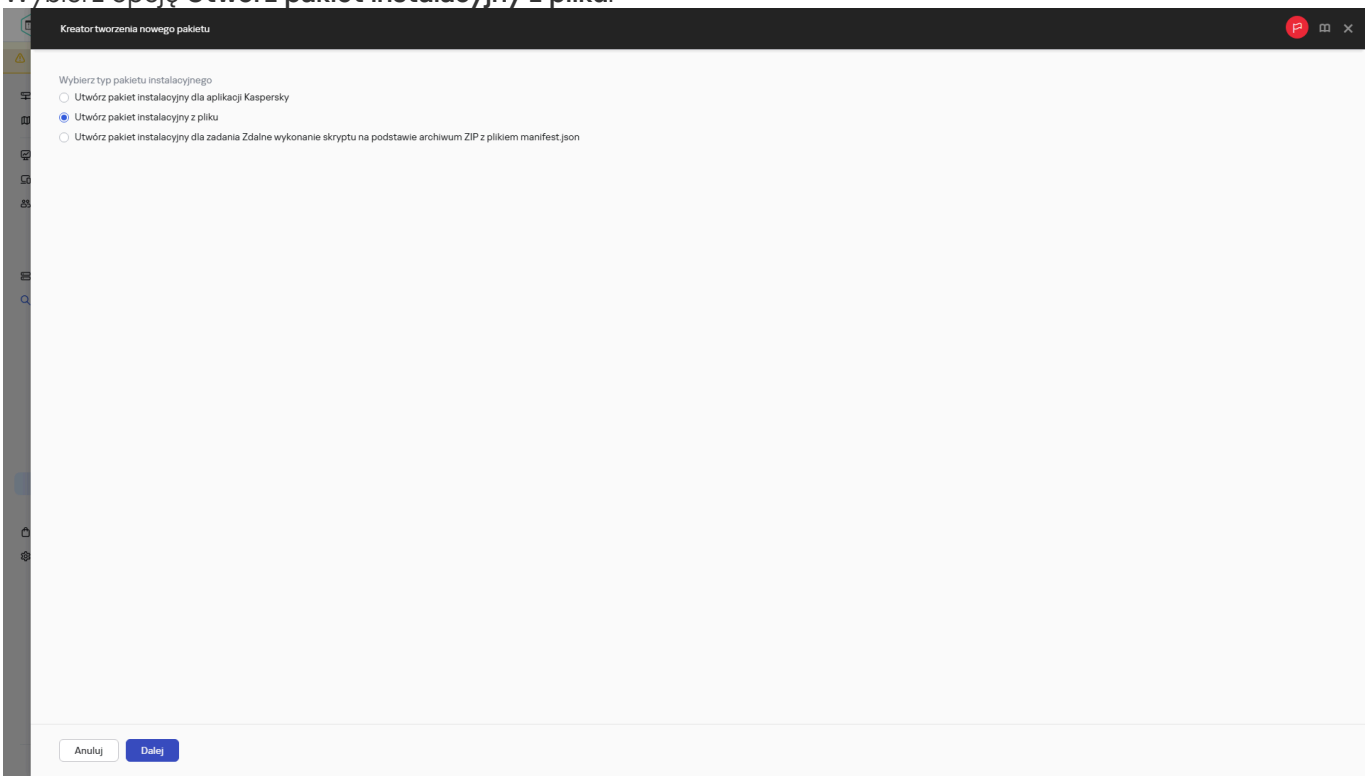


Lista pakietów instalacyjnych

2. Kliknij **Dodaj**.

   Zostanie uruchomiony Kreator tworzenia nowego pakietu. Przejdź przez kroki kreatora, korzystając z przycisku **Dalej**.

3. Wybierz opcję **Utwórz pakiet instalacyjny z pliku**.



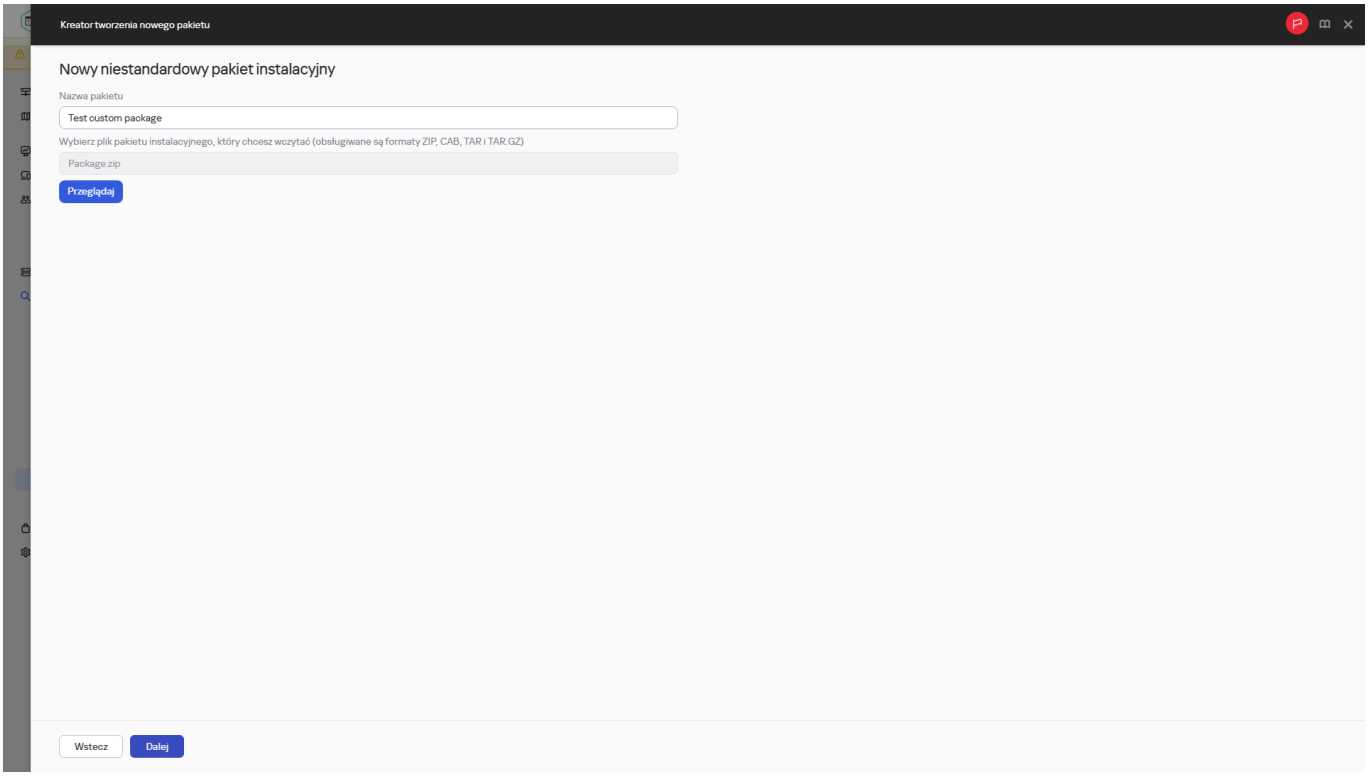
Wybieranie typu pakietu instalacyjnego

4. Podaj nazwę pakietu i kliknij przycisk **Przeglądaj**.

5. W oknie, które zostanie otwarte, wybierz plik archiwum znajdujący się na dostępnych dyskach.

Możesz przesłać plik archiwum ZIP, CAB, TAR lub TAR.GZ. Nie jest możliwe utworzenie pakietu instalacyjnego z pliku SFX (samorozpakowujące się archiwum).

Rozpocznie się przesyłanie pliku do Serwera administracyjnego.



Określanie pliku pakietu instalacyjnego

6. Jeśli określono plik aplikacji Kaspersky, możesz otrzymać prośbę o przeczytanie i zaakceptowanie Umowy licencyjnej użytkownika końcowego (EULA) dla aplikacji. Aby kontynuować, musisz zaakceptować Umowę licencyjną użytkownika końcowego. Wybierz opcję **Zaakceptuj warunki i postanowienia niniejszej Umowy licencyjnej użytkownika końcowego** tylko wtedy, gdy w pełni przeczytano, zrozumiano warunki Umowy licencyjnej użytkownika końcowego je akceptujesz.

   Dodatkowo możesz otrzymać prośbę o przeczytanie i zaakceptowanie Polityki Prywatności. Aby kontynuować, musisz zaakceptować Politykę prywatności. Wybierz opcję **Akceptuję Politykę prywatności** tylko wtedy, gdy rozumiesz i zgadzasz się, że Twoje dane będą przetwarzane i przekazywane (w tym do krajów trzecich) zgodnie z Polityką Prywatności.

7. Wybierz plik (z listy plików, które są wypakowywane z wybranego pliku archiwum) i określ parametry wiersza poleceń pliku wykonywalnego.

   Jak utworzyć pakiet instalacyjny w formacie deb lub rpm

   1. Utwórz `.sh` skrypt z następującymi poleceniami:

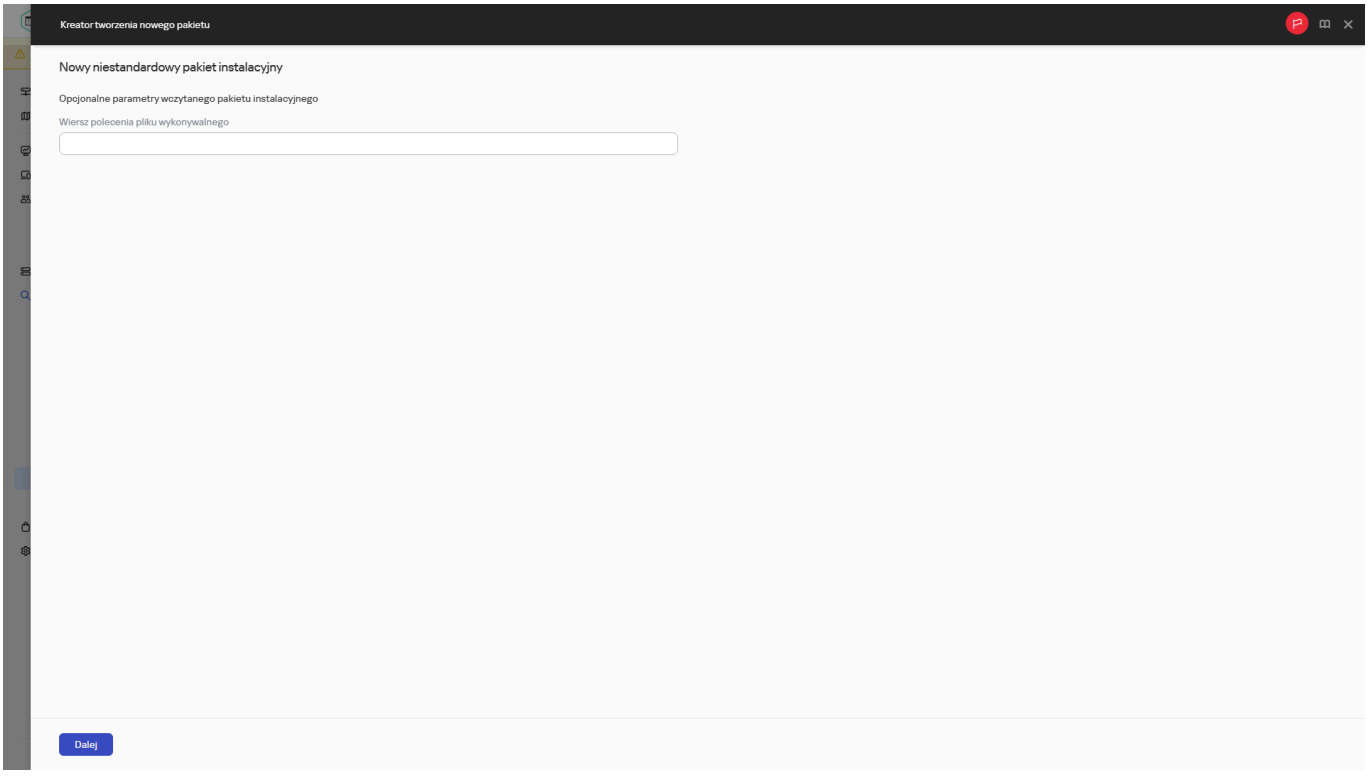
      ```
      #!/bin/sh
      script_dir="$(dirname "$0")"
      apt-get install --yes "$script_dir/<nazwa_pakietu>.deb" </dev/null
      ```

      Zawartość skryptu i polecenia mogą się różnić w zależności od formatu pakietu i innych szczegółów. Możesz zmodyfikować skrypt, aby dopasować go do swojej konkretnej konfiguracji.

   2. Umieść utworzony skrypt w archiwum wraz z `.deb` lub plikiem `.rpm`.

   3. Podczas tworzenia pakietu instalacyjnego wybierz utworzony skrypt jako plik wykonywalny.

Możesz określić parametry wiersza poleceń, aby zainstalować aplikację z pakietu instalacyjnego w trybie cichym. Określanie parametrów wiersza poleceń jest opcjonalne.



Określanie opcjonalnych parametrów wiersza poleceń

Zostanie uruchomiony proces tworzenia pakietu instalacyjnego.

Kreator informuje, gdy proces zostanie zakończony.

Jeśli pakiet instalacyjny nie zostanie utworzony, zostanie wyświetlona odpowiednia wiadomość.

8. W celu zakończenia działania kreatora kliknij przycisk **Zakończ**.

Pakiet instalacyjny, który utworzyłeś, zostanie pobrany do podfolderu Packages folderu współdzielonego Serwera administracyjnego. Po pobraniu, pakiet instalacyjny pojawi się na liście pakietów instalacyjnych.

Na liście pakietów instalacyjnych dostępnych na Serwerze administracyjnym, klikając odnośnik z nazwą niestandardowego pakietu instalacyjnego, możesz:

- Wyświetl następujące właściwości pakietu instalacyjnego:
  - **Nazwa**. Nazwa niestandardowego pakietu instalacyjnego.
  - **Stan pakietu**. Status pobierania pakietu instalacyjnego.
  - **Źródło**. Nazwa producenta aplikacji.
  - **Aplikacja**. Nazwa aplikacji spakowanej w niestandardowy pakiet instalacyjny.
  - **Wersja**. Wersja aplikacji.
  - **Język**. Wersja językowa aplikacji spakowanej w niestandardowy pakiet instalacyjny.
  - **Rozmiar (MB)**. Rozmiar pakietu instalacyjnego.
  - **System operacyjny**. Typ systemu operacyjnego, dla którego przeznaczony jest pakiet instalacyjny.

- **Utworzono**. Data utworzenia pakietu instalacyjnego.
- **Zmodyfikowano**. Data modyfikacji pakietu instalacyjnego.
- **Typ**. Typ pakietu instalacyjnego.

- Zmień parametry wiersza polecenia.

Tworzenie autonomicznych pakietów instalacyjnych

Ty oraz użytkownicy urządzeń w Twojej organizacji mogą używać autonomicznych pakietów instalacyjnych, aby ręcznie instalować aplikacje na urządzeniach.

Autonomiczny pakiet instalacyjny jest plikiem wykonywalnym, który można umieścić na serwerze sieciowym lub w folderze sieciowym, przesłać w wiadomości e-mail lub przenieść na urządzenie klienckie w inny sposób. Na urządzeniu klienckim użytkownik może uruchomić otrzymany plik lokalnie, aby zainstalować aplikację bez udziału Kaspersky Security Center Linux. Możesz tworzyć autonomiczne pakiety instalacyjne dla aplikacji Kaspersky i aplikacji innych firm. Aby utworzyć autonomiczny pakiet instalacyjny dla aplikacji firmy trzeciej, należy utworzyć niestandardowy pakiet instalacyjny.

Jeśli Serwer administracyjny ma dostęp do internetu, zadanie Serwera administracyjnego **Pobierz aktualizacje do repozytorium Serwera administracyjnego** służy do pobrania zależności wymaganych do utworzenia autonomicznych pakietów instalacyjnych Agenta sieciowego. Jeśli Serwer administracyjny nie ma dostępu do internetu, wykonaj następujące kroki:

1. Wykonaj następujące polecenie, aby utworzyć flagę RIUtilsArchiveDirUsed:

   ```
   /opt/kaspersky/ksc64/sbin/klscflag -fset -pv klserver -n RIUtilsArchiveDirUsed -t d -v 1
   ```

2. Uruchom następujące polecenie, aby ponownie uruchomić usługę Serwera administracyjnego:

   ```
   systemctl restart kladminserver_srv.service
   ```

3. Pobierz następujące archiwa ze strony internetowej Kaspersky i umieść je w folderze /var/opt/kaspersky/klnagent_srv/1093/.working/ri_utils_archives:

   - ri_utils_win32.zip
   - ri_utils_arm64.zip

   Nie zmieniaj nazwy archiwum.

Serwer administracyjny ma teraz wymagane zależności.

Upewnij się, że autonomiczny pakiet instalacyjny nie jest dostępny dla innych osób.

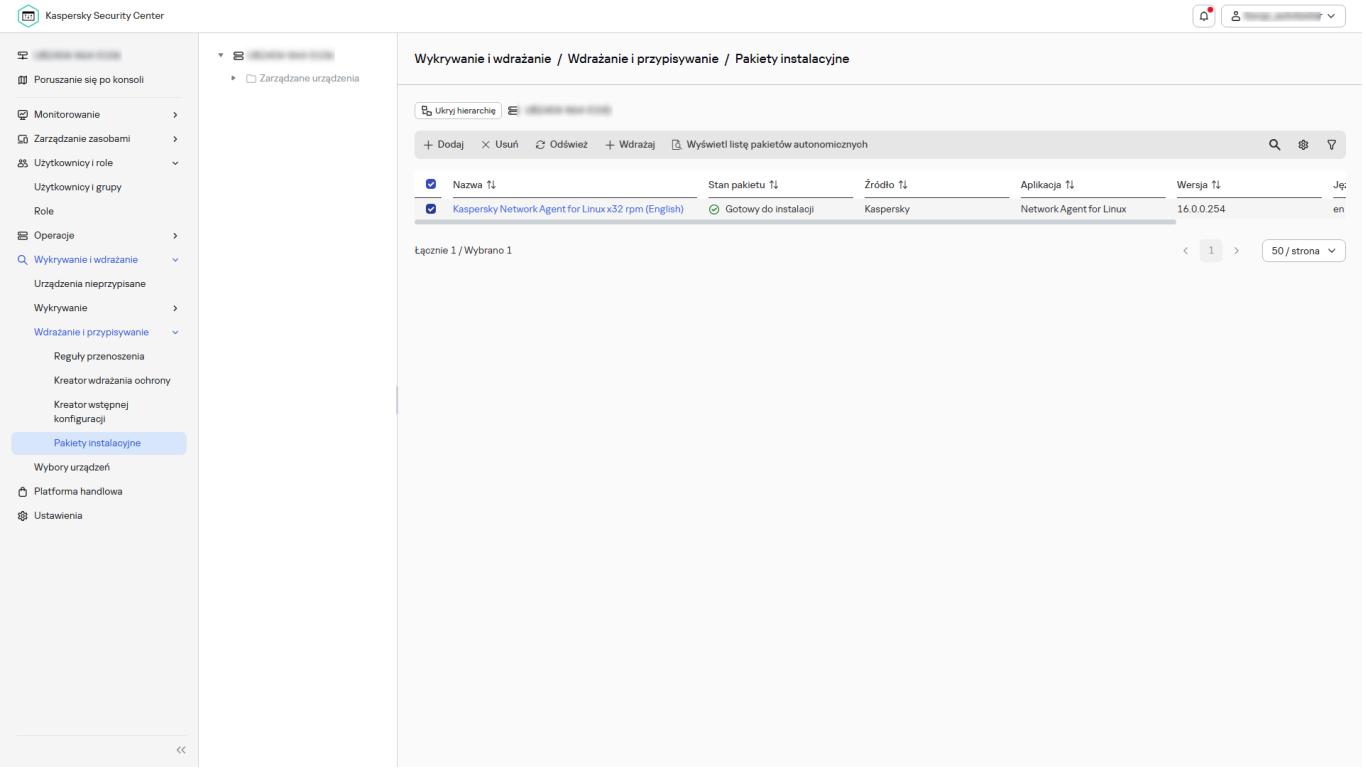
W celu utworzenia autonomicznego pakietu instalacyjnego:

1. W menu głównym przejdź do **Zarządzanie oprogramowaniem** → **Pakiety instalacyjne**.

   Zostanie wyświetlona lista pakietów instalacyjnych dostępnych na Serwerze administracyjnym.

Informacje o rozmiarze, hashu pliku i ścieżce nie są dostępne na liście pakietów instalacyjnych dla pakietu autonomicznego Agenta sieciowego ani dla żadnych pakietów utworzonych na wirtualnych Serwerach administracyjnych. Te pakiety autonomiczne są generowane w momencie pobierania.

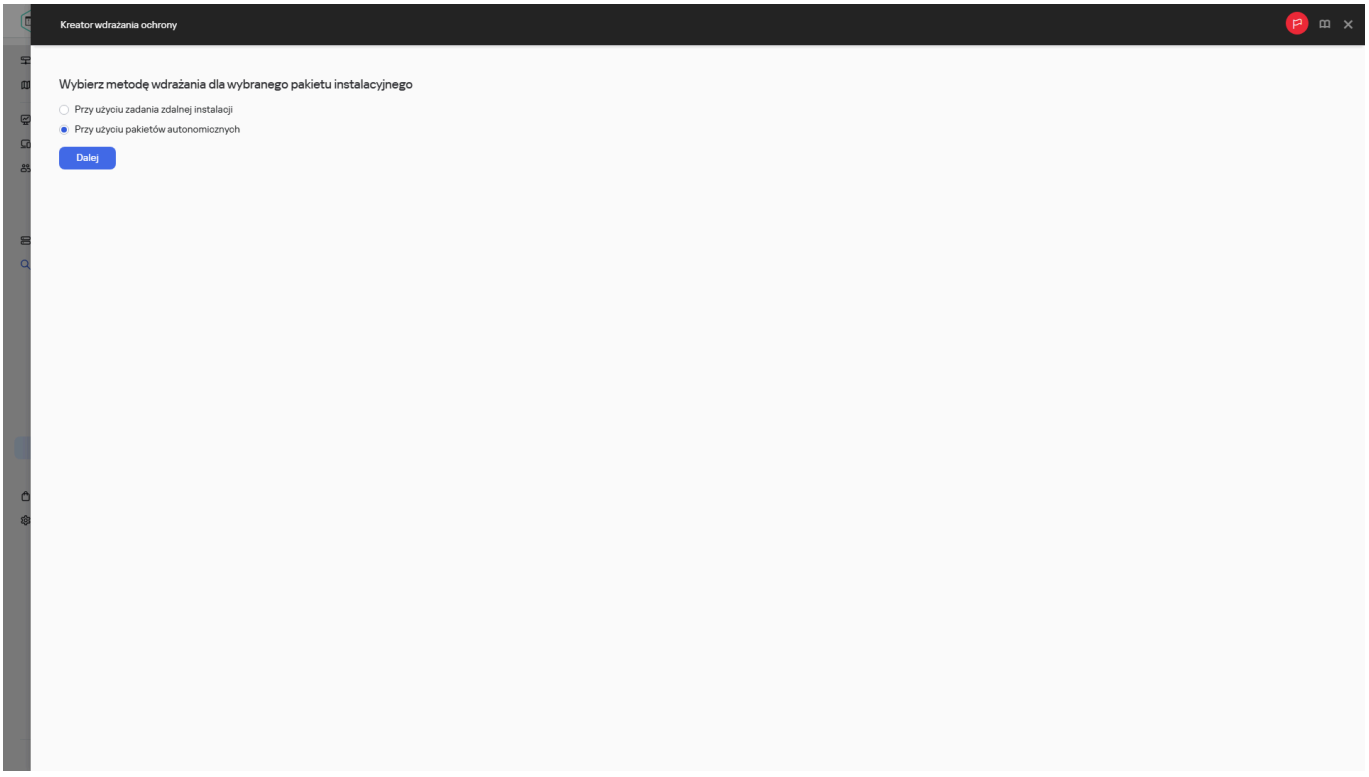
2. Na liście pakietów instalacyjnych wybierz pakiet instalacyjny i nad listą kliknij przycisk **Wdrażaj**.



Lista pakietów instalacyjnych

3. Wybierz opcję **Przy użyciu pakietów autonomicznych**.

   Zostanie uruchomiony Kreator tworzenia autonomicznego pakietu instalacyjnego. Przejdź przez kroki kreatora, korzystając z przycisku **Dalej**.



Wybieranie metody wdrożenia pakietu instalacyjnego

4. Upewnij się, że opcja **Zainstaluj Agenta sieciowego wraz z aplikacją** jest włączona, jeśli chcesz zainstalować Agenta sieciowego wraz z wybraną aplikacją.

   Opcja jest wyświetlana w zależności od aplikacji, dla której tworzysz autonomiczny pakiet instalacyjny.

   Domyślnie opcja ta jest włączona. Zalecane jest włączenie tej opcji, jeśli nie jesteś pewien, czy Agent sieciowy jest zainstalowany na urządzeniu. Jeśli Agent sieciowy jest już zainstalowany na urządzeniu, po zainstalowaniu autonomicznego pakietu instalacyjnego wraz z Agentem sieciowym, Agent sieciowy zostanie zaktualizowany do nowszej wersji.

   Jeśli wyłączysz tę opcję, Agent sieciowy nie zostanie zainstalowany na urządzeniu, a urządzenie będzie niezarządzane.

   Jeśli autonomiczny pakiet instalacyjny dla wybranej aplikacji już istnieje na Serwerze administracyjnym, kreator poinformuje o tym fakcie. W tym przypadku powinieneś wybrać jedno z następujących działań:

   - **Utwórz autonomiczny pakiet instalacyjny**. Wybierz tę opcję, na przykład, jeśli chcesz utworzyć autonomiczny pakiet instalacyjny dla nowej wersji aplikacji oraz chcesz zachować autonomiczny pakiet instalacyjny, który utworzyłeś dla poprzedniej wersji aplikacji. Nowy autonomiczny pakiet instalacyjny zostanie umieszczony w innym folderze.

   - **Użyj istniejącego autonomicznego pakietu instalacyjnego**. Wybierz tę opcję, jeśli chcesz użyć istniejącego autonomicznego pakietu instalacyjnego. Proces tworzenia pakietu nie zostanie uruchomiony.

   - **Ponownie skompiluj istniejący autonomiczny pakiet instalacyjny**. Wybierz tę opcję, jeśli ponownie chcesz utworzyć autonomiczny pakiet instalacyjny dla tej samej aplikacji. Autonomiczny pakiet instalacyjny znajduje się w tym samym folderze.

5. W kroku **Przenieś do listy zarządzanych urządzeń** kreatora, domyślnie jest wybrana opcja **Nie przenoś urządzeń**. Jeśli nie chcesz przenosić urządzenia klienckiego do żadnej grupy administracyjnej po zainstalowaniu Agenta sieciowego, pozostaw tę opcję włączoną.

Jeśli chcesz przenieść urządzenie klienckie po instalacji Agenta sieciowego, wybierz opcję **Przenieś nieprzypisane urządzenia do tej grupy** i określ grupę administracyjną, do której chcesz przenieść urządzenie klienckie. Domyślnie, urządzenie zostanie przeniesione do grupy **Zarządzane urządzenia**.

Wybieranie grupy administracyjnej w celu przeniesienia urządzenia klienckiego

6. Po zakończeniu procesu tworzenia autonomicznego pakietu instalacyjnego kliknij przycisk **Zakończ**.

   Kreator tworzenia autonomicznego pakietu instalacyjnego zostanie zamknięty.

Autonomiczny pakiet instalacyjny jest tworzony i umieszczany w podfolderze PkgInst folderu współdzielonego Serwera administracyjnego. Możesz przejrzeć listę pakietów autonomicznych, klikając przycisk **Wyświetl listę pakietów autonomicznych** nad listą pakietów instalacyjnych.

Ustawienia pakietu instalacyjnego Agenta sieciowego

W celu skonfigurowania pakietu instalacyjnego Agenta sieciowego:

1. W menu głównym przejdź do **Zarządzanie oprogramowaniem** → **Pakiety instalacyjne**.

   Zostanie wyświetlona lista pakietów instalacyjnych dostępnych na Serwerze administracyjnym.

2. Kliknij nazwę pakietu instalacyjnego Agenta sieciowego.

Zostanie otwarte okno właściwości pakietu instalacyjnego Agenta sieciowego.

Ustawienia pakietu instalacyjnego Agenta sieciowego pogrupowane są na następujących zakładkach:

- Zakładka **Ogólne**

  Na tej zakładce wyświetlane są następujące informacje o pakiecie instalacyjnym:

  - Nazwa pakietu instalacyjnego
  - Nazwę i wersję aplikacji, dla której został utworzony pakiet instalacyjny

- Rozmiar pakietu instalacyjnego
- Data utworzenia pakietu instalacyjnego
- Ścieżkę dostępu do folderu pakietu instalacyjnego

- Zakładka **Ustawienia**

  Ta zakładka przedstawia ustawienia wymagane do zapewnienia właściwego działania Agenta sieciowego natychmiast po jego zainstalowaniu.

  - Sekcja **Ustawienia**

    - **Zainstaluj w folderze domyślnym**

      Jeśli ta opcja jest zaznaczona, Agent sieciowy zostanie zainstalowany w folderze <Dysk>:\Program Files\Kaspersky Lab\NetworkAgent. Jeżeli taki folder nie istnieje, zostanie utworzony automatycznie.

      Domyślnie opcja ta jest zaznaczona.

    - **Zainstaluj we wskazanym folderze**

      Jeżeli ta opcja jest zaznaczona, Agent sieciowy zostanie zainstalowany w folderze określonym w polu do wprowadzania danych.

    - **Użyj hasła dezinstalacyjnego**

      Jeśli ta opcja jest włączona, możesz wprowadzić hasło dezinstalacyjne (dostępne tylko dla Agenta sieciowego na urządzeniach z systemem Windows).

      Domyślnie opcja ta jest wyłączona.

    - **Chroń usługę Agenta sieciowego przed nieuprawnionym usuwaniem, zatrzymywaniem i zmianami ustawień**

      Gdy ta opcja pozostaje aktywna, po zainstalowaniu Agenta sieciowego na zarządzanym urządzeniu, składnik nie może zostać usunięty ani ponownie skonfigurowany bez wymaganych uprawnień. Usługa Agenta sieciowego nie może zostać zatrzymana. Ta opcja nie ma wpływu na kontrolery domeny.

      Włącz tę opcję, aby chronić Agenta sieciowego na stacjach roboczych obsługiwanych z uprawnieniami lokalnego administratora.

      Domyślnie opcja ta jest wyłączona.

    - **Automatycznie instaluj możliwe do zainstalowania aktualizacje i poprawki dla składników ze stanem Niezdefiniowany**

      Jeśli ta opcja jest włączona, wszystkie pobrane aktualizacje i poprawki dla Serwera administracyjnego, Agenta sieciowego, konsoli Kaspersky Security Center Web Console i Serwera iOS MDM zostaną zainstalowane automatycznie.

      Jeśli ta opcja jest wyłączona, wszystkie pobrane uaktualnienia i poprawki zostaną zainstalowane dopiero po zmianie ich stanu na *Zatwierdzono*. Uaktualnienia i łaty ze stanem *Nie zdefiniowano* nie zostaną zainstalowane.

      Domyślnie opcja ta jest włączona.

  - Sekcja **Połączenia**

W tej sekcji możesz skonfigurować połączenie Agenta sieciowego z Serwerem administracyjnym. Do nawiązania połączenia możesz użyć protokołu SSL lub UDP. W celu skonfigurowania połączenia, określ następujące ustawienia:

- **Adres Serwera administracyjnego**

  Adres urządzenia z zainstalowanym Serwerem administracyjnym.

- **Numer portu**

  Numer portu używanego do nawiązywania połączenia.

- **Port SSL**

  Numer portu używanego do nawiązywania połączenia po protokole SSL.

- **Użyj certyfikatu Serwera**

  Jeśli ta opcja jest włączona, autoryzacja dostępu Agenta sieciowego do Serwera administracyjnego użyje pliku certyfikatu, który możesz określić, klikając przycisk **Wybierz plik certyfikatu**.

  Jeśli ta opcja jest wyłączona, plik certyfikatu zostanie pobrany z Serwera administracyjnego przy pierwszym połączeniu Agenta sieciowego z adresem określonym w polu **Adres Serwera administracyjnego**.

  Nie jest zalecane wyłączenie tej opcji, ponieważ automatyczne odbieranie certyfikatu Serwera administracyjnego przez Agenta sieciowego po nawiązaniu połączenia z Serwerem administracyjnym jest uznawane z niebezpieczne.

  Domyślnie opcja ta jest wyłączona.

- **Użyj połączenia SSL**

  Jeśli ta opcja jest włączona, połączenie z Serwerem administracyjnym jest nawiązywane poprzez bezpieczny port przy użyciu protokołu SSL.

  Domyślnie opcja ta jest wyłączona. Zalecamy, aby nie wyłączać tej opcji, aby Twoje połączenie pozostało bezpieczne.

- **Użyj portu UDP**

  Jeżeli ta opcja jest włączona, Agent sieciowy nawiązuje połączenie z Serwerem administracyjnym poprzez port UDP. Pozwala to na zarządzanie urządzeniami klienckimi i otrzymywanie informacji o nich.

  Port UDP, który musi być otwarty na zarządzanych urządzeniach, na których jest zainstalowany Agent sieciowy. Dlatego zalecamy, aby nie wyłączać tej opcji.

  Domyślnie opcja ta jest włączona.

- **Port UDP**

  W tym polu możesz określić port do łączenia Serwera administracyjnego z Agentem sieciowym przy użyciu protokołu UDP.

  Domyślny numer portu UDP to 15000.

- **Nie używaj serwera proxy**

  Jeżeli ta opcja jest wyłączona, do połączenia urządzenia z Serwerem administracyjnym wykorzystywane jest połączenie bezpośrednie.

- **Użyj serwera proxy**

  Jeżeli ta opcja jest włączona, określ parametry serwera proxy:

  - **Adres serwera proxy**
  - **Port serwera proxy**

  Jeżeli Twój serwer proxy wymaga uwierzytelnienia, włącz opcję **Uwierzytelnianie na serwerze proxy** oraz podaj **Nazwa użytkownika** i **Hasło** konta, w ramach którego nawiązywane jest połączenie z serwerem proxy. Zalecamy określenie poświadczeń konta, które ma minimalne uprawnienia wymagane tylko do uwierzytelnienia serwera proxy.

- **Otwórz porty dla Agenta sieciowego w Zaporze sieciowej systemu Windows**

  Jeśli ta opcja jest włączona, porty używane przez Agenta sieciowego są dodawane do listy wykluczeń Zapory sieciowej systemu Microsoft Windows.

  Domyślnie opcja ta jest włączona.

  > Opcja ta jest dostępna tylko w przypadku pakietów instalacyjnych Agenta sieciowego przeznaczonych dla urządzeń z systemem Windows.

- Sekwencja **Zaawansowane**

  W tej sekcji możesz skonfigurować sposób korzystania z bramy połączenia.

  W grupie ustawień **Brama połączenia** można skonfigurować metodę połączenia między urządzeniem a Serwerem administracyjnym:

  - **Użyj Agenta sieciowego jako bramy połączenia w DMZ**

    Wybierz tę opcję, aby użyć Agenta sieciowego jako bramy połączenia w strefie zdemilitaryzowanej (DMZ), aby połączyć się z Serwerem administracyjnym, komunikować się z nim i bezpiecznie przechowywać dane w Agencie sieciowym podczas transmisji danych.

  - **Połącz z Serwerem administracyjnym korzystając z bramy połączenia**

    Jeżeli ta opcja jest włączona, połączenie z Serwerem administracyjnym jest nawiązywane przy użyciu bramy połączenia, aby zmniejszyć liczbę połączeń z Serwerem administracyjnym. W takim przypadku wprowadź adres urządzenia, które będzie pełnić funkcję bramy połączenia w polu **Adres bramy połączenia**.

  W grupie ustawień **Maszyna wirtualna** możesz skonfigurować połączenie dla Virtual Desktop Infrastructure (VDI), jeśli Twoja sieć obejmuje maszyny wirtualne:

  - **Włącz tryb dynamiczny VDI**

    Jeżeli ta opcja jest włączona, tryb dynamiczny Virtual Desktop Infrastructure (VDI) będzie włączony dla Agenta sieciowego, zainstalowanego na maszynie wirtualnej.

    Domyślnie opcja ta jest wyłączona.

  - **Optymalizuj ustawienia dla VM**

    Jeśli ta opcja jest włączona, w ustawieniach Agenta sieciowego będą wyłączone następujące funkcje:

    - Zbieranie informacji o zainstalowanym oprogramowaniu
    - Zbieranie informacji o sprzęcie

- Zbieranie informacji o wykrytych lukach
- Zbieranie informacji o wymaganych aktualizacjach

Domyślnie opcja ta jest wyłączona.

Jeśli chcesz, aby użytkownicy byli automatycznie proszeni o rejestrację jako właściciele urządzeń po zainstalowaniu Agenta sieciowego na urządzeniach z systemem Linux, włącz opcję **Zezwól na uruchomienie narzędzia rejestracji użytkownika po instalacji agenta sieciowego**.

Jeżeli ta opcja jest włączona, narzędzie rejestracji użytkownika jako właściciela urządzenia zostanie uruchomione po zainstalowaniu Agenta sieciowego. Domyślnie opcja ta jest wyłączona.

- Sekcja **Znaczniki**

  Sekcja **Znaczniki** wyświetla listę słów kluczowych (tagów), które mogą zostać dodane do urządzeń klienckich po zainstalowaniu Agenta sieciowego. Możesz dodawać i usuwać tagi do/z listy, a także zmieniać ich nazwy.

  Jeśli pole obok tagu jest zaznaczone, ten tag zostanie automatycznie dodany do zarządzanych urządzeń podczas instalacji Agenta sieciowego.

  Jeśli pole obok znacznika jest odznaczone, znacznik nie zostanie automatycznie dodany do zarządzanych urządzeń podczas instalacji Agenta sieciowego. Możesz ręcznie dodać ten tag do urządzeń.

  Podczas usuwania tagu z listy zostanie on automatycznie usunięty ze wszystkich urządzeń, do których został dodany.

  > Reguły automatycznego znakowania nie mają zastosowania do pakietów instalacyjnych Agenta sieciowego przeznaczonych dla urządzeń z systemem Linux i macOS.

- Zakładka **Pakiety autonomiczne**

  Na tej zakładce możesz wykonać następujące czynności:

  - Przeglądać listy dostępnych autonomicznych pakietów instalacyjnych.
  - Opublikować autonomiczny pakiet instalacyjny na serwerze sieciowym, klikając przycisk **Publikuj**. Opublikowany autonomiczny pakiet instalacyjny jest dostępny do pobrania dla użytkowników, do których wysłałeś odnośnik do autonomicznego pakietu instalacyjnego.
  - Anulować publikację autonomicznego pakietu instalacyjnego na serwerze sieciowym, klikając przycisk **Cofnij publikowanie**. Nieopublikowany autonomiczny pakiet instalacyjny jest dostępny do pobrania tylko przez Ciebie i administratora.
  - Pobrać autonomiczny pakiet instalacyjny na swoje urządzenie, klikając przycisk **Pobierz**.
  - Wysłać e-mail z odnośnikiem do autonomicznego pakietu instalacyjnego, klikając przycisk **Wyślij przez e-mail**.
  - Usunąć autonomiczny pakiet instalacyjny, klikając przycisk **Usuń**.

- Zakładka **Historia rewizji**

  Na tej zakładce możesz przeglądać historię rewizji pakietu instalacyjnego. Możesz porównać rewizje, przejrzeć rewizje, zapisać rewizje do pliku oraz dodać i zmodyfikować opisy rewizji.

Uruchamianie pakietów autonomicznych utworzonych przez Kaspersky Security Center Linux

Powyżej opisane metody wstępnej zdalnej instalacji Agenta sieciowego i innych aplikacji nie zawsze będą mogły zostać zaimplementowane, gdyż nie jest możliwe spełnienie wszystkich wymaganych warunków. W takich przypadkach można utworzyć standardowy plik wykonywalny zwany *autonomicznym pakietem instalacyjnym* poprzez Kaspersky Security Center Linux, korzystając z pakietów instalacyjnych z odpowiednimi ustawieniami instalacji, które zostały przygotowane przez administratora. Autonomiczny pakiet instalacyjny może zostać opublikowany na wewnętrznym serwerze WWW (znajdującym się w Kaspersky Security Center Linux), jeśli będzie to uzasadnione (zewnętrzny dostęp do tego serwera WWW został skonfigurowany dla użytkowników urządzeń docelowych), lub na specjalnie wdrożonym serwerze WWW znajdującym się w Kaspersky Security Center Web Console. Możesz także skopiować pakiety autonomiczne na inny serwer WWW.

Korzystając z Kaspersky Security Center Linux, możesz wysłać do wybranych użytkowników wiadomość e-mail zawierającą odnośnik do pliku pakietu autonomicznego na aktualnie używanym serwerze WWW oraz prośbę o jego uruchomienie (w trybie interaktywnym lub z kluczem „-s” dla cichej instalacji). Do wiadomości e-mail możesz załączyć autonomiczny pakiet instalacyjny, a następnie wysłać ją do użytkowników urządzeń, którzy nie mają dostępu do serwera WWW. Administrator może skopiować pakiet autonomiczny na dysk wymienny, dostarczyć go na odpowiednie urządzenie, a następnie uruchomić go.

Pakiet autonomiczny można utworzyć z pakietu Agenta sieciowego, pakietu innej aplikacji (na przykład, zabezpieczającej) lub z obu pakietów. Jeśli pakiet autonomiczny został utworzony z pakietu Agenta sieciowego i innej aplikacji, instalacja rozpocznie się z Agenta sieciowego.

Podczas tworzenia pakietu autonomicznego z pakietu Agenta sieciowego możesz określić grupę administracyjną, do której nowe urządzenia (te, które nie zostały przydzielone do żadnej grup administracyjnych) zostaną automatycznie przeniesione po zakończeniu instalacji Agenta sieciowego na tych urządzeniach.

Pakiety autonomiczne mogą być uruchomione w trybie interaktywnym (opcja domyślna), wyświetlając wynik instalacji aplikacji, które zawierają, lub mogą być uruchomione w trybie cichym (z kluczem "-s"). Tryb cichy może zostać użyty dla instalacji ze skryptów, na przykład, ze skryptów skonfigurowanych do uruchamiania po wdrożeniu obrazu systemu operacyjnego. Wynik instalacji w trybie cichym jest determinowany przez kod zwrotny procesu.

Instalowanie aplikacji przy pomocy pakietów autonomicznych

Kaspersky Security Center umożliwia utworzenie autonomicznych pakietów instalacyjnych dla aplikacji. Autonomiczny pakiet instalacyjny jest plikiem wykonywalnym, który można umieścić na serwerze sieciowym, przesłać w wiadomości e-mail lub przenieść na urządzenie klienckie w inny sposób. Możesz uruchomić odebrany plik lokalnie na urządzeniu klienckim i zainstalować aplikację bez udziału Kaspersky Security Center.

W celu zainstalowania aplikacji przy użyciu autonomicznego pakietu instalacyjnego:

1. W menu głównym przejdź do **Zarządzanie oprogramowaniem** → **Pakiety instalacyjne**.

2. Zaznacz pole wyboru obok pakietu instalacyjnego wymaganej aplikacji, a następnie kliknij przycisk **Wdrażaj**.

3. W otwartym oknie wybierz opcję **Przy użyciu pakietów autonomicznych**, a następnie kliknij przycisk **Dalej**.

   Zostanie uruchomiony Kreator tworzenia autonomicznego pakietu instalacyjnego. Przejdź przez kroki kreatora, korzystając z przycisku **Dalej**.

4. Wybierz opcję **Utwórz autonomiczny pakiet instalacyjny**.

5. Określ, czy urządzenia powinny zostać przeniesione do grupy administracyjnej po zainstalowaniu Agenta sieciowego.

6. W ostatnim kroku kreatora wybierz metodę przeniesienia autonomicznego pakietu instalacyjnego na urządzenie klienckie, a następnie kliknij przycisk **Zakończ**, aby zakończyć działanie kreatora.

7. Prześlij autonomiczny pakiet instalacyjny na urządzenie klienckie.

8. Uruchom autonomiczny pakiet instalacyjny na urządzeniu klienckim.

Aplikacja zostanie zainstalowana na urządzeniu klienckim z ustawieniami określonymi w pakiecie autonomicznym.

Po utworzeniu autonomicznego pakietu instalacyjnego, jest on automatycznie publikowany na serwerze sieciowym. Odnośnik do pobrania pakietu autonomicznego jest wyświetlany na liście utworzonych autonomicznych pakietów instalacyjnych. Jeśli to konieczne, możesz anulować publikację wybranego pakietu autonomicznego i opublikować go ponownie na serwerze sieciowym. Domyślnie, do pobrania autonomicznych pakietów instalacyjnych wykorzystywany jest port 8060.

Aktualizowanie baz danych w pakiecie instalacyjnym aplikacji zabezpieczającej

Przed rozpoczęciem wdrażania ochrony należy pamiętać o możliwości aktualizacji antywirusowych baz danych (w tym modułów i łat), dostarczanych wraz z pakietem dystrybucyjnym aplikacji zabezpieczającej. Dobrym rozwiązaniem jest zaktualizowanie baz danych w pakiecie instalacyjnym aplikacji przed rozpoczęciem wdrożenia (na przykład przy użyciu odpowiedniego polecenia z menu kontekstowego wybranego pakietu instalacyjnego). Zmniejszy to liczbę ponownych uruchomień wymaganych do zakończenia wdrożenia ochrony na urządzeniach docelowych.

Zmienianie ograniczenia rozmiaru danych niestandardowego pakietu instalacyjnego

Całkowity rozmiar danych wypakowanych podczas tworzenia niestandardowego pakietu instalacyjnego jest ograniczony. Domyślne ograniczenie to 1 GB.

Jeśli spróbujesz przesłać plik archiwum, który zawiera dane przekraczające bieżące ograniczenie, zostanie wyświetlony komunikat o błędzie. Konieczne może być zwiększenie tej wartości ograniczenia podczas tworzenia pakietów instalacyjnych z dużych pakietów dystrybucyjnych.

W celu zmiany wartości ograniczenia dla rozmiaru niestandardowego pakietu instalacyjnego:

1. Na urządzeniu Serwera administracyjnego uruchom wiersz poleceń z poziomu konta, które zostało użyte do zainstalowania Serwera administracyjnego.

2. Zmień bieżący katalog na folder instalacyjny Kaspersky Security Center Linux (zwykle /opt/kaspersky/ksc64/sbin).

3. W zależności od rodzaju instalacji Serwera administracyjnego, wprowadź na koncie root jedno z poniższych poleceń:

   - Normalna instalacja lokalna:

     ```
     klscflag -fset -pv klserver -n MaxArchivePkgSize -t d -v <liczba bajtów>
     ```

   - Instalacja klastra trybu failover Kaspersky Security Center Linux:

     ```
     klscflag -fset -pv klserver -n MaxArchivePkgSize -t d -v <liczba bajtów> --stp klfoc
     ```

   Gdzie <liczba bajtów> to liczba bajtów w formacie szesnastkowym lub dziesiętnym.

   Na przykład, jeśli wymagany limit wynosi 2 GB, można określić wartość dziesiętną 2147483648 lub wartość szesnastkową 0x80000000. W takim przypadku w przypadku lokalnej instalacji Serwera administracyjnego możesz użyć następującego polecenia:

   ```
   klscflag -fset -pv klserver -n MaxArchivePkgSize -t d -v 2147483648
   ```

Ograniczenie rozmiaru danych niestandardowego pakietu instalacyjnego zostanie zmienione.

Rozsyłanie pakietów instalacyjnych na podrzędne Serwery administracyjne

Kaspersky Security Center Linux umożliwia tworzenie pakietów instalacyjnych dla aplikacji firmy Kaspersky i aplikacji firm trzecich, a także dystrybucję pakietów instalacyjnych na urządzeniach klienckich i instalowanie aplikacji z pakietów. Aby zoptymalizować obciążenie głównego Serwera administracyjnego, możesz rozesłać pakiety instalacyjne do podrzędnych Serwerów administracyjnych. Serwery pomocnicze przesyłają pakiety do urządzeń klienckich, a następnie można przeprowadzić zdalną instalację aplikacji na urządzeniach klienckich.

W celu rozesłania pakietów instalacyjnych na podrzędne Serwery administracyjne:

1. Upewnij się, że podrzędne Serwery administracyjne są połączone z głównym Serwerem administracyjnym.

2. W menu głównym przejdź do **Zadania**.

   Zostanie wyświetlona lista zadań.

3. Kliknij przycisk **Dodaj**.

   Zostanie uruchomiony Kreator tworzenia nowego zadania. Postępuj zgodnie z krokami kreatora.

4. Na stronie **Ustawienia nowych zadań**, z listy rozwijalnej **Aplikacja** wybierz **Kaspersky Security Center**. Następnie z listy rozwijanej **Typ zadania** wybierz opcję **Rozsyłanie pakietu instalacyjnego**, a następnie określ nazwę zadania.

5. Na stronie **Zakres zadania** wybierz urządzenia, do których zadanie jest przypisane w jeden z następujących sposobów:

   - Jeśli chcesz utworzyć zadanie dla wszystkich podrzędnych Serwerów administracyjnych w określonej grupie administracyjnej, wybierz tę grupę, a następnie utwórz dla niej zadanie grupowe.

   - Jeśli chcesz utworzyć zadanie dla określonych podrzędnych Serwerów administracyjnych, wybierz te Serwery, a następnie utwórz dla nich zadanie.

6. Na stronie **Rozesłane pakiety instalacyjne** wybierz pakiety instalacyjne, które mają zostać skopiowane na podrzędne Serwery administracyjne.

7. Określ konto, aby uruchomić zadanie *Dystrybucja pakietu instalacyjnego w* ramach tego konta. Możesz użyć swojego konta i pozostawić włączoną opcję **Konto domyślne**. Alternatywnie można określić, że zadanie powinno być uruchamiane na innym koncie, które ma niezbędne prawa dostępu. Aby to zrobić, wybierz opcję **Określ konto**, a następnie wprowadź poświadczenia tego konta.

8. Na stronie **Zakończ tworzenie zadania** możesz włączyć opcję **Otwórz szczegóły zadania po jego utworzeniu**, aby otworzyć okno właściwości zadania i zmodyfikować domyślne ustawienia zadania. W przeciwnym razie możesz skonfigurować ustawienia zadania później, w dowolnym momencie.

9. Kliknij przycisk **Zakończ**.

   Zadanie utworzone w celu dystrybucji pakietów instalacyjnych na podrzędne Serwery administracyjne jest wyświetlane na liście zadań.

10. Możesz uruchomić zadanie ręcznie lub poczekać na jego uruchomienie zgodne z terminarzem określonym w ustawieniach zadania.

Po zakończeniu zadania wybrane pakiety instalacyjne są kopiowane na określone podrzędne Serwery administracyjne.

Przeglądanie listy autonomicznych pakietów instalacyjnych

Możesz przejrzeć listę autonomicznych pakietów instalacyjnych i właściwości każdego autonomicznego pakietu instalacyjnego.

W celu przejrzenia listy autonomicznych pakietów instalacyjnych dla wszystkich pakietów instalacyjnych:

Nad listą kliknij przycisk **Wyświetl listę pakietów autonomicznych**.

Na liście autonomicznych pakietów instalacyjnych ich właściwości są wyświetlane w następujący sposób:

- **Nazwa pakietu**. Nazwa autonomicznego pakietu instalacyjnego, który jest automatycznie tworzony jako nazwa aplikacji znajdującej się w pakiecie oraz wersja aplikacji.
- **Nazwa aplikacji**. Nazwa aplikacji znajdującej się w autonomicznym pakiecie instalacyjnym.
- **Wersja aplikacji**.
- **Nazwa pakietu instalacyjnego Agenta sieciowego**. Właściwość jest wyświetlana tylko wtedy, gdy Agent sieciowy znajduje się w autonomicznym pakiecie instalacyjnym.
- **Wersja Agenta sieciowego**. Właściwość jest wyświetlana tylko wtedy, gdy Agent sieciowy znajduje się w autonomicznym pakiecie instalacyjnym.
- **Rozmiar**. Rozmiar pliku w MB.
- **Grupa**. Nazwa grupy, do której urządzenie klienckie jest przenoszone po zainstalowaniu Agenta sieciowego.
- **Utworzono**. Data i godzina utworzenia autonomicznego pakietu instalacyjnego.
- **Zmodyfikowano**. Data i godzina modyfikacji autonomicznego pakietu instalacyjnego.
- **Ścieżka dostępu**. Pełna ścieżka do folderu, w którym znajduje się autonomiczny pakiet instalacyjny.

- **Adres internetowy**. Adres internetowy lokalizacji autonomicznego pakietu instalacyjnego.
- **Hash pliku**. Właściwość jest używana do potwierdzenia, że autonomiczny pakiet instalacyjny nie został zmieniony przez osoby trzecie, a użytkownik posiada ten sam plik, który utworzyłeś i przesłałeś do użytkownika.

Informacje o rozmiarze, hashu pliku i ścieżce nie są dostępne na liście pakietów instalacyjnych dla autonomicznego pakietu Agenta sieciowego ani dla żadnych pakietów utworzonych na wirtualnych Serwerach administracyjnych. Te autonomiczne pakiety są generowane w momencie pobierania.

W celu przejrzenia listy autonomicznych pakietów instalacyjnych dla określonego pakietu instalacyjnego:

Wybierz pakiet instalacyjny na liście i, nad listą, kliknij przycisk **Wyświetl listę pakietów autonomicznych**.

Na liście autonomicznych pakietów instalacyjnych możesz zrobić co następuje:

- Opublikować autonomiczny pakiet instalacyjny na serwerze sieciowym, klikając przycisk **Publikuj**. Opublikowany autonomiczny pakiet instalacyjny jest dostępny do pobrania dla użytkowników, do których wysłałeś odnośnik do autonomicznego pakietu instalacyjnego.
- Anulować publikację autonomicznego pakietu instalacyjnego na serwerze sieciowym, klikając przycisk **Cofnij publikowanie**. Nieopublikowany autonomiczny pakiet instalacyjny jest dostępny do pobrania tylko przez Ciebie i administratora.
- Pobrać autonomiczny pakiet instalacyjny na swoje urządzenie, klikając przycisk **Pobierz**.
- Wysłać e-mail z odnośnikiem do autonomicznego pakietu instalacyjnego, klikając przycisk **Wyślij przez e-mail**.
- Usunąć autonomiczny pakiet instalacyjny, klikając przycisk **Usuń**.

Instalowanie Agenta sieciowego dla systemu Linux

Aby zarządzać urządzeniami w organizacji, na każdym z nich należy zainstalować Agenta sieciowego. Wdrażanie aplikacji Kaspersky Security Center Linux na urządzeniach w firmie zazwyczaj rozpoczyna się od zainstalowania na nich Agenta sieciowego.

Istnieją następujące metody wstępnej instalacji Agenta sieciowego na zarządzanym urządzeniu z systemem Linux:

- Łącząc się z zarządzanym urządzeniem poprzez SSH i uruchamiając zadanie instalacji zdalnej.
- Uruchamiając instalację pakietu na zarządzanym urządzeniu.

Po zainstalowaniu Agenta sieciowego na urządzeniu można wykonać zdalną instalację aplikacji Kaspersky na tym urządzeniu za pośrednictwem tego Agenta sieciowego. Pakiet dystrybucyjny aplikacji, która ma zostać zainstalowana, jest przesyłany za pośrednictwem kanałów komunikacji pomiędzy Agentami sieciowymi i Serwerem administracyjnym wraz z ustawieniami instalacji, zdefiniowanymi przez administratora. Aby przesłać pakiet dystrybucyjny, możesz użyć węzłów pośredniczących, na przykład, punktów dystrybucji, dostarczania multiemisyjnego itd.

Podczas wybierania metody i strategii wdrożenia aplikacji w zarządzanej sieci należy mieć na uwadze kilka czynników (częściowa lista):

- Konfigurację sieci organizacji.
- Całkowitą liczbę urządzeń.
- Obecność w sieci organizacji urządzeń, które nie należą do żadnej domeny, oraz obecność jednakowych kont z uprawnieniami administratora na tych urządzeniach.
- Pojemność kanału pomiędzy Serwerem administracyjnym a urządzeniami.
- Rodzaj komunikacji pomiędzy Serwerem administracyjnym a zdalnymi podsieciami oraz pojemność kanałów sieciowych w tych podsieciach.
- Ustawienia zabezpieczeń zostaną zastosowane na urządzeniach zdalnych na początku wdrożenia. Parametry te umożliwiają nawiązanie zdalnego połączenia z zarządzanym urządzeniem i rozpoczęcie instalacji.

Przygotowanie urządzenia z systemem Linux do zdalnej instalacji Agenta sieciowego

Przed zainstalowaniem Agenta sieciowego na urządzeniu z systemem Linux należy wykonać czynności przygotowawcze wymagane dla każdego urządzenia z systemem Linux.

W celu przygotowania urządzenia z systemem Linux do zdalnej instalacji Agenta sieciowego:

1. Upewnij się, że na urządzeniu, na którym chcesz zainstalować Agenta sieciowego dla systemu Linux, działa jedna z obsługiwanych dystrybucji systemu Linux.
2. Jeśli chcesz zainstalować Agenta sieciowego w systemie AltOS w zamkniętym trybie środowiska programowego, wyłącz ten tryb do czasu zakończenia instalacji.
3. Pobierz pakiet instalacyjny Agenta sieciowego, korzystając z interfejsu Web Console lub ze strony internetowej Kaspersky.

   Jeśli konieczne jest zainstalowanie Agenta sieciowego na urządzeniu z systemem operacyjnym Linux z biblioteką glibc 2.5, musisz pobrać pakiet instalacyjny *Agenta sieciowego Kaspersky dla systemu Linux Legacy*, korzystając z interfejsu Web Console lub ze strony internetowej Kaspersky.
4. Upewnij się, że następujące oprogramowanie jest zainstalowane na docelowym urządzeniu Linux:
   - Sudo (dla Ubuntu 10.04, wersja Sudo to 1.7.2p1 lub nowsza)
   - Perl language interpreter wersja 5.10 lub wyższa
   - narzędzie ps
5. Przetestuj konfigurację urządzenia:
   a. Sprawdź, czy możesz połączyć się z urządzeniem poprzez klienta SSH (np. PuTTY).

      Jeśli nie możesz połączyć się z urządzeniem, otwórz plik `/etc/ssh/sshd_config` i upewnij się, że następujące ustawienia posiadają odpowiednie wartości przedstawione poniżej:

      ```
      PasswordAuthentication no
      ```

```
ChallengeResponseAuthentication yes
```

> Nie modyfikuj pliku /etc/ssh/sshd_config, jeśli możesz połączyć się z urządzeniem bez problemów; w przeciwnym razie podczas uruchamiania zadania zdalnej instalacji może wystąpić błąd uwierzytelniania SSH.

Zapisz plik (jeśli to konieczne) i uruchom ponownie usługę SSH przy pomocy polecenia `sudo service ssh restart`.

b. Upewnij się, że port TCP 22 jest otwarty i dostępny na nieprzypisanym urządzeniu z systemem Linux.

Port TCP 22 musi być dostępny do pomyślnej instalacji Agenta sieciowego dla systemu Linux.

c. Wyłącz hasło do programu sudo dla konta użytkownika, z poziomu którego nawiązywane jest połączenie.

d. Użyj polecenia `visudo` w sudo, aby otworzyć plik konfiguracyjny sudoers.

W otwartym pliku dodaj na końcu pliku następujący wiersz: `<username> ALL = (ALL) NOPASSWD: ALL`. W tym przypadku `<username>` to konto użytkownika, które będzie używane do łączenia urządzenia przy użyciu SSH. Jeśli używasz systemu operacyjnego Astra Linux, w pliku /etc/sudoers dodaj ostatni wiersz z następującym tekstem: `%astra-admin ALL=(ALL:ALL) NOPASSWD: ALL`

e. Zapisz plik sudoers i zamknij go.

f. Ponownie nawiąż połączenie z urządzeniem poprzez SSH i upewnij się, że usługa Sudo nie żąda wprowadzenia hasła. Możesz to zrobić, korzystając z polecenia `sudo whoami`.

6. Aby zainstalować zdalnie Agenta sieciowego na urządzeniach z systemem operacyjnym z inicjalizacją systemd, otwórz plik `/etc/systemd/logind.conf`, a następnie wykonaj jedną z następujących czynności:

- Określ `no` jako wartość dla ustawienia `KillUserProcesses`: `KillUserProcesses=no`.
- Dla ustawienia `KillExcludeUsers` wpisz nazwę użytkownika konta, z poziomu którego zdalna instalacja zostanie uruchomiona, na przykład, `KillExcludeUsers=root`.

Urządzenie docelowe Astra Linux

Jeśli na urządzeniu docelowym działa system Astra Linux, dodaj ciąg `export PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin` w pliku `/home/<nazwa użytkownika>/.bashrc`, gdzie `<nazwa użytkownika>` to konto użytkownika, które ma zostać użyte do połączenia urządzenia przez SSH.

Urządzenie docelowe OSnova

Jeśli na urządzeniu docelowym działa system OSnova, wykonaj następujące czynności:

a. Otwórz plik `/usr/lib/systemd/logind.conf/10-enable-kill-user-processes.conf`, a następnie skomentuj wiersz `#KillUserProcess=yes`.

b. Otwórz plik `/usr/lib/NESS/pam-user-session`, a następnie skomentuj wiersz `#loginctl terminate-session "$XDG_SESSION_ID"`.

W celu zastosowania zmienionych ustawień uruchom urządzenie Linux ponownie lub wykonaj następujące polecenie:

```
sudo systemctl restart systemd-logind.service
```

7. Jeśli chcesz zainstalować Agenta sieciowego na urządzeniach z systemem operacyjnym SUSE Linux Enterprise Server 15, w pierwszej kolejności zainstaluj pakiet insserv-compat, aby skonfigurować Agenta sieciowego.

8. Jeśli chcesz zainstalować Agenta sieciowego na urządzeniach z systemem operacyjnym Astra Linux działającym w trybie zamkniętego środowiska oprogramowania, wykonaj dodatkowe kroki w celu przygotowania urządzeń Astra Linux.

9. Jeśli chcesz zainstalować Agenta sieciowego na urządzeniach z systemem Ubuntu Server lub Ubuntu Desktop w wersji 10.04, wykonaj dodatkowe czynności w celu przygotowania tych urządzeń.

10. Jeśli chcesz zainstalować Agenta sieciowego na urządzeniu z systemem operacyjnym Linux z biblioteką glibc 2.5, wykonaj dodatkowe kroki w celu przygotowania urządzeń docelowych.

11. Jeśli instalujesz Agenta sieciowego na AltOS w trybie zamkniętego środowiska oprogramowania, ponownie włącz tryb zamkniętego środowiska oprogramowania.

12. Jeśli chcesz zainstalować Agenta sieciowego na urządzeniach z systemem operacyjnym RED OS 7.3.4 lub nowszym albo MSVSPHERE 9.2 lub nowszym, zainstaluj pakiet libxcrypt-compat, aby Agent sieciowy działał prawidłowo.

Urządzenie z systemem Linux jest gotowe do instalacji Agenta sieciowego. Możesz zainstalować Agenta sieciowego zdalnie, w trybie interaktywnym lub w trybie cichym.

Przygotowanie urządzenia z systemem SUSE Linux Enterprise Server 15 do instalacji Agenta sieciowego

Przed instalacją Agenta sieciowego na urządzeniu z systemem SUSE Linux Enterprise Server 15 należy wykonać dwie procedury przygotowawcze — tę opisaną w instrukcjach poniżej i ogólne kroki przygotowawcze dla dowolnego urządzenia z systemem Linux.

W celu zainstalowania Agenta sieciowego na urządzeniu z systemem operacyjnym SUSE Linux Enterprise Server 15:

przed instalacją Agenta sieciowego uruchom następujące polecenie:

```
sudo zypper install insserv-compat
```

To umożliwia zainstalowanie pakietu insserv-compat i poprawne skonfigurowanie Agenta sieciowego.

Uruchom polecenie `rpm -q insserv-compat`, aby sprawdzić, czy pakiet jest już zainstalowany.

Jeśli Twoja sieć obejmuje wiele urządzeń z systemem SUSE Linux Enterprise Server 15, możesz użyć specjalnego oprogramowania do konfigurowania i zarządzania infrastrukturą firmy. Korzystając z tego oprogramowania, możesz automatycznie zainstalować pakiet insserv-compat na wszystkich niezbędnych urządzeniach jednocześnie. Na przykład, możesz użyć Puppet, Ansible, Chef, możesz utworzyć własny skrypt — użyj dowolnej wygodnej dla siebie metody.

Jeśli urządzenie nie ma kluczy podpisywania GPG dla SUSE Linux Enterprise, może pojawić się następujące ostrzeżenie: `Package header is not signed!` Wybierz `i` opcję, aby zignorować ostrzeżenie.

Po przygotowaniu urządzenia z systemem Linux możesz zainstalować Agenta sieciowego zdalnie, w trybie interaktywnym lub w trybie cichym.

Przygotowanie urządzenia z systemem Astra Linux w trybie zamkniętego środowiska oprogramowania do instalacji Agenta sieciowego

Przed instalacją Agenta sieciowego na urządzeniu z systemem Astra Linux w trybie zamkniętego środowiska oprogramowania należy wykonać dwie procedury przygotowawcze — tę opisaną w instrukcjach poniżej i ogólne kroki przygotowania dla dowolnego urządzenia z systemem Linux.

W wierszu poleceń uruchom polecenia podane w tej instrukcji na koncie z uprawnieniami administratora.

Przygotowanie urządzenia z systemem Astra Linux w trybie zamkniętego środowiska oprogramowania do instalacji Agenta sieciowego:

1. Otwórz plik `/etc/digsig/digsig_initramfs.conf` a następnie określ następujące ustawienie:

   ```
   DIGSIG_ELF_MODE=1
   ```

2. W wierszu polecenia uruchom następujące polecenie, aby zainstalować pakiet zgodności:

   ```
   apt install astra-digsig-oldkeys
   ```

3. Utwórz katalog dla klucza aplikacji:

   ```
   mkdir -p /etc/digsig/keys/legacy/kaspersky/
   ```

4. Umieść klucz aplikacji /opt/kaspersky/ksc64/share/kaspersky_astra_pub_key.gpg w katalogu utworzonym w poprzednim kroku:

   ```
   cp kaspersky_astra_pub_key.gpg /etc/digsig/keys/legacy/kaspersky/
   ```

   Jeśli pakiet dystrybucyjny Kaspersky Security Center Linux nie zawiera klucza aplikacji kaspersky_astra_pub_key.gpg, możesz go pobrać, klikając łącze: https://media.kaspersky.com/utilities/CorporateUtilities/kaspersky_astra_pub_key.gpg.

5. Zaktualizuj dyski RAM:

   ```
   update-initramfs -u -k all
   ```

   Uruchom ponownie system.

Urządzenie z systemem Linux jest gotowe do instalacji Agenta sieciowego. Możesz zainstalować Agenta sieciowego zdalnie, w trybie interaktywnym lub w trybie cichym.

Przygotowanie do instalacji Agenta sieciowego w systemie operacyjnym Linux z glibc 2.5 (starszy system operacyjny)

Przed zainstalowaniem Agenta sieciowego na urządzeniu z systemem operacyjnym Linux z glibc 2.5 (starszy system operacyjny) należy wykonać dwie procedury przygotowawcze—ogólne kroki przygotowawcze dla dowolnego urządzenia z systemem Linux oraz procedurę opisaną w tym artykule.

Zalecamy użycie instalacji lokalnej w celu zainstalowania Agenta sieciowego w systemie operacyjnym Linux z glibc 2.5 (starszy system operacyjny). Jeśli w tym scenariuszu musisz użyć zadania instalacji zdalnej, musisz wykonać dodatkowe kroki opisane w poniższej instrukcji.

W wierszu poleceń uruchom polecenia podane w tej instrukcji na koncie z uprawnieniami administratora.

Zalecamy użycie instalacji lokalnej do zainstalowania Agenta sieciowego w systemie operacyjnym Linux z biblioteką glibc 2.5 (starszy system operacyjny). Jeśli w tym scenariuszu musisz użyć zadania instalacji zdalnej, musisz wykonać dodatkowe kroki opisane w poniższej instrukcji.

1. Na urządzeniu z systemem operacyjnym Linux z biblioteką glibc 2.5 wykonaj kroki przygotowawcze wspólne dla każdego urządzenia Linux.

2. W pliku `/etc/sudoers` usuń wiersz `Defaults requiretty`.

3. Wyłącz listę zezwolonych prawidłowych algorytmów szyfrowania dla połączeń SSH, aby móc zainstalować Agenta sieciowego na urządzeniu z systemem operacyjnym Linux z biblioteką glibc 2.5.

   Aby to zrobić, na urządzeniu z zainstalowanym Serwerem administracyjnym lub na urządzeniu pełniącym funkcję punktu dystrybucji, którego zakres obejmuje urządzenie docelowe, uruchom następujące polecenie w wierszu poleceń:

   ```
   klscflag -fset -pv ".core/.independent" -s "Transport" -n
   SSH_CLIENT_DISABLE_ALGS_PROTECT -t d -v 1
   ```

Urządzenie z systemem Linux jest gotowe do instalacji zdalnej Agenta sieciowego.

Wyłączenie listy zezwolonych algorytmów szyfrowania może mieć wpływ na bezpieczeństwo połączenia SSH. Zdecydowanie zalecamy ponowne włączenie listy zezwolonych algorytmów szyfrowania natychmiast po zainstalowaniu Agenta sieciowego. Aby ponownie włączyć listę dozwolonych algorytmów szyfrowania, uruchom następujące polecenie:

```
klscflag -fset -pv ".core/.independent" -s "Transport" -n SSH_CLIENT_DISABLE_ALGS_PROTECT
-t d -v 0
```

Po zainstalowaniu Agenta sieciowego i ponownym włączeniu listy dozwolonych algorytmów szyfrowania urządzenie z systemem operacyjnym Linux z glibc 2.5 (starszy system operacyjny) jest teraz zarządzane przez Serwer administracyjny.

Przygotowanie do instalacji Agenta sieciowego w systemie operacyjnym Linux z OpenSSH w wersji 6.4 (starszy system operacyjny)

Przed zainstalowaniem Agenta sieciowego na urządzeniu korzystającym z OpenSSH w wersji 6.4 lub starszej (starszy system operacyjny) należy wykonać dwie procedury przygotowawcze—ogólne kroki przygotowawcze dla dowolnego urządzenia z systemem Linux oraz procedurę opisaną w tym artykule.

Zalecamy użycie instalacji lokalnej w celu zainstalowania Agenta sieciowego w systemie operacyjnym Linux z glibc 2.5 (starszy system operacyjny). Jeśli w tym scenariuszu musisz użyć zadania instalacji zdalnej, musisz wykonać dodatkowe kroki opisane w poniższej instrukcji.

W wierszu poleceń uruchom polecenia podane w tej instrukcji na koncie z uprawnieniami administratora.

Aby przygotować urządzenie, które korzysta z systemu OpenSSH w wersji 6.4 lub starszej do instalacji Agenta sieciowego:

1. Na urządzeniu, które korzysta z systemu OpenSSH w wersji 6.4 lub starszej wykonaj kroki przygotowawcze typowe dla każdego urządzenia z systemem Linux.

2. Wyłącz listę zezwolonych prawidłowych algorytmów szyfrowania dla połączeń SSH, aby móc zainstalować Agenta sieciowego na urządzeniu, które korzysta z systemu OpenSSH w wersji 6.4 lub starszej.

   Aby to zrobić, na urządzeniu z zainstalowanym Serwerem administracyjnym lub na urządzeniu pełniącym funkcję punktu dystrybucji, którego zakres obejmuje urządzenie docelowe, uruchom następujące polecenie w wierszu poleceń:

   ```
   klscflag -fset -pv ".core/.independent" -s "Transport" -n
   SSH_CLIENT_DISABLE_ALGS_PROTECT -t d -v 1
   ```

Urządzenie z systemem Linux jest gotowe do instalacji zdalnej Agenta sieciowego.

Wyłączenie listy zezwolonych algorytmów szyfrowania może mieć wpływ na bezpieczeństwo połączenia SSH. Zdecydowanie zalecamy ponowne włączenie listy zezwolonych algorytmów szyfrowania natychmiast po zainstalowaniu Agenta sieciowego. Aby ponownie włączyć listę dozwolonych algorytmów szyfrowania, uruchom następujące polecenie:

```
klscflag -fset -pv ".core/.independent" -s "Transport" -n SSH_CLIENT_DISABLE_ALGS_PROTECT
-t d -v 0
```

Po zainstalowaniu Agenta sieciowego i ponownym włączeniu listy dozwolonych algorytmów szyfrowania urządzenie z systemem operacyjnym Linux z glibc 2.5 (starszy system operacyjny) jest teraz zarządzane przez Serwer administracyjny.

Zdalna instalacja Agenta sieciowego na urządzeniu z systemem Linux

Przed zainstalowaniem Agenta sieciowego na urządzeniu opartym na systemie Linux należy wykonać ogólne czynności przygotowawcze wymagane dla wszystkich urządzeń opartych na systemie Linux.

Po wykonaniu ogólnych czynności można wykonać dodatkowe instrukcje specyficzne dla używanego systemu operacyjnego:

- Przygotowanie urządzenia z systemem SUSE Linux Enterprise Server 15
- Przygotowanie urządzenia z systemem Astra Linux w trybie zamkniętego środowiska oprogramowania
- Przygotowanie urządzenia z systemem Ubuntu Server/Desktop w wersji 10.04 i 16.04
- Przygotowanie urządzenia z systemem operacyjnym Linux z biblioteką glibc 2.5

Zdalna instalacja Agenta sieciowego na urządzeniach Linux:

1. Pobierz i utwórz pakiet instalacyjny:

   a. Przed zainstalowaniem pakietu na urządzeniu upewnij się, że dla tego pakietu są już zainstalowane wszystkie zależności (programy i biblioteki).

      Dla każdego pakietu można wyświetlić jego zależności, korzystając z narzędzi specyficznych dla dystrybucji Linuksa, na którym ten pakiet ma zostać zainstalowany. Więcej informacji na temat narzędzi można znaleźć w dokumentacji do systemu operacyjnego.

   b. W celu utworzenia zdalnego pakietu instalacyjnego użyj następujących plików:

      - klnagent.kpd
      - akinstall.sh
      - Pakiet .deb lub .rpm Agenta sieciowego

2. Utwórz zadanie zdalnej instalacji z następującymi ustawieniami:

   - Na stronie **Settings** Kreatora tworzenia nowego zadania zaznacz pole **Using operating system resources through Administration Server**. Odznacz wszystkie pozostałe pola.
   - W oknie **Wybieranie konta do uruchomienia zadania** określ ustawienia konta użytkownika, które jest używane do łączenia urządzenia poprzez SSH.

3. Uruchom zadanie zdalnej instalacji. Użyj opcji polecenia `su`, aby zachować środowisko: `-m, -p, --preserve-environment`.

Instalowanie Agenta sieciowego dla systemu Linux w trybie cichym (z plikiem odpowiedzi)

Możesz zainstalować Agenta sieciowego na urządzeniach Linux przy użyciu pliku odpowiedzi—pliku tekstowego, który zawiera niestandardowy zestaw parametrów instalacji: zmienne i ich odpowiednie wartości. Korzystanie z tego pliku odpowiedzi umożliwia uruchomienie instalacji w trybie cichym, czyli bez udziału użytkownika.

Przed zainstalowaniem Agenta sieciowego na urządzeniu opartym na systemie Linux należy wykonać ogólne czynności przygotowawcze wymagane dla wszystkich urządzeń opartych na systemie Linux.

Po wykonaniu ogólnych czynności można wykonać dodatkowe instrukcje specyficzne dla używanego systemu operacyjnego:

- Przygotowanie urządzenia z systemem SUSE Linux Enterprise Server 15
- Przygotowanie urządzenia z systemem Astra Linux w trybie zamkniętego środowiska oprogramowania
- Przygotowanie urządzenia z systemem Ubuntu Server/Desktop w wersji 10.04 i 16.04
- Przygotowanie urządzenia z systemem operacyjnym Linux z biblioteką glibc 2.5

W celu przeprowadzenia instalacji Agenta sieciowego dla systemu Linux w trybie cichym:

1. Przeczytaj Umowę licencyjną użytkownika końcowego. Wykonaj poniższe kroki tylko wtedy, gdy rozumiesz i akceptujesz warunki Umowy licencyjnej użytkownika końcowego.

2. Utwórz plik odpowiedzi (w formacie TXT). Do plików z odpowiedziami dodaj listę zmiennych w formacie VARIABLE_NAME=variable_value, każda zmienna musi być w oddzielnym wierszu.

   W celu poprawnego korzystania z pliku odpowiedzi, musisz umieścić go w minimalnym zestawie trzech wymaganych zmiennych:

   - KLNAGENT_SERVER
   - KLNAGENT_AUTOINSTALL
   - EULA_ACCEPTED

   Możesz także dodać dowolne opcjonalne zmienne, aby korzystać z bardziej określonych parametrów zdalnej instalacji. Poniższa tabela wyświetla listy zmiennych, które mogą znajdować się w pliku odpowiedzi:

   Zmienne pliku odpowiedzi użyte jako parametry instalacji Agenta sieciowego dla systemu Linux w trybie cichym

Zmienne pliku odpowiedzi użyte jako parametry instalacji Agenta sieciowego dla systemu Linux w trybie cichym

Nazwa zmiennej	Wymagane	Opis	Możliwe wartości
KLNAGENT_SERVER	Tak	Zawiera nazwę Serwera administracyjnego przedstawioną jako w pełni kwalifikowaną nazwę domeny (FQDN) lub adres IP.	Nazwa DNS lub adres IP.
KLNAGENT_AUTOINSTALL	Tak	Definiuje, czy tryb cichej instalacji jest włączony.	1—Tryb cichy jest włączony; użytkownik nie zostanie zapytany o żadne działania podczas instalacji. Inna—Tryb cichy jest wyłączony; użytkownik może zostać zapytany o działania podczas instalacji.
EULA_ACCEPTED	Tak	Definiuje, czy użytkownik akceptuje Umowę licencyjną użytkownika końcowego Agenta sieciowego; jeśli brakuje wartości, może być interpretowane jako brak zgody na Umowę licencyjną użytkownika końcowego.	1—Potwierdzam, że w pełni przeczytałem(-am), rozumiem i akceptuję warunki niniejszej Umowy licencyjnej użytkownika końcowego. Inna wartość lub bez wartości—Nie akceptuję postanowień i warunków Umowy licencyjnej (instalacja nie zostanie wykonana).
KLNAGENT_PROXY_USE	Nie	Definiuje, czy połączenie z Serwerem administracyjnym będzie używało ustawień serwera proxy. Domyślna wartość to 0.	1—Ustawienia proxy są używane. Inna—Ustawienia proxy nie są używane.
KLNAGENT_PROXY_ADDR	Nie	Definiuje adres serwera proxy używany do nawiązania połączenia z Serwerem administracyjnym.	Nazwa DNS lub adres IP.
KLNAGENT_PROXY_LOGIN	Nie	Definiuje nazwę użytkownika użytą do zalogowania się do serwera proxy.	Dowolna istniejąca nazwa użytkownika.
KLNAGENT_PROXY_PASSWORD	Nie	Definiuje hasło użytkownika użyte do zalogowania się do serwera proxy.	Dowolny zestaw znaków alfanumerycznych dozwolonych przez format hasła w systemie operacyjnym.

KLNAGENT_VM_VDI	Nie	Definiuje, czy Agent sieciowy jest zainstalowany na obrazie do utworzenia dynamicznych maszyn wirtualnych.	1—Agent sieciowy jest zainstalowany na obrazie, który jest używany jednocześnie do utworzenia dynamicznych maszyn wirtualnych. Inna—Podczas instalacji nie jest używany żaden obraz.
KLNAGENT_VM_OPTIMIZE	Nie	Definiuje, czy ustawienia Agenta sieciowego są optymalne dla hipernadzorcy.	1—Domyślne ustawienia lokalne Agenta sieciowego są modyfikowane w taki sposób, że zezwalają na zoptymalizowane użycie na hipernadzorcy.
KLNAGENT_TAGS	Nie	Wyświetla znaczniki przypisane do instancji Agenta sieciowego.	Jedna lub kilka nazw znaczników oddzielonych średnikami.
KLNAGENT_UDP_PORT	Nie	Definiuje port UDP użyty przez Agenta sieciowego. Domyślna wartość to 15000.	Dowolny istniejący numer portu.
KLNAGENT_PORT	Nie	Definiuje port nie będący TLS, użyty przez Agenta sieciowego. Domyślna wartość to 14000.	Dowolny istniejący numer portu.
KLNAGENT_SSLPORT	Nie	Definiuje port TLS, użyty przez Agenta sieciowego. Domyślna wartość to 13000.	Dowolny istniejący numer portu.
KLNAGENT_USESSL	Nie	Definiuje, czy port Transport Layer Security (TLS) jest używany do nawiązywania połączenia.	1 (domyślna)—TLS jest używany. Inna—TLS nie jest używany.
KLNAGENT_GW_MODE	Nie	Definiuje, czy brama połączenia jest używana.	1 (domyślna)—Bieżące ustawienia nie są modyfikowane (przy pierwszym połączeniu określona jest brama połączenia). 2—Nie jest używana brama połączenia. 3—Brama połączenia jest używana. Wymagany jest KLNAGENT_GW_ADDRESS. 4—Instancja Agenta sieciowego jest używana jako brama połączenia w strefie zdemilitaryzowanej (DMZ). Wymagany jest certyfikat serwera.
KLNAGENT_GW_ADDRESS	Nie	Definiuje adres bramy połączenia. Wartość jest stosowana tylko wtedy, gdy KLNAGENT_GW_MODE=3.	Nazwa DNS lub adres IP.
KLNAGENT_DEVICEOWNER_REGISTRATION_START	Nie	Umożliwia uruchomienie rejestracji użytkownika jako narzędzia właściciela urządzenia po instalacji Agenta sieciowego. Jeśli opcja jest wyłączona, rejestracja jako właściciela urządzenia nie jest dostępna dla użytkownika.	1 — Narzędzie rejestracji użytkownika jako właściciela urządzenia zostanie uruchomione po zainstalowaniu Agenta sieciowego. Inne — wyłączone.
PTCH_ALLOW_APPLY_NONAPROVED_PATCHES	Nie	Określa, czy pobrane aktualizacje mają być automatycznie instalowane dla Agenta sieciowego ze statusem *Niezdefiniowany*.	true (wartość domyślna) — Aktualizacje są instalowane automatycznie. false — Te aktualizacje nie są instalowane automatycznie.

3. Uruchom instalację Agenta sieciowego. Zmienna środowiskowa KLAUTOANSWERS, która określa ścieżkę do pliku odpowiedzi, jest przekazywana do polecenia instalacji. Uruchom jedno z następujących poleceń:

   - Aby zainstalować Agenta sieciowego z pakietu RPM w 32-bitowym systemie operacyjnym, wykonaj następujące polecenie:
     `sudo KLAUTOANSWERS=<ścieżka do pliku odpowiedzi> yum install ./klnagent-<numer kompilacji>.i386.rpm`

   - Aby zainstalować Agenta sieciowego z pakietu RPM w 64-bitowym systemie operacyjnym, wykonaj następujące polecenie:
     `sudo KLAUTOANSWERS=<ścieżka do pliku odpowiedzi> yum install ./klnagent64-<numer kompilacji>.x86_64.rpm`

   - Aby zainstalować Agenta sieciowego z pakietu RPM w 64-bitowym systemie operacyjnym dla architektury Arm, wykonaj następujące polecenie:
     `sudo KLAUTOANSWERS=<ścieżka do pliku odpowiedzi> yum install ./klnagent64-<numer kompilacji>.aarch64.rpm`

   - Aby zainstalować Agenta sieciowego z pakietu DEB w 32-bitowym systemie operacyjnym, wykonaj następujące polecenie:
     `sudo KLAUTOANSWERS=<ścieżka do pliku odpowiedzi> apt install ./klnagent_<numer kompilacji>_i386.deb`

   - Aby zainstalować Agenta sieciowego z pakietu DEB w 64-bitowym systemie operacyjnym, wykonaj następujące polecenie:
     `sudo KLAUTOANSWERS=<ścieżka do pliku odpowiedzi> apt install ./klnagent64_<build number>_amd64.deb`

   - Aby zainstalować Agenta sieciowego z pakietu DEB w 64-bitowym systemie operacyjnym dla architektury Arm, wykonaj następujące polecenie:
     `sudo KLAUTOANSWERS=<ścieżka do pliku odpowiedzi> apt install ./klnagent64_<numer kompilacji>_arm64.deb`

   W zależności od konfiguracji systemu operacyjnego, możesz również użyć menedżerów pakietów rpm, dpkg lub dnf, aby zainstalować Agenta sieciowego.

Instalacja Agenta sieciowego dla systemu Linux zostanie uruchomiona w trybie cichym; użytkownik nie zostanie zapytany o żadne działania podczas procesu.

Instalowanie Agenta sieciowego dla systemu Linux w trybie interaktywnym

W tym artykule opisano, jak zainstalować Agenta sieciowego na urządzeniach z systemem Linux w trybie interaktywnym, określając krok po kroku parametry instalacji. Alternatywnie możesz użyć pliku odpowiedzi — pliku tekstowego, który zawiera niestandardowy zestaw parametrów instalacji: zmienne i ich odpowiednie wartości. Korzystanie z tego pliku odpowiedzi umożliwia uruchomienie instalacji w trybie cichym, czyli bez udziału użytkownika.

Przed zainstalowaniem Agenta sieciowego na urządzeniu opartym na systemie Linux należy wykonać ogólne czynności przygotowawcze wymagane dla wszystkich urządzeń opartych na systemie Linux.

Po wykonaniu ogólnych czynności można wykonać dodatkowe instrukcje specyficzne dla używanego systemu operacyjnego:

- Przygotowanie urządzenia z systemem SUSE Linux Enterprise Server 15
- Przygotowanie urządzenia z systemem Astra Linux w trybie zamkniętego środowiska oprogramowania
- Przygotowanie urządzenia z systemem Ubuntu Server/Desktop w wersji 10.04 i 16.04
- Przygotowanie urządzenia z systemem operacyjnym Linux z biblioteką glibc 2.5

Instalowanie Agenta sieciowego w trybie interaktywnym:

1. Uruchom instalację Agenta sieciowego. W zależności od dystrybucji Linux uruchom jedno z następujących poleceń:
   - Aby zainstalować Agenta sieciowego z pakietu RPM w 32-bitowym systemie operacyjnym:
     ```
     # yum -i klnagent-<numer kompilacji>.i386.rpm
     ```
   - Aby zainstalować Agenta sieciowego z pakietu RPM w 64-bitowym systemie operacyjnym:
     ```
     # yum -i klnagent64-<numer kompilacji>.x86_64.rpm
     ```
   - Aby zainstalować Agenta sieciowego z pakietu RPM w 64-bitowym systemie operacyjnym dla architektury Arm:
     ```
     # yum -i klnagent64-<numer kompilacji>.aarch64.rpm
     ```
   - Aby zainstalować Agenta sieciowego z pakietu DEB w 32-bitowym systemie operacyjnym:
     ```
     # apt install ./klnagent_<numer kompilacji>_i386.deb
     ```
   - Aby zainstalować Agenta sieciowego z pakietu DEB w 64-bitowym systemie operacyjnym:
     ```
     # apt install ./klnagent64_<numer kompilacji>_amd64.deb
     ```
   - Aby zainstalować Agenta sieciowego z pakietu DEB w 64-bitowym systemie operacyjnym dla architektury Arm:
     ```
     # apt install ./klnagent64_<numer kompilacji>_arm64.deb
     ```
2. Uruchom konfigurację Agenta sieciowego:
   ```
   # /opt/kaspersky/klnagent64/lib/bin/setup/postinstall.pl
   ```
3. Przeczytaj Umowę licencyjną użytkownika końcowego (EULA). Tekst jest wyświetlany w oknie wiersza poleceń. Naciśnij spację, aby wyświetlić następny segment tekstu. Następnie po wyświetleniu monitu wprowadź jedną z następujących wartości:
   - Wpisz `y`, jeśli rozumiesz i akceptujesz warunki Umowy licencyjnej użytkownika końcowego.
   - Wpisz `n`, jeśli nie akceptujesz warunków Umowy licencyjnej użytkownika końcowego. Aby korzystać z Agenta sieciowego, musisz zaakceptować warunki Umowy licencyjnej użytkownika końcowego.
   - Wpisz `r`, aby ponownie wyświetlić Umowę licencyjną użytkownika końcowego.
4. Wprowadź nazwę DNS Serwera administracyjnego lub adres IP.
5. Wprowadź numer portu Serwera administracyjnego. Domyślnie wykorzystywany jest port 14000.

6. Wprowadź numer portu SSL Serwera administracyjnego. Domyślnie wykorzystywany jest port 13000.

7. Wpisz `y`, jeśli chcesz używać szyfrowania SSL dla ruchu pomiędzy Agentem sieciowym a Serwerem administracyjnym. W przeciwnym razie wpisz `n`.

8. W celu skonfigurowania Agenta sieciowego wybierz jedną z następujących opcji:

   - `[1]` —nie konfiguruj bramy połączenia.

     Twoje urządzenie nie będzie działać jako brama połączenia i nie będzie łączyć się z Serwerem administracyjnym poprzez bramę połączenia.

   - `[2]` —nie używaj bramy połączenia.

     Twoje urządzenie nie połączy się z Serwerem administracyjnym poprzez bramę połączenia.

   - `[3]` —Nawiąż połączenie z serwerem przy użyciu bramy połączenia.

     Twoje urządzenie połączy się z Serwerem administracyjnym poprzez bramę połączenia.

   - `[4]` —Użyj jako bramy połączenia.

     Twoje urządzenie będzie działać jako brama połączenia.

Agent sieciowy jest zainstalowany na urządzeniu z systemem Linux.

Obsługa przywracania systemu plików dla urządzeń z zainstalowanym Agentem sieciowym

Kaspersky Security Center Linux jest aplikacją oferującą wiele funkcji. Przywrócenie poprzedniego stanu systemu plików na urządzeniu z zainstalowanym Agentem sieciowym doprowadzi do desynchronizacji danych i niepoprawnego działania Kaspersky Security Center Linux.

Wycofanie systemu plików (lub jego części) może zostać wykonane w następujących przypadkach:

- Podczas kopiowania obrazu dysku twardego.
- Podczas przywracania stanu maszyny wirtualnej przy użyciu infrastruktury wirtualnej.
- Podczas przywracania danych z kopii zapasowej lub punktu odzyskiwania.

Scenariusze, w których oprogramowanie firm trzecich na urządzeniach z zainstalowanym Agentem sieciowym wpływa na zawartość folderu /var/opt/kaspersky/klnagent, są dla Kaspersky Security Center Linux tylko krytycznymi scenariuszami. Dlatego też, jeśli to tylko możliwe, powinieneś zawsze wykluczać ten folder z procedury odzyskiwania.

Ponieważ zasady działania niektórych organizacji dopuszczają możliwość wycofania systemu plików urządzeń, obsługa wycofania systemu plików na urządzeniach z zainstalowanym Agentem sieciowym jest dostępna w Kaspersky Security Center Linux od wersji 10 Maintenance Release 1 (Serwer administracyjny i Agenty sieciowe muszą być w wersjach 10 Maintenance Release 1 lub nowszych). Po wykryciu takich urządzeń są one automatycznie ponownie łączone z Serwerem administracyjnym z całkowitym wyczyszczeniem danych i pełną synchronizacją.

Domyślnie obsługa wykrywania wycofania systemu plików jest włączona w Kaspersky Security Center Linux.

Jeśli jest to tylko możliwe, unikaj przywracania poprzedniego stanu folderu /var/opt/kaspersky/klnagent na urządzeniach z zainstalowanym Agentem sieciowym, gdyż całkowita ponowna synchronizacja danych zużywa dużą ilość zasobów.

Wycofanie stanu systemu jest całkowicie zabronione na urządzeniu z zainstalowanym Serwerem administracyjnym. Podobnie jest w przypadku wycofania baz danych używanych przez Serwer administracyjny.

Możesz przywrócić stan Serwera administracyjnego z kopii zapasowej tylko przy użyciu standardowego narzędzia klbackup.

Instalowanie Agenta sieciowego dla systemu Windows

Można również zainstalować Agenta sieciowego na urządzeniach z systemem Windows w organizacji, aby zarządzać nimi przy użyciu Serwera administracyjnego.

W systemie Microsoft Windows XP Agent sieciowy może nie wykonać poprawnie następujących działań: pobranie uaktualnień bezpośrednio z serwerów Kaspersky (jako punkt dystrybucji) i działanie jako serwer proxy KSN (jako punkt dystrybucji); oraz wykrywanie luk firm trzecich (jeśli używane jest Zarządzanie lukami i poprawkami).

Przed zainstalowaniem Agenta sieciowego na urządzeniu z systemem Microsoft Windows opartym na architekturze Arm upewnij się, że nie jest już zainstalowany Agent sieciowy dla Microsoft Windows x86-64. W przeciwnym razie instalacja nie powiedzie się.

Istnieją następujące metody wstępnej instalacji Agenta sieciowego na zarządzanym urządzeniu z systemem Windows:

- Uruchamiając zadanie instalacji zdalnej w punkcie dystrybucji systemu Windows.

  Przed wykonaniem instalacji zdalnej na nieprzypisanym urządzeniu z systemem Windows, punkt dystrybucji z systemem Windows automatycznie sprawdza port UDP 137, aby określić typ systemu operacyjnego urządzenia docelowego. Jeśli port UDP 137 jest niedostępny, punkt dystrybucji próbuje połączyć się z portem TCP 445 na urządzeniu docelowym, który jest wymagany do przeprowadzenia instalacji.

- Za pomocą pakietu instalacyjnego systemu Windows (MSI) dla Agenta sieciowego, przy użyciu narzędzi innych firm do zdalnej instalacji aplikacji.

- Uruchamiając instalator aplikacji na zarządzanym urządzeniu.

- Wysyłając do użytkowników urządzeń odnośniki do pakietów autonomicznych, wygenerowanych przez Kaspersky Security Center Linux. Pakiety autonomiczne to moduły wykonywalne, które zawierają pakiety dystrybucyjne wybranych aplikacji wraz ze zdefiniowanymi ustawieniami.

Instalowanie Agenta sieciowego dla systemu Windows w trybie interaktywnym

W celu zainstalowania Agenta sieciowego lokalnie:

1. Na urządzeniu uruchom plik ksc_<version number>.<build number>_full_<localization language>.exe z pakietu dystrybucyjnego pobranego z Internetu.

   Zostanie otwarte okno z pytaniem o wybranie aplikacji firmy Kaspersky do zainstalowania.

2. W oknie wyboru aplikacji kliknij odnośnik **Zainstaluj tylko Agenta sieciowego Kaspersky Security Center**, aby uruchomić kreatora instalacji Agenta sieciowego. Postępuj zgodnie z instrukcjami kreatora.

   Podczas działania Kreatora instalacji możesz określić zaawansowane ustawienia Agenta sieciowego (patrz niżej).

3. Jeśli chcesz użyć swojego urządzenia jako bramy połączenia dla określonej grupy administracyjnej, w oknie **Brama połączenia** kreatora instalacji wybierz **Użyj Agenta sieciowego jako bramy połączenia w DMZ**.

4. W celu skonfigurowania Agenta sieciowego podczas instalacji na maszynie wirtualnym:

   a. Jeśli planujesz utworzyć dynamiczne maszyny wirtualne z obrazu maszyny wirtualnej, włącz tryb dynamiczny Agenta sieciowego dla Virtual Desktop Infrastructure (VDI). W tym celu, w oknie **Ustawienia zaawansowane** kreatora instalacji wybierz opcję **Włącz tryb dynamiczny VDI**.

      Pomiń ten krok, jeśli nie planujesz utworzyć dynamicznych maszyn wirtualnych z obrazu maszyny wirtualnej.

   b. Zoptymalizuj działanie Agenta sieciowego dla VDI. W tym celu, w oknie **Ustawienia zaawansowane** kreatora instalacji wybierz opcję **Optymalizuj ustawienia dla VM**.

      Skanowanie plików wykonywalnych w poszukiwaniu luk podczas uruchamiania urządzenia zostanie wyłączone. Spowoduje to wyłączenie wysyłania do Serwera administracyjnego informacji o następujących obiektach:

      - Rejestrze sprzętu
      - Aplikacje zainstalowane na urządzeniu
      - Aktualizacje Microsoft Windows, które powinny zostać zainstalowane na lokalnym urządzeniu klienckim
      - Luki w oprogramowaniu wykryte na lokalnym urządzeniu klienckim

      Co więcej, będziesz mógł włączyć wysyłanie tych informacji we właściwościach Agenta sieciowego lub w ustawieniach zasady Agenta sieciowego.

Po zakończeniu działania kreatora instalacji, na urządzeniu zostanie zainstalowany Agent sieciowy.

Możesz wyświetlić właściwości usługi Agenta sieciowego; możesz także uruchamiać, zatrzymywać i monitorować aktywność Agenta sieciowego, korzystając ze standardowych narzędzi Microsoft Windows: Zarządzanie komputerem\Usługi.

Instalowanie Agenta sieciowego dla systemu Windows w trybie cichym

Agent sieciowy może zostać zainstalowany w trybie cichym, czyli bez interaktywnego wprowadzania parametrów instalacji. W trybie cichej instalacji używany jest instalator Windows (MSI) dla Agenta sieciowego. Plik MSI znajduje się w pakiecie dystrybucyjnym Kaspersky Security Center Linux, w folderze Packages\NetAgent\exec.

> Instalacja Agenta sieciowego z pakietu MSI możliwa jest tylko w trybie cichym, instalacja interaktywna z pakietu MSI nie jest obsługiwana.

W celu zainstalowania Agenta sieciowego na urządzeniu lokalnym w trybie cichym:

1. Przeczytaj Umowę licencyjną użytkownika końcowego. Użyj poniższego polecenia tylko wtedy, gdy rozumiesz i akceptujesz warunki Umowy licencyjnej użytkownika końcowego.

2. Uruchom polecenie
   `msiexec /i "Kaspersky Network Agent.msi" /qn <setup_parameters>`

   gdzie `setup_parameters` to lista parametrów i ich odpowiednich wartości oddzielonych spacjami (`PROP1=PROP1VAL PROP2=PROP2VAL`).

   Na liście parametrów będziesz musiał uwzględnić `EULA=1`. W przeciwnym razie Agent sieciowy nie zostanie zainstalowany.

Jeśli używasz standardowych ustawień połączenia dla Kaspersky Security Center oraz Agenta sieciowego na zdalnych urządzeniach, uruchom polecenie:

```
msiexec /i "Kaspersky Network Agent.msi" /qn /l*vx c:\windows\temp\nag_inst.log
SERVERADDRESS=kscserver.mycompany.com EULA=1
```

`/l*vx` to klucz do zapisywania raportów. Dziennik jest tworzony podczas instalacji Agenta sieciowego i zapisywany w C:\windows\temp\nag_inst.log.

Oprócz nag_inst.log aplikacja tworzy plik $klssinstlib.log, który zawiera dziennik instalacji. Ten plik jest przechowywany w folderze %windir%\temp lub %temp%. Do celów rozwiązywania problemów użytkownik lub specjalista z pomocy technicznej Kaspersky może potrzebować obu plików dziennika - nag_inst.log i $klssinstlib.log.

Jeśli chcesz dodatkowo określić port połączenia z Serwerem administracyjnym, uruchom polecenie:

```
msiexec /i "Kaspersky Network Agent.msi" /qn /l*vx c:\windows\temp\nag_inst.log
SERVERADDRESS=kscserver.mycompany.com EULA=1 SERVERPORT=14000
```

Parametr `SERVERPORT` odpowiada numerowi portu połączenia z Serwerem administracyjnym.

Nazwy i możliwe wartości parametrów, które mogą zostać użyte podczas instalacji Agenta sieciowego w trybie cichym znajdują się w sekcji Parametry instalacji Agenta sieciowego.

Jeśli chcesz uaktualnić Agenta sieciowego za pomocą Instalatora Windows, uruchom następujące polecenie:

```
msiexec /i "Kaspersky Network Agent.msi" /qn /l*vx c:\windows\temp\nag_inst.log
REINSTALL=ALL REINSTALLMODE=vomus /norestart
```

Wdrażanie poprzez przechwycenie i skopiowanie obrazu urządzenia

Jeśli konieczne jest zainstalowanie Agenta sieciowego na urządzeniach, na których musi zostać (ponownie) zainstalowany system operacyjny i inne oprogramowanie, możesz wykorzystać mechanizm przechwytywania i kopiowania obrazu tego urządzenia.

W celu przeprowadzenia wdrożenia poprzez przechwycenie i skopiowanie dysku twardego:

1. Utwórz urządzenie referencyjne z zainstalowanym systemem operacyjnym i niezbędnym oprogramowaniem, włączając w to Agenta sieciowego i aplikację zabezpieczającą.

2. Przechwyć obraz urządzenia referencyjnego i roześlij ten obraz na nowe urządzenia przy użyciu dedykowanego zadania z Kaspersky Security Center Linux.

   Aby przechwycić i zainstalować obrazy dysków, użyj narzędzi firm trzecich dostępnych w organizacji.

Kopiowanie dysku przy użyciu narzędzi firm trzecich

Jeśli podczas przechwytywania obrazu urządzenia z zainstalowanym Agentem sieciowym stosujesz narzędzia firm trzecich, użyj jednej z następujących metod:

- Na urządzeniu referencyjnym zatrzymaj usługę Agenta sieciowego i uruchom narzędzie klmover z kluczem `-dupfix`. Narzędzie klmover znajduje się w pakiecie instalacyjnym Agenta sieciowego. Unikaj kolejnych uruchomień usługi Agenta sieciowego, dopóki operacja przechwytywania obrazu nie zostanie zakończona.

- Upewnij się, że narzędzie klmover zostanie uruchomione z kluczem `-dupfix` przed pierwszym uruchomieniem usługi Agenta sieciowego na urządzeniach docelowych. To wymaganie jest obowiązkowe i musi zostać spełnione przy pierwszym uruchomieniu systemu operacyjnego po wdrożeniu obrazu. Narzędzie klmover znajduje się w pakiecie instalacyjnym Agenta sieciowego.

- Użyj trybu klonowania dysku Agenta sieciowego.

Jeśli obraz dysku twardego został niepoprawnie skopiowany, możesz rozwiązać ten problem.

Możesz także przechwycić obraz urządzenia bez zainstalowanego Agenta sieciowego. W tym celu wykonaj wdrożenie obrazu na urządzeniach docelowych, a następnie zainstaluj Agenta sieciowego. W przypadku korzystania z tej metody zapewnij dostęp do folderu sieciowego za pomocą autonomicznych pakietów instalacyjnych z urządzenia.

Tryb klonowania dysku Agenta sieciowego

Klonowanie dysku twardego odpowiedniego urządzenia jest popularną metodą instalacji oprogramowania na nowych urządzeniach. Jeśli Agent sieciowy jest uruchomiony w trybie standardowym na dysku twardym odpowiedniego urządzenia, mogą pojawić się następujące problemy:

Po zainstalowaniu odpowiedniego obrazu dysku przy pomocy Agenta sieciowego na nowych urządzeniach, będą one wyświetlane jako pojedyncze urządzenie w Kaspersky Security Center Web Console. Ten problem pojawia się, ponieważ procedura klonowania powoduje, że nowe urządzenia przechowują identyczne dane wewnętrzne, które umożliwiają Serwerowi administracyjnemu skojarzenie urządzenia z własnym wpisem w konsoli Kaspersky Security Center Web Console.

Specjalny *tryb klonowania dysku Agenta sieciowego* umożliwia uniknięcie problemów z nieprawidłowym wyświetlaniem nowych urządzeń w konsoli Kaspersky Security Center Web Console po klonowaniu. Użyj tego trybu podczas instalowania oprogramowania (z Agentem sieciowym) na nowych urządzeniach za pomocą klonowania dysku.

W trybie klonowania dysku Agent sieciowy pracuje cały czas, ale nie łączy się z Serwerem administracyjnym. Po wyjściu z trybu klonowania, Agent sieciowy usuwa dane wewnętrzne, które umożliwiają Serwerowi administracyjnemu skojarzenie kilku urządzeń z jednym wpisem w konsoli Kaspersky Security Center Web Console. Po zakończeniu klonowania obrazu odpowiedniego urządzenia, nowe urządzenia są wyświetlane w konsoli Kaspersky Security Center Web Console prawidłowo (z indywidualnymi wpisami).

Scenariusz użycia trybu klonowania dysku Agenta sieciowego

1. Administrator instaluje Agenta sieciowego na odpowiednim urządzeniu.
2. Administrator sprawdza połączenie Agenta sieciowego z Serwerem administracyjnym przy użyciu narzędzia klnagchk.
3. Administrator włącza tryb klonowania dysku Agenta sieciowego.
4. Administrator instaluje oprogramowanie i łaty na urządzeniu i uruchamia je ponownie niezbędną ilość razy.
5. Administrator klonuje dysk twardy odpowiedniego urządzenia na dowolnej liczbie urządzeń.
6. Każda sklonowana kopia musi spełniać następujące warunki:
   a. Nazwa urządzenia musi być zmieniona.
   b. Urządzenie musi zostać uruchomione ponownie.
   c. Tryb klonowania dysku musi być wyłączony.

Włączanie i wyłączanie trybu klonowania dysku przy użyciu narzędzia klmover

W celu włączenia / wyłączenia trybu klonowania dysku Agenta sieciowego:

1. Uruchom narzędzie klmover na urządzeniu z zainstalowanym Agentem sieciowym, które potrzebujesz sklonować.

   Narzędzie klmover znajduje się w folderze instalacyjnym Agenta sieciowego.

2. W celu włączenia trybu klonowania dysku, w wierszu poleceń systemu Linux wprowadź następujące polecenie:

   ```
   ./klmover -cloningmode 1
   ```

   Agent sieciowy przełączy się do trybu klonowania dysku.

3. W celu uzyskania bieżącego stanu trybu klonowania dysku, w wierszu poleceń wprowadź następujące polecenie:

   ```
   ./klmover -cloningmode
   ```

   Okno narzędzia wskaże, czy tryb klonowania dysku jest włączony czy wyłączony.

4. W celu wyłączenia trybu klonowania dysku, w wierszu poleceń narzędzia wprowadź następujące polecenie:

   ```
   ./klmover -cloningmode 0
   ```

Parametry instalacji Agenta sieciowego

Poniższa tabela opisuje właściwości MSI, które można skonfigurować podczas instalacji Agenta sieciowego. Wszystkie parametry są opcjonalne, za wyjątkiem EULA i SERVERADDRESS.

Parametry instalacji Agenta sieciowego w trybie cichym

Właściwość MSI	Opis	Dostępne wartości
EULA	Akceptacja postanowień i warunków Umowy licencyjnej	• 1—Potwierdzam, że w pełni przeczytałem(-am), rozumiem i akceptuję warunki niniejszej Umowy licencyjnej użytkownika końcowego. • 0—Nie akceptuję postanowień i warunków Umowy licencyjnej (instalacja nie zostanie wykonana). • Bez wartości—Nie akceptuję postanowień i warunków Umowy licencyjnej (instalacja nie zostanie wykonana).
DONT_USE_ANSWER_FILE	Odczyt ustawień instalacji z pliku odpowiedzi	• 1—Nie używaj. • Inna wartość lub brak wartości—Odczyt.
INSTALLDIR	Ścieżka do folderu instalacyjnego Agenta sieciowego	Wartość wiersza.
SERVERADDRESS	Adres Serwera administracyjnego (wymagane)	Wartość wiersza.
SERVERPORT	Numer portu używanego do nawiązania połączenia z Serwerem administracyjnym	Wartość numeryczna.
SERVERSSLPORT	Numer portu dla szyfrowanego połączenia z Serwerem administracyjnym przy użyciu protokołu SSL	Wartość numeryczna.
USESSL	Czy użyć połączenia SSL	• 1—użyj. • Inna wartość lub brak wartości—nie używaj.
OPENUDPPORT	Czy otworzyć port UDP	• 1—otwórz. • Inna wartość lub brak wartości—nie otwieraj.
UDPPORT	Numer portu UDP	Wartość numeryczna.
USEPROXY	Czy użyć serwera proxy.	• 1—użyj. • Inna wartość lub brak wartości—nie używaj.
PROXYLOCATION (PROXYADDRESS:PROXYPORT)	Adres proxy i numer portu używanego do nawiązania połączenia z serwerem proxy	Wartość wiersza.
PROXYLOGIN	Konto używane do nawiązywania połączenia z serwerem proxy	Wartość wiersza.
PROXYPASSWORD	Hasło do konta dla połączenia z serwerem proxy (W parametrach pakietów instalacyjnych nie należy określać żadnych szczegółów kont użytkowników uprzywilejowanych.)	Wartość wiersza.
GATEWAYMODE	Tryb użycia bramy połączenia	• 0—nie używaj bramy połączenia. • 1—użyj tego Agenta sieciowego jako bramy połączenia. • 2—połącz z Serwerem administracyjnym przy użyciu bramy połączenia.

Właściwość MSI	Opis	Dostępne wartości
GATEWAYADDRESS	Adres bramy połączenia	Wartość wiersza.
CERTSELECTION	Metoda pobierania certyfikatu	• GetOnFirstConnection—uzyskaj certyfikat z Serwera administracyjnego. • GetExistent—wybierz istniejący certyfikat. Jeśli ta opcja zostanie wybrana, należy określić właściwość CERTFILE.
CERTFILE	Ścieżka do pliku certyfikatu	Wartość wiersza.
VMVDI	Włącz tryb dynamiczny dla wirtualnej infrastruktury pulpitu Virtual Desktop Infrastructure (VDI).	• 1—włącz. • 0—nie włączaj. • Brak wartości—nie włączaj.
LAUNCHPROGRAM	Czy uruchomić usługę Agenta sieciowego po instalacji. Parametr jest ignorowany, jeśli VMVDI=1	• 1—uruchom. • Inna wartość lub brak wartości—nie uruchamiaj.
NAGENTTAGS	Znacznik dla Agenta sieciowego (ma priorytet nad znacznikiem podanym w pliku odpowiedzi)	Wartość wiersza.

Instalowanie aplikacji przy pomocy zadania zdalnej instalacji

Kaspersky Security Center Linux umożliwia zdalne instalowanie aplikacji na urządzeniach przy użyciu zadań zdalnej instalacji. Te zadania są tworzone i przydzielane do urządzeń za pośrednictwem dedykowanego kreatora. W celu szybkiego i łatwego przypisywania zadań do urządzeń, możesz wskazać urządzenia (maksymalnie do 1000 urządzeń) w oknie kreatora w jeden z następujących sposobów:

- **Przypisz zadanie do grupy administracyjnej**. W tym przypadku zadanie jest przypisywane do urządzeń znajdujących się we wcześniej utworzonej grupie administracyjnej.

- **Określ adresy urządzeń ręcznie lub zaimportuj adresy z listy**. Możesz określić nazwy NetBIOS, nazwy DNS, adresy IP oraz podsieci IP urządzeń, do których chcesz przydzielić zadanie.

- **Przypisz zadanie do wyboru urządzeń**. W tym przypadku zadanie jest przypisywane do urządzeń znajdujących się we wcześniej utworzonym wyborze. Możesz określić domyślny wybór lub niestandardowy wybór, który utworzyłeś. Można wybrać maksymalnie 1000 urządzeń.

Aby uniknąć problemów, które mogą wystąpić podczas instalacji aplikacji na urządzeniu klienckim bez zainstalowanego Agenta sieciowego, należy postępować zgodnie z opisem procedury wymuszonego wdrożenie przy użyciu zadania zdalnej instalacji z Kaspersky Security Center Linux.

Informacje o zadaniach zdalnej instalacji w Kaspersky Security Center Linux

Kaspersky Security Center Linux oferuje różne mechanizmy zdalnej instalacji aplikacji, które są zaimplementowane pod postacią zadań zdalnej instalacji (instalacja wymuszona, instalacja poprzez skopiowanie obrazu dysku twardego). Możesz utworzyć zadanie zdalnej instalacji dla określonej grupy administracyjnej oraz dla wskazanych urządzeń lub wyboru urządzeń (takie zadania są wyświetlane w konsoli Kaspersky Security Center Web Console, w folderze **Zadania**). Podczas tworzenia zadania możesz wybrać pakiety instalacyjne (Agenta sieciowego i / lub innej aplikacji), które zostaną zainstalowane w obrębie tego zadania, a także określić pewne ustawienia, które definiują metodę zdalnej instalacji. Dodatkowo można użyć kreatora zdalnej instalacji, którego działanie polega na utworzeniu zadania zdalnej instalacji i monitorowaniu wyników.

Zadania dla grup administracyjnych dotyczą urządzeń znajdujących się w określonej grupie oraz wszystkich urządzeń we wszystkich podgrupach tej grupy administracyjnej. Zadanie obejmuje urządzenia podrzędnych Serwerów administracyjnych znajdujących się w grupie lub jej dowolnych podgrupach, jeśli odpowiednie ustawienie zostało włączone w zadaniu.

Zadania dla określonych urządzeń aktualizują listę urządzeń klienckich przy każdym uruchomieniu zgodnie z zawartością wyborów w momencie uruchomienia zadania. Jeśli wybór zawiera urządzenia, które zostały połączone z podrzędnymi Serwerami administracyjnymi, zadanie zostanie uruchomione także na tych urządzeniach. Szczegółowe informacje dotyczące tych ustawień i metod instalacji znajdują się poniżej.

Aby zapewnić pomyślne działanie zadania zdalnej instalacji na urządzeniach połączonych z podrzędnymi Serwerami administracyjnymi, należy użyć zadania przekazywania do przekazania pakietów instalacyjnych używanych przez zadanie użytkownika do odpowiednich podrzędnych Serwerów administracyjnych.

Zdalna instalacja aplikacji

Ta sekcja zawiera informacje o tym, jak zdalnie zainstalować aplikację na urządzeniach w grupie administracyjnej, urządzeniach o określonych adresach lub wybranych urządzeniach.

W celu zainstalowania aplikacji na określonych urządzeniach:

1. W menu głównym przejdź do **Zadania**.
2. Kliknij **Dodaj**.

   Zostanie uruchomiony Kreator tworzenia nowego zadania.
3. W polu **Typ zadania** wybierz **Zdalna instalacja aplikacji**.
4. Wybierz jedną z następujących opcji:

   - **Przypisz zadanie do grupy administracyjnej**

     Zadanie jest przypisywane do urządzeń znajdujących się w grupie administracyjnej. Możesz określić jedną z istniejących grup lub utworzyć nową grupę.

Na przykład, możesz chcieć użyć tej opcji do uruchomienia zadania wysyłania wiadomości do użytkowników, jeśli wiadomość jest specyficzna dla urządzeń znajdujących się w określonej grupie administracyjnej.

Jeśli zadanie jest przypisane do grupy administracyjnej, zakładka **Zabezpieczenia** nie jest wyświetlana w oknie właściwości zadania, ponieważ zadania grupowe podlegają ustawieniom zabezpieczeń grup, do których się odnoszą.

- **Określ adresy urządzeń ręcznie lub zaimportuj adresy z listy**

  Możesz określić nazwy NetBIOS, nazwy DNS, adresy IP oraz podsieci IP urządzeń, do których chcesz przydzielić zadanie.

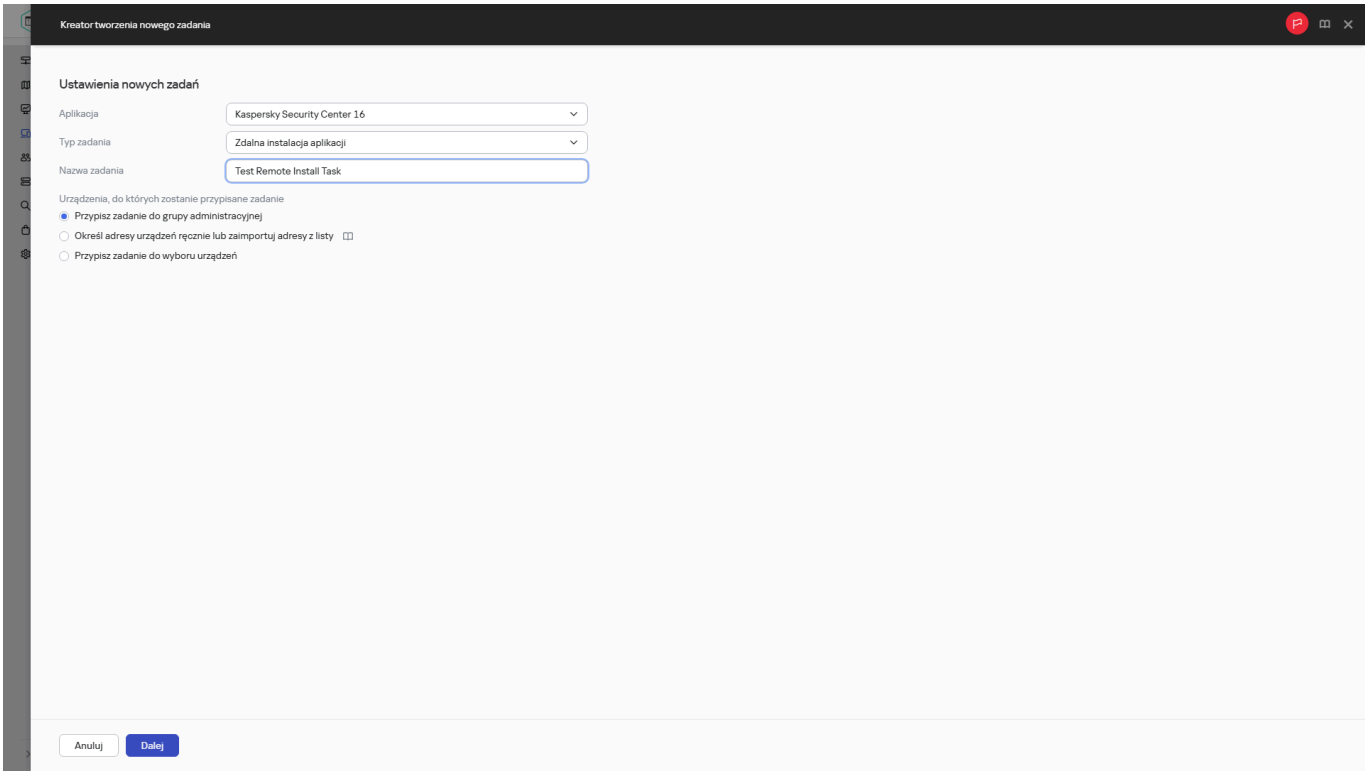
  Możesz użyć tej opcji do wykonania zadania dla określonej podsieci. Na przykład, możesz chcieć zainstalować pewną aplikację na urządzeniach księgowych lub przeskanować urządzenia w podsieci, która jest prawdopodobnie zainfekowana.

- **Przypisz zadanie do wyboru urządzeń**

  Zadanie jest przypisywane do urządzeń znajdujących się w wyborze urządzeń. Możesz określić jeden z istniejących wyborów.

  Na przykład, możesz chcieć użyć tej opcji do uruchomienia zadania na urządzeniach z określoną wersją systemu operacyjnego.

Zadanie *Zdalna instalacja aplikacji* jest tworzone dla określonych urządzeń. Jeśli wybrano opcję **Przypisz zadanie do grupy administracyjnej**, zadanie jest zadaniem grupowym.



Tworzenie zadania Zdalna instalacja aplikacji

5. W kroku **Zakres zadania** określ grupę administracyjną, urządzenia o określonych adresach lub wybór urządzeń.

   Dostępne ustawienia zależą od opcji wybranej w poprzednim kroku.

6. W kroku **Pakiety instalacyjne** określ następujące ustawienia:

- W polu **Wybierz pakiet instalacyjny** wskaż pakiet instalacyjny aplikacji, którą chcesz zainstalować.
- W grupie ustawień **Wymuś pobranie pakietu instalacyjnego** określ sposób rozsyłania na urządzenia klienckie plików, które są niezbędne do zainstalowania aplikacji:
  - **Przy użyciu Agenta sieciowego**

    Jeśli ta opcja jest włączona, pakiety instalacyjne są dostarczane na urządzenia klienckie przez Agenta sieciowego zainstalowanego na tych urządzeniach klienckich.

    Jeśli ta opcja jest wyłączona, pakiety instalacyjne są dostarczane przy użyciu narzędzi systemu operacyjnego urządzeń klienckich.

    Zalecane jest włączenie tej opcji, jeśli zadanie zostało przypisane do urządzeń z zainstalowanymi Agentami sieciowymi.

    Domyślnie opcja ta jest włączona.

  - **Przy użyciu zasobów systemu operacyjnego poprzez punkty dystrybucji**

    Jeśli ta opcja jest włączona, pakiety instalacyjne są przesyłane na urządzenia klienckie przy użyciu narzędzi systemu operacyjnego za pośrednictwem punktów dystrybucyjnych. Możesz wybrać tę opcję, jeżeli w sieci jest przynajmniej jeden punkt dystrybucyjny.

    Jeśli opcja **Przy użyciu Agenta sieciowego** jest włączona, pliki będą dostarczane przy użyciu narzędzi systemu operacyjnego, jeśli narzędzia Agenta sieciowego są niedostępne.

    Domyślnie ta opcja jest włączona dla zadań zdalnej instalacji utworzonych na wirtualnym Serwerze administracyjnym.

    Jedynym sposobem zainstalowania aplikacji dla systemu Windows (w tym Agenta sieciowego dla systemu Windows) na urządzeniu, na którym nie ma zainstalowanego Agenta sieciowego, jest użycie punktu dystrybucji opartego na systemie Windows. Dlatego podczas instalowania aplikacji Windows:

    - Wybierz tę opcję.
    - Upewnij się, że punkt dystrybucji jest przypisany do docelowych urządzeń klienckich.
    - Upewnij się, że punkt dystrybucji jest oparty na systemie Windows.

  - **Przy użyciu zasobów systemu operacyjnego przez Serwer administracyjny**

    Jeśli ta opcja jest włączona, pliki są przesyłane do urządzeń klienckich przy użyciu narzędzi systemu operacyjnego urządzeń klienckich za pośrednictwem Serwera administracyjnego. Możesz włączyć tę opcję, jeśli na urządzeniu klienckim nie ma zainstalowanego Agenta sieciowego, ale urządzenie klienckie jest w tej samej sieci co Serwer administracyjny.

    Domyślnie opcja ta jest włączona.

- W polu **Maksymalna liczba dla jednoczesnego pobierania** określ maksymalną dozwoloną liczbę urządzeń klienckich, do których Serwer administracyjny może jednocześnie przesyłać pliki.
- W polu **Maksymalna liczba prób instalacji** określ maksymalną dozwoloną liczbę uruchomień instalatora.

  Jeśli liczba prób określona w parametrze zostanie przekroczona, Kaspersky Security Center Linux nie uruchomi już instalatora na urządzeniu. Aby ponownie uruchomić zadanie *Zainstaluj aplikację zdalnie*, zwiększ wartość parametru **Maksymalna liczba prób instalacji** i uruchom zadanie. W razie czego możesz utworzyć nowe zadanie *Install application remotely*.

- Jeśli przeprowadzasz migrację z jednej aplikacji Kaspersky do drugiej, a bieżąca aplikacja jest chroniona hasłem, wprowadź hasło w polu **Hasło do odinstalowania bieżącej aplikacji Kaspersky**. Pamiętaj, że podczas migracji bieżąca aplikacja Kaspersky zostanie odinstalowana.

  Pole **Hasło do odinstalowania bieżącej aplikacji Kaspersky** jest dostępne tylko wtedy, gdy w grupie ustawień **Przy użyciu Agenta sieciowego** została wybrana opcja **Wymuś pobranie pakietu instalacyjnego**.

  Hasła dezinstalacji możesz użyć tylko w przypadku scenariusza migracji Kaspersky Security for Windows Server do Kaspersky Endpoint Security for Windows podczas instalacji Kaspersky Endpoint Security for Windows przy użyciu zadania Zdalna instalacja aplikacji. Użycie hasła dezinstalacyjnego podczas instalowania innych komponentów może spowodować błędy instalacji.

  Aby pomyślnie zakończyć scenariusz migracji, upewnij się, że spełnione są następujące wymagania wstępne:

  - Używasz Agenta sieciowego Kaspersky Security Center 14.2 dla Windows lub nowszej wersji.
  - Instalujesz aplikację na urządzeniach z systemem Windows.

- Określ ustawienie dodatkowe:

  - **Nie instaluj aplikacji ponownie, jeżeli jest już zainstalowana**

    Jeśli ta opcja jest włączona, wybrana aplikacja nie zostanie ponownie zainstalowana, jeśli już jest zainstalowana na tym urządzeniu klienckim.

    Jeśli ta opcja jest wyłączona, aplikacja zostanie zainstalowana mimo wszystko.

    Domyślnie opcja ta jest włączona.

  - **Zweryfikuj rodzaj systemu operacyjnego przed pobraniem**

    Przed przesłaniem plików do urządzeń klienckich Kaspersky Security Center Linux sprawdza, czy ustawienia narzędzia instalacyjnego mają zastosowanie do systemu operacyjnego urządzenia klienckiego. Jeśli ustawienia nie są stosowane, Kaspersky Security Center Linux nie przesyła plików i nie próbuje instalować aplikacji. Na przykład, aby zainstalować aplikację na urządzenia grupy administracyjnej, która zawiera urządzenia działające pod kontrolą różnych systemów operacyjnych, możesz przypisać zadanie instalacji do grupy administracyjnej, a następnie włączyć tę opcję, aby pominąć urządzenia, na których jest uruchomiony system operacyjny inny niż wymagany.

    Podczas instalacji zdalnej Agenta Sieciowego na urządzeniach nieprzypisanych, Kaspersky Security Center Linux lub punkt dystrybucji automatycznie określa typ systemu operacyjnego urządzenia niezależnie od ustawienia **Zweryfikuj rodzaj systemu operacyjnego przed pobraniem**.

  - **Przypisz pakiet instalacyjny do zasad grupy Active Directory**

    Jeśli ta opcja jest włączona, pakiet instalacyjny jest instalowany przy użyciu zasad grupy Active Directory.

    Ta opcja jest dostępna, jeśli wybrany jest pakiet instalacyjny Agenta sieciowego.

    Domyślnie opcja ta jest wyłączona.

  - **Poproś użytkowników o zamknięcie uruchomionych aplikacji**

    Uruchomione aplikacje mogą uniemożliwić ponowne uruchomienie urządzenia klienckiego. Na przykład, jeśli dokument jest edytowany w edytorze tekstu i nie zostanie zapisany, aplikacja nie zezwoli na ponowne uruchomienie urządzenia.

Jeśli ta opcja jest włączona, zostaje wymuszone zamknięcie takich aplikacji na zablokowanym urządzeniu przed jego ponownym uruchomieniem. W wyniku tego działania użytkownicy mogą utracić niezapisane zmiany.

Jeśli ta opcja jest wyłączona, zablokowane urządzenie nie zostanie uruchomione ponownie. Stan zadania na tym urządzeniu informuje, że wymagane jest ponowne uruchomienie urządzenia. Użytkownicy muszą ręcznie zamknąć wszystkie aplikacje uruchomione na zablokowanych urządzeniach i uruchomić ponownie te urządzenia.

Domyślnie opcja ta jest wyłączona.

- Wybierz na jakich urządzeniach chcesz zainstalować aplikację:
  - **Zainstaluj na wszystkich urządzeniach**

    Aplikacja zostanie zainstalowana nawet na urządzeniach zarządzanych przez inne Serwery administracyjne.

    Opcja ta jest wybrana domyślnie. Nie musisz zmieniać tego ustawienia, jeśli masz tylko jeden Serwer administracyjny w swojej sieci.

  - **Zainstaluj tylko na urządzeniach zarządzanych przez ten Serwer administracyjny**

    Aplikacja zostanie zainstalowana tylko na urządzeniach zarządzanych przez ten Serwer administracyjny. Wybierz tę opcję, jeśli posiadasz więcej niż jeden Serwer administracyjny w swojej sieci i chcesz uniknąć konfliktów między nimi.

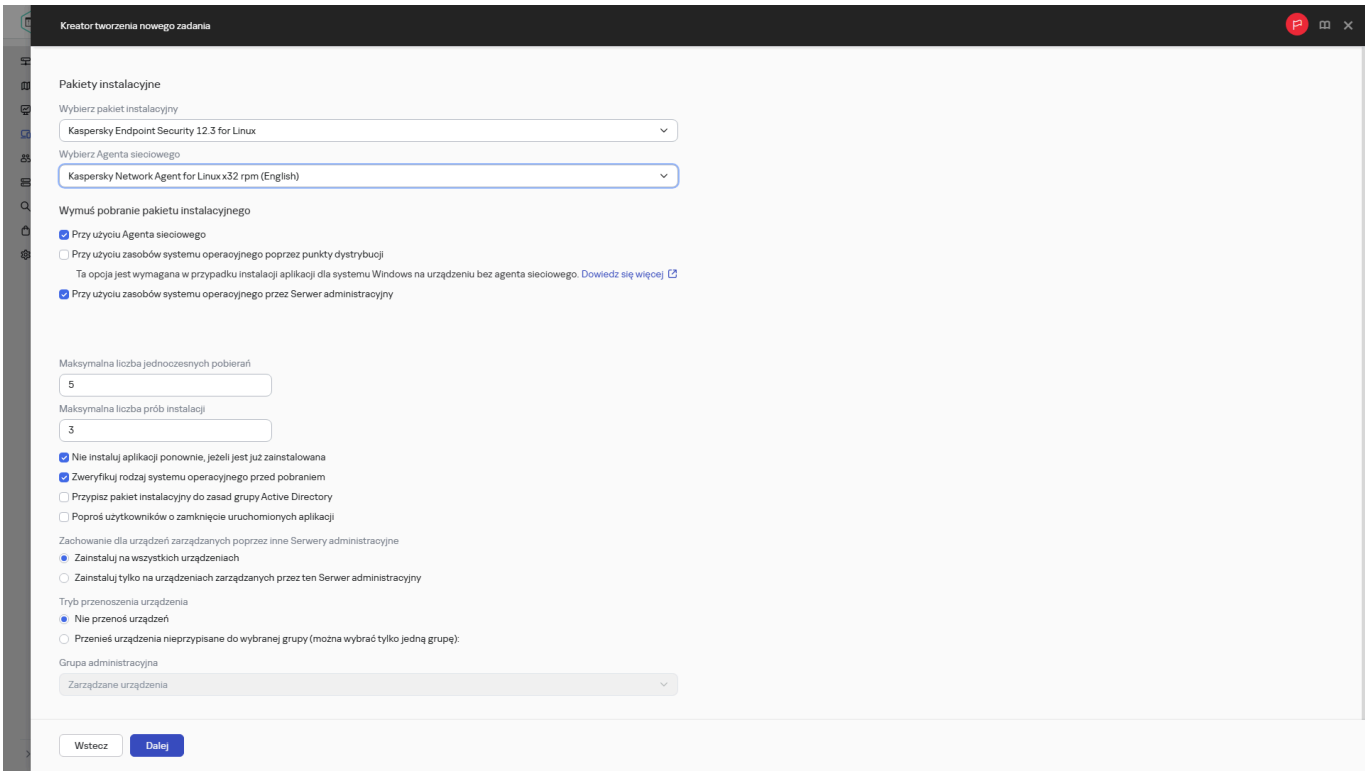
- Określ, czy urządzenia powinny zostać przeniesione do grupy administracyjnej po instalacji:
  - **Nie przenoś urządzeń**

    Urządzenia pozostają w grupach, w których aktualnie się znajdują. Urządzenia, które zostały umieszczone w dowolnej grupie, pozostaną nieprzypisane.

  - **Przenieś urządzenia nieprzypisane do wybranej grupy (można wybrać tylko jedną grupę)**

    Urządzenia są przenoszone do wybranej grupy administracyjnej.

  Zwróć uwagę, że opcja **Nie przenoś urządzeń** została wybrana domyślnie. W celach bezpieczeństwa możesz ręcznie przenieść urządzenia.



Określanie ustawień zadania

7. W tym kroku kreatora określ, czy urządzenia mają zostać ponownie uruchomione podczas instalacji aplikacji:

   - **Nie uruchamiaj ponownie urządzenia**

     Jeśli ta opcja jest zaznaczona, urządzenie nie zostanie ponownie uruchomione po zainstalowaniu aplikacji zabezpieczającej.

   - **Uruchom urządzenie ponownie**

     Jeśli ta opcja jest zaznaczona, urządzenie zostanie ponownie uruchomione po zainstalowaniu aplikacji zabezpieczającej.

8. W razie potrzeby w kroku **Wybierz konta w celu uzyskania dostępu do urządzeń** dodaj konta, które będą używane do uruchomienia zadania *Zdalna instalacja aplikacji*.

   - **Konto nie jest wymagane (Agent sieciowy jest zainstalowany)**

     Jeśli ta opcja jest zaznaczona, nie musisz określić konta, z poziomu którego zostanie uruchomiony instalator aplikacji. Zadanie zostanie uruchomione z poziomu konta, z którego uruchomiona jest usługa Serwera administracyjnego.

     Jeśli Agent sieciowy nie został zainstalowany na urządzeniach klienckich, ta opcja nie będzie dostępna.

- **Konto wymagane (Agent sieciowy nie jest używany)**

  Wybierz tę opcję, jeśli Agent sieciowy nie jest zainstalowany na urządzeniach, do których przypisano zadanie zdalnej instalacji. W takim przypadku możesz określić konto użytkownika lub certyfikat SSH, aby zainstalować aplikację.

  - **Konto lokalne lub domenowe**. Jeśli ta opcja jest zaznaczona, określ konto użytkownika, z poziomu którego zostanie uruchomiony instalator aplikacji. Kliknij przycisk **Dodaj**, wybierz **Konto lokalne lub domenowe**, a następnie określ poświadczenia konta użytkownika.

    Możesz określić wiele kont użytkowników, jeśli na przykład żadne z nich nie ma wszystkich wymaganych uprawnień na wszystkich urządzeniach, do których przypisujesz zadanie. W tym przypadku wszystkie dodane konta są używane do uruchomienia zadania, zaczynając od góry.

  - **Certyfikat SSH**. Jeśli chcesz zainstalować aplikację na urządzeniu klienckim opartym na systemie Linux, możesz określić certyfikat SSH zamiast konta użytkownika. Kliknij przycisk **Dodaj**, wybierz **Certyfikat SSH**, a następnie określ klucze prywatny i publiczny certyfikatu.

    Aby wygenerować klucz prywatny, możesz użyć narzędzia ssh-keygen. Należy zauważyć, że Kaspersky Security Center Linux obsługuje format PEM kluczy prywatnych, ale narzędzie ssh-keygen domyślnie generuje klucze SSH w formacie OPENSSH. Format OPENSSH nie jest obsługiwany przez Kaspersky Security Center Linux. Aby utworzyć klucz prywatny w obsługiwanym formacie PEM, dodaj opcję -m PEM w poleceniu ssh-keygen. Na przykład:

    ```
    ssh-keygen -m PEM -t rsa -b 4096 -C "< adres e-mail użytkownika >"
    ```

9. Na etapie **Zakończ tworzenie zadania** kliknij przycisk **Zakończ**, aby utworzyć zadanie i zamknąć kreatora.

   Jeśli włączyłeś opcję **Otwórz szczegóły zadania po jego utworzeniu**, zostanie otwarte okno ustawień zadania. W tym oknie możesz sprawdzić parametry zadania, zmodyfikować je lub skonfigurować harmonogram uruchamiania zadania, jeśli to konieczne.

10. Na liście zadań wybierz utworzone zadanie, a następnie kliknij przycisk **Start**.

    Ewentualnie poczekaj na uruchomienie zadania zgodnie z harmonogramem określonym w ustawieniach zadania.

Po zakończeniu zadania zdalnej instalacji wybrana aplikacja zostanie zainstalowana na określonych urządzeniach.

Instalacja zdalna aplikacji na urządzeniach z systemem macOS

Aby zainstalować aplikacje na urządzeniach z systemem macOS za pomocą zadania instalacji zdalnej:

1. Utwórz archiwum składające się z pakietu instalacyjnego i skryptu instalatora .sh.

2. Wyłącz opcję **Zweryfikuj rodzaj systemu operacyjnego przed pobraniem** w Kreatorze tworzenia nowego zadania.

Alternatywnie możesz skorzystać z zadania **Zdalne wykonanie skryptu**. W poniższym artykule opisano sposób konfiguracji plików dla tego zadania: Zdalna instalacja aplikacji na urządzeniach przy użyciu zadania Zdalne wykonanie skryptu.

Instalowanie aplikacji na podrzędnych Serwerach administracyjnych

Jeśli Twój Serwer administracyjny ma wersję 15.4 lub nowszą, możesz instalować aplikacje na podrzędnym Serwerze administracyjnym tylko wtedy, gdy jego wersja to 15.4 lub nowsza.

W celu zainstalowania aplikacji na podrzędnych Serwerach administracyjnych:

1. Nawiąż połączenie z Serwerem administracyjnym kontrolującym odpowiednie podrzędne Serwery administracyjne.

2. Upewnij się, że pakiet instalacyjny dla instalowanej aplikacji znajduje się na każdym z wybranych podrzędnych Serwerów administracyjnych. Jeśli nie możesz znaleźć pakietu instalacyjnego na żadnym z serwerów podrzędnych, dystrybuuj go. W tym celu utwórz zadanie z typem zadania **Rozsyłanie pakietu instalacyjnego**.

3. Utwórz zadanie zdalnej instalacji aplikacji na podrzędnych Serwerach administracyjnych. Wybierz typ zadania **Zdalna instalacja aplikacji na podrzędnym Serwerze administracyjnym**.

   Kreator nowego zadania tworzy zadanie zdalnej instalacji aplikacji wybranej w Kreatorze na określonych podrzędnych Serwerach administracyjnych.

4. Uruchom zadanie ręcznie lub poczekaj na jego uruchomienie zgodne z terminarzem określonym w ustawieniach zadania.

Po zakończeniu zadania zdalnej instalacji wybrana aplikacja zostanie zainstalowana na podrzędnych Serwerach administracyjnych.

Zdalna instalacja aplikacji na urządzeniach z zainstalowanym Agentem sieciowym

Jeśli na urządzeniu jest zainstalowany działający Agent sieciowy, połączony z głównym Serwerem administracyjnym (lub jednym z jego Serwerów podrzędnych), możesz zaktualizować Agenta sieciowego na tym urządzeniu, a także zainstalować, zaktualizować lub usunąć dowolne obsługiwane aplikacje poprzez Agenta sieciowego.

Możesz włączyć opcję **Przy użyciu Agenta sieciowego** we właściwościach zadania zdalnej instalacji.

Jeśli ta opcja jest zaznaczona, pakiety instalacyjne z ustawieniami instalacji, zdefiniowanymi przez administratora, zostaną przesłane na urządzenia docelowe poprzez kanały komunikacyjne między Agentem sieciowym a Serwerem administracyjnym.

Aby zoptymalizować obciążenie na Serwerze administracyjnym oraz zminimalizować ruch pomiędzy Serwerem administracyjnym a urządzeniami, należy wskazać punkty dystrybucji w każdej sieci zdalnej lub domenie rozgłoszeniowej (sekcja „Informacje o punktach dystrybucji" oraz sekcja „Tworzenie struktury grup administracyjnych i przydzielanie punktów dystrybucji"). W tym przypadku pakiety instalacyjne oraz ustawienia instalatora są rozsyłane z Serwera administracyjnego na urządzenia docelowe poprzez punkty dystrybucji.

Co więcej, możliwe jest użycie punktów dystrybucji do transmisyjnego (multiemisja) dostarczania pakietów instalacyjnych, co pozwala znacząco zmniejszyć ruch sieciowy podczas zdalnej instalacji aplikacji.

Podczas wysyłania pakietów instalacyjnych na urządzenia docelowe poprzez kanały komunikacyjne między Agentami sieciowymi a Serwerem administracyjnym, wszystkie pakiety instalacyjne, które zostały przygotowane do wysłania, zostaną także zbuforowane w folderze /var/opt/kaspersky/klnagent_srv/1093/.working/. Jeśli używanych jest kilka dużych pakietów instalacyjnych różnych typów oraz wykorzystywana jest duża liczba punktów dystrybucji, rozmiar tego folderu może drastycznie się powiększyć.

Nie można ręcznie usunąć plików z folderu FTServer. Jeśli oryginalne pakiety instalacyjne zostaną usunięte, odpowiednie dane zostaną automatycznie usunięte z folderu FTServer.

Dane otrzymane przez punkty dystrybucji zapisywane są w folderze /var/opt/kaspersky/klnagent_srv/1103/.

Nie można ręcznie usunąć plików z folderu $FTClTmp. Po zakończeniu działania zadań korzystających z danych z tego folderu, jego zawartość zostanie automatycznie usunięta.

Ponieważ pakiety instalacyjne są rozsyłane poprzez kanały komunikacyjne między Serwerem administracyjnym a Agentami sieciowymi z repozytorium pośredniczącego w formacie zoptymalizowanym dla transferów sieciowych, nie można wprowadzać żadnych zmian w pakietach instalacyjnych, przechowywanych w oryginalnym folderze każdego pakietu instalacyjnego. Takie zmiany nie zostałyby automatycznie zarejestrowane przez Serwer administracyjny. Jeśli chcesz ręcznie zmodyfikować pliki pakietów instalacyjnych (chociaż zalecane jest unikanie takiego rozwiązania), należy zmodyfikować dowolne ustawienia pakietu instalacyjnego w konsoli Kaspersky Security Center Web Console. Zmodyfikowanie ustawień pakietu instalacyjnego w konsoli Kaspersky Security Center Web Console spowoduje, że Serwer administracyjny zaktualizuje obraz pakietu w pamięci podręcznej, który został przygotowany do przesłania na urządzenia docelowe.

Serwer wysyła żądania ICMP Echo-Request (tak samo jak polecenie ping) do urządzenia docelowego podczas instalacji zdalnej.

Zarządzanie ponownym uruchamianiem urządzeń w zadaniu zdalnej instalacji

Aby zakończyć zdalną instalację aplikacji, często wymagane jest ponowne uruchomienie urządzeń (szczególnie w systemie Windows).

Jeśli korzystasz z zadania zdalnej instalacji z Kaspersky Security Center Linux, w Kreatorze tworzenia nowego zadania lub w oknie właściwości zadania, które zostało utworzone (sekcja **Ponowne uruchomienie systemu operacyjnego**), możesz wybrać akcję, która zostanie wykonana, gdy urządzenie z systemem Windows wymaga ponownego uruchomienia:

- **Nie uruchamiaj ponownie urządzenia**. W tym przypadku komputer nie zostanie automatycznie uruchomiony ponownie. Aby zakończyć instalację, należy uruchomić urządzenie ponownie (na przykład ręcznie lub przy użyciu zadania zarządzania urządzeniem). Informacje o wymaganym ponownym uruchomieniu zostaną zapisane w wynikach zadania oraz w statusie urządzenia. Opcja ta jest odpowiednia dla zadań instalacji na serwerach i innych urządzeniach, na których działanie ciągłe jest krytyczne.

- **Uruchom urządzenie ponownie**. W tym przypadku urządzenie jest zawsze automatycznie uruchamiane ponownie, jeśli jest to wymagane do zakończenia instalacji. Opcja jest przydatna, gdy zadania instalacji są uruchamiane na urządzeniach, na których możliwe są regularne przerwy w działaniu (wyłączenie lub ponowne uruchomienie).

- **Pytaj użytkownika o akcję**. W tym przypadku, na urządzeniu klienckim wyświetlane jest przypomnienie o ręcznym ponownym uruchomieniu urządzenia. Dla tej opcji można zdefiniować pewne ustawienia zaawansowane: treść wyświetlanego komunikatu, częstotliwość wyświetlania wiadomości oraz przedział czasu, po upływie którego ponowne uruchomienie zostanie wymuszone (bez potwierdzenia ze strony użytkownika). Opcja **Pytaj użytkownika o akcję** jest najodpowiedniejsza dla stacji roboczych, na których użytkownicy muszą mieć możliwość wyboru odpowiedniej godziny ponownego uruchomienia komputera.

Wymuszone wdrożenie przy użyciu zadania zdalnej instalacji z Kaspersky Security Center Linux

Aby wykonać wstępne wdrożenie Agenta sieciowego lub innych aplikacji, możesz wymusić instalację wybranych pakietów instalacyjnych, korzystając z zadania zdalnej instalacji programu Kaspersky Security Center Linux – pod warunkiem, że każde urządzenie ma konto(-a) użytkownika z uprawnieniami administratora lokalnego.

Instalacja wymuszona może być zastosowana także wtedy, gdy urządzenia nie są dostępne bezpośrednio dla Serwera administracyjnego, na przykład: urządzenia znajdują się w odizolowanych sieciach lub urządzenia są w sieci lokalnej, a Serwer administracyjny znajduje się w strefie DMZ.

W przypadku wdrożenia początkowego Agent sieciowy nie jest instalowany. Dlatego w ustawieniach zadania zdalnej instalacji nie można wybrać opcji dystrybucji plików wymaganych do instalacji aplikacji za pomocą Agenta sieciowego. Dystrybucję plików można przeprowadzić wyłącznie za pośrednictwem zasobów systemu operacyjnego, za pośrednictwem Serwera administracyjnego lub punktów dystrybucji.

Usługa Serwera administracyjnego musi być uruchomiona na koncie posiadającym uprawnienia administracyjne na urządzeniach docelowych. Alternatywnie możesz określić konto, które ma dostęp do części admin$ w ustawieniach ogólnych zadania zdalnej instalacji.

> Domyślnie zadanie zdalnej instalacji jest stosowane na urządzeniach poprzez użycie danych logowania konta, na którym uruchomiony jest Serwer administracyjny. Należy wyjaśnić, że chodzi o konto używane do uzyskiwania dostępu do części admin$, a nie o konto, na którym uruchamiane jest zadanie zdalnej instalacji. Instalacja zostanie przeprowadzona z poziomu konta SystemLokalny.

Możesz bezpośrednio wskazać urządzenia docelowe (za pomocą listy), wybrać grupę administracyjną Kaspersky Security Center Linux, do której należą; lub utworzyć wybór urządzeń w oparciu o określone kryterium. Instalacja rozpoczyna się zgodnie z terminarzem zadania. Jeśli we właściwościach zadania włączone jest ustawienie **Uruchom pominięte zadania**, zadanie może zostać uruchomione albo natychmiast po włączeniu urządzeń docelowych, albo po ich przeniesieniu do docelowej grupy administracyjnej.

Instalacja wymuszona obejmuje dostarczenie pakietów instalacyjnych do urządzeń docelowych, skopiowanie plików do zasobu admin$ na każdym urządzeniu docelowym, a także zdalną rejestrację usług pomocniczych na tych urządzeniach. Dostarczenie pakietów instalacyjnych do punktów dystrybucji odbywa się poprzez funkcję Kaspersky Security Center Linux zapewniającą interakcję z siecią. W tym przypadku muszą być spełnione następujące warunki:

- Dostęp do urządzeń docelowych jest możliwy od strony Serwera administracyjnego lub od strony punktu dystrybucji.
- Rozwiązywanie nazw urządzeń docelowych działa poprawnie w sieci.
- Zasób administracyjny (admin$) pozostanie włączony na urządzeniach docelowych.
- Na urządzeniach docelowych uruchomione są następujące usługi systemowe:
  - Serwer (LanmanServer)

    Domyślnie ta usługa jest uruchomiona.
  - Program uruchamiający procesy serwera DCOM (DcomLaunch)
  - Mapowanie punktów końcowych RPC (RpcEptMapper)
  - Zdalne wywoływanie procedur (RpcSs)
- Port TCP 445 jest otwarty na urządzeniach docelowych, aby umożliwić zdalny dostęp za pomocą Windows Management Instrumentation.

  > Protokoły TCP 139, UDP 137 i UDP 138 są używane przez starsze protokoły i nie są już potrzebne w obecnych aplikacjach.

  W zaporze sieciowej muszą być dozwolone dynamiczne porty dostępu wychodzącego w celu nawiązywania połączeń z Serwera administracyjnego i punktów dystrybucji do urządzeń docelowych.
- Ustawienia zabezpieczeń zasad domeny usługi Active Directory umożliwiają działanie protokołu NTLM podczas wdrażania Agenta Sieciowego.
- Na urządzeniach docelowych z systemem Microsoft Windows XP tryb Proste udostępnianie plików jest wyłączony.
- Na urządzeniach docelowych model współdzielenia dostępu i zabezpieczeń jest ustawiony jako *Klasyczny – lokalni użytkownicy uwierzytelniają się jako oni sami*. W żadnym wypadku nie może to być *tylko Gość – lokalni użytkownicy uwierzytelniają się jako Gość*.
- Urządzenia docelowe są członkami domeny lub wcześniej są tworzone na urządzeniach docelowych jednakowe konta z uprawnieniami administratora.

> Aby pomyślnie zainstalować Agenta sieciowego lub inne aplikacje na urządzeniu, które nie jest przyłączone do domeny Active Directory systemu Windows Server 2003 lub nowszego, należy wyłączyć zdalną kontrolę konta użytkownika (UAC) na tym urządzeniu. Zdalna kontrola konta użytkownika (UAC) jest jednym z powodów uniemożliwiających lokalnym kontom administracyjnym dostęp do admin$, który jest konieczny do wymuszonej instalacji Agenta sieciowego lub innych aplikacji. Wyłączenie zdalnej kontroli konta użytkownika (UAC) nie ma wpływu na lokalną UAC.

Podczas instalacji na nowych urządzeniach, które jeszcze nie zostały przydzielone do żadnej grupy administracyjnej Kaspersky Security Center Linux, możesz otworzyć właściwości zadania zdalnej instalacji i określić grupę administracyjną, do której urządzenia zostaną przeniesione po zakończeniu instalacji Agenta sieciowego.

> Podczas tworzenia zadania grupowego należy pamiętać, że każde zadanie grupowe ma wpływ na wszystkie urządzenia we wszystkich grupach zagnieżdżonych w wybranej grupie. Dlatego też należy unikać powielania zadań instalacji w podgrupach.

Prostszym sposobem tworzenia zadań wymuszonej instalacji aplikacji jest instalacja automatyczna. We właściwościach grupy administracyjnej należy otworzyć listę pakietów instalacyjnych a następnie wybrać te, które muszą zostać zainstalowane na urządzeniach w tej grupie. W rezultacie, wybrane pakiety instalacyjne zostaną automatycznie zainstalowane na wszystkich urządzeniach w tej grupie i wszystkich jej podgrupach. Przedział czasu, w trakcie którego pakiety zostaną zainstalowane, zależy od przepustowości sieci i całkowitej liczby urządzeń w sieci.

Aby zmniejszyć obciążenie Serwera administracyjnego podczas dostarczania pakietów instalacyjnych do urządzeń docelowych, w zadaniu instalacji można wybrać instalację za pośrednictwem punktów dystrybucji. Należy zauważyć, że ta metoda instalacji powoduje duże obciążenie urządzeń pełniących role punktów dystrybucji. W związku z tym zaleca się wybór urządzeń spełniających wymagania stawiane punktom dystrybucji. Jeśli korzystasz z punktów dystrybucji, upewnij się, że znajdują się one w każdej z odizolowanych podsieci, w których znajdują się urządzenia docelowe.

Korzystanie z punktów dystrybucji jako lokalnych centrów instalacji jest dobrym rozwiązaniem, gdy instalacja na urządzeniach w podsieciach komunikujących się z Serwerem administracyjnym odbywa się poprzez kanały o małej przepustowości, a pomiędzy urządzeniami w tej samej podsieci dostępny jest szeroki kanał.

Wolna przestrzeń na dysku, na którym znajduje się folder /var/opt/kaspersky/KSC_Backups* musi wielokrotnie przekraczać całkowity rozmiar pakietów dystrybucyjnych instalowanych aplikacji.

Instalowanie aplikacji w trybie cichym

W celu zainstalowania aplikacji w trybie cichym:

1. W menu głównym przejdź do **Zarządzanie oprogramowaniem** → **Pakiety instalacyjne**.

2. Zaznacz pole wyboru obok pakietu instalacyjnego wymaganej aplikacji lub utwórz nowy pakiet dla tej aplikacji.

   > Pakiet instalacyjny będzie przechowywany na Serwerze administracyjnym w folderze Pakiety, który znajduje się w folderze współdzielonym. Każdemu pakietowi instalacyjnemu odpowiada oddzielny podfolder.

3. Otwórz folder, w którym przechowywany jest żądany pakiet instalacyjny, w jeden z następujących sposobów:

   - Skopiuj folder żądanego pakietu instalacyjnego z Serwera administracyjnego na urządzenie klienckie. Następnie otwórz skopiowany folder na urządzeniu klienckim.

   - Z poziomu urządzenia klienckiego otwórz folder współdzielony na Serwerze administracyjnym, który odpowiada wymaganemu pakietowi instalacyjnemu.

Jeśli folder współdzielony znajduje się na urządzeniu z systemem operacyjnym Microsoft Windows Vista, należy wybrać wartość **Wyłączony** dla ustawienia **Kontrola konta użytkownika: Uruchom wszystkich administratorów w trybie Zatwierdzenie administratora** (**Start** → **Panel sterowania** → **Administracja** → **Zasady zabezpieczeń lokalnych** → **Ustawienia zabezpieczeń**).

4. Następnie, w zależności od wybranej aplikacji:

   - Dla programów Kaspersky Anti-Virus for Windows Workstations, Kaspersky Anti-Virus for Windows Servers oraz Kaspersky Security Center przejdź do podfolderu exec i przy pomocy klucza /s uruchom plik wykonywalny (plik z rozszerzeniem .exe).

   - Dla pozostałych aplikacji firmy Kaspersky, z otwartego folderu, przy pomocy klucza /s uruchom plik wykonywalny (plik z rozszerzeniem .exe).

   Uruchomienie pliku wykonywalnego z kluczami `EULA=1` i `PRIVACYPOLICY=1` oznacza, że w pełni przeczytałeś, zrozumiałeś i akceptujesz warunki, odpowiednio Umowy licencyjnej użytkownika końcowego i Polityki prywatności. Jesteś także świadomy, że Twoje dane będą zarządzane i przesyłane (w tym do innych krajów) w sposób opisany w Polityce prywatności. Treść Umowy licencyjnej i Polityki prywatności znajduje się w pakiecie dystrybucyjnym Kaspersky Security Center Linux. Akceptacja warunków Umowy licencyjnej i Polityki prywatności jest niezbędna do zainstalowania aplikacji lub jej aktualizacji z poprzedniej wersji aplikacji.

Przygotowanie urządzenia macOS do zdalnej instalacji Agenta sieciowego

Istnieją następujące metody wstępnej instalacji Agenta sieciowego na zarządzanym urządzeniu z systemem macOS:

- Uruchamiając zadanie instalacji zdalnej w punkcie dystrybucji systemu macOS.

- Wysyłając do użytkowników urządzeń odnośniki do pakietów autonomicznych, wygenerowanych przez Kaspersky Security Center Linux. Pakiety autonomiczne to moduły wykonywalne, które zawierają pakiety dystrybucyjne wybranych aplikacji wraz ze zdefiniowanymi ustawieniami.

W celu przygotowania urządzenia z systemem macOS do zdalnej instalacji Agenta sieciowego:

1. Upewnij się, że narzędzie sudo jest zainstalowane na docelowym urządzeniu macOS.

2. Przetestuj konfigurację urządzenia:

   a. Upewnij się, że port 22 jest otwarty na urządzeniu klienckim. Aby to zrobić w **Preferencjach systemowych** otwórz panel **Udostępnianie** i upewnij się, że pole **Zdalne logowanie** jest zaznaczone.

   Możesz połączyć się z urządzeniem klienckim przez Secure Shell (SSH) tylko przez port 22. Nie można zmienić numeru portu.

   Możesz użyć polecenia `ssh <nazwa_urządzenia>`, aby zdalnie zalogować się na urządzenie macOS. W panelu **Udostępnianie** możesz użyć opcji **Zezwalaj na dostęp przez**, aby określić zakres użytkowników, którzy mogą uzyskać dostęp do urządzenia macOS.

b. Wyłącz hasło do programu sudo dla konta użytkownika, z poziomu którego nawiązywane jest połączenie.

Użyj polecenia `sudo visudo` w Terminalu, aby otworzyć plik konfiguracyjny sudoers. W otwartym pliku, we wpisie `Specyfikacja uprawnień użytkownika` określ następujące elementy: `username ALL = (ALL) NOPASSWD: ALL`. W tym przypadku `username` to konto użytkownika, które będzie używane do łączenia urządzenia przy użyciu SSH.

c. Zapisz plik sudoers i zamknij go.

d. Ponownie nawiąż połączenie z urządzeniem poprzez SSH i upewnij się, że usługa Sudo nie żąda wprowadzenia hasła. Możesz to zrobić, korzystając z polecenia `sudo whoami`.

3. Pobierz i utwórz pakiet instalacyjny:

a. Pobierz pakiet instalacyjny Agenta sieciowego, korzystając z jednej z następujących metod:

- Za pomocą interfejsu aplikacji
- Pobierając odpowiednią wersję Agenta sieciowego ze strony internetowej pomocy technicznej: https://support.kaspersky.com/pl
- Prosząc specjalistów z pomocy technicznej o pakiet

b. W celu utworzenia zdalnego pakietu instalacyjnego użyj następujących plików:

- klnagent.kud
- install.sh
- klnagentmac.dmg

4. Utwórz zadanie zdalnej instalacji z następującymi ustawieniami:

- Na stronie **Ustawienia** Kreatora tworzenia nowego zadania zaznacz pole **Przy użyciu zasobów systemu operacyjnego przez Serwer administracyjny**. Odznacz wszystkie pozostałe pola.
- Na stronie **Wybieranie konta do uruchomienia zadania** określ ustawienia konta użytkownika, które jest używane do łączenia urządzenia poprzez SSH.

Urządzenie klienckie jest gotowe do zdalnej instalacji Agenta sieciowego za pośrednictwem odpowiedniego zadania, które utworzyłeś.

Infrastruktura wirtualna

Kaspersky Security Center Linux obsługuje użycie maszyn wirtualnych. Możesz zainstalować Agenta sieciowego i aplikację zabezpieczającą na każdej maszynie wirtualnej, a także wdrożyć ochronę maszyn wirtualnych na poziomie hipernadzorcy. W pierwszym przypadku, do ochrony maszyn wirtualnych możesz użyć standardowej aplikacji zabezpieczającej lub Kaspersky Security for Virtualization Light Agent. W drugim przypadku możesz użyć Kaspersky Security for Virtualization Agentless.

Kaspersky Security Center Linux obsługuje przywracanie maszyn wirtualnych do ich poprzedniego stanu.

Wskazówki dotyczące zmniejszenia obciążenia na maszynach wirtualnych

Podczas instalacji Agenta sieciowego na maszynie wirtualnej zalecane jest rozważenie wyłączenia funkcji Kaspersky Security Center Linux, które nie będą zbyt przydatne dla maszyn wirtualnych.

Podczas instalacji Agenta sieciowego na maszynie wirtualnej lub na szablonie przeznaczonym do wygenerowania maszyn wirtualnych, zalecane jest wykonanie następujących czynności:

- Jeśli uruchamiasz zdalną instalację, w oknie właściwości pakietu instalacyjnego Agenta sieciowego, w sekcji **Zaawansowane** zaznacz opcję **Optymalizuj ustawienia dla VDI**.
- Jeśli uruchamiasz instalację w trybie interaktywnym z udziałem kreatora, w oknie kreatora zaznacz opcję **Optymalizuj ustawienia Agenta sieciowego dla infrastruktury wirtualnej**.

Zaznaczenie tych opcji spowoduje zmianę ustawień Agenta sieciowego w taki sposób, że poniższe funkcje pozostaną domyślnie wyłączone (przed zastosowaniem zasady):

- Zbieranie informacji o zainstalowanym oprogramowaniu
- Zbieranie informacji o sprzęcie
- Zbieranie informacji o wykrytych lukach
- Zbieranie informacji o wymaganych aktualizacjach

Zazwyczaj te funkcje nie są potrzebne na maszynach wirtualnych, gdyż wykorzystują stałe oprogramowanie i sprzęt wirtualny.

Wyłączenie tych funkcji jest odwracalne. Jeśli jakakolwiek z wyłączonych funkcji jest potrzebna, możesz ją włączyć poprzez zasadę Agenta sieciowego lub poprzez ustawienia lokalne Agenta sieciowego. Ustawienia lokalne Agenta sieciowego są dostępne poprzez menu kontekstowe odpowiedniego urządzenia w konsoli Kaspersky Security Center Web Console.

Obsługa dynamicznych maszyn wirtualnych

Kaspersky Security Center Linux obsługuje dynamiczne maszyny wirtualne. Jeśli w sieci organizacji została wdrożona infrastruktura wirtualna, w pewnych przypadkach możliwe będzie korzystanie z dynamicznych (tymczasowych) maszyn wirtualnych. Dynamiczne maszyny wirtualne są tworzone pod unikatowymi nazwami w oparciu o szablony, które zostały przygotowane przez administratora. Użytkownik pracuje na maszynie wirtualnej przez jakiś czas, a następnie, po wyłączeniu maszyny zostanie ona usunięta z infrastruktury wirtualnej. Jeśli w sieci organizacji jest zainstalowany program Kaspersky Security Center Linux, maszyna wirtualna z zainstalowanym Agentem sieciowym zostanie dodana do bazy danych Serwera administracyjnego. Po wyłączeniu maszyny wirtualnej, odpowiedni wpis musi także zostać usunięty z bazy danych Serwera administracyjnego.

Aby funkcja automatycznego usuwania wpisów na temat maszyn wirtualnych mogła działać, podczas instalacji Agenta sieciowego na szablonie dla dynamicznych maszyn wirtualnych wybierz opcję **Włącz tryb dynamiczny VDI**:

- Dla zdalnej instalacji—w oknie właściwości pakietu instalacyjnego Agenta sieciowego (sekcja **Zaawansowane**)
- Dla instalacji w trybie interaktywnym—w Kreatorze instalacji Agenta sieciowego

Staraj się unikać zaznaczania opcji **Włącz tryb dynamiczny VDI** podczas instalacji Agenta sieciowego na urządzeniach fizycznych.

Jeśli chcesz, żeby zdarzenia z dynamicznych maszyn wirtualnych były przechowywane na Serwerze administracyjnym przez jakiś czas po usunięciu tych maszyn wirtualnych, w oknie właściwości Serwera administracyjnego, w sekcji **Repozytorium zdarzeń** wybierz opcję **Przechowuj zdarzenia po usunięciu urządzeń** i określ maksymalny czas przechowywania zdarzeń (w dniach).

Nie zalecamy włączania szyfrowania dysku na dynamicznych maszynach wirtualnych.

Obsługa kopiowania maszyn wirtualnych

Kopiowanie maszyn wirtualnych z zainstalowanym Agentem sieciowym lub tworzenie maszyny wirtualnej z szablonu z zainstalowanym Agentem sieciowym odbywa się w ten sam sposób co zdalna instalacja Agenta sieciowego poprzez przechwycenie i skopiowanie obrazu dysku twardego. Oznacza to, że podczas kopiowania maszyn wirtualnych należy wykonać te same czynności, co podczas instalacji Agenta sieciowego poprzez skopiowanie obrazu dysku.

Jednakże dwa poniższe przypadki przedstawiają sytuacje, gdy Agent sieciowy automatycznie wykrywa kopiowanie. Dzięki temu nie ma potrzeby wykonywania wszystkich skomplikowanych działań wymienionych w sekcji "Wdrożenie poprzez przechwycenie i skopiowanie obrazu dysku twardego urządzenia":

- Opcja **Włącz tryb dynamiczny VDI** została wybrana po zainstalowaniu Agenta sieciowego - po każdym ponownym uruchomieniu systemu operacyjnego ta maszyna wirtualna będzie rozpoznawana jako nowe urządzenie, niezależnie od tego, czy została skopiowana.
- Używany jest jeden z następujących hipernadzorców: VMware™, HyperV® lub Xen®: Agent sieciowy wykrywa kopiowanie maszyny wirtualnej po zmienionych numerach ID sprzętu wirtualnego.

Analiza zmian w sprzęcie wirtualnym nie jest całkowicie wiarygodna. Przed szerszym zastosowaniem tej metody należy ją sprawdzić na małej puli maszyn wirtualnych dla wersji hipernadzorcy, który jest aktualnie używany w organizacji.

Określanie ustawień zdalnej instalacji na urządzeniach z systemem Unix

Podczas instalowania aplikacji na urządzeniu z systemem UNIX przy użyciu zadania instalacji zdalnej można określić ustawienia zadania specyficzne dla systemu Unix. Te ustawienia są dostępne we właściwościach zadania po jego utworzeniu.

W celu określenia ustawień specyficznych dla systemu Unix dla zadania zdalnej instalacji:

1. W menu głównym przejdź do **Zadania**.
2. Kliknij nazwę zadania zdalnej instalacji, dla którego chcesz określić ustawienia specyficzne dla systemu Unix.

   Zostanie otwarte okno właściwości zadania.
3. Przejdź do **Ustawienia aplikacji** → **Ustawienia specyficzne dla systemu Unix**.
4. Określ następujące ustawienia:
   - **Ustaw hasło do konta root (tylko do wdrożenia przez SSH)**

     Jeśli polecenie `sudo` nie może być używane na urządzeniu docelowym bez określenia hasła, wybierz tę opcję, a następnie określ hasło dla konta root. Kaspersky Security Center Linux przesyła hasło w postaci zaszyfrowanej na urządzenie docelowe, odszyfrowuje hasło, a następnie rozpoczyna procedurę instalacji w imieniu konta root z określonym hasłem.

     > Kaspersky Security Center Linux nie używa konta ani określonego hasła do tworzenia połączenia SSH.

   - **Określ ścieżkę do folderu tymczasowego z uprawnieniami do wykonywania na urządzeniu docelowym (tylko do wdrożenia przez SSH)**

     Jeśli katalog /tmp na urządzeniu docelowym nie ma uprawnień do wykonywania, wybierz tę opcję, a następnie określ ścieżkę do katalogu z uprawnieniem do wykonywania. Kaspersky Security Center Linux używa określonego katalogu jako katalogu tymczasowego w celu uzyskania dostępu przez SSH. Aplikacja umieszcza pakiet instalacyjny w katalogu i uruchamia procedurę instalacji.
5. Kliknij przycisk **Zapisz**.

Określone ustawienia zadania zostaną zapisane.

Monitorowanie wdrożenia

Aby monitorować wdrożenie Kaspersky Security Center Linux i upewnić się, że aplikacja zabezpieczająca i Agent sieciowy są zainstalowane na zarządzanych urządzeniach, użyj funkcji monitorowania i raportowania:

- Użyj widżetu wdrożenia na pulpicie nawigacyjnym, aby monitorować wdrożenie w czasie rzeczywistym.
- Aby uzyskać szczegółowe informacje, należy użyć raportów.

Uruchamianie i zatrzymywania działania aplikacji Kaspersky

Możesz użyć zadania *Uruchom lub zatrzymaj aplikację* do uruchamiania i zatrzymywania aplikacji Kaspersky na zarządzanych urządzeniach.

Aby utworzyć zadanie Uruchom lub zatrzymaj aplikację:

1. W menu głównym przejdź do **Zadania**.
2. Kliknij **Dodaj**.

   Zostanie uruchomiony Kreator tworzenia nowego zadania. Przejdź przez kroki kreatora, korzystając z przycisku **Dalej**.
3. Z listy rozwijanej **Aplikacja** wybierz aplikację, do której chcesz utworzyć zadanie.

   Aplikacje Kaspersky są wyświetlane na liście, jeśli wcześniej dodałeś webowe wtyczki administracyjne dla tych aplikacji.
4. Z listy **Typ zadania** wybierz zadanie **Aktywacja aplikacji**.
5. W polu **Nazwa zadania** podaj nazwę nowego zadania.

   Nazwa zadania nie może zawierać więcej niż 100 znaków oraz nie może zawierać żadnych znaków specjalnych ("* <>?\:|).
6. Wybierz urządzenia, do których zadanie zostanie przypisane.
7. W oknie **Aplikacje** wykonaj następujące czynności:
   - Zaznacza pola obok nazw aplikacji, dla których chcesz utworzyć zadanie.
   - Wybierz opcję **Uruchom aplikację** lub **Zatrzymaj aplikację**.
8. Jeśli chcesz zmodyfikować domyślne ustawienia zadania, włącz opcję **Otwórz szczegóły zadania po jego utworzeniu** w kroku **Zakończ tworzenie zadania**. Jeśli nie włączysz tej opcji, zadanie zostanie utworzone z domyślnymi ustawieniami. Możesz zmodyfikować domyślne ustawienia później w dowolnym momencie.
9. Kliknij przycisk **Zakończ**.

   Zadanie zostanie utworzone i będzie wyświetlane na liście zadań.
10. Kliknij nazwę utworzonego zadania, aby otworzyć okno właściwości zadania.
11. W oknie właściwości zadania określ ogólne ustawienia zadania zgodnie ze swoimi potrzebami, a następnie zapisz ustawienia.

Zadanie zostało utworzone i skonfigurowane.

Aby uruchomić zadanie, na liście zadań wybierz zadanie i kliknij przycisk **Uruchom**.

Zastępowanie aplikacji zabezpieczających firm trzecich

Instalacja aplikacji zabezpieczających Kaspersky za pośrednictwem Kaspersky Security Center Linux może wymagać usunięcia oprogramowania firmy trzeciej niekompatybilnego z instalowaną aplikacją. Kaspersky Security Center Linux oferuje kilka sposobów usunięcia aplikacji firm trzecich.

Usuwanie niekompatybilnych aplikacji podczas konfigurowania zdalnej instalacji aplikacji

Możesz włączyć opcję **Automatycznie odinstaluj niekompatybilne aplikacje**, gdy konfigurujesz zdalną instalację aplikacji zabezpieczającej w kreatorze wdrażania ochrony. Jeśli ta opcja jest włączona, Kaspersky Security Center Linux usunie niekompatybilne aplikacje przed zainstalowaniem aplikacji zabezpieczającej na zarządzanym urządzeniu.

Dezinstalowanie niekompatybilnych aplikacji przy użyciu dedykowanego zadania

Aby usunąć niekompatybilne aplikacje, użyj zadania *Zdalna dezinstalacja aplikacji*. Zadanie to powinno być uruchomione na urządzeniach przed zadaniem instalacji aplikacji zabezpieczającej. Na przykład, w zadaniu instalacji możesz wybrać opcję terminarza **Po zakończeniu wykonywania innego zadania**, gdzie inne zadanie to *Zdalna dezinstalacja aplikacji*

Ta metoda dezinstalacji jest przydatna, jeśli instalator aplikacji zabezpieczającej nie może skutecznie usunąć niekompatybilnej aplikacji.

Zdalne usuwanie aplikacji lub aktualizacji oprogramowania

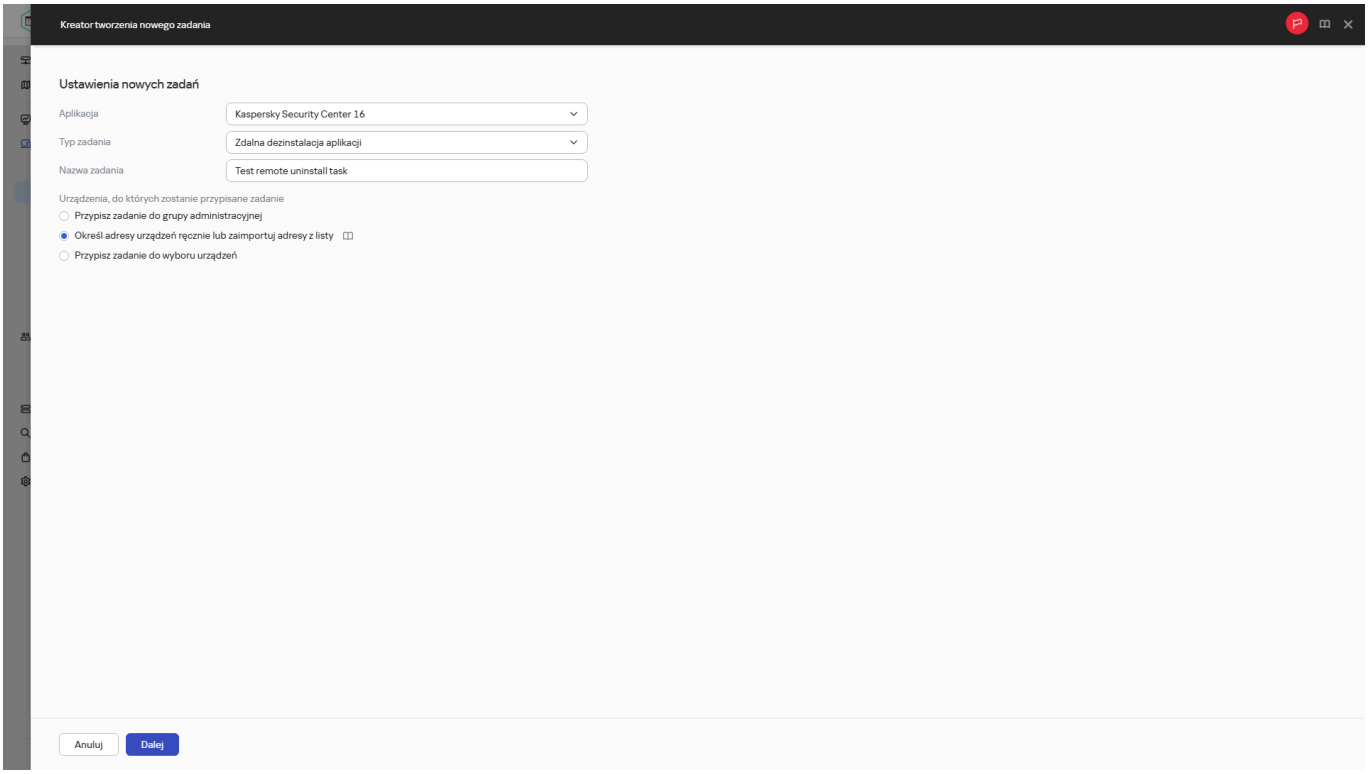
Aplikacje lub aktualizacje oprogramowania na zarządzanych urządzeniach z systemem Linux można usuwać zdalnie tylko za pomocą Agenta sieciowego.

W celu zdalnego usunięcia aplikacji lub aktualizacji oprogramowania z wybranych urządzeń:

1. W menu głównym przejdź do **Zadania**.
2. Kliknij **Dodaj**.

   Zostanie uruchomiony Kreator tworzenia nowego zadania. Przejdź przez kroki kreatora, korzystając z przycisku **Dalej**.
3. Z listy rozwijanej **Aplikacja** wybierz Kaspersky Security Center Linux.
4. Z listy **Typ zadania** wybierz typ zadania **Zdalna dezinstalacja aplikacji**.
5. W polu **Nazwa zadania** podaj nazwę nowego zadania.

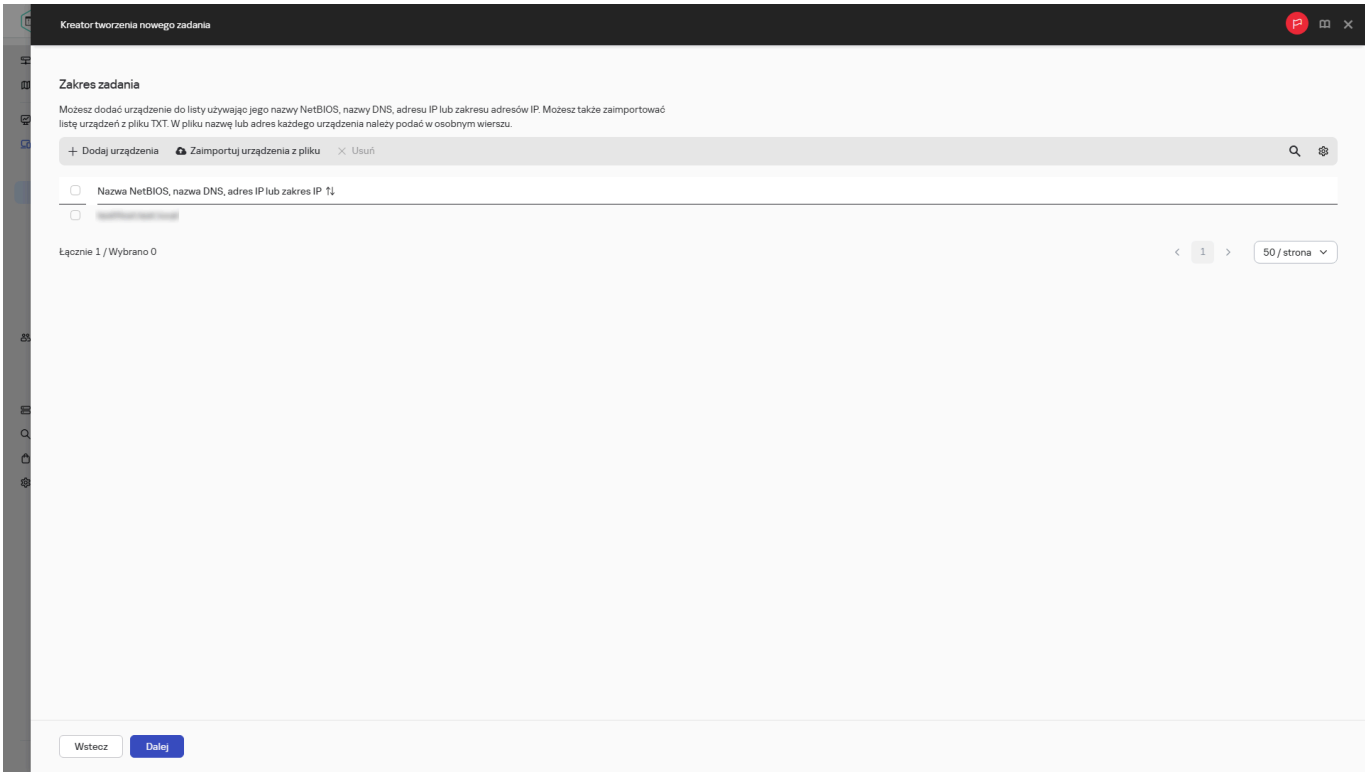
Nazwa zadania nie może zawierać więcej niż 100 znaków oraz nie może zawierać żadnych znaków specjalnych ("* <>?\:|).



Tworzenie zadania Zdalna dezinstalacja aplikacji

6. Wybierz urządzenia, do których zadanie zostanie przypisane.

   Przejdź do następnego kroku kreatora.



Określanie zakresu zadania

7. Wybierz rodzaj oprogramowania, które chcesz usunąć, a następnie wybierz określone aplikacje, aktualizacje lub łaty, które chcesz usunąć:

- **Odinstaluj zarządzane aplikacje**

  Zostanie wyświetlona lista aplikacji Kaspersky. Wybierz aplikację, którą chcesz usunąć.

- **Odinstaluj niekompatybilną aplikację**

  Zostanie wyświetlona lista aplikacji niekompatybilnych z aplikacjami zabezpieczającymi firmy Kaspersky lub Kaspersky Security Center Linux. Zaznacz pola obok aplikacji, które chcesz usunąć.

- **Odinstaluj aplikację z rejestru aplikacji**

  Domyślnie, Agenty sieciowe wysyłają do Serwera administracyjnego informacje o aplikacjach zainstalowanych na zarządzanych urządzeniach. Lista zainstalowanych aplikacji jest przechowywana w rejestrze aplikacji.

  W celu wybrania aplikacji z rejestru aplikacji:

  a. Kliknij pole **Aplikacja do odinstalowania**, a następnie wybierz aplikację, którą chcesz usunąć.

  > Jeśli wybierzesz Agenta sieciowego Kaspersky Security Center, po uruchomieniu zadania stan *Ukończono pomyślnie* oznacza, że rozpoczął się proces usuwania. Jeśli Agent sieciowy Kaspersky Security Center zostanie usunięty, jego stan się nie zmieni. Jeśli zadanie nie powiedzie się, status zmieni się na *Niepowodzenie.*

  b. Określ opcje dezinstalacji:

  - **Tryb dezinstalacji**

    Wybierz sposób dezinstalacji aplikacji:

    - **Określ polecenie dezinstalacji automatycznie**

      Jeśli aplikacja posiada polecenie dezinstalacji zdefiniowane przez producenta aplikacji, Kaspersky Security Center Linux użyje tego polecenia. Nie jest zalecane wybranie tej opcji.

    - **Określ polecenie dezinstalacji**

      Wybierz tę opcję, jeśli chcesz określić swoje polecenie do dezinstalacji aplikacji.

      > W pierwszej kolejności zalecane jest usunięcie aplikacji przy użyciu opcji **Określ polecenie dezinstalacji automatycznie**. Jeśli dezinstalacja za pośrednictwem automatycznie zdefiniowanego polecenia nie powiedzie się, wówczas użyj swojego polecenia.

      W polu wpisz polecenie instalacji, a następnie określ następującą opcję:

      Użyj tego polecenia do dezinstalacji, dopóki nie zostanie ono wykryte automatycznie

      Kaspersky Security Center Linux sprawdza, czy wybrana aplikacja posiada polecenie dezinstalacji zdefiniowane przez producenta aplikacji. Jeśli polecenie zostało wykryte, Kaspersky Security Center Linux użyje go zamiast polecenia określonego w polu **Polecenie do dezinstalacji aplikacji**.

      Nie jest zalecane włączenie tej opcji.

- **Wykonaj ponowne uruchomienie po pomyślnym odinstalowaniu aplikacji**

  Jeśli po pomyślnej dezinstalacji aplikacji wymagane jest ponowne uruchomienie systemu operacyjnego na zarządzanym urządzeniu, system operacyjny zostanie automatycznie uruchomiony ponownie.

- **Odinstaluj wybraną aktualizację aplikacji, poprawkę lub aplikację firmy trzeciej**

  Zostanie wyświetlona lista aktualizacji, łat i aplikacji innych firm. Wybierz element, który chcesz usunąć.

  Wyświetlona lista jest ogólną listą aplikacji i aktualizacji i nie odpowiada aplikacjom i aktualizacjom zainstalowanym na zarządzanych urządzeniach. Przed wybraniem elementu zalecane jest zapewnienie, że aplikacja lub aktualizacja jest zainstalowana na urządzeniu zdefiniowanym w obszarze zadania. Listę urządzeń, na których aplikacja lub aktualizacja została zainstalowana, możesz przejrzeć w oknie właściwości.

  W celu wyświetlenia listy urządzeń:

  a. Kliknij nazwę aplikacji lub aktualizacji.

     Zostanie otwarte okno właściwości.

  b. Otwórz sekcję **Urządzenia**.

     Listę zainstalowanych aplikacji i aktualizacji możesz przejrzeć także w oknie właściwości urządzenia.

8. Określ sposób, w jaki urządzenia klienckie pobiorą narzędzie do dezinstalacji:

- **Przy użyciu Agenta sieciowego**

  Pliki są dostarczane do urządzeń klienckich przez Agenta sieciowego zainstalowanego na tych urządzeniach klienckich.

  Jeśli ta opcja została wyłączona, pliki zostaną dostarczone przy użyciu narzędzi operacyjnych Linux.

  Zalecane jest włączenie tej opcji, jeśli zadanie zostało przypisane do urządzeń, na których zainstalowano Agenty sieciowe.

- **Przy użyciu zasobów systemu operacyjnego przez Serwer administracyjny**

  Opcja jest przestarzała. Zamiast tego użyj opcji **Przy użyciu Agenta sieciowego** lub **Przy użyciu zasobów systemu operacyjnego poprzez punkty dystrybucji**.

  Pliki są przesyłane do urządzeń klienckich przy użyciu narzędzi systemu operacyjnego Serwera administracyjnego. Możesz włączyć tę opcję, jeśli na urządzeniu klienckim nie ma zainstalowanego Agenta sieciowego, ale urządzenie klienckie jest w tej samej sieci, co Serwer administracyjny.

- **Przy użyciu zasobów systemu operacyjnego poprzez punkty dystrybucji**

  Pliki są przesyłane do urządzeń klienckich przy użyciu narzędzi systemu operacyjnego za pośrednictwem punktów dystrybucyjny. Możesz włączyć tę opcję, jeżeli w sieci jest przynajmniej jeden punkt dystrybucyjny.

  Jeśli opcja **Przy użyciu Agenta sieciowego** jest włączona, pliki będą dostarczane przy użyciu narzędzi systemu operacyjnego, jeśli narzędzia Agenta sieciowego będą niedostępne.

- **Maksymalna liczba jednoczesnych pobierań**

  Maksymalna dozwolona liczba urządzeń klienckich, do których Serwer administracyjny może jednocześnie przesłać pliki. Im większa ta liczba, tym szybciej aplikacja zostanie odinstalowana, ale obciążenie na Serwerze administracyjnym jest większe.

- **Maksymalna liczba prób dezinstalacji**

  Jeśli podczas wykonywania zadania *Zdalna dezinstalacja aplikacji* programowi Kaspersky Security Center Linux nie uda się zainstalować aplikacji na zarządzanym urządzeniu w obrębie liczby uruchomień instalatora określonych przez parametr, Kaspersky Security Center Linux zatrzyma dostarczanie narzędzia do dezinstalacji na to zarządzane urządzenie i już nie uruchomi instalatora na urządzeniu.

  Parametr **Maksymalna liczba prób dezinstalacji** umożliwia zachowanie zasobów zarządzanego urządzenia, a także zmniejszyć ruch sieciowy (dezinstalacja, uruchomienie pliku MSI i wiadomości o błędach).

  Powtarzające się próby uruchomienia zadania mogą wskazywać na problem na urządzeniu i uniemożliwiać przeprowadzenie dezinstalacji. Administrator powinien rozwiązać problem w określonej liczbie prób dezinstalacji, a następnie uruchomić zadanie ponownie (ręcznie lub zgodnie z terminarzem).

  Jeśli dezinstalacja się nie powiedzie, problem jest uznawany za nierozwiązalny i wszelkie dalsze uruchomienia zadania są postrzegane jako niepotrzebne zużywanie zasobów i ruchu sieciowego.

  Po utworzeniu zadania, licznik prób jest ustawiony na `0`. Każde uruchomienie instalatora, które zwraca błąd na urządzeniu, zwiększa wartość licznika o jeden.

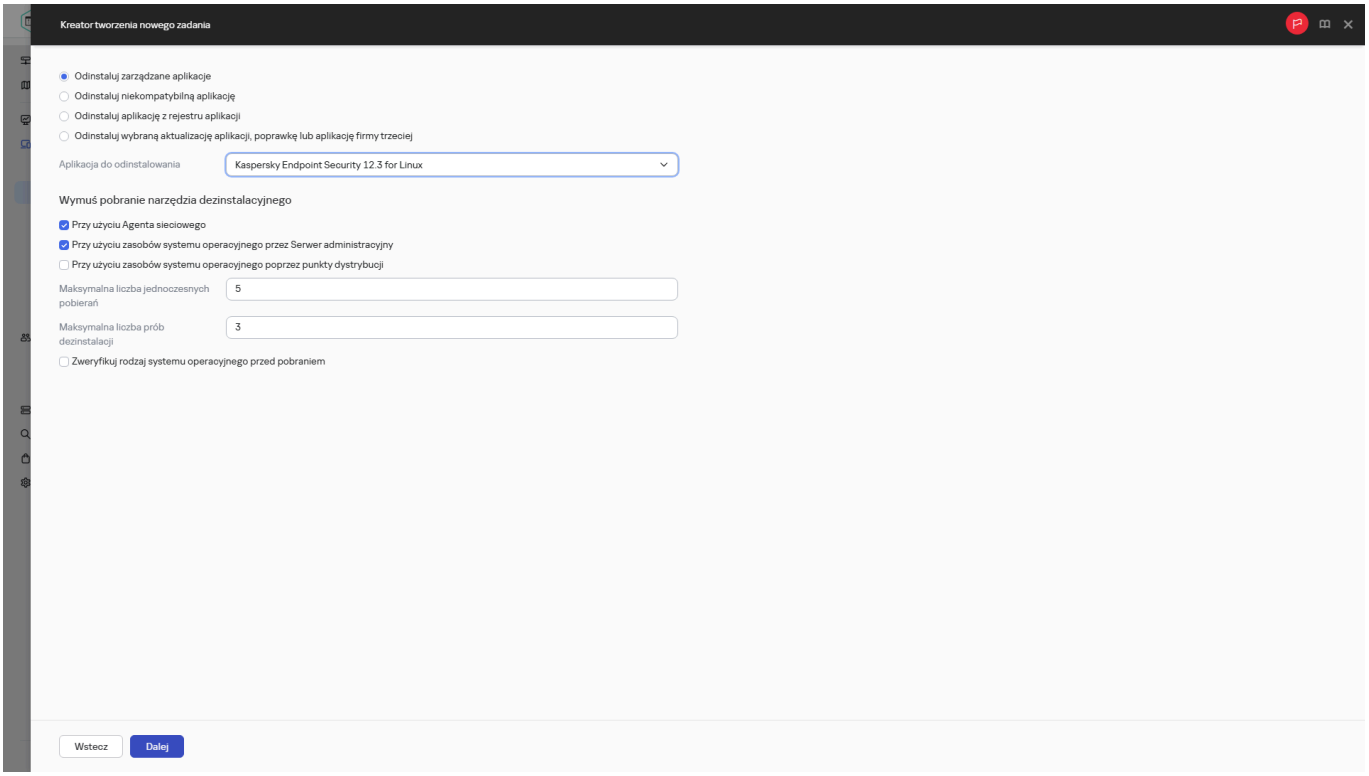
  Jeśli liczba prób określonych w parametrze została przekroczona, a urządzenie jest gotowe do odinstalowania aplikacji, możesz zwiększyć wartość parametru **Maksymalna liczba prób dezinstalacji** i uruchomić zadanie do odinstalowania aplikacji. W razie czego możesz utworzyć nowe zadanie *Zdalna dezinstalacja aplikacji*.

- **Zweryfikuj rodzaj systemu operacyjnego przed pobraniem**

  Przed przesłaniem plików do urządzeń klienckich Kaspersky Security Center Linux sprawdza, czy ustawienia narzędzia instalacyjnego mają zastosowanie do systemu operacyjnego urządzenia klienckiego. Jeśli ustawienia nie są stosowane, Kaspersky Security Center Linux nie przesyła plików i nie próbuje instalować aplikacji. Na przykład, aby zainstalować aplikację na urządzenia grupy administracyjnej, która zawiera urządzenia działające pod kontrolą różnych systemów operacyjnych, możesz przypisać zadanie instalacji do grupy administracyjnej, a następnie włączyć tę opcję, aby pominąć urządzenia, na których jest uruchomiony system operacyjny inny niż wymagany.

  Podczas instalacji zdalnej Agenta Sieciowego na urządzeniach nieprzypisanych, Kaspersky Security Center Linux lub punkt dystrybucji automatycznie określa typ systemu operacyjnego urządzenia niezależnie od ustawienia **Zweryfikuj rodzaj systemu operacyjnego przed pobraniem**.

Przejdź do następnego kroku kreatora.



Określanie ustawień zadania

9. Określ ustawienia ponownego uruchamiania systemu operacyjnego:

- **Nie uruchamiaj ponownie urządzenia**

  Urządzenia klienckie nie są automatycznie uruchamiane ponownie po działaniu. Aby zakończyć działanie, należy uruchomić urządzenie ponownie (na przykład ręcznie lub przy użyciu zadania zarządzania urządzeniem). Informacje o wymaganym ponownym uruchomieniu zostaną zapisane w wynikach zadania oraz w statusie urządzenia. Opcja ta jest odpowiednia dla zadań na serwerach i innych urządzeniach, na których działanie ciągłe jest krytyczne.

- **Uruchom urządzenie ponownie**

  Urządzenia klienckie są zawsze automatycznie uruchamiane ponownie, jeśli jest to wymagane do zakończenia działania. Opcja jest przydatna, gdy zadania są uruchamiane na urządzeniach, na których możliwe są regularne przerwy w działaniu (wyłączenie lub ponowne uruchomienie).

- **Pytaj użytkownika o akcję**

  Na urządzeniu klienckim wyświetlane jest przypomnienie o ręcznym ponownym uruchomieniu urządzenia. Dla tej opcji można zdefiniować pewne ustawienia zaawansowane: treść wyświetlanego komunikatu, częstotliwość wyświetlania wiadomości oraz przedział czasu, po upływie którego ponowne uruchomienie zostanie wymuszone (bez potwierdzenia ze strony użytkownika). Ta opcja jest najodpowiedniejsza dla stacji roboczych, na których użytkownicy muszą mieć możliwość wyboru odpowiedniej godziny ponownego uruchomienia.

  Domyślnie opcja ta jest zaznaczona.

  - **Ponawiaj pytanie co (min)**

  - **Uruchom ponownie po (min)**

- **Wymuś zamknięcie aplikacji dla zablokowanych sesji**

  Uruchomione aplikacje mogą uniemożliwić ponowne uruchomienie urządzenia klienckiego. Na przykład, jeśli dokument jest edytowany w edytorze tekstu i nie zostanie zapisany, aplikacja nie zezwoli na ponowne uruchomienie urządzenia.

  Jeśli ta opcja jest włączona, zostaje wymuszone zamknięcie takich aplikacji na zablokowanym urządzeniu przed jego ponownym uruchomieniem. W wyniku tego działania użytkownicy mogą utracić niezapisane zmiany.

  Jeśli ta opcja jest wyłączona, zablokowane urządzenie nie zostanie uruchomione ponownie. Stan zadania na tym urządzeniu informuje, że wymagane jest ponowne uruchomienie urządzenia. Użytkownicy muszą ręcznie zamknąć wszystkie aplikacje uruchomione na zablokowanych urządzeniach i uruchomić ponownie te urządzenia.

  Domyślnie opcja ta jest wyłączona.

Przejdź do następnego kroku kreatora.

10. Jeśli to konieczne, dodaj konta, które będą używane do uruchamiania zadania zdalnej dezinstalacji:

    - **Konto nie jest wymagane (Agent sieciowy jest zainstalowany)**

      Jeśli ta opcja jest zaznaczona, nie musisz określić konta, z poziomu którego zostanie uruchomiony instalator aplikacji. Zadanie zostanie uruchomione z poziomu konta, z którego uruchomiona jest usługa Serwera administracyjnego.

      Jeśli Agent sieciowy nie został zainstalowany na urządzeniach klienckich, ta opcja nie będzie dostępna.

    - **Konto wymagane (Agent sieciowy nie jest używany)**

      Wybierz tę opcję, jeśli Agent sieciowy nie jest zainstalowany na urządzeniach, do których przypisujesz zadanie *Zdalna dezinstalacja aplikacji*. W takim przypadku możesz określić konto użytkownika lub certyfikat SSH, aby zainstalować aplikację.

      - **Konto lokalne lub domenowe**. Jeśli ta opcja jest zaznaczona, określ konto użytkownika, z poziomu którego zostanie uruchomiony instalator aplikacji. Kliknij przycisk **Dodaj**, wybierz **Konto lokalne lub domenowe**, a następnie określ poświadczenia konta użytkownika.

        Możesz określić wiele kont użytkowników, jeśli na przykład żadne z nich nie ma wszystkich wymaganych uprawnień na wszystkich urządzeniach, do których przypisujesz zadanie. W tym przypadku wszystkie dodane konta są używane do uruchomienia zadania, zaczynając od góry.

      - **Certyfikat SSH**. Jeśli chcesz zainstalować aplikację na urządzeniu klienckim opartym na systemie Linux, możesz określić certyfikat SSH zamiast konta użytkownika. Kliknij przycisk **Dodaj**, wybierz **Certyfikat SSH**, a następnie określ klucze prywatny i publiczny certyfikatu.

        Aby wygenerować klucz prywatny, możesz użyć narzędzia ssh-keygen. Należy zauważyć, że Kaspersky Security Center Linux obsługuje format PEM kluczy prywatnych, ale narzędzie ssh-keygen domyślnie generuje klucze SSH w formacie OPENSSH. Format OPENSSH nie jest obsługiwany przez Kaspersky Security Center Linux. Aby utworzyć klucz prywatny w obsługiwanym formacie PEM, dodaj opcję -m PEM w poleceniu ssh-keygen.

        Na przykład:

        ```
        ssh-keygen -m PEM -t rsa -b 4096 -C "<adres e-mail użytkownika>"
        ```

11. W kroku **Zakończ tworzenie zadania** kreatora, włącz opcję **Otwórz szczegóły zadania po jego utworzeniu**, aby zmodyfikować domyślne ustawienia zadania.

    Jeśli nie włączysz tej opcji, zadanie zostanie utworzone z domyślnymi ustawieniami. Możesz zmodyfikować domyślne ustawienia później.

12. Kliknij przycisk **Zakończ**.

Kreator tworzy zadanie. Jeśli włączyłeś opcję **Otwórz szczegóły zadania po jego utworzeniu**, automatycznie zostanie otwarte okno właściwości zadania. W tym oknie możesz określić ogólne ustawienia zadania oraz w razie potrzeby zmienić ustawienia określone podczas tworzenia zadania.

> Możesz także otworzyć okno właściwości zadania, klikając nazwę utworzonego zadania na liście zadań.

Zadanie zostanie utworzone, skonfigurowane i będzie wyświetlane na liście zadań w sekcji **Zadania**.

13. Aby uruchomić zadanie, na liście zadań wybierz zadanie i kliknij przycisk **Uruchom**.

    Możesz także ustawić harmonogram uruchamiania zadania na karcie **Terminarz** w oknie właściwości zadania.

    Szczegółowy opis ustawień zaplanowanego uruchomienia znajduje się w ogólnych ustawieniach zadania.

Po wykonaniu zadania, wybrana aplikacja zostanie usunięta z wybranych urządzeń.

Problemy związane ze zdalną instalacją

Czasami podczas zdalnego usuwania aplikacji innych firm można napotkać ostrzeżenie: „Zdalna dezinstalacja została zakończona na tym urządzeniu z ostrzeżeniami: Aplikacja do usunięcia nie jest zainstalowana". Problem ten występuje, gdy aplikacja przeznaczona do odinstalowania została już odinstalowana lub została zainstalowana wyłącznie dla pojedynczego użytkownika. Aplikacje zainstalowane dla pojedynczego użytkownika (nazywane również aplikacjami dla konkretnego użytkownika) stają się niewidoczne i nie mogą być odinstalowanie zdalnie, jeśli użytkownik nie jest zalogowany.

Takie zachowanie różni się od z zachowania aplikacji przeznaczonych do użytku przez wielu użytkowników na tym samym urządzeniu (nazywanych także aplikacjami na urządzenie). Aplikacje na urządzenie są widoczne i dostępne dla wszystkich użytkowników urządzenia.

W związku z tym aplikacje dla konkretnego użytkownika należy odinstalowywać tylko wtedy, gdy użytkownik jest zalogowany.

Źródła informacji o zainstalowanych aplikacjach

Agent sieciowy pobiera informacje o oprogramowaniu zainstalowanym na urządzeniach z systemem Windows z następujących kluczy rejestru:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall

  Zawiera informacje o aplikacjach zainstalowanych dla wszystkich użytkowników.

- HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall

  Zawiera informacje o aplikacjach zainstalowanych dla wszystkich użytkowników.

- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Uninstall

  Zawiera informacje o aplikacjach zainstalowanych dla bieżącego użytkownika.

- HKEY_USER<...>\Software\Microsoft\Windows\CurrentVersion\Uninstall

  Zawiera informacje o aplikacjach zainstalowanych dla konkretnych użytkowników.

Przygotowanie urządzenia z systemem Windows do zdalnej instalacji

Zdalna instalacja aplikacji na urządzeniu klienckim może zakończyć się błędem z następujących powodów:

- Zadanie to było już wykonane na tym urządzeniu i zakończyło się powodzeniem.

  W tym przypadku zadanie nie musi być wykonywane ponownie.

- W momencie uruchamiania zadania urządzenie było wyłączone.

  W tym przypadku wyłącz urządzenie i ponownie uruchom zadanie.

- Nie istnieje połączenie między Serwerem administracyjnym a Agentem sieciowym zainstalowanym na urządzeniu klienckim.

  Aby określić przyczynę wystąpienia tego problemu, użyj narzędzia do zdalnej diagnostyki urządzeń klienckich (klactgui).

- Jeśli na urządzeniu nie ma zainstalowanego Agenta sieciowego, podczas zdalnej instalacji mogą wystąpić następujące problemy:

  - Na urządzeniu klienckim jest włączona opcja **Wyłącz proste udostępnianie plików**.
  - Na urządzeniu klienckim nie jest uruchomiona usługa serwera.
  - Na urządzeniu klienckim zamknięte są wymagane porty.
  - Konto, z poziomu którego wykonywane jest zadanie, ma niewystarczające uprawnienia.

  Aby uniknąć problemów, które mogą wystąpić podczas instalacji aplikacji na urządzeniu klienckim bez zainstalowanego Agenta sieciowego, należy postępować zgodnie z opisem procedury wymuszonego wdrożenie przy użyciu zadania zdalnej instalacji z Kaspersky Security Center Linux.

Wcześniej wykorzystywano narzędzie riprep, aby przygotować urządzenie do zdalnej instalacji. Obecnie uważa się, że jest to przestarzała metoda konfiguracji systemów operacyjnych. Narzędzie riprep nie jest zalecane do stosowania w systemach operacyjnych nowszych niż Windows XP i Windows Server 2003 R2.

Tworzenie zadania zdalnego wykonywania skryptów

Możesz utworzyć zadanie *Zdalne wykonanie skryptu* aby wykonać pakiet instalacyjny na urządzeniu klienckim i zdalnie zainstalować aplikację.

Pakiet instalacyjny zawiera archiwum ZIP z zestawem skryptów do wykonania na urządzeniach klienckich oraz plik manifest.json. Więcej informacji na temat tworzenia tego typu pakietu instalacyjnego znajdziesz w tym artykule.

To zadanie należy uruchomić tylko na urządzeniach z Agentem sieciowym dla systemu Linux.

Aby uruchomić zadanie Zdalne wykonanie skryptu:

1. Przejdź do **Kreator tworzenia nowego zadania** i wybierz typ zadania **Zdalne wykonanie skryptu**.

2. Wpisz nazwę zadania i wybierz urządzenia, do których zostanie przypisane zadanie. Kliknij przycisk **Dalej**.

3. Wybierz pakiet instalacyjny oparty na archiwum ZIP z plikiem manifest.json do zdalnego wykonania.

   Jeśli nie chcesz ponownie uruchamiać zadania na urządzeniach, na których zostało już zakończone, włącz opcję **Nie uruchamiaj tego zadania na urządzeniach, na których zostało ono już ukończone**.

4. Wybierz konto, aby uruchomić zadanie.

   Jeżeli wybierzesz konto domyślne, zadanie wykona Agent sieciowy (konto root).

   > Po uruchomieniu zadania *Zdalne wykonanie skryptu* nie można zmienić konta, do którego jest ono przypisane. Aby zmienić konto, do którego przypisane jest zadanie, zatrzymaj zadanie w ustawieniach zadania i utwórz je ponownie z prawidłowymi szczegółami konta.

5. Jeśli chcesz zmodyfikować domyślne ustawienia zadania, włącz opcję **Otwórz szczegóły zadania po jego utworzeniu** na stronie **Zakończ tworzenie zadania**. Jeśli nie włączysz tej opcji, zadanie zostanie utworzone z domyślnymi ustawieniami. Możesz zmodyfikować domyślne ustawienia później w dowolnym momencie.

6. Kliknij przycisk **Zakończ**.

   Zadanie *Zdalne wykonywanie skryptów* zostanie utworzone i będzie wyświetlane na liście zadań.

> Po odebraniu danych z zadania *Zdalne wykonywanie skryptów* Agent sieciowy ogranicza dostęp do otrzymanych danych wszystkim użytkownikom z wyjątkiem administratora i użytkownika określonego w ustawieniach zadania.

Tworzenie pakietu instalacyjnego na podstawie pliku manifestu

Aby utworzyć pakiet instalacyjny na podstawie pliku manifestu:

1. W menu głównym przejdź do **Zarządzanie oprogramowaniem** → **Pakiety instalacyjne**.

   Zostanie wyświetlona lista pakietów instalacyjnych dostępnych na Serwerze administracyjnym.

2. Kliknij **Dodaj**.

   Zostanie uruchomiony Kreator tworzenia nowego pakietu. Przejdź przez kroki kreatora, korzystając z przycisku **Dalej**.

3. Wybierz opcję **Utwórz pakiet instalacyjny dla zadania Zdalne wykonanie skryptu na podstawie archiwum ZIP z plikiem manifest.json**.

4. Podaj nazwę pakietu i kliknij przycisk **Przeglądaj**.

   W oknie, które zostanie otwarte, wybierz plik do utworzenia pakietu instalacyjnego.

5. Wybierz plik archiwum znajdujący się na dostępnych dyskach. Z tego artykułu dowiesz się, jak przygotować archiwum do tego zadania.

   Rozpocznie się przesyłanie pliku na Serwer administracyjny Kaspersky Security Center Linux.

Zostanie uruchomiony proces tworzenia pakietu instalacyjnego.

Kreator informuje, gdy proces zostanie zakończony.

Jeśli pakiet instalacyjny nie zostanie utworzony, zostanie wyświetlona odpowiednia wiadomość.

6. W celu zakończenia działania kreatora kliknij przycisk **Zakończ**.

Pakiet instalacyjny, który utworzyłeś, zostanie pobrany do podfolderu Packages folderu współdzielonego Serwera administracyjnego. Po pobraniu, pakiet instalacyjny pojawi się na liście pakietów instalacyjnych.

Na liście pakietów instalacyjnych dostępnych na Serwerze administracyjnym możesz kliknąć odnośnik z nazwą niestandardowego pakietu instalacyjnego:

- Wyświetl następujące właściwości pakietu instalacyjnego:
  - **Nazwa.** Nazwa niestandardowego pakietu instalacyjnego.
  - **Źródło.** Nazwa producenta aplikacji.
  - **Wersja.** Wersja aplikacji.
  - **Utworzono.** Data utworzenia pakietu instalacyjnego.
  - **Zmodyfikowano.** Data modyfikacji pakietu instalacyjnego.
  - **Ścieżka dostępu.** Ścieżka do niestandardowego pakietu instalacyjnego na Serwerze administracyjnym.
- Zmień nazwę pakietu instalacyjnego i parametry wiersza poleceń. Ta funkcja jest dostępna tylko dla pakietów, które nie są tworzone na podstawie aplikacji Kaspersky.

Przygotowanie archiwum dla zadania Zdalne wykonywanie skryptów

Archiwum dla zadania *Zdalne wykonanie skryptu* w oparciu o plik manifest.json musi spełniać następujące wymagania:

- Format archiwum: ZIP.
- Całkowity rozmiar: nie więcej niż 1 GB.
- Liczba plików i folderów w archiwum jest nieograniczona.
- Plik manifestu archiwum musi być zgodny ze schematem poniżej i mieć nazwę manifest.json. Schemat jest sprawdzany tylko podczas wykonywania zadania na urządzeniu.

  Schemat JSON pliku manifestu i opis macierzy

  Schemat JSON

```
{
 "$schema": "http://json-schema.org/draft-07/schema#",
```

```
"title": "Schema for execute scripts task",
 "type": "object",
  "properties": {
      "version": {
          "type": "integer",
          "enum": [1]
      },
      "actions":{
          "type": "array",
          "items": {
              "type": "object",
              "properties": {
                  "type": {
                      "type": "string",
                      "enum": ["execute"]
                  },
                  "path": {
                      "type": "string"
                  },
                  "args": {
                      "type": "string"
                  },
                  "results":{
                      "type": "array",
                      "items": {
                          "type": "object",
                          "properties": {
                              "code": {
                                  "type": "integer",
                                  "minimum": -255,
                                  "maximum": 255
                              },
                              "next":{
                                  "type": "string",
                                  "enum": ["break", "continue"]
                              }
                          },
                          "required": [
                              "code",
                              "next"
                          ]
                      }
                  },
                  "default_next":{
                      "type": "string",
                      "enum": ["break", "continue"]
                  }
              },
              "required": [
                  "type",
                  "path",
                  "default_next"
              ]
          }
      }
  },
  "required": [
      "version",
```

```
        "actions"
    ]
}
```

Przykład pliku manifestu

```
{
  "version": 1,
  "actions": [
    {
      "type": "execute",
      "path": "scripts/run1.cmd",
      "args": "testArg",
      "results": [
        {
          "code": 0,
          "next": "continue"
        }
      ],
      "default_next": "break"
    },
    {
      "type": "execute",
      "path": "scripts/run2.cmd",
      "results": [
        {
          "code": 0,
          "next": "continue"
        }
      ],
      "default_next": "break"
    },
    {
      "type": "execute",
      "path": "scripts/run3.cmd",
      "results": [
        {
          "code": 0,
          "next": "continue"
        }
      ],
      "default_next": "break"
    }
  ]
}
```

- Archiwum musi mieć następującą strukturę:

  `manifest.json`

  `<file1>`

  `<file2>`

  `<folder1>/<file3>`

  `<folder2>/<folder3>/<file4>`

  `...`

  `<fileX>`

  manifest.json to plik manifestu zadania.

`<file1>, ...., <fileX>` to zestaw plików ze skryptami do wykonania.

Zdalne instalowanie aplikacji na urządzeniach za pomocą zadania Zdalne wykonywanie skryptów

Zadanie *Zdalne wykonanie skryptu* umożliwia zdalną instalację aplikacji na urządzeniu klienckim poprzez utworzenie niestandardowego pakietu instalacyjnego.

Z tego artykułu dowiesz się, jak przygotować archiwum do tego zadania.

Aby utworzyć pakiet instalacyjny do zdalnej instalacji aplikacji na urządzeniu klienckim, w archiwum, które chcesz załadować w ramach tego zadania, muszą znajdować się następujące pliki:

- `< nazwa pakietu>`.deb
- **install.sh**

  ```
  sudo apt-get install < nazwa pakietu >.deb
  ```

- **manifest.json**

  Schemat JSON do zdalnej instalacji aplikacji

  ```
  {
    "version": 1,
    "actions": [
      {
        "type": "execute",
        "path": "install.sh",
        "args": "< wprowadź argumenty w razie konieczności >",
        "results": [
          {
            "code": 0,
            "next": "continue"
          }
        ],
        "default_next": "break"
      }
    ]
  }
  ```

  Opis tablic

  1. `version`—wersja pliku manifestu i zadania.

     Obecnie jedyną akceptowalną wartością jest 1.

  2. Elementy tablicy `actions` określają skład i kolejność skryptów wykonywanych w zadaniu.

     Kolejność wykonywania skryptu odpowiada indeksowi (miejscu) elementu w tablicy.

3. Dla każdego elementu tablicy `actions` definiowane są następujące elementy.

   a. `type`—typ wykonywalnego polecenia ze skryptów. Obecnie wartość jest zawsze `execute`.

   b. `path`—ścieżka do pliku skryptu w archiwum.

   c. `args`—argumenty przekazywane do skryptu jako część wykonywalnego polecenia.

   d. `results`—tablica określająca dalsze działania w zależności od wyniku zadania.

      1. `code`—wartość zwracająca skrypt.

      2. `next`—czynność do wykonania w następnej kolejności. Akcja `continue` powoduje wykonanie następnego skryptu (element w tablicy `actions`); akcja `break` zatrzymuje zadanie.

   e. `default_next`—akcja, jeśli skrypt zwróci wartość, która nie jest zawarta w `results`.

Po uruchomieniu zadania *Zdalne wykonanie skryptu* Agent sieciowy prześle pakiet instalacyjny z aplikacją na urządzenie klienckie. Gdy urządzenie klienckie odbierze pakiet instalacyjny, Agent sieciowy na tym urządzeniu analizuje plik manifest.json i w zależności od wyniku określa kolejność wykonywania skryptów i akcji, a następnie rozpoczyna wykonywanie.

Po zakończeniu zadania *Zdalne wykonanie skryptu* aplikacja zostanie zainstalowana na urządzeniu klienckim.

Konfigurowanie powiadomień i monitorowania dla zadania Zdalne wykonywanie skryptów

Możesz skonfigurować monitorowanie, zachowanie zapisywania zdarzeń i powiadomienia dla zadania *Zdalne wykonanie skryptu*.

Aby Zdalne wykonanie skryptu:

1. W menu głównym przejdź do **Zadania**.

   Zostanie wyświetlona lista zadań.

2. Wybierz zadanie i kliknij **Historia urządzenia**.

   Wyświetlany jest postęp zadania.

Aby skonfigurować zachowanie zapisywania zdarzeń:

1. Na liście zadań kliknij zadanie i przejdź do zakładki **Ustawienia**.

2. W sekcji **Powiadomienia** kliknij przycisk **Ustawienia**.

3. Wybierz jedną z poniższych opcji zachowania aplikacji po zakończeniu zadania:

   - **Zapisz wszystkie zdarzenia**.

   - **Zapisz zdarzenia dotyczące postępu zadania**.

   - **Zapisz jedynie wyniki wykonywania zadania**.

     Zdarzenia zapisywane są w **Historia urządzenia** i **Repozytorium zdarzeń**.

Domyślnie zapisywane są tylko wyniki wykonania zadania.

> Jeśli wybierzesz opcję **Zapisz wszystkie zdarzenia**, zapisane zostaną jedynie wyniki wykonania zadania.

4. Jeśli chcesz zapisywać zdarzenia w bazie danych Serwera administracyjnego, w dzienniku zdarzeń na Serwerze administracyjnym lub na urządzeniu, włącz odpowiednią opcję.

Więcej o konfigurowaniu powiadomień dowiesz się z tego artykułu.

Licencjonowanie

Ta sekcja zawiera następujące informacje:

- Ogólne pojęcia związane z licencjonowaniem oprogramowania Kaspersky Security Center Linux
- Instrukcje dotyczące zarządzania licencjami zarządzanych aplikacji Kaspersky

Licencjonowanie Kaspersky Security Center Linux

Ta sekcja zawiera opis dotyczący ogólnych zasad związanych z licencjonowaniem Kaspersky Security Center Linux.

Informacje o Umowie licencyjnej użytkownika końcowego

Umowa licencyjna użytkownika końcowego to wiążąca umowa prawna zawierana pomiędzy Tobą a firmą AO Kaspersky Lab, która określa zasady korzystania z zakupionej aplikacji.

Przed rozpoczęciem korzystania z aplikacji uważnie przeczytaj Umowę licencyjną.

Program Kaspersky Security Center Linux i jego komponenty, na przykład, Agent sieciowy, ma swoją własną Umowę licencyjną użytkownika końcowego.

Z warunkami Umowy Licencyjnej Użytkownika Końcowego dla Kaspersky Security Center Linux można zapoznać się, korzystając z następujących metod:

- Podczas instalacji Kaspersky Security Center.
- W dokumencie license.txt, znajdującym się w pakiecie dystrybucyjnym Kaspersky Security Center.
- W dokumencie license.txt, znajdującym się w folderze instalacyjnym Kaspersky Security Center.
- Pobierając plik license.txt ze strony Kaspersky.

Z warunkami Umowy Licencyjnej Użytkownika Końcowego Agenta sieciowego dla systemu Linux można zapoznać się, korzystając z następujących metod:

- Podczas pobierania pakietu dystrybucyjnego Agenta sieciowego z serwerów sieciowych Kaspersky.
- Podczas instalacji Agenta sieciowego dla systemu Linux.
- Czytając dokument license.txt dołączony do pakietu dystrybucyjnego Agenta sieciowego dla systemu Linux.
- Czytając dokument license.txt w folderze instalacyjnym Agenta sieciowego dla systemu Linux.
- Pobierając plik license.txt ze strony Kaspersky.

Akceptujesz warunki Umowy licencyjnej użytkownika końcowego, zaznaczając odpowiednią opcję podczas instalacji aplikacji. Jeśli nie akceptujesz warunków Umowy licencyjnej, anuluj instalację aplikacji i nie używaj aplikacji.

Informacje o licencji

Licencja to czasowo ograniczone prawo do korzystania z Kaspersky Security Center Linux nadane zgodnie z warunkami Umowy licencyjnej (Umowa licencyjna użytkownika końcowego).

Zakres świadczonych usług oraz okres ważności zależą od licencji do korzystania z aplikacji.

Dostępne są następujące typy licencji:

- *Wersja próbna*

  Darmowa licencja udostępniana w celu zapoznania się z aplikacją. Licencja testowa ma zazwyczaj krótki okres ważności.

  Jeśli licencja testowa wygaśnie, wszystkie funkcje Kaspersky Security Center Linux zostają wyłączone. Aby kontynuować korzystanie z aplikacji, należy zakupić licencję komercyjną.

  Z aplikacji można korzystać w ramach licencji próbnej tylko przez jeden okres próbny.

- *Wersja komercyjna*

  Płatna licencja.

  Po wygaśnięciu licencji komercyjnej kluczowe funkcje aplikacji zostają wyłączone. Aby kontynuować korzystanie z Kaspersky Security Center, musisz odnowić swoją licencję komercyjną. Po wygaśnięciu licencji komercyjnej nie można kontynuować korzystania z aplikacji i należy ją usunąć z urządzenia.

  Zalecamy odnowienie licencji przed jej wygaśnięciem, aby zapewnić stałą ochronę przed wszystkimi zagrożeniami.

Informacje o certyfikacie licencji

Certyfikat licencyjny to dokument, który otrzymujesz wraz z plikiem klucza lub kodem aktywacyjnym.

Certyfikat licencji zawiera następujące informacje o dostarczonej licencji:

- ID licencji lub numer zamówienia
- Informacje o użytkowniku, który otrzymał licencję
- Informacje o aplikacji, która może być aktywowana za pomocą zakupionej licencji
- Ograniczenie liczby jednostek licencyjnych (np. urządzeń, na których może być używana aplikacja na podstawie dostarczonej licencji)
- Data rozpoczęcia okresu ważności licencji
- Data wygaśnięcia licencji lub okres licencji
- Typ licencji

Informacje o kluczu licencyjnym

Klucz licencyjny jest to sekwencja bitów, które możesz zastosować w celu aktywacji, a następnie użyć aplikacji zgodnie z warunkami Umowy licencyjnej. Klucze licencyjne są generowane przez specjalistów z Kaspersky.

Możesz dodać klucz licencyjny do aplikacji, korzystając z następujących metod: stosując *plik klucza* lub wprowadzając *kod aktywacyjny*. Po dodaniu klucza licencyjnego do aplikacji jest on wyświetlany w interfejsie aplikacji jako unikatowa sekwencja alfanumeryczna.

Klucz licencyjny może zostać zablokowany przez Kaspersky w przypadku naruszenia warunków Umowy licencyjnej. Jeśli klucz licencyjny został zablokowany, aby móc korzystać z aplikacji, musisz dodać inny klucz.

Klucz licencyjny musi być aktywny lub dodatkowy (lub zapasowy).

Aktywny klucz licencyjny to klucz licencyjny, który jest aktualnie używany przez aplikację. Aktywny klucz licencyjny może zostać dodany dla licencji testowej lub komercyjnej. Aplikacja nie może posiadać więcej niż jednego aktywnego klucza licencyjnego.

Dodatkowy (lub zapasowy) klucz licencyjny to klucz licencyjny, który upoważnia użytkownika do korzystania z aplikacji, ale nie jest aktualnie w użyciu. Dodatkowy klucz licencyjny staje się aktywny automatycznie po wygaśnięciu licencji skojarzonej z bieżącym aktywnym kluczem licencyjnym. Dodatkowy klucz licencyjny może zostać dodany tylko wtedy, gdy aktywny klucz licencyjny został już dodany.

Klucz licencyjny dla licencji testowej można dodać tylko jako aktywny klucz licencyjny. Klucz licencyjny dla licencji testowej nie może zostać dodany jako dodatkowy klucz licencyjny.

Przeglądanie Polityki prywatności

Polityka prywatności jest dostępna online pod adresem https://www.kaspersky.com/products-and-services-privacy-policy.

Polityka Prywatności dostępna jest również w trybie offline:

- Możesz przeczytać Politykę prywatności przed zainstalowaniem Kaspersky Security Center.
- Tekst Polityki prywatności znajduje się w pliku license.txt w folderze instalacyjnym Kaspersky Security Center Linux.
- Plik privacy_policy.txt jest dostępny na zarządzanym urządzeniu w folderze instalacyjnym Agenta sieciowego.
- Możesz rozpakować plik privacy_policy.txt z pakietu dystrybucyjnego Agenta sieciowego.

Opcje licencjonowania Kaspersky Security Center

Kaspersky Security Center może pracować w następujących trybach:

- **Podstawowe funkcje Konsoli administracyjnej**

  Kaspersky Security Center działa w tym trybie przed aktywacją aplikacji lub po wygaśnięciu licencji komercyjnej. Kaspersky Security Center z obsługą podstawowej funkcjonalności Konsoli administracyjnej jest dostarczany jako część aplikacji Kaspersky do ochrony sieci firmowych. Można ją również pobrać ze strony firmy Kaspersky.

- **Licencja komercyjna**

  Jeśli potrzebujesz dodatkowej funkcjonalności, która nie jest zawarta w podstawowych funkcjach Konsoli administracyjnej, musisz zakupić licencję komercyjną.

  Podczas dodawania klucza licencyjnego w oknie właściwości Serwera administracyjnego upewnij się, że dodasz klucz licencyjny, który umożliwia użycie Kaspersky Security Center Linux. Możesz odszukać te informacje na stronie internetowej firmy Kaspersky. Każda strona internetowa rozwiązania zawiera listę aplikacji znajdujących się w rozwiązaniu. Serwer administracyjny może akceptować nieobsługiwane klucze licencyjne, na przykład klucz licencyjny dla Kaspersky Endpoint Security Cloud, ale takie klucze licencyjne nie udostępniają żadnych nowych funkcji poza podstawową funkcjonalnością Konsoli administracyjnej.

Funkcja lub właściwość	Tryb pracy Kaspersky Security Center Linux	
	Brak licencji	Licencja komercyjna
Podstawowe funkcje Konsoli administracyjnej Dostępne są następujące funkcje: • Tworzenie wirtualnych Serwerów administracyjnych, które są używane do zarządzania siecią zdalnych biur lub organizacji klientów. • Tworzenie hierarchii grup administracyjnych w celu zarządzania określonymi urządzeniami jako pojedynczą jednostką. • Zdalna instalacja aplikacji. • Scentralizowana konfiguracja aplikacji zainstalowanych na urządzeniach klienckich. • Kontrola stanu ochrony antywirusowej firmy. • Zarządzanie rolami użytkownika. • Statystyki i raporty z działania aplikacji, a także powiadomienia o zdarzeniach krytycznych. • Scentralizowana praca z plikami przeniesionymi do Kwarantanny lub Kopii zapasowej i plikami, których przetwarzanie zostało odroczone. • Zarządzanie szyfrowaniem i ochroną danych. • Wyświetlanie i ręczne modyfikowanie listy komponentów sprzętu wykrytych poprzez przeszukiwanie sieci. • Wyświetlanie listy obrazów systemów operacyjnych dostępnych do zdalnej instalacji.	✓	✓
Zarządzanie lukami i poprawkami: podstawowa funkcjonalność Następujące zadania nie wymagają licencji komercyjnej: • Zadanie *Wyszukiwanie luk i wymaganych aktualizacji* Za pośrednictwem tego zadania Kaspersky Security Center Linux otrzymuje listy wykrytych luk w zabezpieczeniach i wymaganych aktualizacji dla oprogramowania firm trzecich zainstalowanego na zarządzanych urządzeniach. • Tworzenie zadania *Napraw luki* Zadanie *Napraw luki* używa zalecanych poprawek dla oprogramowania firmy Microsoft oraz poprawek użytkownika dla programów innych firm. Aby użyć tego zadania, należy ręcznie określić poprawki użytkownika dla luk wymienionych w ustawieniach zadania.	✓	✓

Funkcja lub właściwość	Tryb pracy Kaspersky Security Center Linux	
	Brak licencji	Licencja komercyjna
Zarządzanie lukami i poprawkami: zaawansowana funkcjonalność Możesz zdefiniować zasady automatycznej zdalnej instalacji aktualizacji oprogramowania i automatycznego usuwania luk.	—	✓
Zarządzanie systemami Dostępne są następujące funkcje: • Możliwość zdalnego połączenia z urządzeniami klienckimi poprzez komponent systemu Microsoft® Windows® o nazwie Podłączanie pulpitu zdalnego. • Nawiązywanie zdalnego połączenia z urządzeniami klienckimi poprzez udostępnianie pulpitu Windows.	—	✓
Eksport zdarzeń do systemów SIEM: z wykorzystaniem protokołu Syslog Korzystając z protokołu Syslog, możesz przekazywać dowolne zdarzenia, które wystąpiły na Serwerze administracyjnym Kaspersky Security Center i w aplikacjach firmy Kaspersky zainstalowanych na zarządzanych urządzeniach. Protokół Syslog jest standardowym protokołem rejestrowania wiadomości. Możesz go użyć do eksportowania zdarzeń do systemu SIEM.	✓	✓
Agregowanie alertów i wykonywanie działań reagowania za pośrednictwem usługi Active Directory, KASAP i Kaspersky TIP Sandbox	—	✓

Informacje o pliku klucza

Plik klucza to plik z rozszerzeniem .key, dostarczony przez firmę Kaspersky. Pliki kluczy zostały zaprojektowane do aktywowania aplikacji poprzez dodanie klucza licencyjnego.

Plik klucza otrzymasz na adres e-mail, który określiłeś podczas zakupu Kaspersky Security Center lub po zamówieniu wersji testowej Kaspersky Security Center.

Aby aktywować aplikację przy użyciu pliku klucza, nie ma konieczności nawiązywania połączenia z serwerami aktywacji Kaspersky.

W sytuacji przypadkowego usunięcia pliku klucza istnieje możliwość jego odzyskania. Plik klucza może być niezbędny, na przykład, do zarejestrowania konta Kaspersky CompanyAccount.

W celu odzyskania pliku klucza, należy wykonać jedną z poniższych czynności:

- Skontaktuj się ze sprzedawcą licencji.
- Uzyskaj plik klucza poprzez stronę internetową Kaspersky, korzystając z dostępnego kodu aktywacyjnego.

Informacje o przekazywaniu danych

Dane przesyłane do firm trzecich

Jeśli korzystasz z funkcji Zarządzania urządzeniami mobilnymi Oprogramowania, do czasowego dostarczenia poleceń na urządzenia działające pod kontrolą systemu operacyjnego Android poprzez mechanizm powiadomień push używana jest usługa Google Firebase Cloud Messaging. Jeżeli Użytkownik skonfigurował korzystanie z usługi Google Firebase Cloud Messaging, Użytkownik zgadza się na przekazanie następujących informacji usłudze Google Firebase Cloud Messaging w trybie automatycznym:

- Identyfikator instancji
- Identyfikator oprogramowania w usłudze Google Firebase Cloud Messaging
- Wersja zainstalowanego oprogramowania
- Pełna wersja oprogramowania
- Wersja Google Play
- Nazwa pakietu dystrybucyjnego oprogramowania
- Wersja schematu dla dostarczonych danych
- Wersja systemu operacyjnego
- Identyfikator oprogramowania

Aby zapobiec wymianie informacji z usługą Google Firebase Cloud Messaging, Użytkownik musi wycofać ustawienia korzystania z usługi Google Firebase Cloud Messaging do wartości fabrycznych.

Jeśli korzystasz z funkcji Zarządzania urządzeniami mobilnymi Oprogramowania, do czasowego dostarczenia poleceń na urządzenia działające pod kontrolą systemu operacyjnego iOS poprzez mechanizm powiadomień push używana jest usługa Apple Push Notification Service (APNs). Jeśli Użytkownik zainstalował certyfikat APNs na serwerze iOS MDM, utworzył profil iOS MDM ze zbiorem ustawień do podłączenia urządzeń mobilnych iOS z Oprogramowaniem i zainstalował ten profil na urządzeniach mobilnych, Użytkownik wyraża zgodę na dostarczenie następujących informacji do APNs w trybie automatycznym:

- Token—push token urządzenia. Serwer używa tego tokena podczas wysyłania powiadomień push do urządzenia.
- PushMagic—ciąg znaków, który musi zostać zawarty w powiadomieniu push. Ta wartość ciągu znaków jest generowana przez urządzenie.

Dane przesyłane do AO Kaspersky Lab

Jeśli Użytkownik ma dostęp do funkcjonalności Kaspersky Extended Detection and Response Optimum, Kaspersky Security Center Linux przesyła dane w następujących przypadkach:

- Aby przypisać pracownikowi szkolenie, Kaspersky Security Center Linux przesyła następujące dane do Kaspersky Automated Security Awareness Platform (KASAP): adres e-mail użytkownika, alternatywny adres e-mail użytkownika (jeśli jest dostępny), identyfikator użytkownika w KASAP, identyfikator grupy szkoleniowej.

- Aby automatycznie wykonywać i wykrywać szkodliwe zachowania za pomocą usługi Kaspersky Cloud Sandbox, zarządzana aplikacja Kaspersky przesyła obiekty poddane kwarantannie oraz pliki utworzone podczas wykonywania przesyłanych obiektów z Serwera administracyjnego za pośrednictwem Agenta sieciowego, a następnie za pośrednictwem Kaspersky Security Center Web Console do usługi Kaspersky Cloud Sandbox.

Dane przetwarzane lokalnie

Kaspersky Security Center Linux służy do scentralizowanego wykonywania podstawowych zadań dotyczących administracji i zarządzania w sieci firmy. Kaspersky Security Center Linux zapewnia administratorowi dostęp do szczegółowych informacji dotyczących poziomu ochrony sieci organizacji; Kaspersky Security Center Linux umożliwia administratorowi skonfigurowanie wszystkich składników ochrony opartych o aplikacje Kaspersky. Kaspersky Security Center Linux wykonuje następujące główne funkcje:

- Wykrywanie urządzeń i ich użytkowników w sieci organizacji

- Tworzenie hierarchii grup administracyjnych dla zarządzania urządzeniem

- Instalowanie aplikacji firmy Kaspersky na urządzeniach

- Zarządzanie ustawieniami i zadaniami zainstalowanych aplikacji

- Zarządzanie aktualizacjami dla aplikacji firmy Kaspersky oraz aplikacji firm trzecich, a także wyszukiwanie i eliminowanie luk

- Aktywowanie aplikacji firmy Kaspersky na urządzeniach

- Zarządzanie kontami użytkowników

- Przeglądanie informacji o działaniu aplikacji firmy Kaspersky na urządzeniach

- Przeglądanie raportów

- Włączanie integracji z usługami Kaspersky

Aby program Kaspersky Security Center Linux mógł wykonywać główne funkcje, może otrzymywać, przechowywać i przetwarzać następujące informacje:

- Informacje o urządzeniach w sieci organizacji uzyskane poprzez skanowanie kontrolerów domeny (Active Directory, Samba, FreeIPA i ALD Pro) lub poprzez skanowanie przedziałów czasu IP. Serwer administracyjny gromadzi dane niezależnie lub pobiera dane z Agenta sieciowego.

- Informacje z kontrolerów domeny (Active Directory, Samba, FreeIPA i ALD Pro) na temat jednostek organizacyjnych, domen, użytkowników i grup. Serwer administracyjny pobiera dane samodzielnie lub otrzymuje dane od Agenta sieciowego przypisanego do pracy jako punkt dystrybucji.

- Szczegóły dotyczące zarządzanych urządzeń. Agent sieciowy przesyła dane wymienione poniżej z urządzenia na Serwer administracyjny. Użytkownik wprowadza wyświetlaną nazwę oraz opis urządzenia w interfejsie Kaspersky Security Center Web Console:

  - Specyfikacje techniczne zarządzanego urządzenia i jego komponentów wymaganych do identyfikacji urządzenia: nazwa i opis urządzenia, nazwa i typ domeny Windows (dla urządzeń należących do domeny Windows), nazwa urządzenia w środowisku Windows (dla urządzeń należących do domeny Windows), Domena DNS i nazwa DNS, adres IPv4, adres IPv6, lokalizacja sieciowa, adres MAC, numer seryjny, typ systemu operacyjnego, czy urządzenie jest maszyną wirtualną wraz z typem hiperwizora oraz czy urządzenie jest dynamiczną maszyną wirtualną w ramach VDI.

  - Inne specyfikacje zarządzanych urządzeń i ich składników wymagane do audytu zarządzanych urządzeń i do podejmowania decyzji odnośnie tego, czy określone poprawki i aktualizacje są stosowane: architektura systemu operacyjnego, dostawca systemu operacyjnego, numer kompilacji systemu operacyjnego, identyfikator wydania systemu operacyjnego, folder lokalizacji systemu operacyjnego, jeśli urządzenie jest maszyną wirtualną — typ maszyny wirtualnej, nazwa wirtualnego Serwera administracyjnego zarządzającego urządzeniem.

  - Szczegóły dotyczące działań na zarządzanych urządzeniach: data i godzina ostatniej aktualizacji, czas, gdy urządzenie było ostatnio widoczne w sieci, stan oczekiwania na ponowne uruchomienie oraz czas, gdy urządzenie było włączone.

  - Szczegóły kont użytkownika na urządzeniu i sesji ich pracy.

- Dane uzyskane podczas zdalnej diagnostyki na zarządzanym urządzeniu: pliki śledzenia, informacje o systemie, szczegóły aplikacji Kaspersky zainstalowanych na urządzeniu, pliki zrzutów, dzienniki zdarzeń, wyniki uruchomienia skryptów diagnostycznych otrzymane od pomocy technicznej Kaspersky.

- Statystyki działania punktu dystrybucji, jeśli urządzenie jest punktem dystrybucji. Agent sieciowy przesyła dane z urządzenia na Serwer administracyjny.

- Ustawienia punktu dystrybucji wprowadzone przez Użytkownika w Kaspersky Security Center Web Console.

- Dane niezbędne do nawiązania połączenia między urządzeniami mobilnymi a Serwerem administracyjnym: certyfikat, port połączenia urządzenia mobilnego, adres połączenia Serwera administracyjnego. Użytkownik wprowadza dane w Kaspersky Security Center Web Console.

- Szczegóły urządzeń mobilnych przesyłane przy użyciu protokołu mobilnego. Dane wymienione poniżej są przesyłane z urządzenia mobilnego na Serwer administracyjny:
  - Informacje o aplikacji: nazwa aplikacji, pełna wersja aplikacji, data i godzina instalacji aplikacji, stan ochrony urządzenia w czasie rzeczywistym, identyfikator sesji.
  - Informacje o kluczach licencyjnych używanych przez aplikację: numer seryjny klucza licencyjnego i typ licencji, status klucza licencyjnego, okres ważności klucza licencyjnego w dniach, data wygenerowania i wygaśnięcia klucza licencyjnego, nazwa firmy, której licencja została dostarczona, dodatkowe informacje, w przypadku korzystania z subskrypcji (flaga subskrypcji, data wygaśnięcia i liczba dni dostępnych na odnowienie subskrypcji, adres internetowy dostawcy subskrypcji oraz bieżący status subskrypcji i przyczyna uzyskania tego statusu), data i godzina aktywacji aplikacji na urządzeniu, data i godzina wygaśnięcia licencji na urządzeniu.
  - Informacje o zarządzanym urządzeniu: nazwa urządzenia, identyfikator urządzenia, typ urządzenia, numer IMEI urządzenia (jeśli jest dostępny), numer seryjny urządzenia (jeśli jest dostępny), producent urządzenia, nazwa rodziny procesorów urządzenia, odcisk palca certyfikatu właściciela urządzenia, typ systemu operacyjnego, wersja systemu operacyjnego, nazwa systemu operacyjnego, całkowita ilość miejsca na dysku urządzenia, nazwa serwera, do którego należy urządzenie, adres IP urządzenia, nazwa grupy urządzeń, nazwa wyróżniająca użytkownika, nazwa wyróżniająca domeny, hasło jednorazowe lub hasło domeny.
  - Informacje o wyniku wykonania poleceń niestandardowych: identyfikator polecenia, status wykonania polecenia, wynik wykonania polecenia; w przypadku polecenia zlokalizowania urządzenia: szerokość geograficzna, długość geograficzna, wysokość i prędkość ruchu urządzenia; w przypadku polecenia Zdjęcie (mugshot): zdjęcia wykonane przednim aparatem urządzenia mobilnego podczas próby odblokowania.
  - Informacje o skanowaniu urządzenia: data i godzina ostatniego skanowania urządzenia; pełna ścieżka w systemie plików, z którego rozpoczęto skanowanie; liczba przeskanowanych obiektów; liczba wykrytych szkodliwych obiektów; liczba zablokowanych, usuniętych i wyleczonych obiektów; liczba obiektów, których nie można było zdezynfekować; liczba błędów walidacji; liczba zakończonych procesów.
  - Informacje o działaniu każdego komponentu aplikacji i o wykonaniu każdego zadania, przedstawione jako zdarzenia:
    - Identyfikator zdarzenia.
    - Istotność.
    - Nazwa i typ zdarzenia.
    - Opis przyczyny zdarzenia.
    - Data i godzina wystąpienia zdarzenia.
    - Informacje o zdarzeniach operacji Anti-Theft (kod odblokowania urządzenia, współrzędne urządzenia, metoda dostarczania poleceń, lista usuniętych danych).
    - Wyniki przetwarzania wykrytego obiektu lub działania (nazwa pliku na urządzeniu; nazwa aplikacji; nazwa zagrożenia; typ zagrożenia; typ działania wykonanego z plikiem; wynik działania; kod błędu, w przypadku wystąpienia).
    - Informacje o uruchomionej regule zgodności (kryterium reguły; zastosowane działanie; opis błędu w zastosowaniu działania, w przypadku wystąpienia).
    - Informacje o błędzie działania aplikacji (wersja aplikacji, wersja systemu operacyjnego, nazwa urządzenia, opis błędu).

    - Informacje o błędzie programu Samsung KNOX (kod błędu, adres URL, z którego nie można pobrać pliku).
    - Informacje o uprawnieniach udzielonych aplikacji.
    - Informacje o każdej aplikacji zainstalowanej na zarządzanym urządzeniu (nazwa aplikacji, status instalacji).
    - Informacje na temat globalnej akceptacji Umowy licencyjnej użytkownika końcowego (EULA): identyfikator EULA, znacznik czasu EULA, tekst EULA.
    - Ustawienia usługi Google Firebase Cloud Messaging: identyfikator nadawcy, identyfikator rejestracji urządzenia.
  - Informacje o publicznym adresie IP urządzenia.
- Szczegóły urządzeń mobilnych przesyłane przy użyciu protokołu iOS MDM. Dane wymienione poniżej są przesyłane z urządzenia mobilnego na Serwer administracyjny:
  - Specyfikacje techniczne urządzenia mobilnego i jego składników wymagane do identyfikacji urządzenia: nazwa urządzenia, model, nazwa systemu operacyjnego, numer wersji i kompilacji, numer modelu urządzenia, numer IMEI, numer telefonu, UDID, MEID, numer seryjny, ilość całkowitej i dostępnej pamięci, wersja oprogramowania firmware modemu, adres MAC Bluetooth, adres MAC Wi-Fi i szczegóły karty SIM (identyfikator ICCID jako część identyfikatora karty SIM).
  - Szczegóły dotyczące sieci komórkowej używanej przez zarządzane urządzenie: typ sieci komórkowej, nazwa aktualnie używanej sieci komórkowej, nazwa domowej sieci komórkowej, wersja ustawień operatora sieci mobilnej, stan roamingu połączeń głosowych i stan roamingu danych, kod kraju sieci domowej, kod kraju zamieszkania, kod kraju aktualnie używanej sieci i poziom szyfrowania.
  - Ustawienia zabezpieczeń urządzenia mobilnego: użycie hasła i jego zgodność z ustawieniami zasad, lista zainstalowanych certyfikatów, aplikacji i profili konfiguracji.
  - Data i godzina ostatniej synchronizacji z Serwerem administracyjnym i stan zarządzania urządzeniem.
- Szczegóły danych urządzenia mobilnego przesłanych za pomocą protokołu WebRTC: obraz ekranu urządzenia.
- Szczegóły plików przeznaczonych do przesłania na urządzenia mobilne. Użytkownik wprowadza dane w interfejsie konsoli Kaspersky Security Center Web Console.
- Szczegóły aplikacji Kaspersky zainstalowanych na urządzeniu. Zarządzana aplikacja przesyła dane z urządzenia na Serwer administracyjny poprzez Agenta sieciowego:
  - Ustawienia aplikacji firmy Kaspersky zainstalowanych na zarządzanym urządzeniu: nazwa i wersja aplikacji firmy Kaspersky, stan ochrony w czasie rzeczywistym, data i godzina ostatniego skanowania, liczba wykrytych zagrożeń, liczba obiektów, których wyleczenie się nie powiodło, dostępność i stan komponentów aplikacji, szczegóły dotyczące zadań i ustawień aplikacji Kaspersky, informacje o aktywnym i zapasowym kluczu licencyjnym, data i identyfikator instalacji aplikacji.
  - Statystyki działania aplikacji: zdarzenia dotyczące zmian w stanie komponentów aplikacji Kaspersky na zarządzanym urządzeniu i wykonywanie zadań zainicjowanych przez komponenty aplikacji.
  - Stan urządzenia zdefiniowany przez aplikację Kaspersky.
  - Znaczniki przypisane przez aplikację Kaspersky.
- Dane znajdujące się w zdarzeniach z komponentów Kaspersky Security Center Linux i zarządzanych aplikacji firmy Kaspersky. Agent sieciowy przesyła dane z urządzenia na Serwer administracyjny.

- Dane niezbędne do integracji Kaspersky Security Center Linux z systemem SIEM w celu eksportowania zdarzeń. Użytkownik wprowadza dane w Kaspersky Security Center Web Console.

- Dane wymagane do integracji Kaspersky Security Center Linux z kontrolerami domeny (Active Directory, Samba, FreeIPA i ALD Pro). Użytkownik wprowadza dane w Kaspersky Security Center Web Console.

- Pliki tabeli kluczy do łączenia się z Kerberosem przy użyciu pojedynczego logowania (SSO). Użytkownik wprowadza dane w Kaspersky Security Center Web Console.

- Dane wymagane do skonfigurowania połączenia z serwerem proxy w celu nawiązania połączenia internetowego. Użytkownik wprowadza dane w Kaspersky Security Center Web Console.

- Ustawienia komponentów Kaspersky Security Center Linux i zarządzanych aplikacji firmy Kaspersky, przedstawionych w zasadach i profilach zasad. Użytkownik wprowadza dane w interfejsie konsoli Kaspersky Security Center Web Console.

- Ustawienia zadania komponentów Kaspersky Security Center Linux i zarządzanych aplikacji firmy Kaspersky. Użytkownik wprowadza dane w interfejsie konsoli Kaspersky Security Center Web Console.

- Dane przetwarzane przez funkcję zarządzania systemem. Agent sieciowy przesyła z urządzenia do Serwera administracyjnego następujące informacje:

  - Informacje o sprzęcie wykrytym na zarządzanych urządzeniach (Rejestr sprzętu).

    Jeżeli Agent sieciowy jest zainstalowany na urządzeniu z systemem Windows, wysyła on do Serwera administracyjnego następujące informacje o sprzęcie urządzenia:

    - Pamięć RAM
    - Urządzenia pamięci masowej
    - Płyta główna
    - Procesor
    - Karty sieciowe
    - Monitory
    - Karta graficzna
    - Karta dźwiękowa

    Jeżeli Agent sieciowy jest zainstalowany na urządzeniu z systemem Linux lub macOS, wysyła on do Serwera administracyjnego następujące informacje o sprzęcie urządzenia, jeżeli informacje te są dostarczane przez system operacyjny:

    - Całkowita ilość pamięci RAM
    - Całkowita pojemność urządzeń pamięci masowej
    - Płyta główna
    - Procesor
    - Karty sieciowe

- Szczegóły dotyczące aplikacji i poprawek zainstalowanych na zarządzanych urządzeniach (Rejestr aplikacji). Aplikacje można porównać z informacjami o plikach wykonywalnych wykrytych na urządzeniach przez funkcję Kontroli aplikacji.

- Szczegóły dotyczące luk w oprogramowaniu innej firmy wykrytych na zarządzanych urządzeniach.

- Szczegóły dotyczące aktualizacji dostępnych dla aplikacji innych firm, zainstalowanych na zarządzanych urządzeniach.

- Dane wymagane do pobrania aktualizacji na izolowanym serwerze administracyjnym w celu naprawienia luk w zabezpieczeniach oprogramowania firm trzecich na zarządzanych urządzeniach. Użytkownik wprowadza i przesyła dane za pomocą narzędzia klscflag serwera administracyjnego.

- Kategorie użytkownika dla aplikacji. Użytkownik wprowadza dane w interfejsie konsoli Kaspersky Security Center Web Console.

- Szczegóły plików wykonywalnych wykrytych na zarządzanych urządzeniach przez funkcję Kontroli aplikacji. Zarządzana aplikacja przesyła dane z urządzenia na Serwer administracyjny poprzez Agenta sieciowego. Pełna lista danych jest dostarczona w plikach pomocy odpowiedniej aplikacji.

- Szczegóły dotyczące plików w Kopii zapasowej. Zarządzana aplikacja przesyła dane z urządzenia na Serwer administracyjny poprzez Agenta sieciowego. Pełna lista danych jest dostarczona w plikach pomocy odpowiedniej aplikacji.

- Szczegóły dotyczące plików w Kwarantannie. Zarządzana aplikacja przesyła dane z urządzenia na Serwer administracyjny poprzez Agenta sieciowego. Pełna lista danych jest dostarczona w plikach pomocy odpowiedniej aplikacji.

- Szczegóły dotyczące plików, o które poprosili specjaliści z Kaspersky, w celu przeprowadzenia szczegółowej analizy. Zarządzana aplikacja przesyła dane z urządzenia na Serwer administracyjny poprzez Agenta sieciowego. Pełna lista danych jest dostarczona w plikach pomocy odpowiedniej aplikacji.

- Szczegóły dotyczące stanu i wyzwolenia reguł Adaptacyjnej kontroli anomalii. Zarządzana aplikacja przesyła dane z urządzenia na Serwer administracyjny poprzez Agenta sieciowego. Pełna lista danych jest dostarczona w plikach pomocy odpowiedniej aplikacji.

- Szczegóły dotyczące urządzeń zewnętrznych (jednostki pamięci, informacje o narzędziach do przenoszenia danych, informacje o narzędziach do drukowania oraz magistrale połączeń), zainstalowane lub podłączone do zarządzanego urządzenia i wykryte przez funkcję Kontroli urządzeń. Zarządzana aplikacja przesyła dane z urządzenia na Serwer administracyjny poprzez Agenta sieciowego. Pełna lista danych jest dostarczona w plikach pomocy odpowiedniej aplikacji.

- Informacje o zaszyfrowanych urządzeniach z systemem Windows i stanie szyfrowania. Zarządzana aplikacja przesyła dane z urządzenia na Serwer administracyjny poprzez Agenta sieciowego.

- Informacje o błędach szyfrowania danych na urządzeniach. Szyfrowanie jest wykonywane przez funkcję Szyfrowanie danych aplikacji Kaspersky. Zarządzana aplikacja przesyła dane z urządzenia na Serwer administracyjny poprzez Agenta sieciowego. Pełna lista danych jest dostarczona w plikach pomocy online odpowiedniej aplikacji.

- Lista zarządzanych programowalnych sterowników logicznych (PLC). Zarządzana aplikacja przesyła dane z urządzenia na Serwer administracyjny poprzez Agenta sieciowego. Pełna lista danych jest dostarczona w plikach pomocy odpowiedniej aplikacji.

- Dane wymagane do utworzenia łańcucha rozprzestrzeniania się zagrożeń. Zarządzana aplikacja przesyła dane z urządzenia na Serwer administracyjny poprzez Agenta sieciowego. Pełna lista danych jest dostarczona w plikach pomocy odpowiedniej aplikacji.

- Informacje o próbach uzyskania przez pracowników organizacji dostępu do usług w chmurze. Zarządzana aplikacja przesyła dane z urządzenia na Serwer administracyjny poprzez Agenta sieciowego. Pełna lista danych jest dostarczona w plikach pomocy odpowiedniej aplikacji.

- Dane wymagane do integracji Kaspersky Security Center z usługą Kaspersky Managed Detection and Response (dedykowana wtyczka musi być zainstalowana dla Kaspersky Security Center Web Console): token inicjujący integrację, token integracji i token sesji użytkownika. Użytkownik wprowadza token inicjujący integrację w interfejsie konsoli Kaspersky Security Center Web Console. Usługa Kaspersky MDR przesyła token integracji i token sesji użytkownika za pośrednictwem dedykowanej wtyczki.

- Dane wymagane do integracji Kaspersky Security Center Linux z Kaspersky Cloud Sandbox i Kaspersky Threat Intelligence Portal (wymaga zainstalowania odpowiedniej wtyczki dla Kaspersky Security Center Web Console): token integracji, token autoryzacji. Użytkownik wprowadza token do integracji w interfejsie Kaspersky Security Center Web Console. Kaspersky Security Center Web Console przesyła token autoryzacji w żądaniu do interfejsu API Kaspersky Cloud Sandbox.

- Dane wymagane do zintegrowania Kaspersky Security Center Linux z usługą Kaspersky Automated Security Awareness Platform (KASAP): token API do dostępu do KASAP Open API, adres URL (odnośnik umożliwiający dostęp do KASAP za pośrednictwem Open API).

- Szczegóły wprowadzonych kodów aktywacyjnych oraz plików kluczy. Użytkownik wprowadza dane w interfejsie konsoli Kaspersky Security Center Web Console.

- Konta użytkowników: nazwa, opis, imię i nazwisko, adres e-mail, główny numer telefonu, hasło, klucz tajny wygenerowany przez Serwer administracyjny oraz hasło jednorazowe do weryfikacji dwuetapowej. Użytkownik wprowadza dane w interfejsie konsoli Kaspersky Security Center Web Console.

- Historia rewizji zarządzanych obiektów. Użytkownik wprowadza dane w interfejsie konsoli Kaspersky Security Center Web Console.

- Adres IP urządzenia, na którym użytkownik utworzył rewizję. Adres IP jest definiowany automatycznie przez Serwer administracyjny.

- Rejestr usuniętych zarządzanych obiektów. Użytkownik wprowadza dane w interfejsie konsoli Kaspersky Security Center Web Console.

- Pakiety instalacyjne utworzone z pliku, a także ustawienia instalacji. Użytkownik wprowadza dane w interfejsie konsoli Kaspersky Security Center Web Console.

- Dane wymagane do wyświetlania ogłoszeń z Kaspersky w Kaspersky Security Center Web Console. Użytkownik wprowadza dane w interfejsie konsoli Kaspersky Security Center Web Console.

- Dane wymagane do działania wtyczek zarządzanych aplikacji w konsoli Kaspersky Security Center Web Console i zapisywane przez wtyczki w bazie danych Serwera administracyjnego podczas ich rutynowego działania. Opis i sposoby podawania danych znajdują się w plikach pomocy odpowiedniej aplikacji.

- Ustawienia użytkownika Kaspersky Security Center Web Console: wersja językowa oraz temat interfejsu, ustawienia wyświetlania panelu Monitorowanie, informacje o stanie powiadomień (Przeczytane / Nieprzeczytane), stan kolumn w arkuszach kalkulacyjnych (Pokaż / Ukryj), postęp trybu Uczenie. Użytkownik wprowadza dane w interfejsie konsoli Kaspersky Security Center Web Console.

- Certyfikaty dla bezpiecznego podłączania zarządzanych urządzeń do komponentów Kaspersky Security Center Linux. Użytkownik wprowadza i przesyła dane za pomocą narzędzia klsetsrvcert serwera administracyjnego.

- Certyfikaty potwierdzające zaufanie do wewnętrznych zasobów sieciowych organizacji. Użytkownik wprowadza dane w interfejsie konsoli Kaspersky Security Center Web Console.

- Informacje o tym, które warunki prawne umowy firmy Kaspersky zostały zaakceptowane przez użytkownika.
- Dane Serwera administracyjnego, które Użytkownik wprowadza w Kaspersky Security Center Web Console lub interfejsie programu Kaspersky Security Center OpenAPI.
- Wszelkie dane, jakie Użytkownik wprowadza w interfejsie konsoli Kaspersky Security Center Web Console.

Dane wymienione powyżej mogą zostać przedstawione w Kaspersky Security Center Linux, jeśli stosowana jest jedna z następujących metod:

- Użytkownik wprowadza dane w interfejsie konsoli Kaspersky Security Center Web Console.
- Agent sieciowy automatycznie pobiera dane z urządzenia i przesyła je na Serwer administracyjny.
- Agent sieciowy pobiera dane otrzymane przez zarządzaną aplikację firmy Kaspersky i przesyła je na Serwer administracyjny. Listy danych przetwarzanych przez zarządzane aplikacje firmy Kaspersky są dostarczane w plikach pomocy dla odpowiednich aplikacji.
- Serwer administracyjny samodzielnie pobiera informacje o urządzeniach sieciowych lub odbiera dane od Agenta sieciowego przypisanego do pracy jako punkt dystrybucji.
- Dane są przesyłane z urządzenia mobilnego do Serwera administracyjnego przy użyciu protokołu iOS MDM lub protokołu mobilnego.

Wymienione dane są przechowywane w bazie danych Serwera administracyjnego. Sumy kontrolne haseł są przechowywane w postaci zaszyfrowanej.

Wszystkie przetworzone lokalnie dane mogą być przesyłane do Kaspersky tylko poprzez pliki zrzutów, pliki śledzenia lub pliki raportów komponentów Kaspersky Security Center Linux, w tym pliki raportów utworzone przez instalatory i narzędzia.

Pliki zrzutu, pliki śledzenia lub pliki dziennika komponentów Kaspersky Security Center Linux zawierają dowolne dane Serwera administracyjnego, Agenta sieciowego i Kaspersky Security Center Web Console. Pliki mogą zawierać dane osobowe lub poufne. Pliki zrzutu, pliki śledzenia lub pliki dziennika są przechowywane na urządzeniach w postaci jawnej. Pliki zrzutu, pliki śledzenia lub pliki dziennika nie są automatycznie przesyłane do Kaspersky, ale administrator może ręcznie przesłać te pliki do Kaspersky na żądanie pomocy technicznej w celu rozwiązania problemów związanych z wydajnością Kaspersky Security Center Linux.

Firma Kaspersky chroni wszelkie zebrane informacje zgodnie z prawem oraz obowiązującymi przepisami stosowanymi w firmie Kaspersky. Dane są przesyłane za pośrednictwem bezpiecznego kanału.

Klikając odnośniki w Kaspersky Security Center Web Console, Użytkownik wyraża zgodę na automatyczne przesyłanie następujących danych:

- Kod Kaspersky Security Center Linux
- Wersja Kaspersky Security Center Linux
- Lokalizacja Kaspersky Security Center Linux
- Identyfikator licencji
- Typ licencji
- Czy licencja została zakupiona u partnera

Lista danych dostarczonych za pośrednictwem odnośników zależy od celu i lokalizacji odnośnika.

Firma Kaspersky wykorzystuje uzyskane dane tylko jako ogólne statystyki. Ogólne statystyki są generowane automatycznie z otrzymanych informacji i nie zawierają żadnych danych osobowych ani poufnych informacji. Jak tylko nowe dane zostaną zebrane, poprzednie dane zostaną usunięte (raz na rok). Statystyki podsumowujące są przechowywane cały czas.

Informacje o subskrypcji

Subskrypcja na Kaspersky Security Center Linux jest to zamówienie aplikacji z wybranymi ustawieniami (data wygaśnięcia subskrypcji, liczba chronionych urządzeń). Możesz zarejestrować swoją subskrypcję na Kaspersky Security Center Linux u swojego dostawcy usługi (na przykład, dostawcy Internetu). Subskrypcja może być odnawiana ręcznie lub automatycznie. Istnieje również możliwość jej anulowania.

Subskrypcja może być ograniczona (na przykład, na jeden rok) lub nieograniczona (bez daty wygaśnięcia). Aby możliwe było kontynuowanie korzystania z Kaspersky Security Center po wygaśnięciu ograniczonej subskrypcji, należy ją odnowić. Nieograniczona subskrypcja jest odnawiana automatycznie, jeśli została opłacona u dostawcy usług w odpowiednim terminie.

Po wygaśnięciu ograniczonej subskrypcji, może zostać zaoferowany okres karencji na odnowienie subskrypcji, w trakcie którego aplikacja będzie dalej działała. Dostępność i czas trwania okresu karencji są definiowane przez dostawcę usługi.

Aby używać Kaspersky Security Center Linux z subskrypcją, należy wprowadzić kod aktywacyjny otrzymany od dostawcy usługi.

Możesz zastosować dla Kaspersky Security Center Linux inny kod aktywacyjny dopiero wtedy, gdy Twoja subskrypcja wygaśnie lub gdy ją anulujesz.

W zależności od dostawcy usługi, zestaw możliwych działań do zarządzania subskrypcją może się różnić. Dostawca usługi może nie zaoferować okresu karencji na odnowienie subskrypcji i wówczas aplikacja przestanie działać.

Kody aktywacyjne zakupione dla subskrypcji nie mogą zostać użyte do aktywowania wcześniejszych wersji Kaspersky Security Center.

Jeśli korzystasz z aplikacji z subskrypcją, Kaspersky Security Center Linux automatycznie próbuje uzyskać dostęp do serwera aktywacji w określonych przedziałach czasu, aż do wygaśnięcia subskrypcji. Jeżeli dostęp do serwera za pomocą systemowego DNS nie jest możliwy, aplikacja korzysta z publicznych serwerów DNS. Możesz odnowić swoją subskrypcję na stronie dostawcy usługi.

Aktywowanie Kaspersky Security Center Linux

Możesz aktywować Kaspersky Security Center Linux, aby korzystać z jego dodatkowych funkcji. Istnieją dwa sposoby wykonania tego zadania: użyj Kreatora wstępnej konfiguracji Serwera administracyjnego lub właściwości Serwera administracyjnego.

W celu aktywowania Kaspersky Security Center Linux:

1. W menu głównym kliknij nazwę Serwera administracyjnego.

   Zostanie otwarte okno właściwości Serwera administracyjnego.

2. Na zakładce **Ogólne** wybierz sekcję **Klucze licencyjne**.

3. W obszarze **Bieżąca licencja** kliknij przycisk **Wybierz**.

4. W oknie, które zostanie otwarte, wybierz klucz licencyjny, którego chcesz użyć do aktywacji Kaspersky Security Center Linux. Jeśli klucza licencyjnego nie ma na liście, kliknij przycisk **Dodaj nowy klucz licencyjny**, a następnie określ nowy klucz licencyjny.

5. W razie potrzeby możesz również dodać zapasowy klucz licencyjny. W tym celu w obszarze **Zapasowy klucz licencyjny** kliknij przycisk **Wybierz**, a następnie wybierz istniejący klucz licencyjny lub dodaj nowy. Pamiętaj, że nie możesz dodać zapasowego klucza licencyjnego, jeśli nie ma aktywnego klucza licencyjnego.

6. Kliknij przycisk **Zapisz**.

Licencjonowanie zarządzanych aplikacji Kaspersky

Ta sekcja opisuje funkcje Kaspersky Security Center związane z pracą z kluczami licencyjnymi dla zarządzanych aplikacji Kaspersky.

Kaspersky Security Center Linux pozwala na wykonywanie scentralizowanego rozsyłania kluczy licencyjnych dla aplikacji Kaspersky na urządzenia klienckie, monitorowanie ich wykorzystania i odnawianie licencji.

Dodając klucz licencyjny przy pomocy Kaspersky Security Center, jego ustawienia są zapisywane na Serwerze administracyjnym. W oparciu o te informacje, aplikacja generuje raport użycia klucza licencyjnego i powiadamia administratora o wygaśnięciu licencji oraz naruszeniu ograniczeń licencyjnych, określonych we właściwościach kluczy licencyjnych. Możesz skonfigurować powiadomienia związane z korzystaniem z kluczy licencyjnych w ustawieniach Serwera administracyjnego.

Licencjonowanie zarządzanych aplikacji

Aplikacje Kaspersky, zainstalowane na zarządzanych urządzeniach, muszą być licencjonowane poprzez zastosowanie pliku klucza lub kodu aktywacyjnego do każdej z aplikacji. Plik klucza lub kod aktywacyjny może zostać rozesłany w następujące sposoby:

- Automatyczne wdrażanie
- Pakiet instalacyjny zarządzanej aplikacji
- Zadanie Dodaj klucz licencyjny dla zarządzanej aplikacji
- Ręczna aktywacja zarządzaną aplikacją

Możesz dodać nowy aktywny lub zapasowy klucz licencyjny za pomocą dowolnej z metod wymienionych powyżej. Aplikacja firmy Kaspersky używa w danej chwili aktywnego klucza i przechowuje klucz rezerwowy do zastosowania po wygaśnięciu aktywnego klucza. Aplikacja, dla której dodajesz klucz licencyjny, określa, czy klucz jest aktywny, czy zapasowy. Definicja klucza nie zależy od metody użytej do dodania nowego klucza licencyjnego.

Automatyczne wdrażanie

Jeśli używasz różnych zarządzanych aplikacji i musisz rozesłać określony plik klucza lub kod aktywacyjny na urządzenia, zdecyduj się na inne sposoby wdrożenia tego kodu aktywacyjnego lub pliku klucza.

Kaspersky Security Center umożliwia automatyczne rozesłanie dostępnych kluczy licencyjnych na urządzenia. Na przykład, trzy klucze licencyjne są przechowywane w repozytorium Serwera administracyjnego. Włączyłeś opcję **Klucz licencyjny rozesłany automatycznie** dla wszystkich trzech kluczy licencyjnych. Aplikacja zabezpieczająca Kaspersky — na przykład Kaspersky Endpoint Security for Linux — jest zainstalowana na urządzeniach w organizacji. Zostanie wykryte nowe urządzenie, do którego musi być rozesłany klucz licencyjny. Aplikacja określi, na przykład, że na urządzenie mogą zostać rozesłane dwa klucze licencyjne z repozytorium: klucz licencyjny o nazwie *Key_1* oraz klucz licencyjny o nazwie *Key_2*. Jeden z tych kluczy licencyjnych zostanie zastosowany na urządzeniu. W tym przypadku nie można przewidzieć, który z dwóch kluczy licencyjnych zostanie wdrożony na urządzeniu, ponieważ automatyczne wdrażanie kluczy licencyjnych nie oferuje administratorowi podejmowania żadnych działań.

Podczas rozsyłania klucza licencyjnego urządzenia są zliczane dla tego klucza licencyjnego. Musisz upewnić się, że liczba urządzeń, na których klucz licencyjny został zastosowany, nie przekracza limitu określonego przez licencję. Jeśli liczba urządzeń przekracza limit określony przez licencję, wszystkie urządzenia, które nie zostały objęte licencją, otrzymają stan *Krytyczny*.

Przed wdrożeniem, plik klucza lub kod aktywacyjny musi zostać dodany do repozytorium Serwera administracyjnego.

Dostępne instrukcje:

- Dodawanie klucza licencyjnego do repozytorium Serwera administracyjnego
- Automatyczne rozsyłanie kluczy licencyjnych

Należy pamiętać, że automatycznie dystrybuowany klucz licencyjny może nie zostać wyświetlony w repozytorium wirtualnego Serwera administracyjnego w następujących przypadkach:

- Klucz licencyjny nie jest ważny dla aplikacji.
- Wirtualny Serwer administracyjny nie ma zarządzanych urządzeń.
- Klucz licencyjny został już użyty dla urządzeń zarządzanych przez inny wirtualny Serwer administracyjny i osiągnięto limit liczby urządzeń.

Dodawanie pliku klucza lub kodu aktywacyjnego do pakietu instalacyjnego zarządzanej aplikacji

Z powodów bezpieczeństwa, ta opcja nie jest zalecana. Plik klucza lub kod aktywacyjny dodane do pakietu instalacyjnego mogą być zagrożone.

Jeśli instalujesz zarządzaną aplikację przy użyciu pakietu instalacyjnego, możesz określić kod aktywacyjny lub plik klucza w tym pakiecie instalacyjnym lub w zasadzie aplikacji. Klucz licencyjny zostanie rozesłany na zarządzane urządzenia podczas kolejnej synchronizacji urządzenia z Serwerem administracyjnym.

Instrukcje: Dodawanie klucza licencyjnego do pakietu instalacyjnego

Wdrażanie poprzez zadanie Dodaj klucz licencyjny dla zarządzanej aplikacji

Jeśli zdecydujesz się na użycie zadania Dodaj klucz licencyjny dla zarządzanej aplikacji, możesz wybrać klucz licencyjny, który musi zostać rozesłany na urządzenia, oraz wybrać urządzenia w dowolny sposób—na przykład, wybierając grupę administracyjną lub wybór urządzeń.

Przed wdrożeniem, plik klucza lub kod aktywacyjny musi zostać dodany do repozytorium Serwera administracyjnego.

Dostępne instrukcje:

- Dodawanie klucza licencyjnego do repozytorium Serwera administracyjnego
- Rozsyłanie klucza licencyjnego na urządzenia klienckie

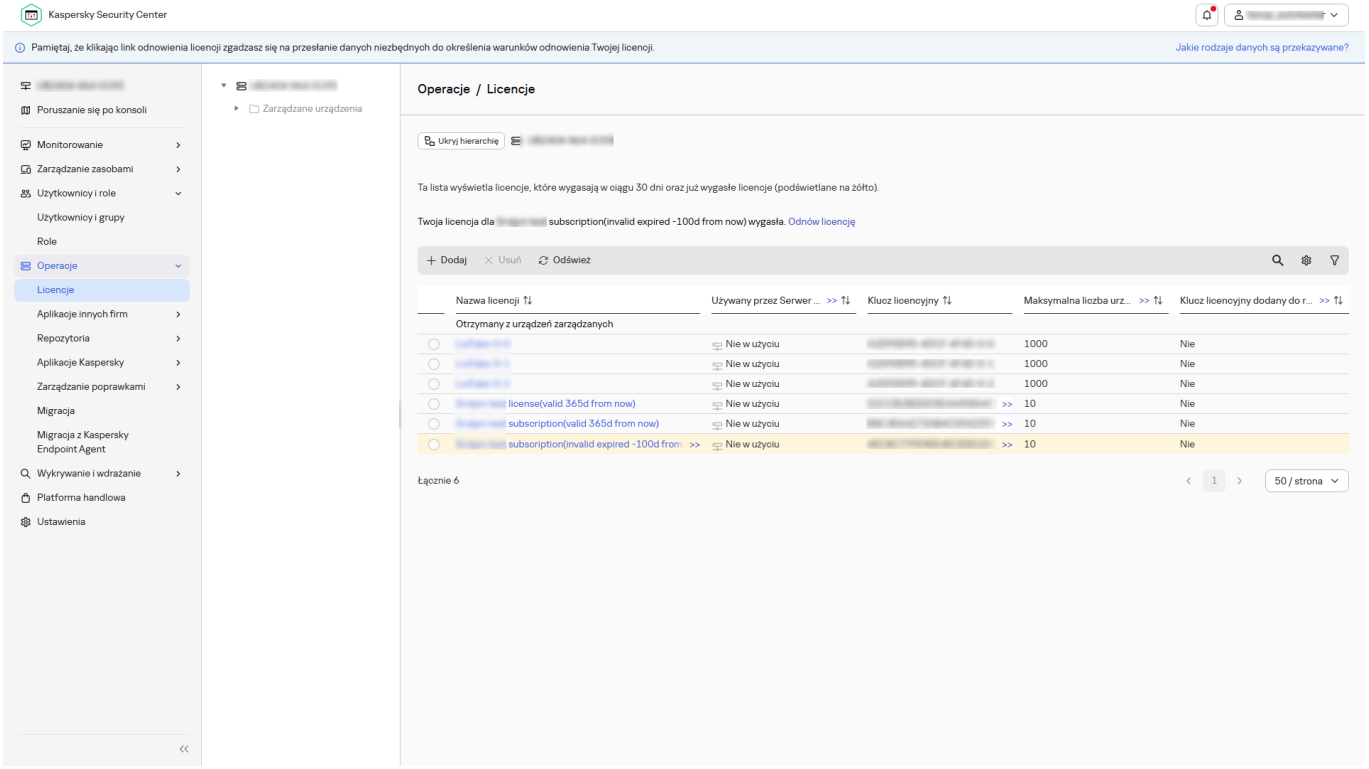
Ręczne dodawanie kodu aktywacyjnego lub pliku klucza do urządzeń

Możesz aktywować zainstalowaną aplikację Kaspersky lokalnie, przy użyciu narzędzi dostępnych w interfejsie aplikacji. Więcej informacji można znaleźć w dokumentacji dla zainstalowanej aplikacji.

Dodawanie klucza licencyjnego do repozytorium Serwera administracyjnego

W celu dodania klucza licencyjnego do repozytorium Serwera administracyjnego:

1. W menu głównym przejdź do **Operacje** → **Licencje**.



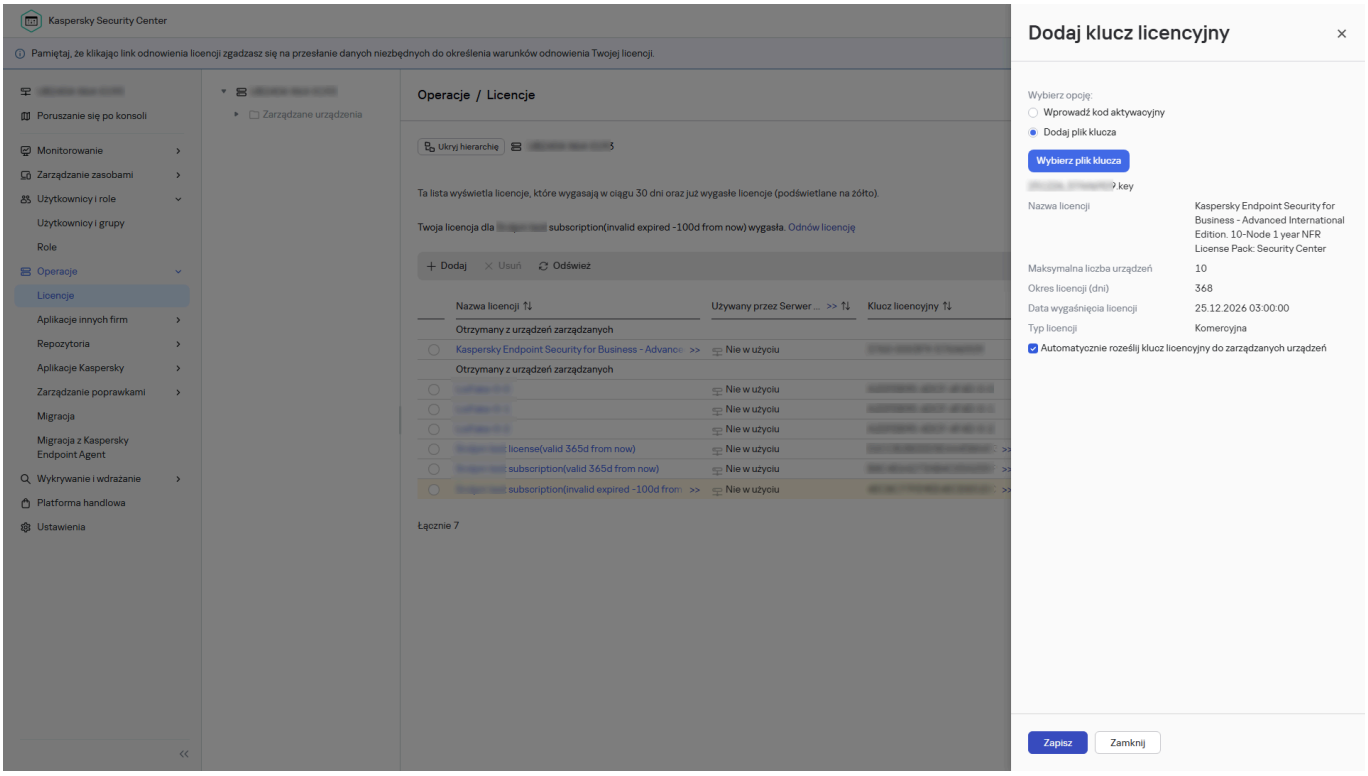
Lista dodanych kluczy licencyjnych Kaspersky

2. Kliknij przycisk **Dodaj**.

3. Wybierz, co chcesz dodać:

- **Dodaj plik klucza**

  Kliknij przycisk **Wybierz plik klucza** i odszukaj plik .key, który chcesz dodać.



Dodanie klucza licencyjnego poprzez zastosowanie pliku klucza

- **Wprowadź kod aktywacyjny**

  Określ kod aktywacyjny w polu tekstowym i kliknij przycisk **Wyślij**.

4. Kliknij przycisk **Zamknij**.

Klucz licencyjny lub kilka kluczy licencyjnych zostaną dodane do repozytorium Serwera administracyjnego.

Rozsyłanie klucza licencyjnego na urządzenia klienckie

Kaspersky Security Center Web Console umożliwia rozesłanie klucza licencyjnego na urządzenia klienckie automatycznie lub przy pomocy zadania **Aktywacja aplikacji**. Za pomocą tego zadania można przydzielić klucze określonej grupie urządzeń. Podczas automatycznego rozsyłania klucza licencyjnego ograniczenie licencyjne dotyczące liczby urządzeń nie jest uwzględniane. Użyj opcji automatycznego rozsyłania kluczy, aby automatycznie zakończyć rozsyłanie klucza licencyjnego po osiągnięciu limitu licencji.

Jeśli włączysz automatyczne rozsyłanie kluczy licencyjnych, nie twórz zadania **Aktywacja aplikacji** w celu rozsyłania kluczy na urządzenia klienckie. W przeciwnym wypadku obciążenie Serwera administracyjnego wzrośnie ze względu na częstą synchronizację.

Przed wdrożeniem należy dodać klucz licencyjny do repozytorium Serwera administracyjnego.

*Aby rozesłać klucz licencyjny do urządzeń klienckich za pomocą zadania **Aktywacja aplikacji**:*

1. W menu głównym przejdź do **Zadania**.

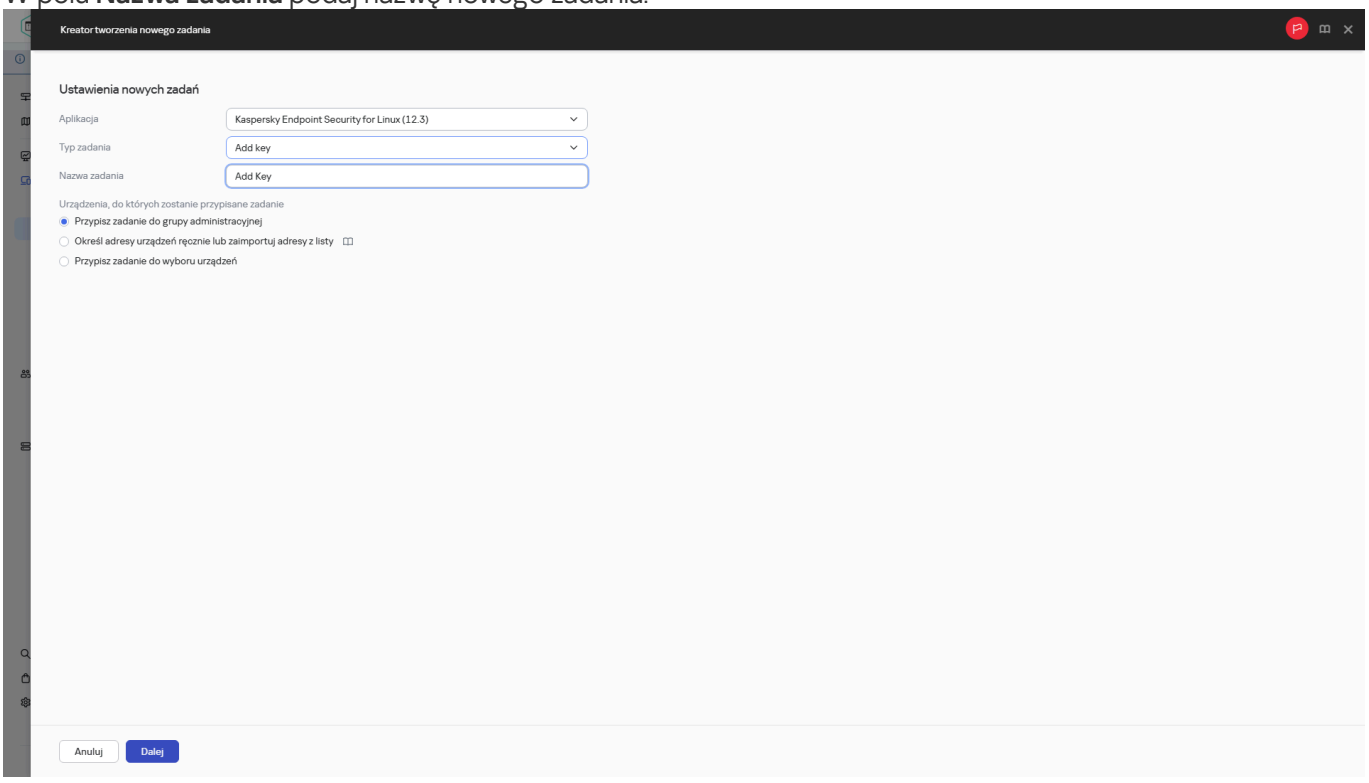
2. Kliknij **Dodaj**.

   Zostanie uruchomiony **Kreator tworzenia nowego zadania**. Przejdź przez kroki kreatora, korzystając z przycisku **Dalej**.

3. Z listy rozwijanej **Aplikacja** wybierz aplikację, do której chcesz dodać klucz licencyjny.

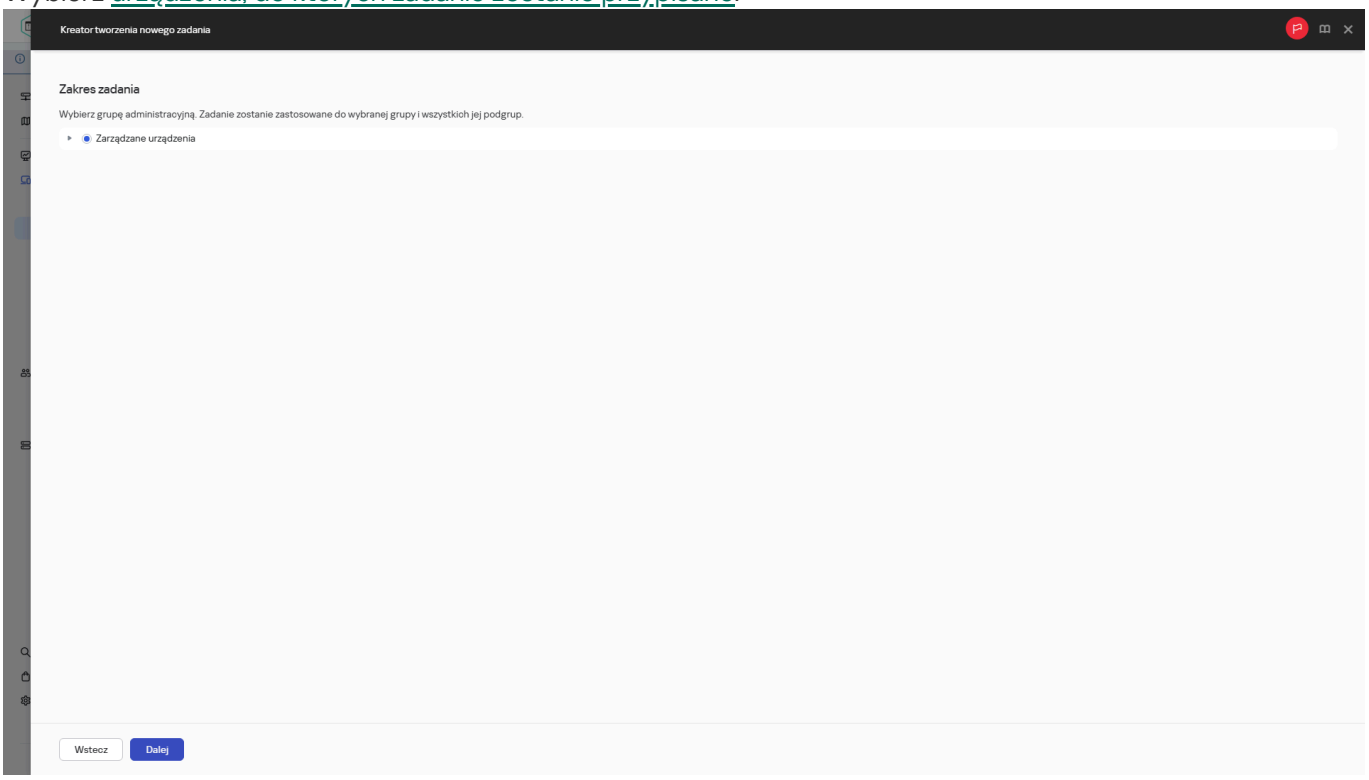
4. Z listy **Typ zadania** wybierz zadanie **Aktywacja aplikacji**.

5. W polu **Nazwa zadania** podaj nazwę nowego zadania.



Tworzenie zadania Dodaj klucz

6. Wybierz urządzenia, do których zadanie zostanie przypisane.



Określanie zakresu zadania

7. Na etapie **Wybór klucza licencyjnego** kreatora kliknij łącze **Dodaj klucz**, aby dodać klucz licencyjny.

8. W oknie dodawania klucza dodaj klucz licencyjny, korzystając z jednej z następujących opcji:

> Musisz dodać klucz licencyjny tylko wtedy, gdy nie dodałeś go do repozytorium Serwera administracyjnego przed utworzeniem zadania /**Aktywacja aplikacji**.

- Wybierz opcję **Wprowadź kod aktywacyjny**, aby wprowadzić kod aktywacyjny, a następnie wykonaj następujące czynności:

  a. Podaj kod aktywacyjny, a następnie kliknij przycisk **Wyślij**.

  Informacja o kluczu licencyjnym pojawi się w oknie dodawania klucza.

  b. Kliknij przycisk **Zapisz**.

  > Jeśli chcesz automatycznie rozsyłać klucz licencyjny do zarządzanych urządzeń, włącz opcję **Automatycznie roześlij klucz licencyjny do zarządzanych urządzeń**.

  Okno dodawania klucza zostanie zamknięte.

- Wybierz opcję **Dodaj plik klucza**, aby dodać plik klucza, a następnie wykonaj następujące czynności:

  a. Kliknij przycisk **Wybierz plik klucza**.

  b. W otwartym oknie wybierz plik klucza, a następnie kliknij przycisk **Otwórz**.

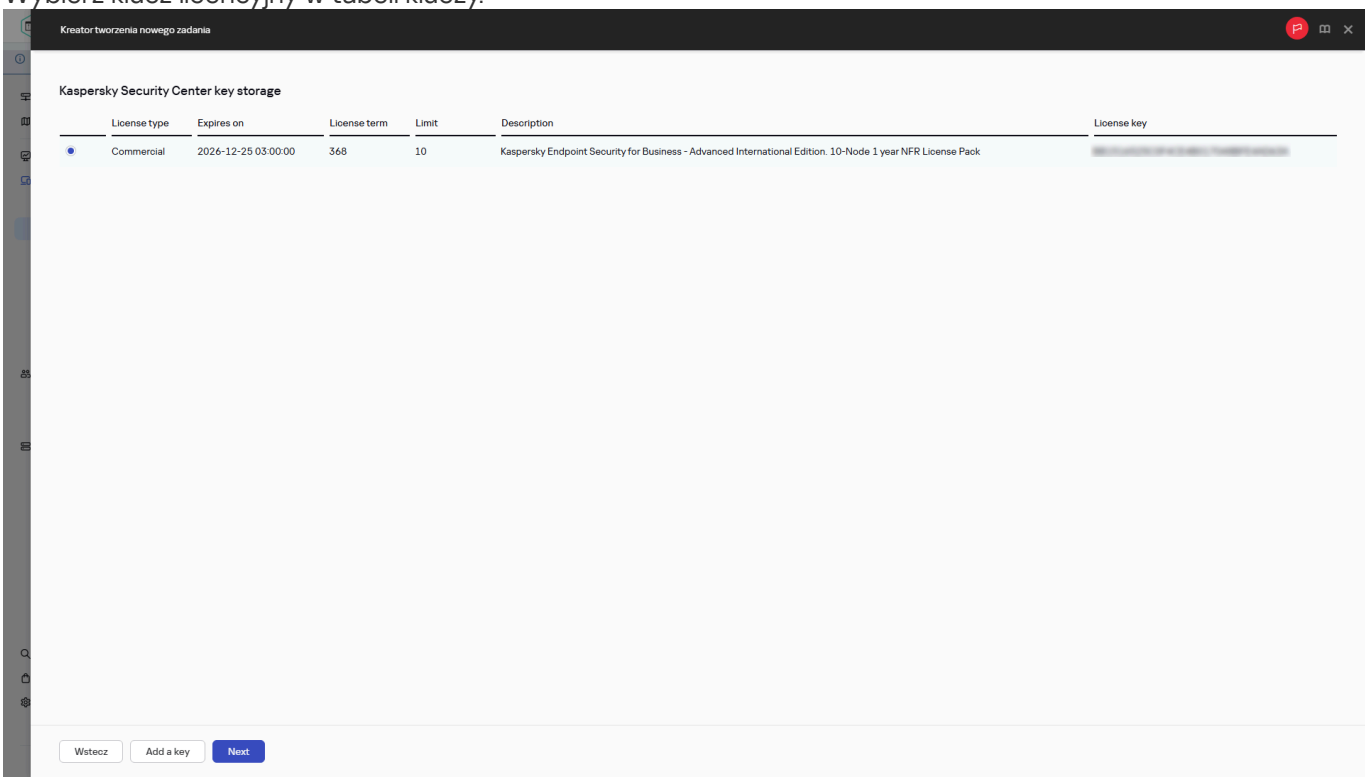
  Informacje o kluczu licencyjnym pojawią się w oknie dodawania klucza licencyjnego.

  c. Kliknij przycisk **Zapisz**.

Jeśli chcesz automatycznie rozsyłać klucz licencyjny do zarządzanych urządzeń, włącz opcję **Automatycznie roześlij klucz licencyjny do zarządzanych urządzeń**.

Okno dodawania klucza zostanie zamknięte.

9. Wybierz klucz licencyjny w tabeli kluczy.

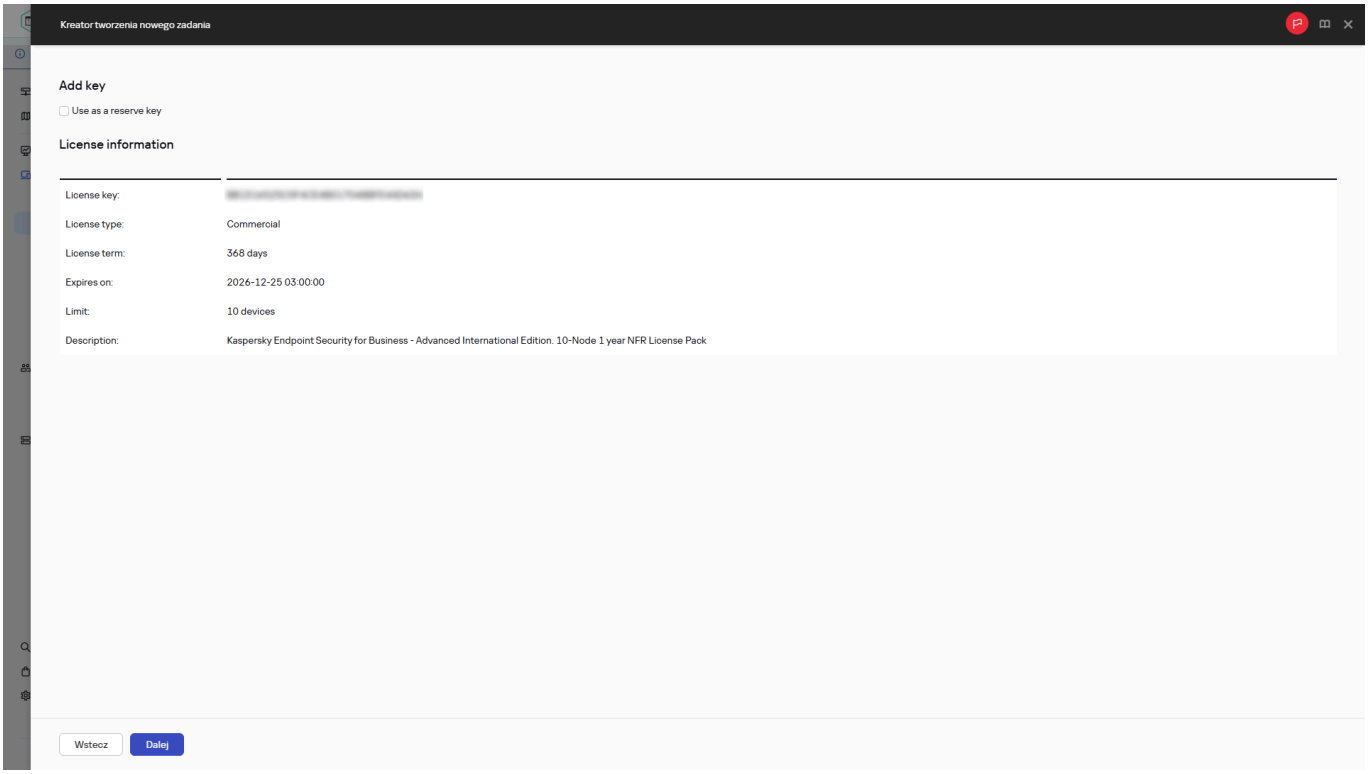


Wybieranie klucza licencyjnego

10. Na etapie **informacji o licencji** kreatora usuń zaznaczenie domyślnego pola wyboru **Użyj jako klucza rezerwowego**, jeśli chcesz zastąpić bieżący aktywny klucz licencyjny.

    Na przykład jest to konieczne w przypadku zmiany organizacji i urządzenie wymaga klucza innej organizacji; lub jeśli klucz został wydany ponownie, a nowa licencja wygasa wcześniej niż bieżąca. Aby uniknąć błędów, odznacz pole wyboru **Użyj jako klucza zapasowego**.

Jeśli chcesz uzyskać więcej informacji o problemach, które mogą wystąpić podczas dodawania klucza licencyjnego do Kaspersky Security Center oraz o sposobach ich rozwiązania, zapoznaj się z bazą wiedzy Kaspersky Security Center.



Określanie zapasowego klucza licencyjnego

11. W kroku **Zakończ tworzenie zadania** kreatora, włącz opcję **Otwórz szczegóły zadania po jego utworzeniu**, aby zmodyfikować domyślne ustawienia zadania.

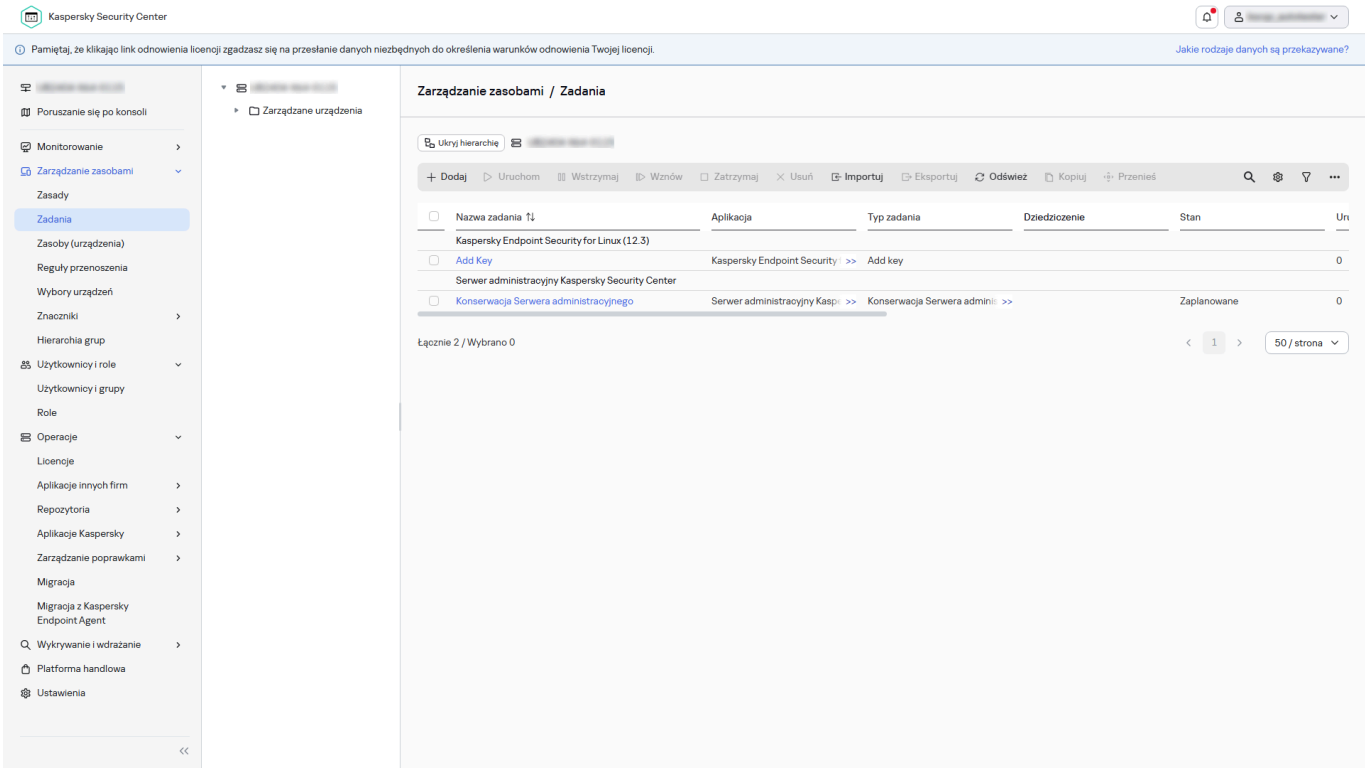
    Jeśli nie włączysz tej opcji, zadanie zostanie utworzone z domyślnymi ustawieniami. Możesz zmodyfikować domyślne ustawienia później.

12. Kliknij przycisk **Zakończ**.

    Kreator tworzy zadanie. Jeśli włączyłeś opcję **Otwórz szczegóły zadania po jego utworzeniu**, automatycznie zostanie otwarte okno właściwości zadania. W tym oknie możesz określić ogólne ustawienia zadania oraz w razie potrzeby zmienić ustawienia określone podczas tworzenia zadania.

    Możesz także otworzyć okno właściwości zadania, klikając nazwę utworzonego zadania na liście zadań.

Zadanie zostanie utworzone, skonfigurowane i będzie wyświetlane na liście zadań.



Lista zadań

13. Aby uruchomić zadanie, na liście zadań wybierz zadanie i kliknij przycisk **Uruchom**.

    Możesz także ustawić harmonogram uruchamiania zadania na karcie **Terminarz** w oknie właściwości zadania.

    Szczegółowy opis ustawień zaplanowanego uruchomienia znajduje się w ogólnych ustawieniach zadania.

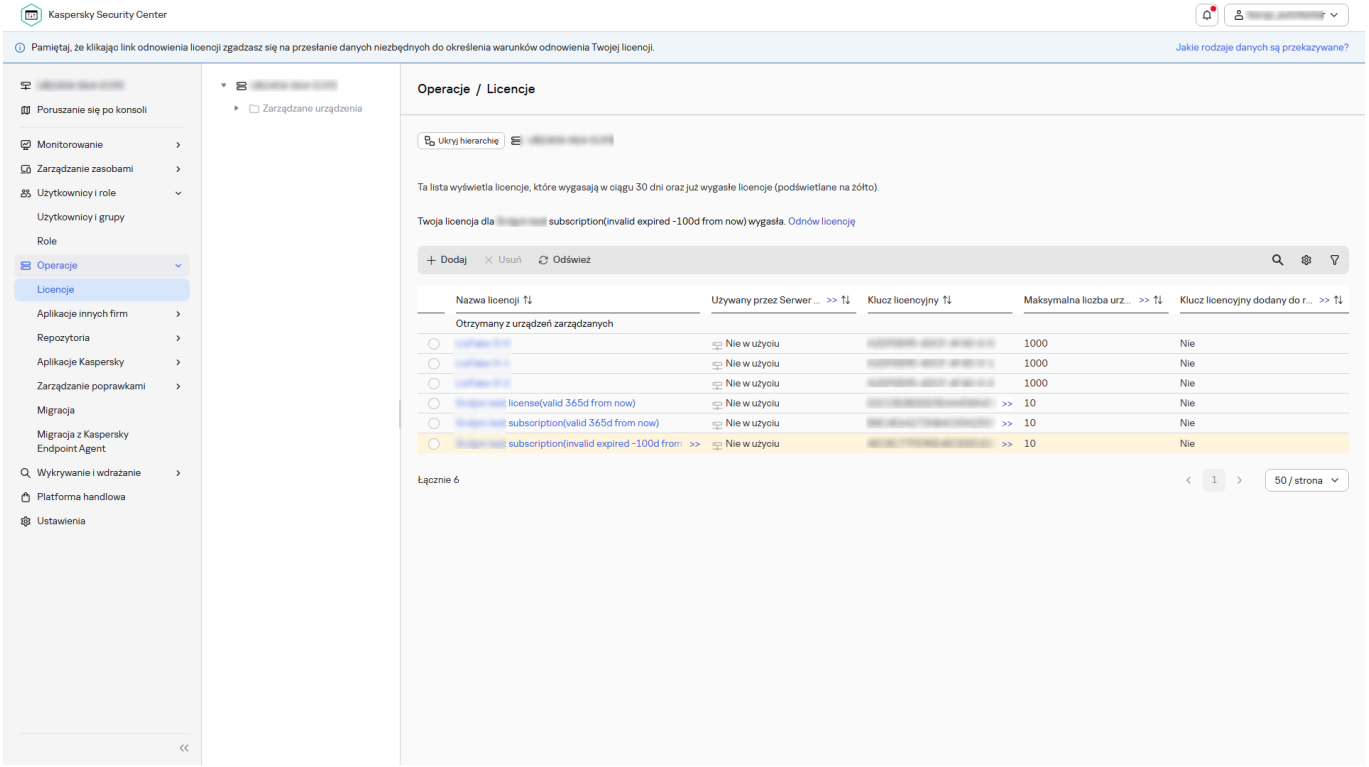
Po wykonaniu zadania, klucz licencyjny zostanie rozesłany na wybrane urządzenia.

Automatyczne rozsyłanie kluczy licencyjnych

Kaspersky Security Center Linux umożliwia automatyczne instalowanie kluczy licencyjnych na zarządzanych urządzeniach, jeśli znajdują się one w repozytorium kluczy licencyjnych na Serwerze administracyjnym.

W celu automatycznego rozsyłania kluczy licencyjnych do zarządzanych urządzeń:

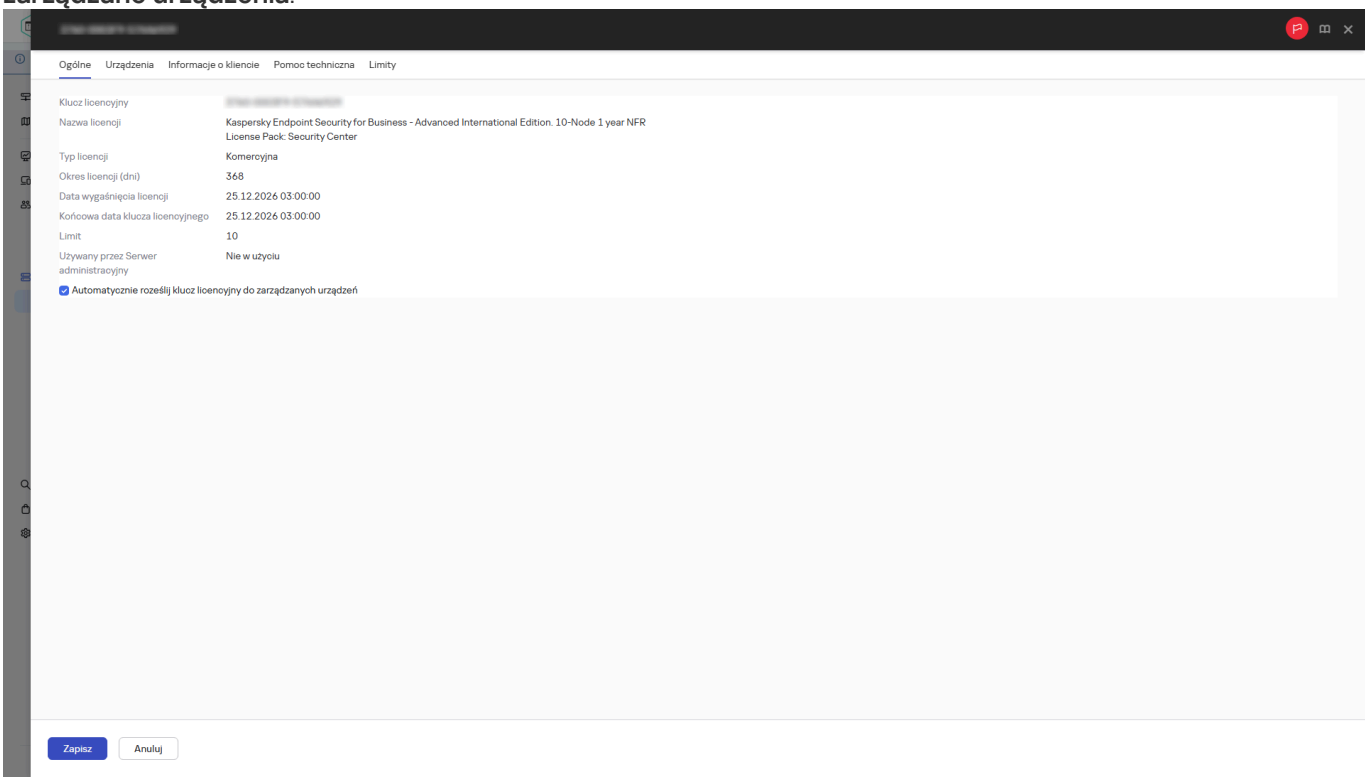
1. W menu głównym przejdź do **Operacje** → **Licencjonowanie** → **Licencje**.



Lista licencji

2. Kliknij nazwę klucza licencyjnego, który chcesz automatycznie rozesłać na urządzenia.

3. W otwartym oknie właściwości klucza licencyjnego zaznacz pole **Automatycznie roześlij klucz licencyjny na zarządzane urządzenia**.



Zamknij okno właściwości klucza licencyjnego

4. Kliknij przycisk **Zapisz**.

   Klucz licencyjny jest automatycznie rozsyłany do wszystkich kompatybilnych urządzeń.

Rozsyłanie klucza licencyjnego odbywa się przy pomocy Agenta sieciowego. Dla aplikacji nie są tworzone żadne zadania rozsyłania kluczy licencyjnych.

Podczas automatycznego rozsyłania klucza licencyjnego brane jest pod uwagę ograniczenie licencyjne dotyczące liczby urządzeń. Ograniczenie licencyjne jest ustawione we właściwościach klucza licencyjnego. Jeśli ograniczenie licencji zostanie osiągnięte, rozesłanie tego klucza licencyjnego na urządzenia zostanie przerwane automatycznie.

Należy pamiętać, że automatycznie dystrybuowany klucz licencyjny może nie zostać wyświetlony w repozytorium wirtualnego Serwera administracyjnego w następujących przypadkach:

- Klucz licencyjny nie jest ważny dla aplikacji.
- Wirtualny Serwer administracyjny nie ma zarządzanych urządzeń.
- Klucz licencyjny został już użyty dla urządzeń zarządzanych przez inny wirtualny Serwer administracyjny i osiągnięto limit liczby urządzeń.

Wirtualny Serwer administracyjny automatycznie dystrybuuje klucze licencyjne ze swojego repozytorium oraz z repozytorium Serwera administracyjnego. Zalecamy:

- Użyj zadania *Dodaj klucz licencyjny*, aby wybrać klucz licencyjny do wdrożenia na urządzeniach.
- Unikaj wyłączania opcji **Zezwól na automatyczne wdrażanie kluczy licencyjnych z tego wirtualnego Serwera administracyjnego do jego urządzeń** w ustawieniach wirtualnego Serwera administracyjnego. W przeciwnym razie wirtualny Serwer administracyjny nie będzie dystrybuował kluczy licencyjnych do urządzeń, łącznie z kluczami licencyjnymi z repozytorium Serwera administracyjnego.

Jeśli zaznaczysz pole **Automatycznie roześlij klucz licencyjny na zarządzane urządzenia** w oknie właściwości klucza licencyjnego, klucz licencyjny jest natychmiast rozpowszechniany w Twojej sieci. Jeśli nie wybierzesz tej opcji, możesz użyć zadania do rozpowszechniania klucza licencyjnego później.

Automatyczna dystrybucja kluczy licencyjnych skonfigurowana na głównym Serwerze administracyjnym nie obejmuje urządzeń zarządzanych przez inne niż wirtualne podrzędne Serwery administracyjne.

Wyświetlanie informacji o używanych kluczach licencyjnych

W celu przejrzenia listy kluczy licencyjnych dodanych do repozytorium Serwera administracyjnego:

W menu głównym przejdź do **Operacje** → **Licencjonowanie** → **Licencje**.

Wyświetlona lista zawiera pliki klucza i kody aktywacyjne dodane do repozytorium Serwera administracyjnego.

W celu wyświetlenia szczegółowych informacji i kluczu licencyjnym:

1. W menu głównym przejdź do **Operacje** → **Licencjonowanie** → **Licencje**.
2. Kliknij nazwę żądanego klucza licencyjnego.

W otwartym oknie właściwości klucza licencyjnego możesz przejrzeć:

- Na zakładce **Ogólne**—główne informacje o kluczu licencyjnym
- Na zakładce **Urządzenia**—lista urządzeń klienckich, na których klucz licencyjny został użyty do aktywacji zainstalowanej aplikacji Kaspersky
- Na zakładce **Limity**—lista limitów licencji

  Jeśli aktywowałeś Serwer administracyjny w ramach licencji Kaspersky Next XDR Optimum, zakładka **Limity** wyświetla pole **XDR-O** z wartością **Włączone**.

W celu sprawdzenia, które klucze licencyjne zostały rozesłane na określone urządzenie klienckie:

1. W menu głównym przejdź do **Zarządzanie zasobami** → **Zasoby (urządzenia)**.
2. Kliknij nazwę żądanego urządzenia.
3. W otwartym oknie właściwości urządzenia wybierz zakładkę **Aplikacje**.
4. Kliknij nazwę aplikacji, dla której chcesz sprawdzić informacje o kluczu licencyjnym.
5. W otwartym oknie właściwości aplikacji wybierz zakładkę **Ogólne**, a następnie otwórz sekcję **Licencja**.

Zostaną wyświetlone główne informacje o aktywnych i zapasowych kluczach licencyjnych.

Aby określić aktualne ustawienia kluczy licencyjnych wirtualnego Serwera administracyjnego, Serwer administracyjny wysyła żądanie do serwerów aktywacji Kaspersky przynajmniej raz dziennie. Jeżeli dostęp do serwerów za pomocą systemowego DNS nie jest możliwy, aplikacja korzysta z publicznych serwerów DNS.

Zdarzenia przekroczenia limitu licencji

Kaspersky Security Center Linux pozwala uzyskać informacje o zdarzeniach, gdy pewne limity licencji zostaną przekroczone przez aplikacje firmy Kaspersky zainstalowane na urządzeniach klienckich.

Istotność takich zdarzeń, gdy limity licencji zostaną przekroczone, jest definiowana zgodnie z następującymi regułami:

- Jeśli liczba aktualnie używanych jednostek objętych jedną licencją mieści się w 90% do 100% całkowitej liczby jednostek objętych licencją, istotność publikowanego zdarzenia to **Informacja**.
- Jeśli liczba aktualnie używanych jednostek objętych jedną licencją mieści się w 100% do 110% całkowitej liczby jednostek objętych licencją, publikowane zdarzenie posiada istotność: **Ostrzeżenie**.
- Jeśli liczba aktualnie używanych jednostek objętych jedną licencją przekracza 110% całkowitej liczby jednostek objętych licencją, istotność publikowanego zdarzenia to **Zdarzenie krytyczne**.

Usuwanie klucza licencyjnego z repozytorium

Jeśli usuniesz aktywny klucz licencyjny rozesłany na zarządzane urządzenie, aplikacja będzie kontynuować pracę na zarządzanym urządzeniu.

W celu usunięcia pliku klucza lub kodu aktywacyjnego z repozytorium Serwera administracyjnego:

1. Sprawdź, czy Serwer administracyjny nie używa pliku klucza lub kodu aktywacyjnego, który chcesz usunąć. Jeśli tak, nie możesz usunąć klucza. Aby przeprowadzić kontrolę:

   a. W menu głównym kliknij nazwę Serwera administracyjnego.

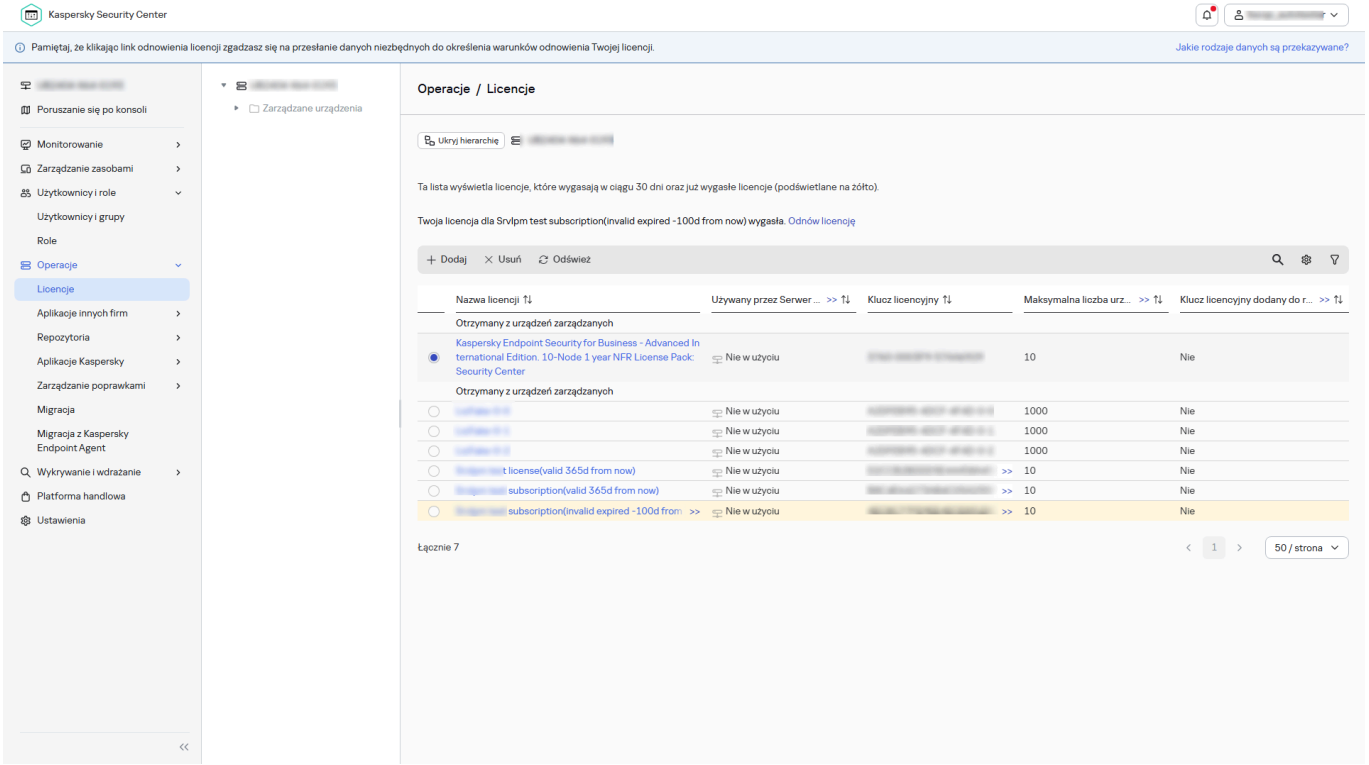
      Zostanie otwarte okno właściwości Serwera administracyjnego.

   b. Na zakładce **Ogólne** wybierz sekcję **Klucze licencyjne**.

   c. Jeżeli w sekcji, która zostanie otwarta, pojawi się wymagany plik klucza lub kod aktywacyjny, kliknij przycisk **Usuń aktywny klucz licencyjny**, a następnie potwierdź operację. Następnie Serwer administracyjny nie używa usuniętego klucza licencyjnego, ale klucz pozostaje w repozytorium Serwera administracyjnego. Jeśli wymagany plik klucza lub kod aktywacyjny nie jest wyświetlany, serwer administracyjny go nie używa.

2. W menu głównym przejdź do **Operacje** → **Licencjonowanie** → **Licencje**.

3. Wybierz wymagany plik klucza lub kod aktywacyjny, a następnie kliknij przycisk **Usuń**.



Lista licencji

Wybrany plik klucza lub kod aktywacyjny zostanie usunięty z repozytorium.

Możesz ponownie dodać usunięty klucz licencyjny lub dodać nowy klucz licencyjny.

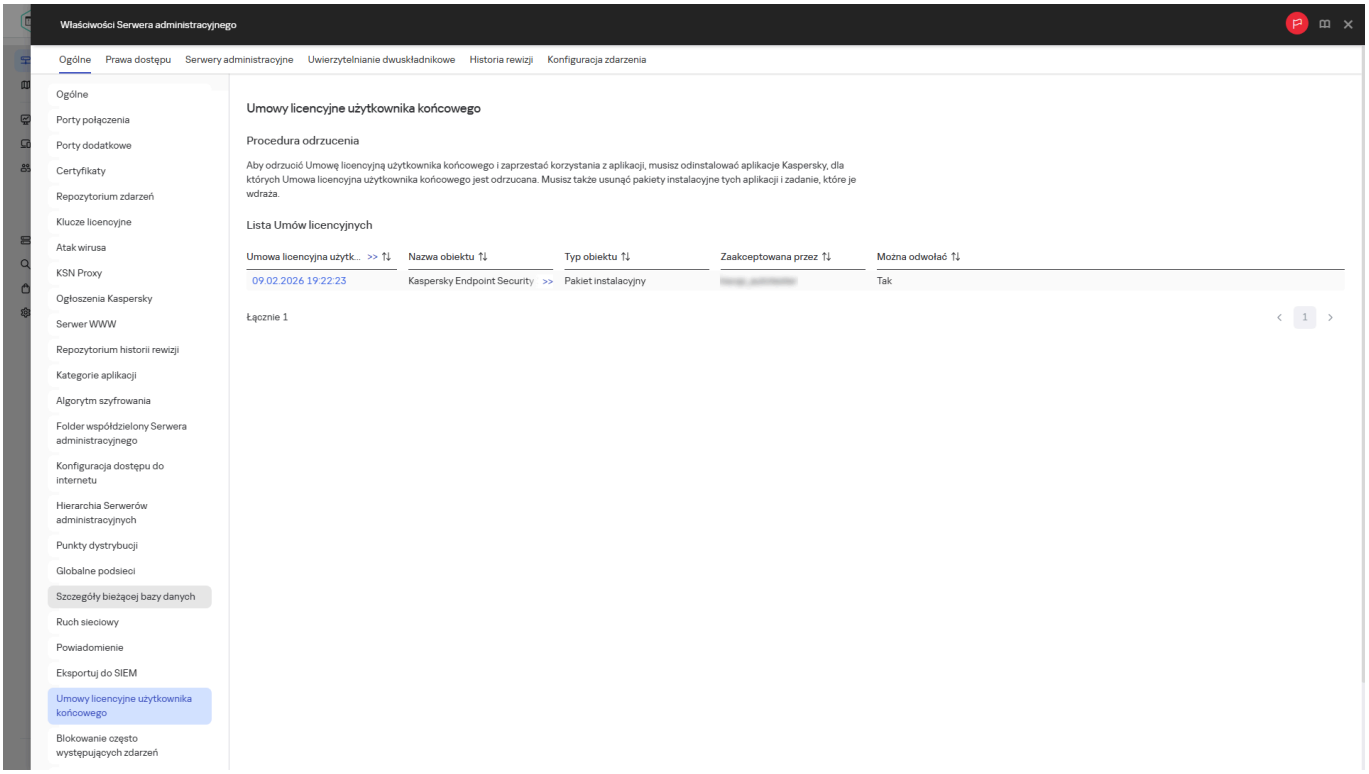
Wycofanie zgody z Umową Licencyjną Użytkownika Końcowego

Jeśli zdecydujesz się na zatrzymanie ochrony niektórych swoich urządzeń klienckich, możesz wycofać zgodę z Umową licencyjną użytkownika końcowego dla każdej zarządzanej aplikacji firmy Kaspersky. Przed wycofaniem zgody z Umową licencyjną użytkownika końcowego należy odinstalować wybraną aplikację.

W celu anulowania Umowy licencyjnej użytkownika końcowego dla zarządzanych aplikacji Kaspersky:

1. Otwórz okno właściwości Serwera administracyjnego i na zakładce **Ogólne** wybierz sekcję **Umowy licencyjne użytkownika końcowego**.

Wyświetlana jest lista Umów licencyjnych użytkownika końcowego, zaakceptowanych po utworzeniu pakietów instalacyjnych, w momencie bezproblemowej instalacji aktualizacji lub po wdrożeniu Kaspersky Security for Mobile.



Lista Umów licencyjnych użytkownika końcowego

2. Z listy wybierz Umowę licencyjną użytkownika końcowego, którą chcesz anulować.

   Możesz sprawdzić następujące właściwości Umowy licencyjnej użytkownika końcowego:

   - Datę zaakceptowania Umowy licencyjnej użytkownika końcowego
   - Nazwę użytkownika, który zaakceptował Umowę licencyjną użytkownika końcowego

3. Kliknij datę zaakceptowania dowolnej Umowy licencyjnej użytkownika końcowego, aby otworzyć jej okno właściwości wyświetlające następujące dane:

   - Nazwę użytkownika, który zaakceptował Umowę licencyjną użytkownika końcowego
   - Datę zaakceptowania Umowy licencyjnej użytkownika końcowego
   - Unikatowy identyfikator (UID) Umowy licencyjnej użytkownika końcowego
   - Pełną treść Umowy licencyjnej użytkownika końcowego
   - Listę obiektów (pakiety instalacyjne, aktualizacje typu seamless, aplikacje mobilne) powiązanych z Umową licencyjną użytkownika końcowego oraz ich odpowiednie nazwy i typy

4. W lewej części okna właściwości Umowy licencyjnej użytkownika końcowego kliknij przycisk **Odrzuć Umowę licencyjną**.

   Jeśli istnieją jakiekolwiek obiekty (pakiety instalacyjne i ich odpowiednie zadania), które uniemożliwiają wycofanie Umowy licencyjnej użytkownika końcowego, zostanie wyświetlone odpowiednie powiadomienie. Jeśli nie usunąłeś tych obiektów, nie możesz przejść do wycofania.

W otwartym oknie zostanie wyświetlona informacja, że w pierwszej kolejności musisz odinstalować aplikację firmy Kaspersky odpowiadającą Umowie licencyjnej użytkownika końcowego.

5. Kliknij przycisk, aby potwierdzić wycofanie.

Umowa licencyjna użytkownika końcowego zostanie wycofana. Nie jest już wyświetlana na liście Umów licencyjnych w sekcji **Umowy licencyjne użytkownika końcowego**. Okno właściwości Umowy licencyjnej użytkownika końcowego zostanie zamknięte; aplikacja nie będzie już zainstalowana.

Odnawianie licencji dla aplikacji Kaspersky

Możesz odnowić licencję dla aplikacji Kaspersky, która utraciła ważność lub wkrótce utraci ważność (za mniej niż 30 dni).

W celu odnowienia licencji, która utraciła ważność, lub licencji, która wkrótce utraci ważność:

1. Wykonaj jedną z poniższych czynności:

   - W menu głównym przejdź do **Operacje** → **Licencjonowanie** → **Licencje**.
   - W oknie głównym przejdź do **Monitorowanie** → **Pulpit nawigacyjny**, a następnie kliknij odnośnik **Zobacz wygasające licencje** obok powiadomienia.

   Zostanie otwarte okno **Licencje**, w którym możesz przejrzeć i odnowić licencje.

2. Kliknij łącze **Odnów licencję** obok wymaganej licencji.

   Klikając odnośnik do odnowienia licencji, wyrażasz zgodę na przeniesienie do Kaspersky następujących informacji o programie Kaspersky Security Center Linux: jego wersję, wersję językową, której używasz, identyfikator licencji oprogramowania (czyli identyfikator odnawianej licencji), a także, czy zakupiłeś licencję u partnera firmy.

3. W otwartym oknie usługi odnowienia licencji wykonaj instrukcje w celu odnowienia licencji.

   Licencja zostanie odnowiona.

W Kaspersky Security Center Web Console powiadomienia o licencji, która wkrótce utraci ważność, są wyświetlane zgodnie z następującym terminarzem:

- 30 dni przed utratą ważności
- 7 dni przed utratą ważności
- 3 dni przed utratą ważności
- 24 godziny przed utratą ważności
- Po wygaśnięciu licencji

Korzystanie z Kaspersky Marketplace do wyboru rozwiązań biznesowych firmy Kaspersky

Platforma handlowa to sekcja w menu głównym, która umożliwia przeglądanie całej gamy rozwiązań biznesowych firmy Kaspersky, wybranie tych, których potrzebujesz, i przejście do zakupu na stronie internetowej Kaspersky. Możesz użyć filtrów, aby wyświetlić tylko te rozwiązania, które pasują do Twojej organizacji i wymagań systemu bezpieczeństwa informacji. Po wybraniu rozwiązania Kaspersky Security Center Linux przekieruje Cię do powiązanej strony internetowej w witrynie Kaspersky, aby dowiedzieć się więcej o tym rozwiązaniu. Każda strona internetowa umożliwia przejście do zakupu lub zawiera instrukcje dotyczące procesu zakupu.

W sekcji **Platforma handlowa** możesz filtrować rozwiązania firmy Kaspersky z użyciem następujących kryteriów:

- Liczba urządzeń (punktów końcowych, serwerów i innych typów zasobów), które chcesz chronić:
  - 50–250
  - 250–1000
  - Więcej niż 1000
- Poziom dojrzałości zespołu ds. bezpieczeństwa informacji w Twojej organizacji:
  - **Podstawowy**

    Ten poziom jest typowy dla przedsiębiorstw, które posiadają tylko zespół ds. IT. Maksymalna możliwa liczba zagrożeń jest blokowana automatycznie.
  - **Optymalny**

    Ten poziom jest typowy dla przedsiębiorstw, które posiadają określoną funkcję bezpieczeństwa IT w zespole ds. IT. Na tym poziomie firmy potrzebują rozwiązań, które umożliwią im przeciwdziałanie zagrożeniom towarowym oraz zagrożeniom omijającym istniejące mechanizmy prewencyjne.
  - **Ekspert**

    Ten poziom jest typowy dla przedsiębiorstw o złożonych i rozproszonych środowiskach IT. Zespół ds. bezpieczeństwa IT jest dojrzały lub firma posiada zespół SOC (Security Operations Center). Wymagane rozwiązania umożliwiają firmom przeciwdziałanie złożonym zagrożeniom i atakom ukierunkowanym.
- Typy zasobów, które chcesz chronić:
  - **Punkty końcowe**: stacje robocze pracowników, maszyny fizyczne i wirtualne, systemy wbudowane
  - **Serwery**: serwery fizyczne i wirtualne
  - **Chmura**: środowiska chmury publicznej, prywatnej lub hybrydowej; usługi w chmurze
  - **Sieć**: sieć lokalna, infrastruktura IT
  - **Usługa**: usługi związane z bezpieczeństwem świadczone przez Kaspersky

W celu znalezienia i zakupu rozwiązania biznesowego firmy Kaspersky:

1. W oknie głównym przejdź do **Platforma handlowa**.

   Domyślnie sekcja wyświetla wszystkie dostępne rozwiązania biznesowe firmy Kaspersky.

2. Aby wyświetlić tylko te rozwiązania, które odpowiadają Twojej organizacji, wybierz wymagane wartości w filtrach.

3. Kliknij rozwiązanie, które chcesz kupić lub chcesz dowiedzieć się więcej.

   Zostaniesz przekierowany na stronę rozwiązania. Możesz postępować zgodnie z instrukcjami wyświetlanymi na ekranie, aby przejść do zakupu.

Konfigurowanie aplikacji Kaspersky

Ta sekcja zawiera informacje o ręcznej konfiguracji zasad i zadań, informacje o rolach użytkownika, informacje o tworzeniu struktury grupy administracyjnej oraz hierarchii zadań.

Scenariusz: Konfigurowanie ochrony sieci

Kreator wstępnej konfiguracji tworzy zasady i zadania z domyślnymi ustawieniami. Te ustawienia mogą okazać się nieoptymalne lub nawet niedopuszczalne przez organizację. Dlatego zalecane jest dostrojenie tych zasad i zadań oraz utworzenie innych zasad i zadań, jeśli są konieczne w Twojej sieci.

Wymagania wstępne

Przed rozpoczęciem upewnij się, że:

- Zainstalowałeś Serwer administracyjny Kaspersky Security Center Linux
- Zainstalowano Kaspersky Security Center Web Console
- Zakończyłeś główny scenariusz instalacji Kaspersky Security Center Linux
- Zakończono działanie kreatora wstępnej konfiguracji lub ręcznie utworzono następujące zasady i zadania w grupie administracyjnej **Zarządzane urządzenia**:
  - Zasada Kaspersky Endpoint Security
  - Grupowe zadanie aktualizacji Kaspersky Endpoint Security
  - Zasada Agenta sieciowego
  - Zadanie *Wyszukiwania luk i wymaganych aktualizacji*

Etapy

Konfigurowanie ochrony sieci odbywa się w etapach:

1. **Konfiguracja i przesyłanie zasad i profili zasad aplikacji firmy Kaspersky**

   Aby skonfigurować i przesłać ustawienia dla aplikacji Kaspersky, zainstalowanych na zarządzanych urządzeniach, możesz użyć dwóch różnych metod zarządzania ochroną—skoncentrowaną na urządzeniu lub skoncentrowaną na użytkowniku. Te dwie metody można połączyć.

2. **Konfigurowanie zadań zdalnego zarządzania aplikacjami firmy Kaspersky**

   Sprawdź zadania utworzone przy pomocy kreatora wstępnej konfiguracji i dostosuj je (jeśli to konieczne).

Dostępne instrukcje: Konfigurowanie zadania grupowego aktualizacji Kaspersky Endpoint Security, Tworzenie zadania Wyszukiwania luk i wymagane aktualizacje.

Jeśli to konieczne, utwórz dodatkowe zadania do zarządzania aplikacjami Kaspersky zainstalowanymi na urządzeniach klienckich.

3. **Oszacowanie i ograniczenie nagromadzenia zdarzeń w bazie danych**

   Informacje o zdarzeniach występujących podczas działania zarządzanych aplikacji są przesyłane z urządzenia klienckiego i zapisywane w bazie danych Serwera administracyjnego. Aby zmniejszyć obciążenie na Serwerze administracyjnym, oszacuj i ogranicz maksymalną liczbę zdarzeń przechowywanych w bazie danych.

   Jak to zrobić: ustawianie maksymalnej liczby zdarzeń.

Wyniki

Po zakończeniu tego scenariusza, Twoja sieć będzie chroniona przez konfigurację aplikacji Kaspersky, zadania i zdarzenia otrzymane przez Serwer administracyjny:

- Aplikacje firmy Kaspersky są konfigurowane zgodnie z zasadami i profilami zasad.
- Aplikacje są zarządzane za pośrednictwem zestawu zadań.
- Maksymalna liczba zdarzeń, jaka może być przechowywana w bazie danych, została ustawiona.

Jeśli konfiguracja ochrony sieci zostanie zakończona, możesz przejść do konfigurowania regularnych aktualizacji baz danych i aplikacji Kaspersky.

Informacje o metodach zarządzania ochroną skoncentrowaną na urządzeniu i użytkowniku

Możesz zarządzać ustawieniami zabezpieczeń z poziomu funkcji urządzenia i z poziomu roli użytkownika. Pierwsza metoda nosi nazwę *zarządzanie ochroną skoncentrowaną na urządzeniu*, a druga nazywa się *zarządzania ochroną skoncentrowaną na użytkowniku*. Aby zastosować różne ustawienia aplikacji na różnych urządzeniach, możesz użyć połączonych typów zarządzania.

Zarządzanie bezpieczeństwem skoncentrowane na urządzeniu umożliwia zastosowanie różnych ustawień aplikacji zabezpieczającej na zarządzanych urządzeniach w zależności od funkcji charakterystycznych dla urządzeń. Na przykład, możesz zastosować różne ustawienia do urządzeń przydzielonych w różnych grupach administracyjnych.

Zarządzanie bezpieczeństwem skoncentrowanym na użytkowniku umożliwia zastosowanie różnych ustawień aplikacji zabezpieczającej do różnych ról użytkownika. Możesz utworzyć kilka ról użytkownika, przypisać odpowiednią rolę użytkownika do każdego użytkownika oraz określić różne ustawienia aplikacji do urządzeń należących do użytkowników z różnymi rolami. Na przykład, chcesz zastosować różne ustawienia aplikacji na urządzeniach księgowych i specjalistów z działu HR. W rezultacie, gdy zaimplementowane jest zarządzanie ochroną skoncentrowaną na użytkowniku, każdy dział—dział księgowych i dział HR—posiada swoją własną konfigurację ustawień dla aplikacji firmy Kaspersky. Konfiguracja ustawień definiuje, które ustawienia aplikacji mogą być zmieniane przez użytkowników i dla których wymuszone jest ustawienie i zablokowanie przez administratora.

Korzystając z zarządzania ochroną skoncentrowaną na użytkowniku, możesz zastosować określone ustawienia aplikacji do pojedynczych użytkowników. Może to być wymagane, gdy pracownik posiada unikatową rolę w firmie lub gdy chcesz monitorować problemy bezpieczeństwa dotyczące urządzeń określonej osoby. W zależności od roli tego pracownika w firmie, możesz rozszerzyć lub ograniczyć uprawnienia tej osoby do zmiany ustawień aplikacji. Na przykład, możesz rozszerzyć uprawnienia administratora systemu, który zarządza urządzeniami klienckimi w biurze lokalnym.

Możesz połączyć metody zarządzania ochroną skoncentrowaną na urządzeniu i użytkowniku. Na przykład, możesz skonfigurować określoną zasadę aplikacji dla każdej grupy administracyjnej, a następnie utworzyć profile zasad dla jednej lub kilku ról użytkownika Twojej firmy. W tym przypadku zasady i profile zasad są stosowane w następującej kolejności:

1. Zostaną zastosowane zasady utworzone dla zarządzania ochroną skoncentrowaną na urządzeniu.
2. Są one modyfikowane przez profile zasad zgodnie z priorytetami profili zasad.
3. Zasady są modyfikowane przez profile zasad skojarzone z rolami użytkownika.

Konfiguracja i przydzielanie zasad: Metoda skoncentrowana na urządzeniu

Po zakończeniu tego scenariusza, aplikacje zostaną skonfigurowane na wszystkich zarządzanych urządzeniach zgodnie z zasadami i profilami zasad aplikacji, które określiłeś.

Wymagania wstępne

Przed rozpoczęciem konfiguracji upewnij się, że zainstalowano Serwer administracyjny Kaspersky Security Center Linux i Kaspersky Security Center Web Console. Możesz wziąć pod uwagę zarządzanie ochroną skoncentrowaną na użytkowniku jako alternatywę lub dodatkową opcję dla metody skoncentrowanej na urządzeniu. Dowiedz się więcej na temat dwóch metod zarządzania.

Etapy

Scenariusz skoncentrowanego na urządzeniu zarządzania aplikacjami Kaspersky obejmuje następujące kroki:

1. **Konfigurowanie zasad aplikacji**

   Skonfiguruj ustawienia dla aplikacji firmy Kaspersky, zainstalowanych na zarządzanych urządzeniach poprzez utworzenie zasady dla każdej aplikacji. Zestaw zasad zostanie przesłany na urządzenia klienckie.

   Podczas konfigurowania ochrony sieci w kreatorze wstępnej konfiguracji Kaspersky Security Center Linux tworzy domyślną zasadę dla następujących aplikacji:

   - Kaspersky Endpoint Security for Linux — dla urządzeń klienckich z Linux
   - Kaspersky Endpoint Security for Windows — dla urządzeń klienckich z systemem Windows

   Jeśli zakończyłeś proces konfiguracji przy użyciu tego kreatora, nie musisz tworzyć nowej zasady dla tej aplikacji.

Jeśli masz hierarchiczną strukturę kilku Serwerów administracyjnych i/lub grup administracyjnych, domyślnie podrzędne Serwery administracyjne i podrzędne grupy administracyjne dziedziczą zasady z głównego Serwera administracyjnego. Możesz wymusić dziedziczenie przez grupy podrzędne i podrzędne Serwery administracyjne, aby zabronić wszelkich modyfikacji ustawień skonfigurowanych w nadrzędnej zasadzie. Jeśli chcesz, żeby wymuszone było dziedziczenie tylko części ustawień, możesz zablokować je w zasadzie nadrzędnej. Pozostałe niezablokowane ustawienia będą dostępne do modyfikacji w zasadach podrzędnych. Utworzona hierarchia zasad umożliwi efektywne zarządzanie urządzeniami w grupach administracyjnych.

Dostępne instrukcje: Tworzenie zasady

2. **Tworzenie profili zasad (opcjonalnie)**

Jeśli chcesz, żeby urządzenia w jednej grupie administracyjnej były uruchamiane z różnymi ustawieniami zasady, utwórz profile zasad dla tych urządzeń. Profil zasad jest to inaczej podzbiór ustawień zasady. Ten podzbiór jest stosowany na urządzeniach docelowych wraz z zasadą i uzupełnia ją zgodnie z określonym warunkiem zwanym *warunkiem aktywacji profilu*. Profile mogą zawierać tylko ustawienia różniące się od „podstawowej" zasady, która jest aktywna na zarządzanym urządzeniu.

Korzystając z warunków aktywacji profilu, możesz zastosować różne profile zasad, na przykład do urządzeń z określoną konfiguracją sprzętową lub oznaczoną określonymi znacznikami. Użyj znaczników do filtrowania urządzeń, które spełniają określone kryteria. Na przykład możesz utworzyć znacznik nazwany *CentOS*, oznaczyć tym znacznikiem wszystkie urządzenia działające pod kontrolą systemu operacyjnego CentOS, a następnie określić ten znacznik jako warunek aktywacji profilu zasad. W wyniku tego działania aplikacje Kaspersky zainstalowane na wszystkich urządzeniach działających pod kontrolą systemu CentOS będą zarządzane przez własny profil zasad.

Dostępne instrukcje:

- Tworzenie profilu zasad
- Tworzenie reguły aktywacji profilu zasad

3. **Przesyłanie zasad i profili zasad na zarządzane urządzenia**

Domyślnie Serwer administracyjny automatycznie synchronizuje się z zarządzanymi urządzeniami co 15 minut. Podczas synchronizacji nowe lub zmienione zasady i profile zasad zostają rozesłane na zarządzane urządzenia. Możesz obejść automatyczną synchronizację i ręcznie uruchomić synchronizację przy pomocy polecenia Wymuś synchronizację. Po zakończeniu synchronizacji, aby zapewnić dostarczenie i zastosowanie zasad i profili zasad do zainstalowanych aplikacji Kaspersky.

Możesz sprawdzić, czy zasady i profile zasad zostały dostarczone na urządzenie. Kaspersky Security Center Linux określa datę i godzinę dostarczenia we właściwościach urządzenia.

Dostępne instrukcje: Wymuszona synchronizacja

Wyniki

Po zakończeniu scenariusza skoncentrowanego na urządzeniu, aplikacje Kaspersky są konfigurowane zgodnie z ustawieniami określonymi i przesłanymi poprzez hierarchię zasad.

Skonfigurowane zasady i profile zasad aplikacji zostaną automatycznie zastosowane do nowych urządzeń dodanych do grup administracyjnych.

Konfiguracja i przydzielanie zasad: Metoda skoncentrowana na użytkowniku

Ta sekcja opisuje scenariusz skoncentrowanej na użytkowniku scentralizowanej konfiguracji aplikacji Kaspersky zainstalowanych na zarządzanych urządzeniach. Po zakończeniu tego scenariusza, aplikacje zostaną skonfigurowane na wszystkich zarządzanych urządzeniach zgodnie z zasadami i profilami zasad aplikacji, które określiłeś.

Wymagania wstępne

Przed rozpoczęciem konfiguracji upewnij się, że pomyślnie zainstalowano Serwer administracyjny Kaspersky Security Center Linux i Kaspersky Security Center Web Console, a także zakończono główny scenariusz wdrażania. Możesz wziąć pod uwagę zarządzanie ochroną skoncentrowaną na urządzeniu jako alternatywę lub dodatkową opcję dla metody skoncentrowanej na użytkowniku. Dowiedz się więcej na temat dwóch metod zarządzania.

Proces

Scenariusz skoncentrowanego na użytkowniku zarządzania aplikacjami Kaspersky obejmuje następujące kroki:

1. **Konfigurowanie zasad aplikacji**

   Skonfiguruj ustawienia dla aplikacji firmy Kaspersky, zainstalowanych na zarządzanych urządzeniach poprzez utworzenie zasady dla każdej aplikacji. Zestaw zasad zostanie przesłany na urządzenia klienckie.

   Jeśli konfigurujesz ochronę swojej sieci w kreatorze wstępnej konfiguracji, Kaspersky Security Center Linux tworzy domyślną zasadę dla Kaspersky Endpoint Security. Jeśli zakończyłeś proces konfiguracji przy użyciu tego kreatora, nie musisz tworzyć nowej zasady dla tej aplikacji.

   Jeśli masz hierarchiczną strukturę kilku Serwerów administracyjnych i/lub grup administracyjnych, domyślnie podrzędne Serwery administracyjne i podrzędne grupy administracyjne dziedziczą zasady z głównego Serwera administracyjnego. Możesz wymusić dziedziczenie przez grupy podrzędne i podrzędne Serwery administracyjne, aby zabronić wszelkich modyfikacji ustawień skonfigurowanych w nadrzędnej zasadzie. Jeśli chcesz, żeby wymuszone było dziedziczenie tylko części ustawień, możesz zablokować je w zasadzie nadrzędnej. Pozostałe niezablokowane ustawienia będą dostępne do modyfikacji w zasadach podrzędnych. Utworzona hierarchia zasad umożliwi efektywne zarządzanie urządzeniami w grupach administracyjnych.

   Dostępne instrukcje: Tworzenie zasady

2. **Określanie właścicieli urządzeń**

   Przypisz zarządzane urządzenia do odpowiednich użytkowników.

   Dostępne instrukcje: Wskazywanie użytkownika jako właściciela urządzenia

3. **Określanie ról użytkownika typowych dla Twojej firmy**

   Pomyśl o różnych rodzajach pracy, jaką pracownicy Twojej firmy zazwyczaj wykonują. Musisz podzielić wszystkich pracowników zgodnie z ich rolami. Na przykład, możesz podzielić ich według działów, profesji lub pozycji. Następnie musisz utworzyć rolę użytkownika dla każdej grupy. Pamiętaj, że każda rola użytkownika będzie posiadała swój własny profil zasad zawierający ustawienia aplikacji specyficzne dla tej roli.

4. **Tworzenie ról użytkownika**

   Utwórz i skonfiguruj rolę użytkownika dla każdej grupy pracowników, którą określiłeś w poprzednim kroku, lub użyj predefiniowanej roli użytkownika. Role użytkownika będą zawierały zestaw uprawnień dostępu do funkcji aplikacji.

   Dostępne instrukcje: Tworzenie roli użytkownika

5. **Określanie obszaru każdej roli użytkownika**

   Dla każdej utworzone roli użytkownika określ użytkowników i/lub grupy bezpieczeństwa oraz grupy administracyjne. Ustawienia skojarzone z rolą użytkownika są stosowane tylko do urządzeń, które należą do użytkowników posiadających tę rolę i tylko wtedy, gdy te urządzenia należą do grup skojarzonych z tą rolą, w tym grup podrzędnych.

   Dostępne instrukcje: Edytowanie obszaru roli użytkownika

6. **Tworzenie profili zasad**

   Utwórz profil zasad dla każdej roli użytkownika w Twojej firmie. Profile zasad określają, które ustawienia zostaną zastosowane w aplikacjach zainstalowanych na urządzeniach użytkowników w zależności od roli każdego użytkownika.

   Dostępne instrukcje: Tworzenie profilu zasad

7. **Kojarzenie profili zasad z rolami użytkownika**

   Skojarz utworzone profile zasad z rolami użytkownika. Następnie: profil zasad stanie się aktywny dla użytkowników, którzy posiadają określoną rolę. Ustawienia skonfigurowane w profilu zasad zostaną zastosowane do aplikacji Kaspersky zainstalowanych na urządzeniach użytkownika.

   Dostępne instrukcje: Kojarzenie profili zasad z rolami

8. **Przesyłanie zasad i profili zasad na zarządzane urządzenia**

   Domyślnie Kaspersky Security Center Linux automatycznie synchronizuje Serwer administracyjny z zarządzanymi urządzeniami co 15 minut. Podczas synchronizacji nowe lub zmienione zasady i profile zasad zostają rozesłane na zarządzane urządzenia. Możesz obejść automatyczną synchronizację i ręcznie uruchomić synchronizację przy pomocy polecenia Wymuś synchronizację. Po zakończeniu synchronizacji, aby zapewnić dostarczenie i zastosowanie zasad i profili zasad do zainstalowanych aplikacji Kaspersky.

   Możesz sprawdzić, czy zasady i profile zasad zostały dostarczone na urządzenie. Kaspersky Security Center Linux określa datę i godzinę dostarczenia we właściwościach urządzenia.

   Dostępne instrukcje: Wymuszona synchronizacja

Wyniki

Po zakończeniu scenariusza skoncentrowanego na użytkowniku, aplikacje Kaspersky są konfigurowane zgodnie z określonymi ustawieniami i przesyłane poprzez hierarchię zasad i profili zasad.

Dla nowego użytkownika konieczne będzie utworzenie nowego konta, przypisanie użytkownikowi jednej z utworzonych ról użytkownika, a także przypisane urządzeń do użytkownika. Skonfigurowane zasady i profile zasad aplikacji zostaną automatycznie zastosowane do urządzeń tego użytkownika.

Zasady i profile zasad

W Kaspersky Security Center Web Console możesz tworzyć zasady dla aplikacji Kaspersky. Ta sekcja opisuje zasady i profile zasad, a także zawiera instrukcje dotyczące ich tworzenia i modyfikowania.

Informacje o zasadach i profilach zasad

Zasada to zbiór ustawień aplikacji Kaspersky, które są stosowane do grupy administracyjnej i jej podgrup. Możesz zainstalować kilka aplikacji Kaspersky na urządzeniach należących do grupy administracyjnej. Kaspersky Security Center zapewnia jedną zasadę dla każdej aplikacji Kaspersky w grupie administracyjnej. Zasada ma jeden z następujących stanów:

Stan zasady

Stan	Opis
Aktywny	Bieżąca zasada, która jest stosowana do urządzenia. W każdej grupie administracyjnej dla aplikacji Kaspersky może być aktywna tylko jedna zasada. Urządzenia stosują wartości ustawień aktywnej zasady aplikacji Kaspersky.
Nieaktywna	Zasada, która nie jest obecnie stosowana do urządzenia.
Profil użytkownika mobilnego	Jeżeli ta opcja jest zaznaczona, zasada stanie się aktywna, gdy urządzenie znajdzie się poza siecią korporacyjną.

Zasady działają zgodnie z następującymi regułami:

- Dla jednej aplikacji można skonfigurować kilka zasad z różnymi wartościami.
- Tylko jedna zasada może być aktywna dla bieżącej aplikacji.
- Zasada może mieć zasady podrzędne.

Zazwyczaj można używać zasad w celu przygotowania się na sytuacje awaryjne, takie jak atak wirusa. Na przykład, jeśli wystąpi atak za pośrednictwem dysków flash, można aktywować zasadę blokującą dostęp do dysków flash. W takim przypadku bieżąca aktywna zasada automatycznie stanie się nieaktywna.

Aby zapobiec utrzymywaniu wielu zasad, na przykład, gdy przy różnych okazjach zakłada się zmianę tylko kilku ustawień, można użyć profili zasad.

Profil zasad to nazwany podzbiór wartości ustawień zasad, który zastępuje wartości ustawień zasady. Profil zasad wpływa na efektywne tworzenie ustawień na zarządzanym urządzeniu. *Obowiązujące ustawienia* to zbiory ustawień zasad, ustawień profilu zasad i lokalnych ustawień aplikacji, które są aktualnie zastosowane do urządzenia.

Profile zasad działają zgodnie z następującymi regułami:

- Profil zasad zaczyna obowiązywać, gdy wystąpi określony warunek aktywacji.
- Profile zasad zawierają wartości ustawień, które różnią się od ustawień zasad.
- Aktywacja profilu zasad zmienia obowiązujące ustawienia zarządzanego urządzenia.
- Zasada może zawierać maksymalnie 100 profili zasad.

Informacje o blokadzie i zablokowanych ustawieniach

Każde ustawienie zasady ma ikonę przycisku blokady (🔒). Poniższa tabela przedstawia stany przycisków blokady:

Stany przycisków blokady

Stan	Opis
Undefined	Jeśli obok ustawienia jest wyświetlana otwarta kłódka, a przycisk przełącznika jest wyłączony, ustawienie nie jest określone w zasadzie. Użytkownik może zmienić te ustawienia w interfejsie zarządzanej aplikacji. Tego typu ustawienia nazywane są *odblokowanymi*.
Enforce	Jeśli obok ustawienia jest wyświetlana zamknięta kłódka, a przycisk przełącznika jest włączony, ustawienie jest stosowane do urządzeń, na których zasada jest wymuszana. Użytkownik nie może zmodyfikować wartości tych ustawień w interfejsie zarządzanej aplikacji. Tego typu ustawienia nazywane są *zablokowanymi*.

Zdecydowanie zalecamy zamknięcie blokad dla ustawień zasad, które chcesz zastosować na zarządzanych urządzeniach. Odblokowane ustawienia zasady można ponownie przypisać przez ustawienia aplikacji Kaspersky na zarządzanym urządzeniu.

Możesz użyć przycisku blokady, aby wykonać następujące czynności:

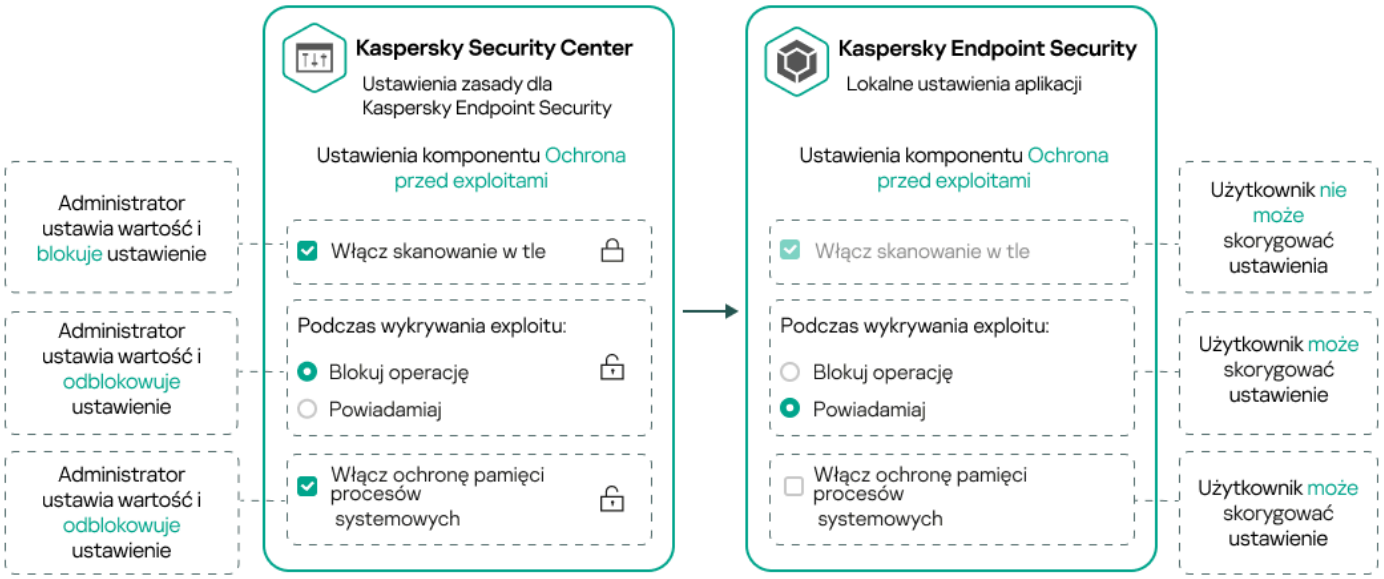
- Blokowanie ustawień dla zasady podgrupy administracyjnej
- Blokowanie ustawień aplikacji Kaspersky na zarządzanym urządzeniu

W ten sposób zablokowane ustawienie jest używane do implementacji obowiązujących ustawień na zarządzanym urządzeniu.

Proces skutecznego wdrażania ustawień obejmuje następujące działania:

- Zarządzane urządzenie stosuje wartości ustawień aplikacji Kaspersky.
- Zarządzane urządzenie stosuje zablokowane wartości ustawień zasady.

Zasada i zarządzana aplikacja Kaspersky zawierają ten sam zbiór ustawień. Po skonfigurowaniu ustawień zasady, wartości ustawień aplikacji Kaspersky ulegają zmianie na zarządzanym urządzeniu. Użytkownik nie może dostosować zablokowanych ustawień na zarządzanym urządzeniu (patrz rysunek poniżej):



Blokady i ustawienia aplikacji Kaspersky

Dziedziczenie zasad i profili zasad

Ta sekcja zawiera informacje o hierarchii i dziedziczeniu zasad oraz profilach zasad.

Hierarchia zasad

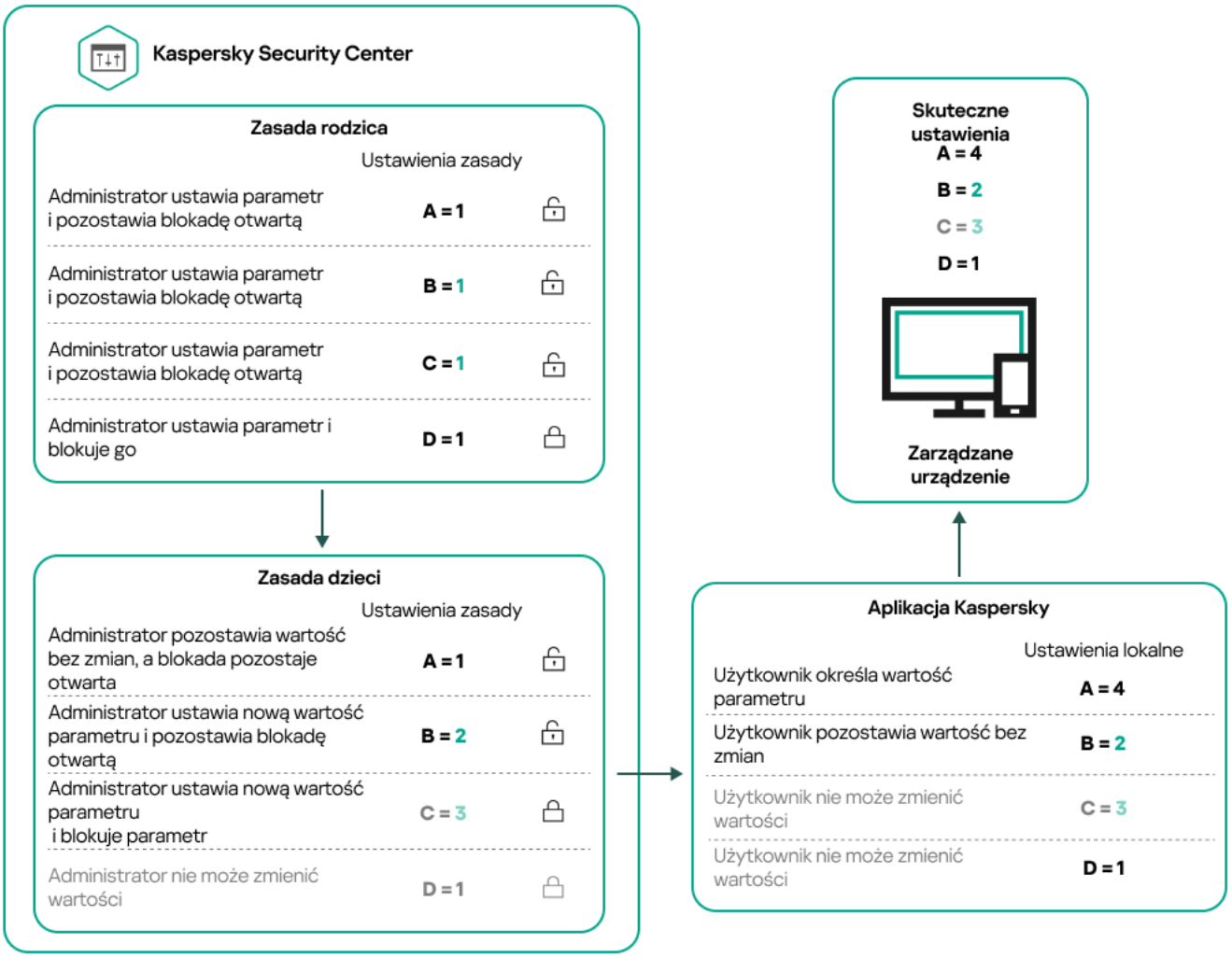
Jeśli różne urządzenia wymagają różnych ustawień, możesz zorganizować je w grupy administracyjne.

Możesz określić zasadę dla pojedynczej grupy administracyjnej. Ustawienia zasad mogą być *dziedziczone*. Dziedziczenie oznacza odbieranie wartości ustawień zasad w podgrupach (grupach podrzędnych) z zasady grupy administracyjnej wyższego poziomu (nadrzędnej).

Dalej zasada dla grupy nadrzędnej jest też zwana *zasadą nadrzędną*. Dalej zasada dla podgrupy (grupy podrzędnej) jest też zwana *zasadą podrzędną*.

Domyślnie co najmniej jedna grupa zarządzane urządzenia istnieje na Serwerze administracyjnym. Jeśli chcesz utworzyć grupy niestandardowe, są one tworzone jako podgrupy (grupy podrzędne) w ramach grupy zarządzane urządzenia.

Zasady tej samej aplikacji oddziałują na siebie zgodnie z hierarchią grup administracyjnych. Zablokowane ustawienia z zasady grupy administracyjnej wyższego poziomu (nadrzędnej) spowodują ponowne przypisanie wartości ustawień zasad podgrupy (patrz rysunek poniżej).



Hierarchia zasad

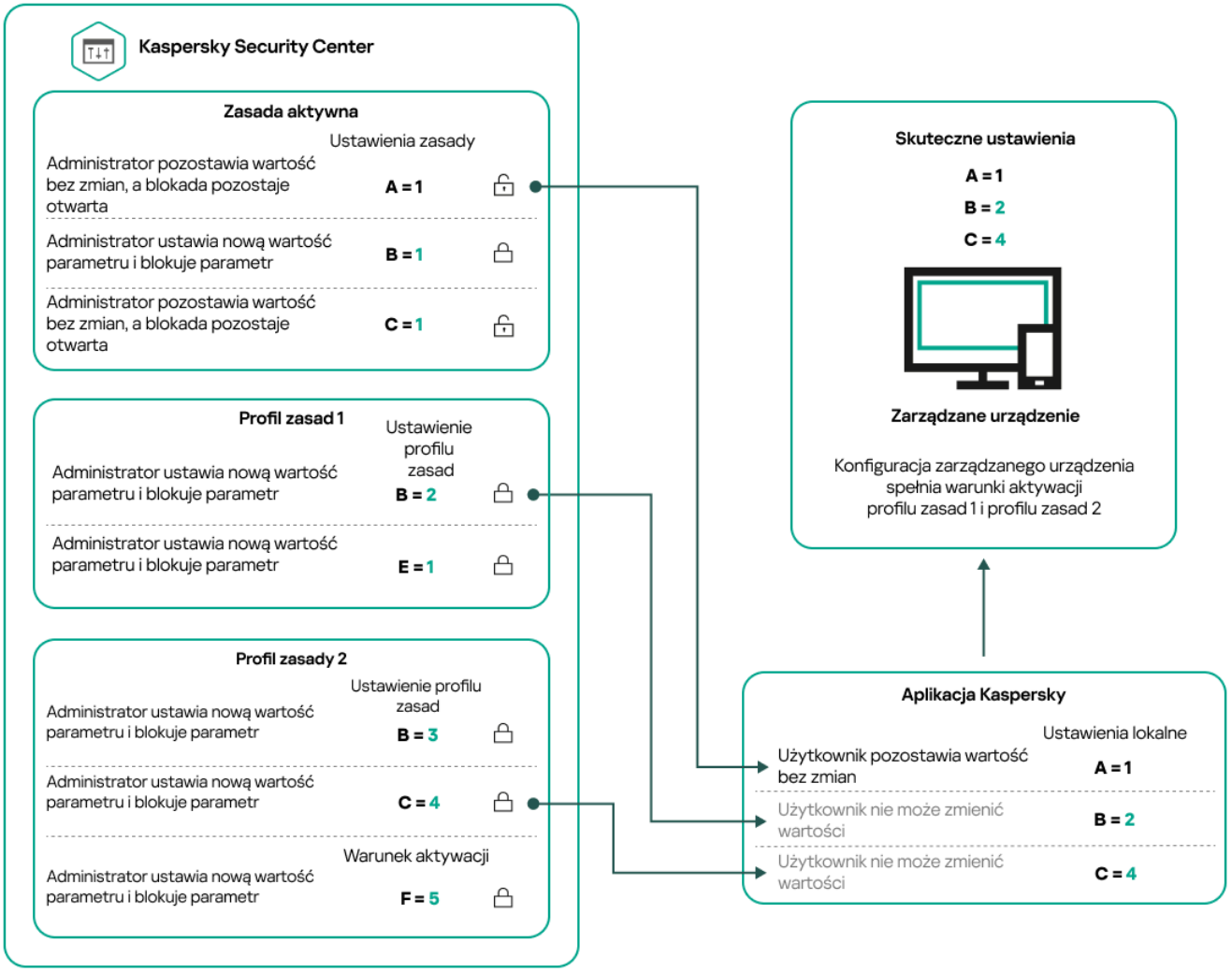
Profile zasad w hierarchii zasad

Profile zasad mają następujące warunki przypisywania priorytetów:

- Pozycja profilu na liście profili zasad wskazuje jego priorytet. Możesz zmienić priorytet profilu zasad. Najwyższa pozycja na liście oznacza najwyższy priorytet (patrz rysunek poniżej).

Definicja priorytetu profilu zasad

- Warunki aktywacji profili zasad nie są od siebie zależne. Jednocześnie można aktywować kilka profili zasad. Jeśli kilka profili zasad wpływa na to samo ustawienie, urządzenie przyjmuje wartość ustawienia z profilu zasad o najwyższym priorytecie (patrz rysunek poniżej).



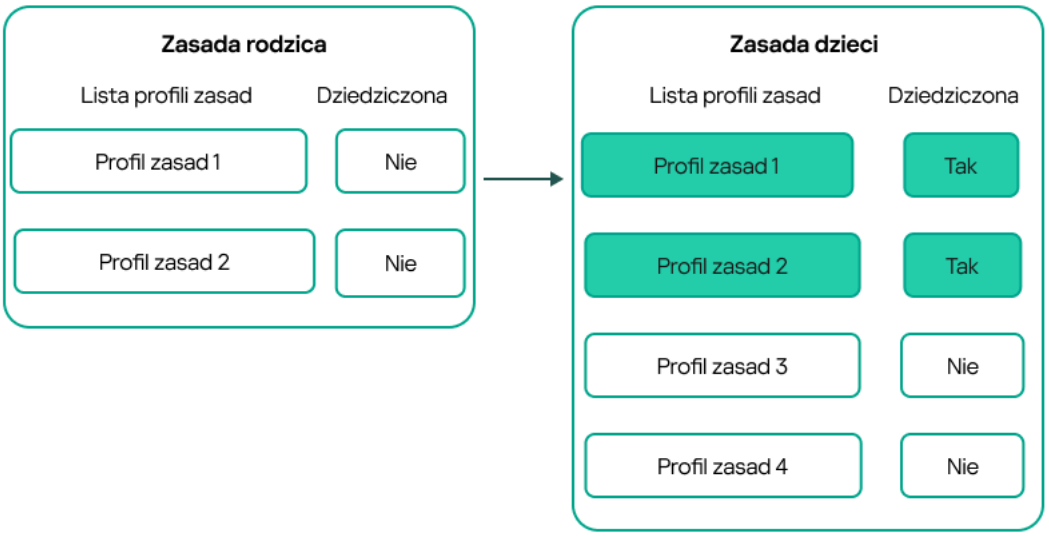
Konfiguracja zarządzanego urządzenia spełnia warunki aktywacji kilku profili zasad

Profile zasad w hierarchii dziedziczenia

Profile zasad z zasad różnych poziomów hierarchii spełniają następujące warunki:

- Zasada niższego poziomu dziedziczy profile zasad z zasady wyższego poziomu. Profil zasad odziedziczony z zasady wyższego poziomu uzyskuje wyższy priorytet niż poziom oryginalnego profilu zasad.

- Nie można zmienić priorytetu odziedziczonego profilu zasad (zobacz poniższy rysunek).

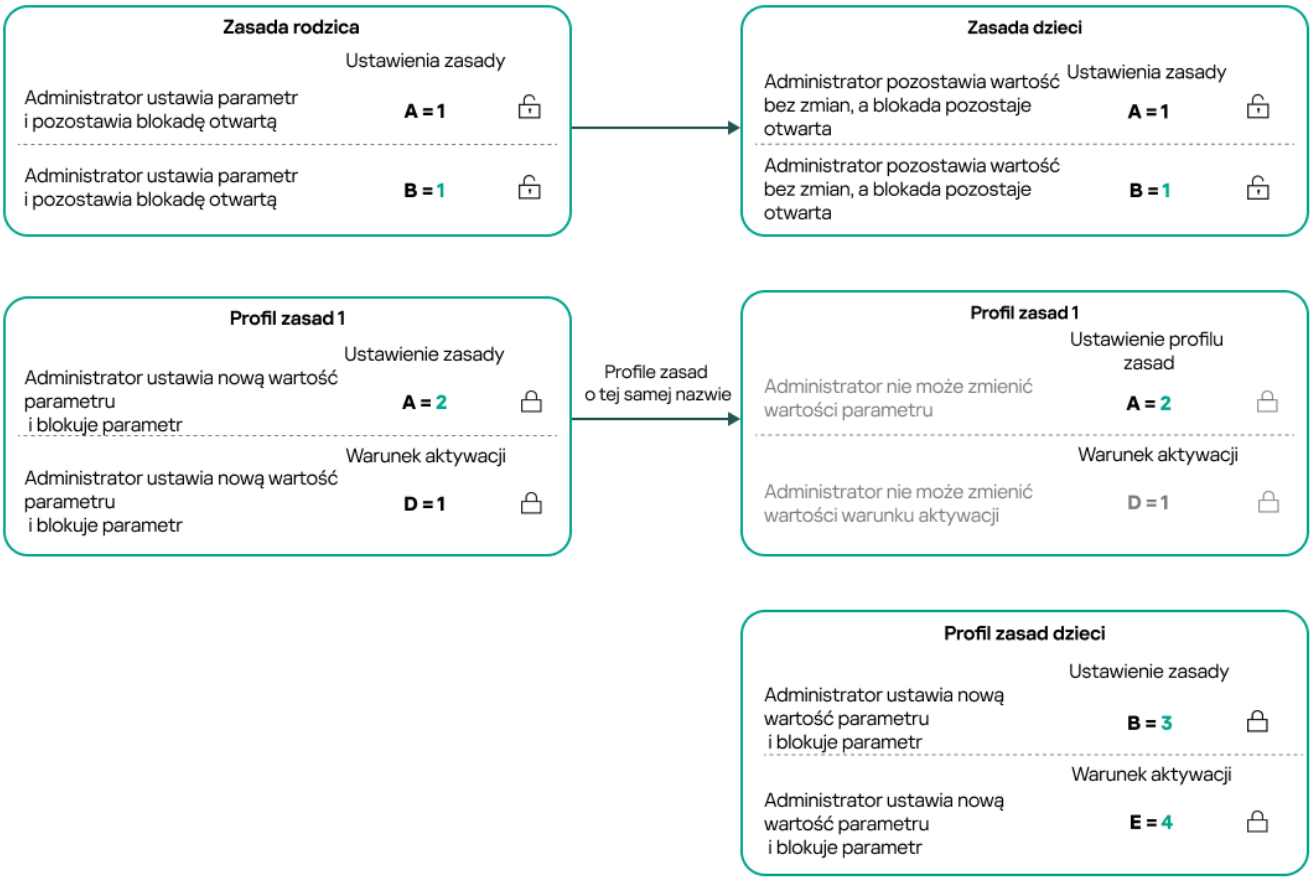


Dziedziczenie profili zasad

Profile zasad o tej samej nazwie

Jeśli istnieją dwie zasady o tych samych nazwach na różnych poziomach hierarchii, te zasady działają zgodnie z następującymi regułami:

- Ustawienia zablokowane i warunek aktywacji profilu zasad wyższego poziomu zmieniają ustawienia i warunek aktywacji profilu zasad niższego poziomu (patrz rysunek poniżej).



Profil podrzędny dziedziczy wartości ustawień z nadrzędnego profilu zasad

- Ustawienia odblokowane i warunek aktywacji profilu zasad wyższego poziomu nie zmieniają ustawień i warunku aktywacji profilu zasad niższego poziomu.

Implementacja ustawień na zarządzanym urządzeniu

Implementację obowiązujących ustawień na zarządzanym urządzeniu można opisać w następujący sposób:

- Wartości wszystkich ustawień, które nie zostały zablokowane, są pobierane z zasady.
- Następnie są nadpisywane wartościami ustawień zarządzanej aplikacji.
- Następnie stosowane są zablokowane wartości ustawień z obowiązującej zasady. Zablokowane wartości ustawień zmieniają wartości odblokowanych obowiązujących ustawień.

Zarządzanie zasadami

Ta sekcja opisuje zarządzanie zasadami i zawiera informacje o przeglądaniu listy zasad, tworzeniu zasady, modyfikowaniu zasady, kopiowaniu zasady, przenoszeniu zasady, wymuszonej synchronizacji, przeglądaniu wykresu stanu dystrybucji zasad i usuwaniu zasady.

Przeglądanie listy zasad

Możesz przejrzeć listy zasad utworzonych dla Serwera administracyjnego lub dla dowolnej grupy administracyjnej.

W celu wyświetlenia listy zasad:

1. W menu głównym przejdź do **Zarządzanie zasobami** → **Hierarchia grup**.

2. W strukturze grupy administracyjnej należy wybrać grupę administracyjną, dla której chcesz przejrzeć listę zasad.

   Lista zasad zostanie wyświetlona w postaci tabeli. Jeśli nie ma zasad, tabela jest pusta. Możesz wyświetlać lub ukrywać kolumny tabeli, zmieniać ich kolejność, przeglądać tylko wiersze, które zawierają określoną przez Ciebie wartość, lub korzystać z wyszukiwania.

Tworzenie zasady

Możesz tworzyć zasady, a także modyfikować i usuwać istniejące zasady.

W celu utworzenia zasady:

1. W menu głównym przejdź do **Zarządzanie zasobami** → **Zasady**.

2. Wybierz grupę administracyjną dla której chcesz utworzyć zasadę:

   - Dla grupy głównej.

     W takim przypadku możesz przejść do następnego kroku.

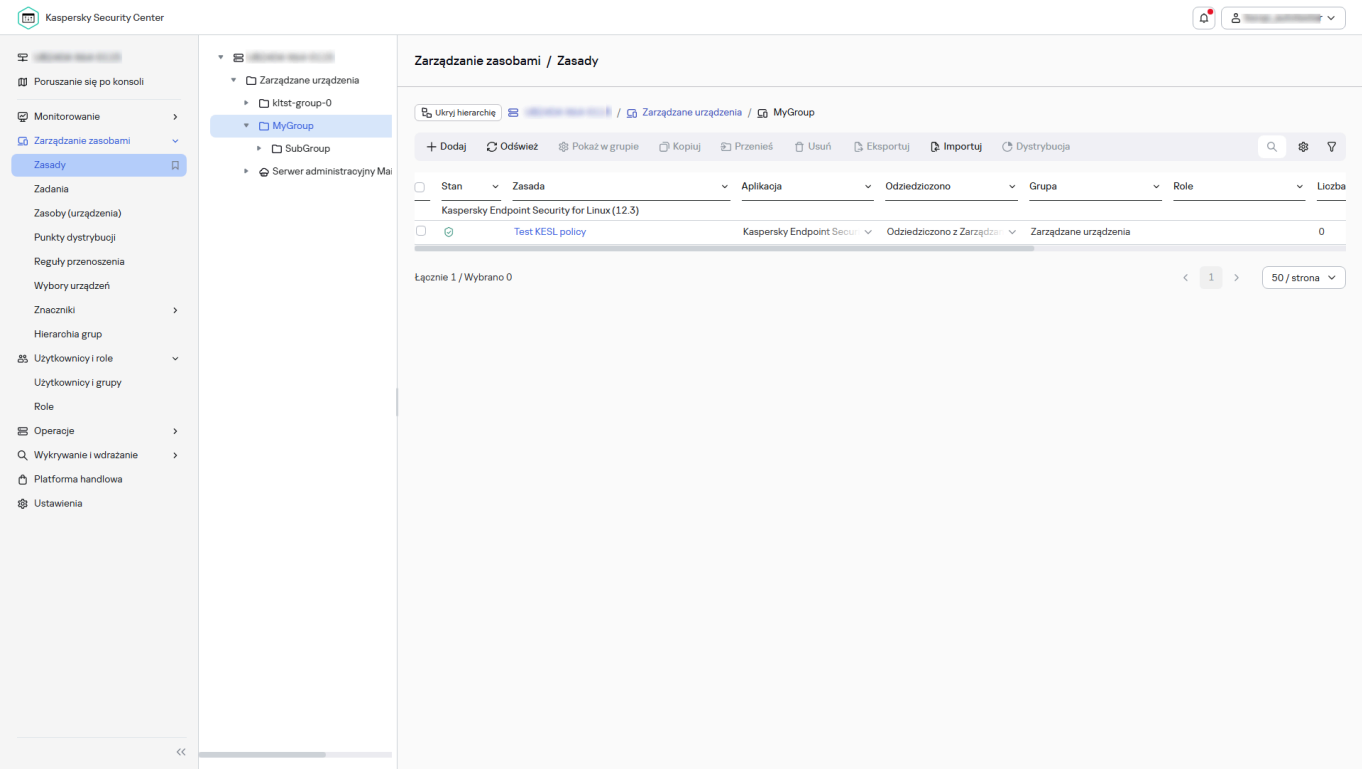
   - Dla grupy podrzędnej:

     a. Kliknij przycisk **Pokaż hierarchię** znajdujący się na górze strony.

     Nazwa przycisku zmieni się na **Ukryj hierarchię**.

     b. W otwartym oknie kliknij odnośnik z nazwą żądanej podgrupy.

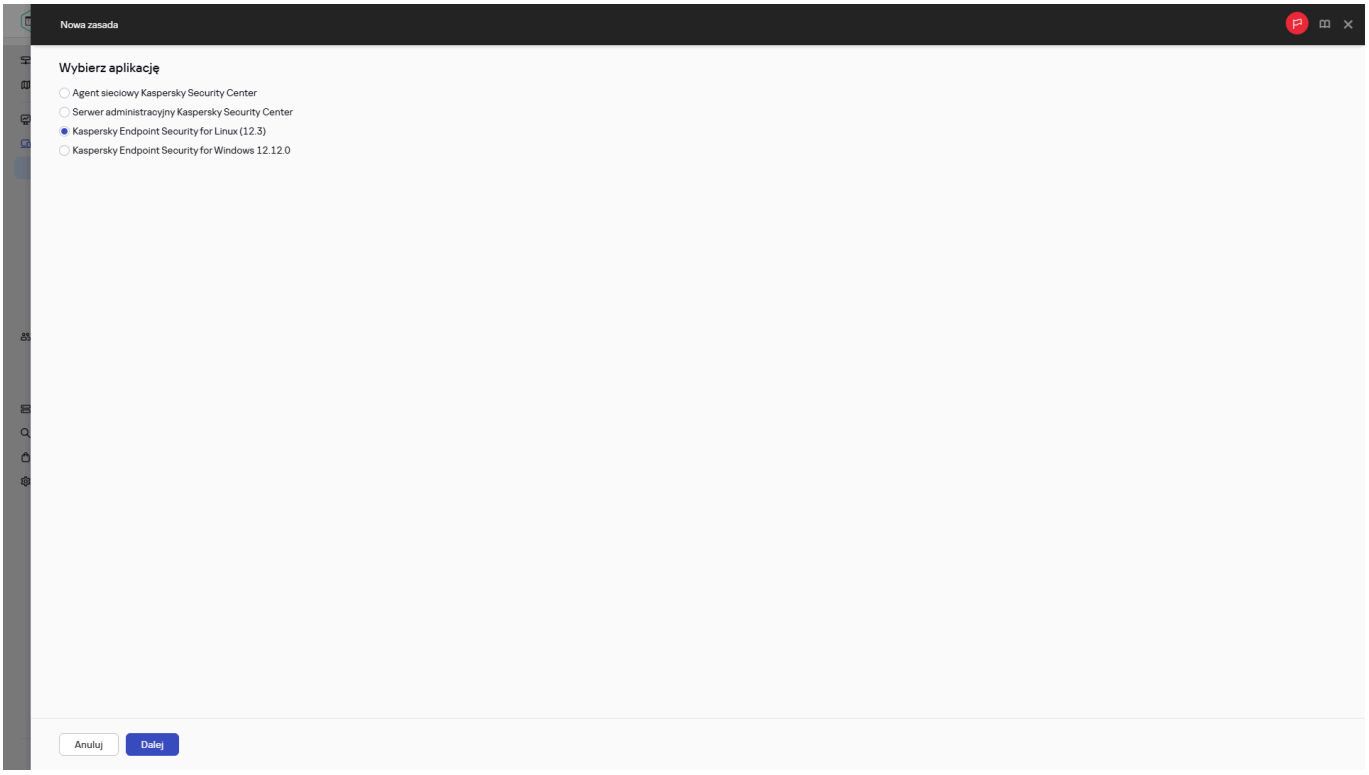
Ścieżka do wybranej grupy jest wyświetlana na górze strony. W razie potrzeby możesz kliknąć odnośnik z nazwą grupy administracyjnej, aby do niej przejść. Domyślnie ostatni odnośnik na ścieżce jest nieaktywny. Można również zamknąć okno hierarchii, klikając przycisk **Ukryj hierarchię**.



Lista zasad

3. Kliknij **Dodaj**.

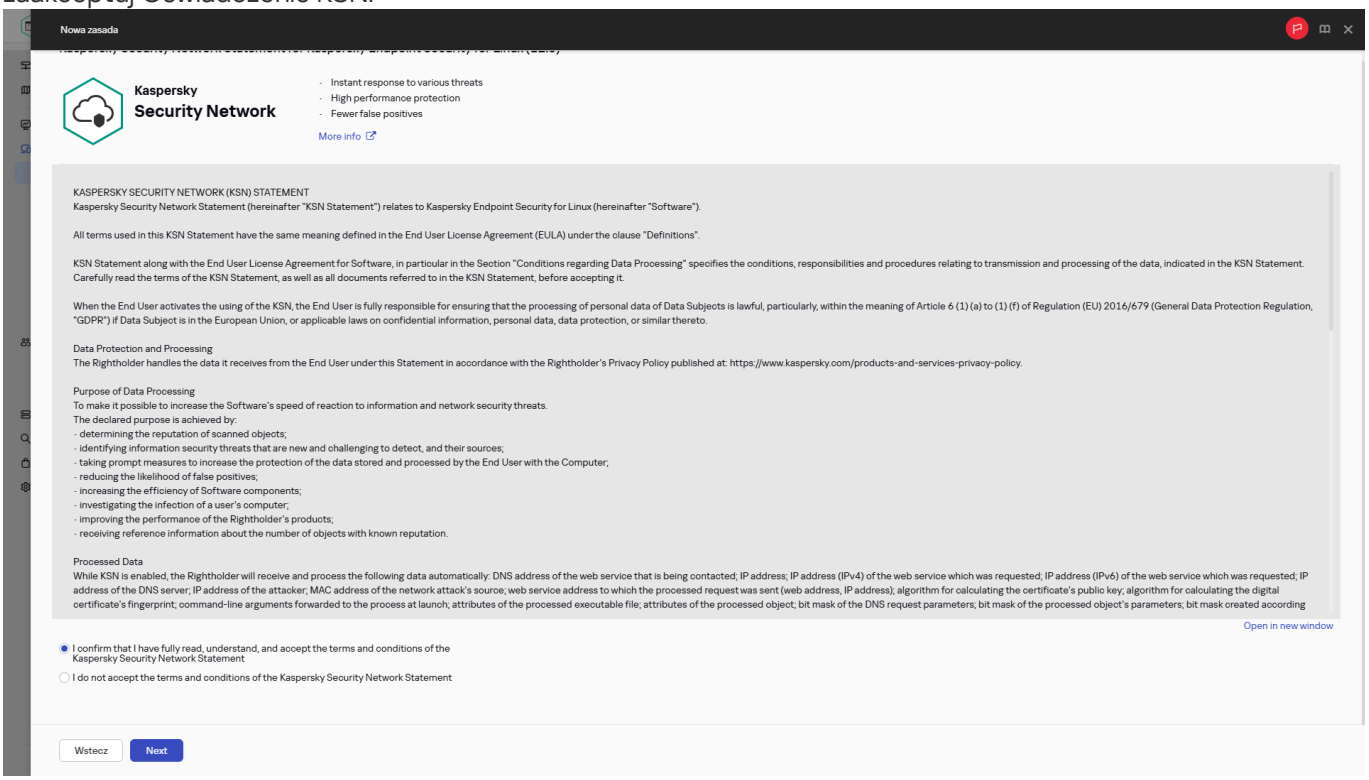
   Zostanie otwarte okno **Wybierz aplikację**.



Tworzenie nowej zasady

4. Wybierz aplikację, dla której chcesz utworzyć zasadę.

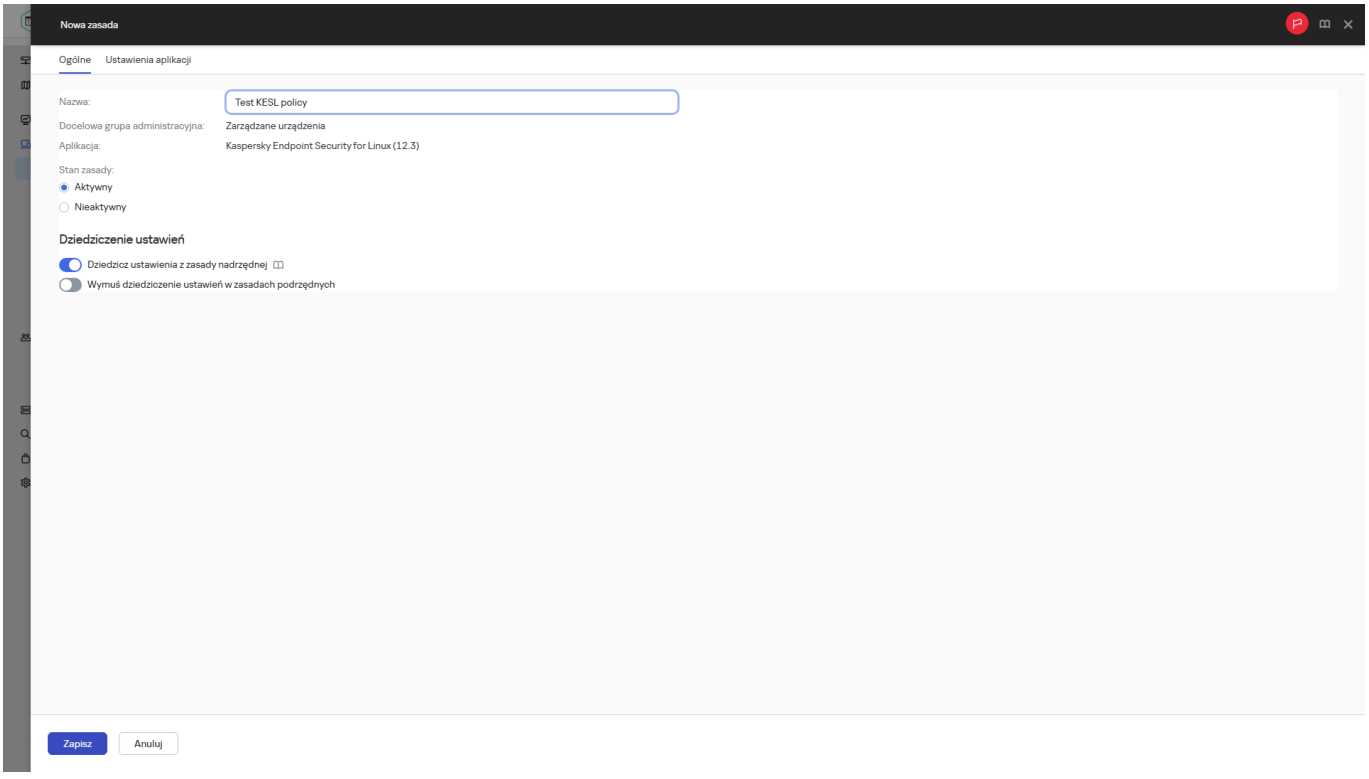
5. Jeśli aplikacja Kaspersky, dla której tworzysz zasadę, obsługuje Kaspersky Security Network, zostaniesz poproszony o zaakceptowanie Oświadczenia KSN. Jeśli chcesz korzystać z Kaspersky Security Network, zaakceptuj Oświadczenie KSN.



Akceptacja Oświadczenia KSN

6. Kliknij **Dalej**.

Zostanie otwarte okno ustawień nowej zasady na zakładce **Ogólne**. Jeśli chcesz, zmień domyślną nazwę, domyślny stan oraz domyślne ustawienia dziedziczenia zasady.



Okno ustawień nowej zasady

7. Wybierz zakładkę **Ustawienia aplikacji**.

Lub kliknij **Zapisz** i zakończ działanie. Zasada pojawi się na liście zasad i będziesz mógł w późniejszym czasie edytować jego ustawienia.

8. Na zakładce **Ustawienia aplikacji**, w lewej części okna wybierz żądaną kategorię, a w prawej części okna zmień ustawienia zasady. Możesz edytować ustawienia zasady w każdej kategorii (sekcja).

   Zestaw ustawień zależy od aplikacji, dla której tworzysz zasadę. Więcej informacji można znaleźć w:

   - Konfiguracja Serwera administracyjnego
   - Ustawienia zasady Agenta sieciowego
   - Kaspersky Endpoint Security for Linux — pomoc
   - Pomoc Kaspersky Endpoint Security for Windows

   Szczegółowe informacje dotyczące ustawień innych aplikacji zabezpieczających można znaleźć w dokumentacji dla odpowiedniej aplikacji.

   Podczas edytowania ustawień możesz kliknąć **Anuluj**, aby anulować ostatnie działanie.

9. Kliknij **Zapisz**, aby zapisać zasadę.

   Wyświetlane jest powiadomienie o następującej treści: **Zasada jest zapisywana i dystrybuowana przez hierarchię Serwerów administracyjnych**.

   Jeśli zasada przejdzie walidację, wyświetlane jest następujące powiadomienie: **Zasada została zapisana**.

   Jeśli zasada nie przejdzie walidacji, wyświetlane jest następujące powiadomienie: **Nie udało się zapisać ani dystrybuować zasady przez hierarchię Serwerów administracyjnych. Skontaktuj się z Pomocą techniczną**. Możesz przejrzeć i zmienić ustawienia zasady, a następnie spróbować ponownie. Jeśli problem nadal występuje, skontaktuj się z Pomocą techniczną.

Zasada zostanie wyświetlona na liście zasad. Po utworzeniu zasady zdarzenia dotyczące zmiany zasady są eksportowane do systemu SIEM, jeśli ta opcja jest włączona.

Ogólne ustawienia zasady

Ogólne

Na zakładce **Ogólne** możesz zmodyfikować stan zasady oraz określić dziedziczenie ustawień zasady:

- W sekcji **Stan zasady** możesz wybrać jeden z trybów zasady:

  - **Aktywny**

    Jeśli wybrano tę opcję, zasada jest aktywna.

    Domyślnie opcja ta jest zaznaczona.

  - **Użytkownik mobilny**

    Jeżeli ta opcja jest zaznaczona, zasada stanie się aktywna, gdy urządzenie znajdzie się poza siecią korporacyjną.

- **Nieaktywny**

  Jeśli ta opcja jest zaznaczona, zasada stanie się nieaktywna, ale wciąż będzie przechowywana w folderze **Zasady**. Jeśli jest to wymagane, zasadę można aktywować.

- W grupie ustawień **Dziedziczenie ustawień** możesz skonfigurować dziedziczenie zasady:

  - **Dziedzicz ustawienia z zasady nadrzędnej**

    Jeśli ta opcja jest włączona, wartości ustawień zasady są dziedziczone z zasady grupy najwyższego poziomu, są więc zablokowane.

    Domyślnie opcja ta jest włączona.

  - **Wymuś dziedziczenie ustawień w zasadach podrzędnych**

    Jeśli ta opcja jest włączona, po zastosowaniu zmian w zasadzie zostaną wykonane następujące czynności:

    - Wartości ustawień zasady zostaną rozesłane do zasad podgrup administracyjnych, czyli do zasad podrzędnych.

    - Opcja **Dziedzicz ustawienia z zasady nadrzędnej** będzie automatycznie włączona w podsekcji **Dziedziczenie ustawień** sekcji **Ogólne** okna właściwości każdej zasady podrzędnej.

    Jeśli ta opcja jest włączona, ustawienia zasad podrzędnych są zablokowane.

    Domyślnie opcja ta jest wyłączona.

Konfiguracja zdarzenia

Zakładka **Konfiguracja zdarzenia** umożliwia skonfigurowanie zapisywania zdarzeń oraz powiadamiania o zdarzeniach. Zdarzenia są grupowane według istotności na następujących zakładkach:

- **Krytyczny**

  Sekcja **Krytyczny** nie jest wyświetlana we właściwościach zasad Agenta sieciowego.

- **Błąd funkcjonalny**

- **Ostrzeżenie**

- **Informacja**

W każdej sekcji, lista wyświetla typy zdarzeń oraz domyślny czas przechowywania zdarzeń na Serwerze administracyjnym (w dniach). Kliknięcie typu zdarzenia umożliwia określenie następujących ustawień:

- **Rejestracja zdarzenia**

  Możesz określić ilość dni przechowywania zdarzenia oraz wybrać miejsce przechowywania zdarzenia:

  - **Eksportuj do systemu SIEM przez Dziennik systemowy**

  - **Przechowuj w systemowym dzienniku zdarzeń urządzenia**

  - **Przechowuj w systemowym dzienniku zdarzeń Serwera administracyjnego**

- **Powiadomienia o zdarzeniu**

Możesz wybrać, jeśli chcesz być powiadamiany o zdarzeniu w jeden z następujących sposobów:

- **Powiadom przez e-mail**
- **Powiadom przez SMS**
- **Powiadom, uruchamiając plik wykonywalny lub skrypt**
- **Powiadom przez SNMP**

Domyślnie, używane są ustawienia powiadamiania, określone na zakładce Właściwości Serwera administracyjnego (takie, jak adres odbiorcy). Jeśli chcesz, możesz zmienić te ustawienia na zakładkach: **E-mail**, **SMS** i **Plik wykonywalny do uruchomienia**.

Zakładka **Konfiguracja zdarzenia** wyświetla również powiadomienie, gdy dodawane są nowe typy zdarzeń (np. w nowej wersji aplikacji) i umożliwia zastosowanie nowych ustawień poprzez kliknięcie przycisku **Zapisz** lub przycisku **Zapisz i zamknij**.

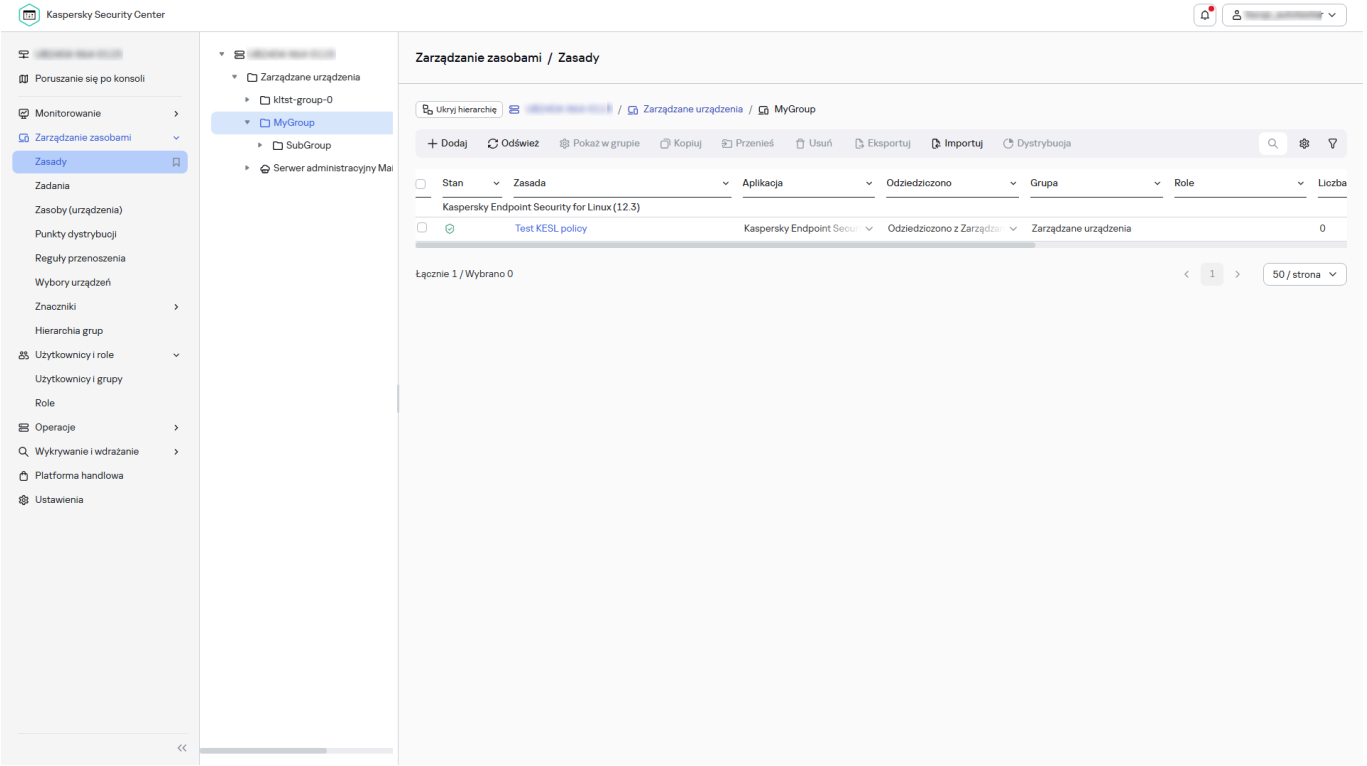
Historia rewizji

Zakładka **Historia rewizji** umożliwia przeglądanie listy rewizji zasady, porównywanie rewizji zasady i wycofanie zmian wprowadzonych do zasady, jeśli to konieczne.

Modyfikowanie zasady

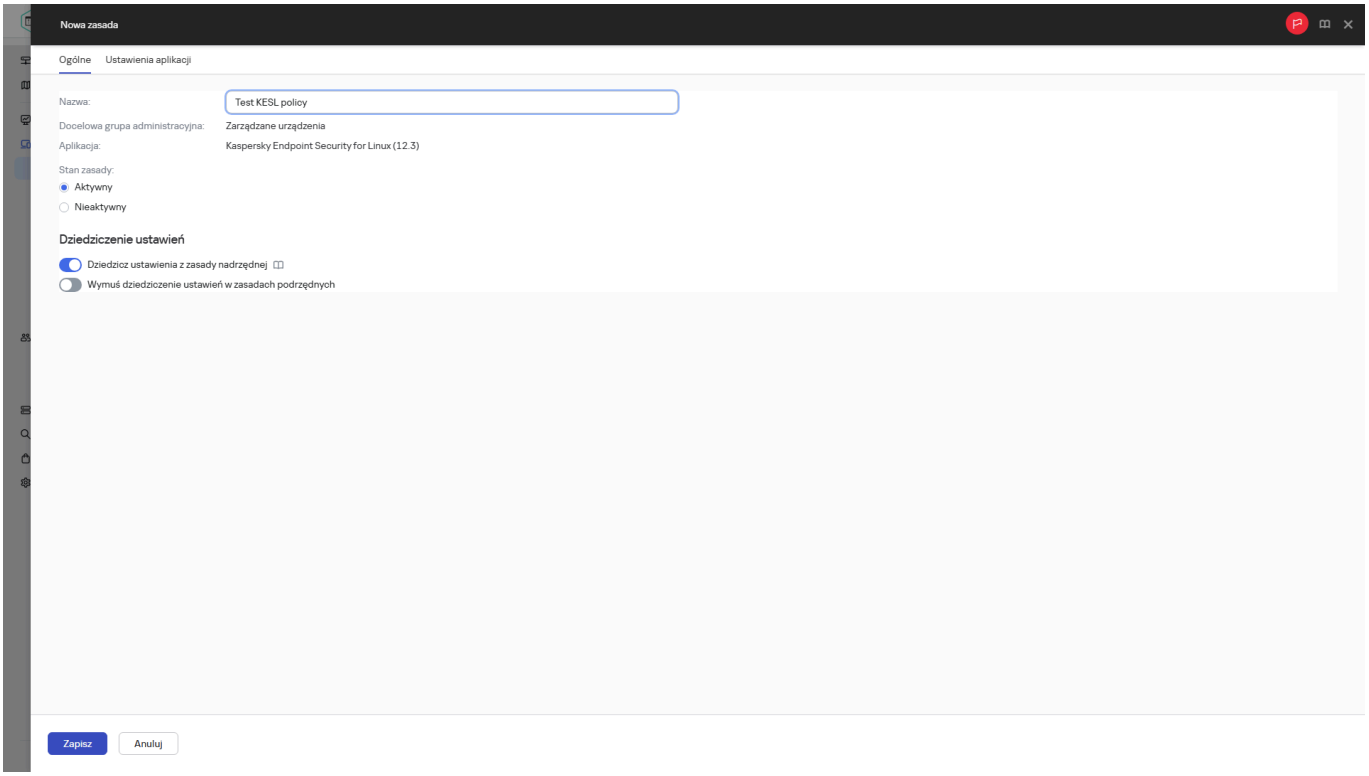
W celu zmodyfikowania zasady:

1. W menu głównym przejdź do **Zarządzanie zasobami** → **Zasady**.



2. Kliknij zasadę, którą chcesz zmodyfikować.

Zostanie otwarte okno ustawień zasady.



3. Określ ustawienia główne oraz ustawienia aplikacji, dla której tworzysz zasadę. Więcej informacji można znaleźć w:

   - Konfiguracja Serwera administracyjnego
   - Ustawienia zasady Agenta sieciowego
   - Kaspersky Endpoint Security for Linux — pomoc
   - Pomoc Kaspersky Endpoint Security for Windows

   Szczegółowe informacje dotyczące ustawień innych aplikacji zabezpieczających można znaleźć w dokumentacji dla tej aplikacji.

4. Kliknij **Zapisz**.

   Wyświetlane jest powiadomienie o następującej treści: **Zasada jest zapisywana i dystrybuowana przez hierarchię Serwerów administracyjnych**.

   Jeśli zasada przejdzie walidację, wyświetlane jest następujące powiadomienie: **Zasada została zapisana**.

   Jeśli zasada nie przejdzie walidacji, wyświetlane jest następujące powiadomienie: **Nie udało się zapisać ani dystrybuować zasady przez hierarchię Serwerów administracyjnych. Skontaktuj się z Pomocą techniczną**. Możesz przejrzeć i zmienić ustawienia zasady, a następnie spróbować ponownie. Jeśli problem nadal występuje, skontaktuj się z Pomocą techniczną.

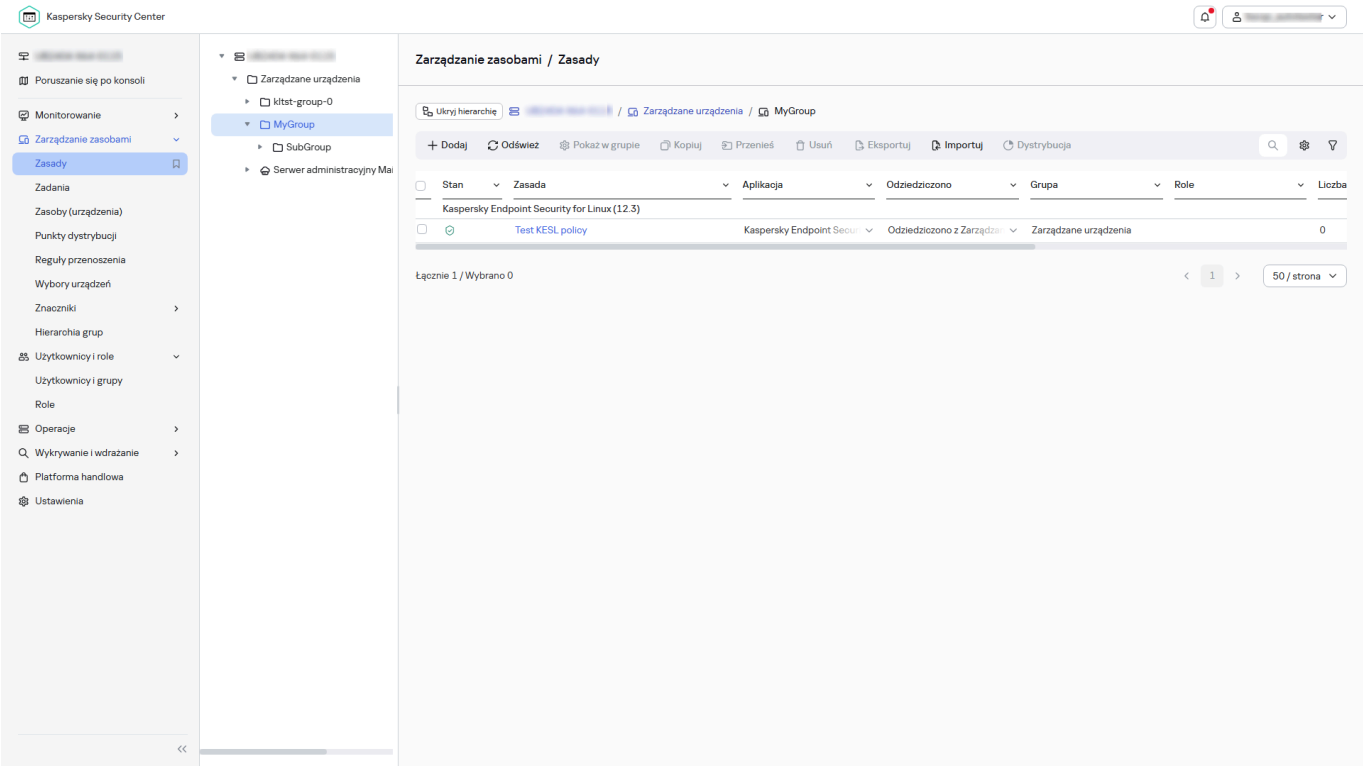
Zmiany wprowadzone w zasadzie zostaną zapisane we właściwościach zasady i pojawią się w sekcji **Historia rewizji**. Po zmodyfikowaniu zasady zdarzenia zmiany zasady są eksportowane do systemu SIEM, jeśli ta opcja jest włączona.

W razie potrzeby możesz porównać rewizje zasad. Ta opcja jest dostępna dla zasad Serwera administracyjnego, Agenta sieciowego, Kaspersky Endpoint Security for Windows (od wersji 14.0 wtyczki webowej) oraz Kaspersky Endpoint Security for Mac (od wersji 12.2.1 z poprawką A wtyczki webowej).

Włączanie i wyłączanie opcji dziedziczenia zasady

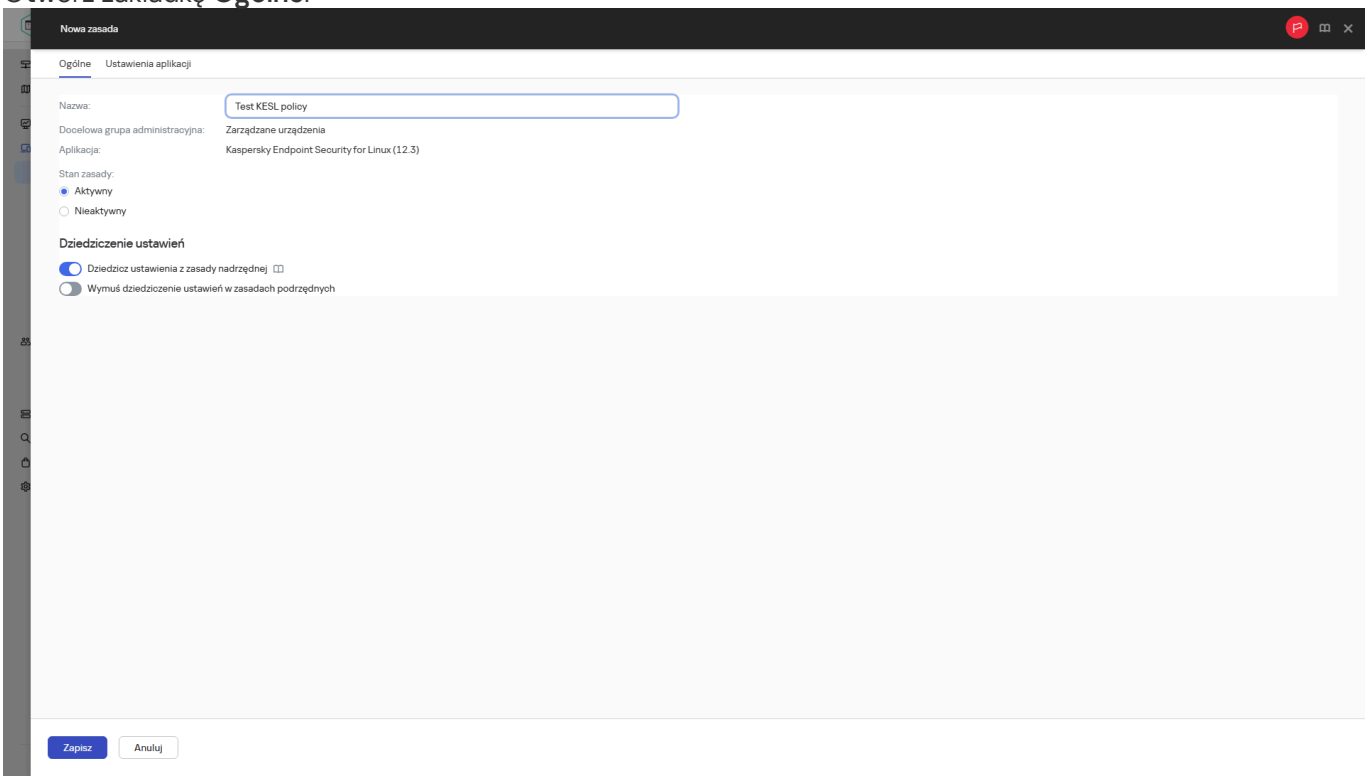
Aby włączyć lub wyłączyć opcję dziedziczenia w zasadzie:

1. Otwórz wymaganą zasadę.



Lista zasad

2. Otwórz zakładkę **Ogólne**.



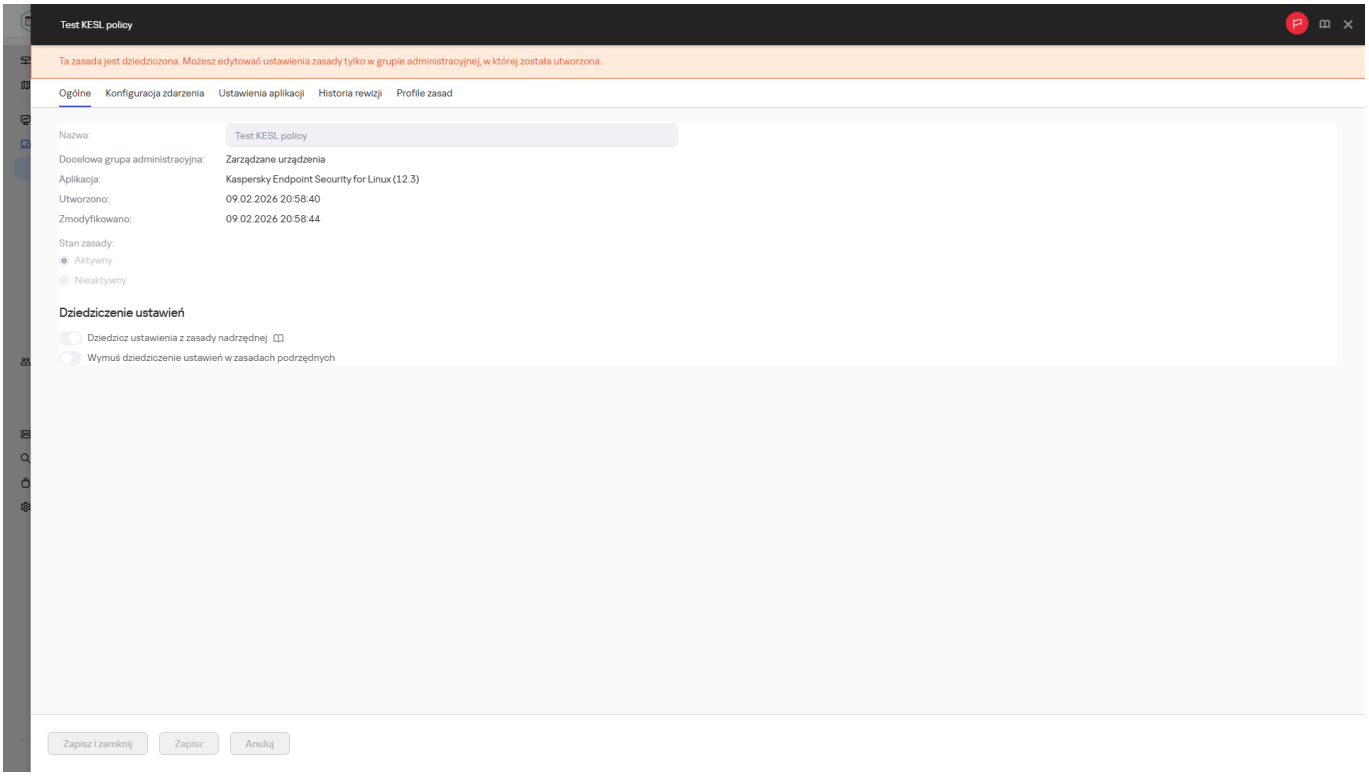
Tworzenie nowej zasady

3. Włącz lub wyłącz dziedziczenie zasad:

- Jeśli włączysz opcję **Dziedzicz ustawienia z zasady nadrzędnej** w zasadzie podrzędnej i administrator zablokuje niektóre ustawienia w zasadzie nadrzędnej, wówczas nie będzie można zmienić tych ustawień w zasadzie podrzędnej.

- Jeśli wyłączysz opcję **Dziedzicz ustawienia z zasady nadrzędnej** w zasadzie podrzędnej, wówczas możesz zmienić wszystkie ustawienia w zasadzie podrzędnej nawet wtedy, gdy niektóre ustawienia są zablokowane w zasadzie nadrzędnej.

- Jeśli włączysz opcję **Wymuś dziedziczenie ustawień w zasadach podrzędnych** w grupie nadrzędnej, spowoduje to włączenie opcji **Dziedzicz ustawienia z zasady nadrzędnej** dla każdej zasady podrzędnej. W tym przypadku nie możesz wyłączyć tej opcji dla żadnej zasady podrzędnej. Wszystkie ustawienia, które są zablokowane w zasadzie nadrzędnej, są dziedziczone w grupach podrzędnych w sposób wymuszony i nie możesz zmienić tych ustawień w grupach podrzędnych.



Zablokowane ustawienia zasady

4. Kliknij przycisk **Zapisz**, aby zapisać zmiany, lub kliknij przycisk **Anuluj**, aby odrzucić zmiany.

Domyślnie, opcja **Dziedzicz ustawienia z zasady nadrzędnej** jest włączona dla nowej zasady.

Jeśli zasada zawiera profile, wszystkie zasady podrzędne dziedziczą te profile.

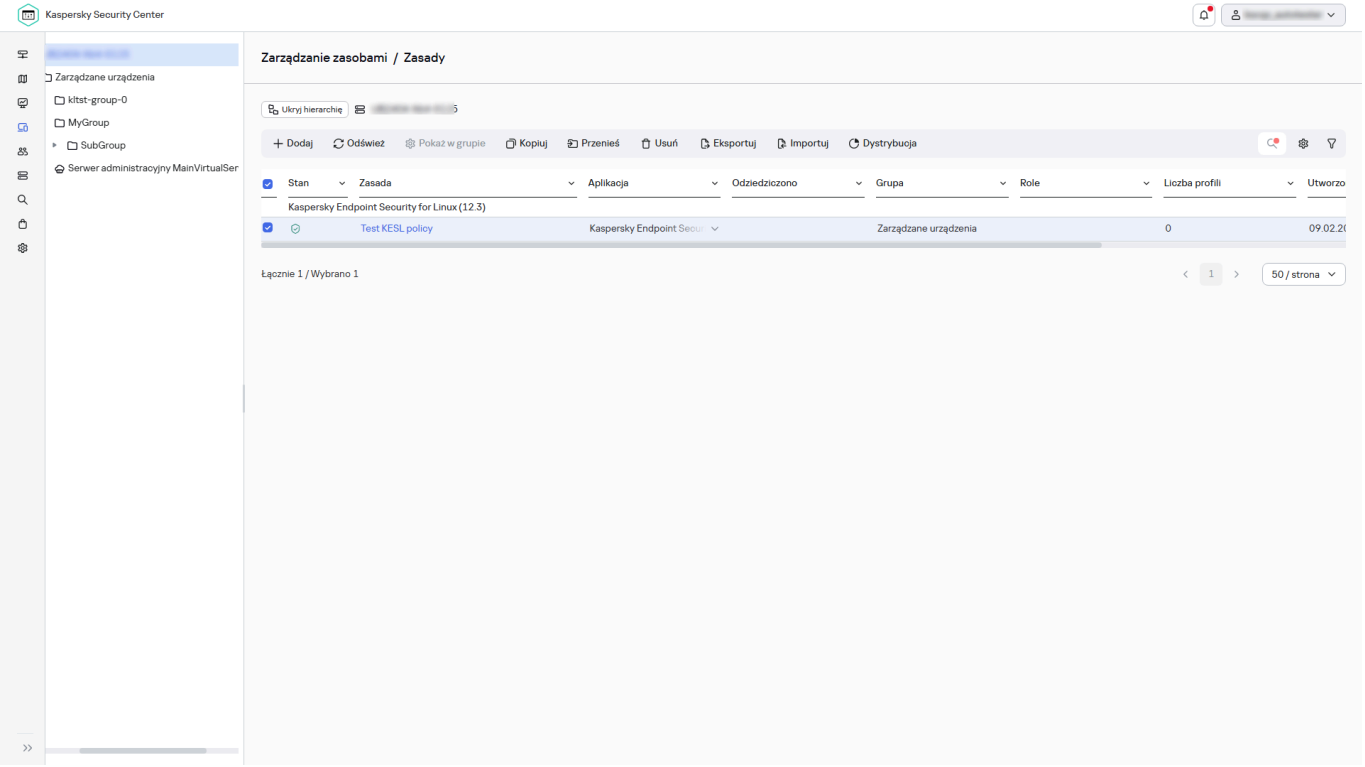
Kopiowanie zasady

Możesz skopiować zasady z jednej grupy administracyjnej do innej.

W celu skopiowania zasady do innej grupy administracyjnej:

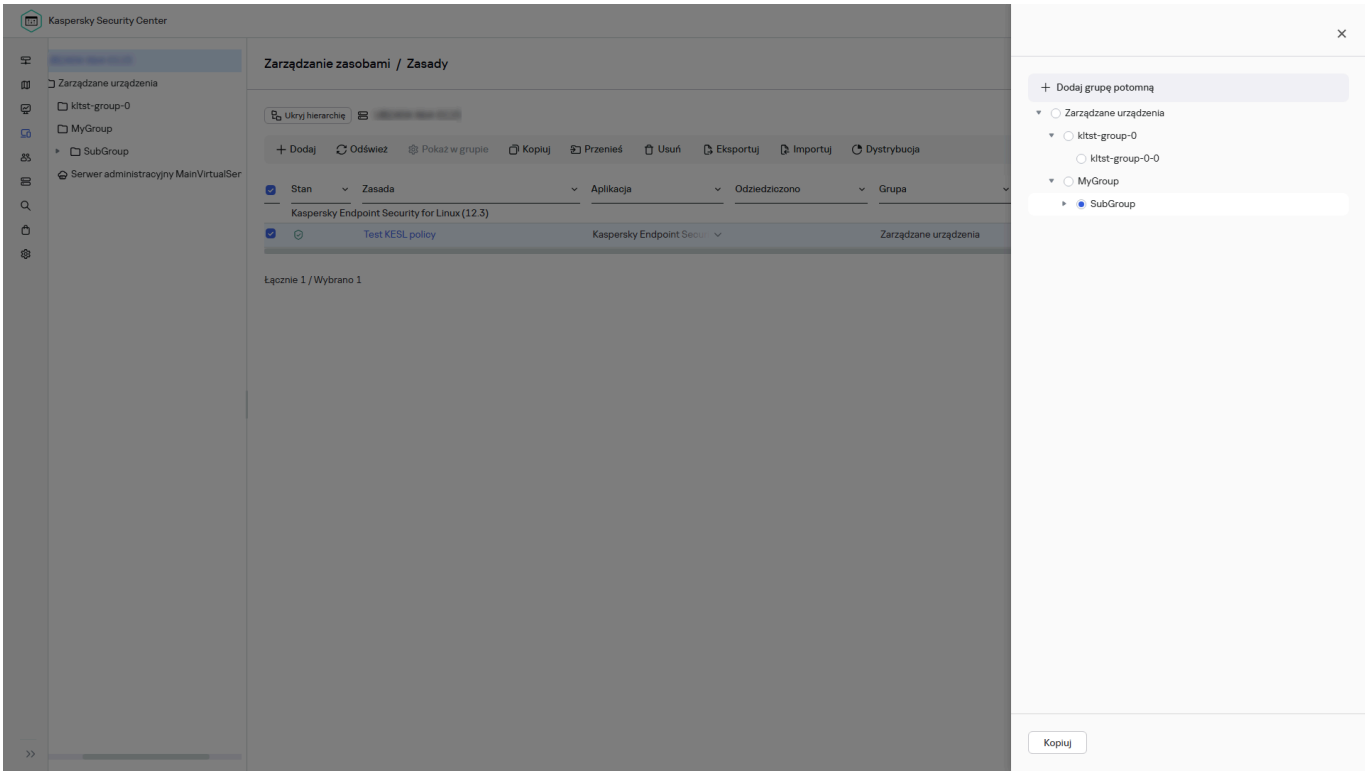
1. W menu głównym przejdź do **Zarządzanie zasobami** → **Zasady**.

2. Zaznacz pole obok zasady (lub zasad), którą (które) chcesz skopiować.



3. Kliknij przycisk **Kopiuj**.

   W prawej części okna pojawi się drzewo grup administracyjnych.



4. Z drzewa wybierz grupę docelową, czyli grupę, do której chcesz skopiować zasadę (zasady).

5. W dolnej części okna kliknij przycisk **Kopiuj**.

6. Kliknij **OK**, aby potwierdzić działanie.

Zasada (zasady) zostanie skopiowana do grupy docelowej ze wszystkimi swoimi profilami. Stan każdej skopiowanej zasady w grupie docelowej będzie **Nieaktywny**. W dowolnym momencie możesz zmienić stan na **Aktywny**.

Jeżeli zasada z nazwą podobną do nazwy nowo przeniesionej zasady znajduje się już w grupie docelowej, do nazwy nowo przeniesionej zasady zostanie dodany przyrostek (<kolejny numer>), na przykład: (1).

Przenoszenie zasady

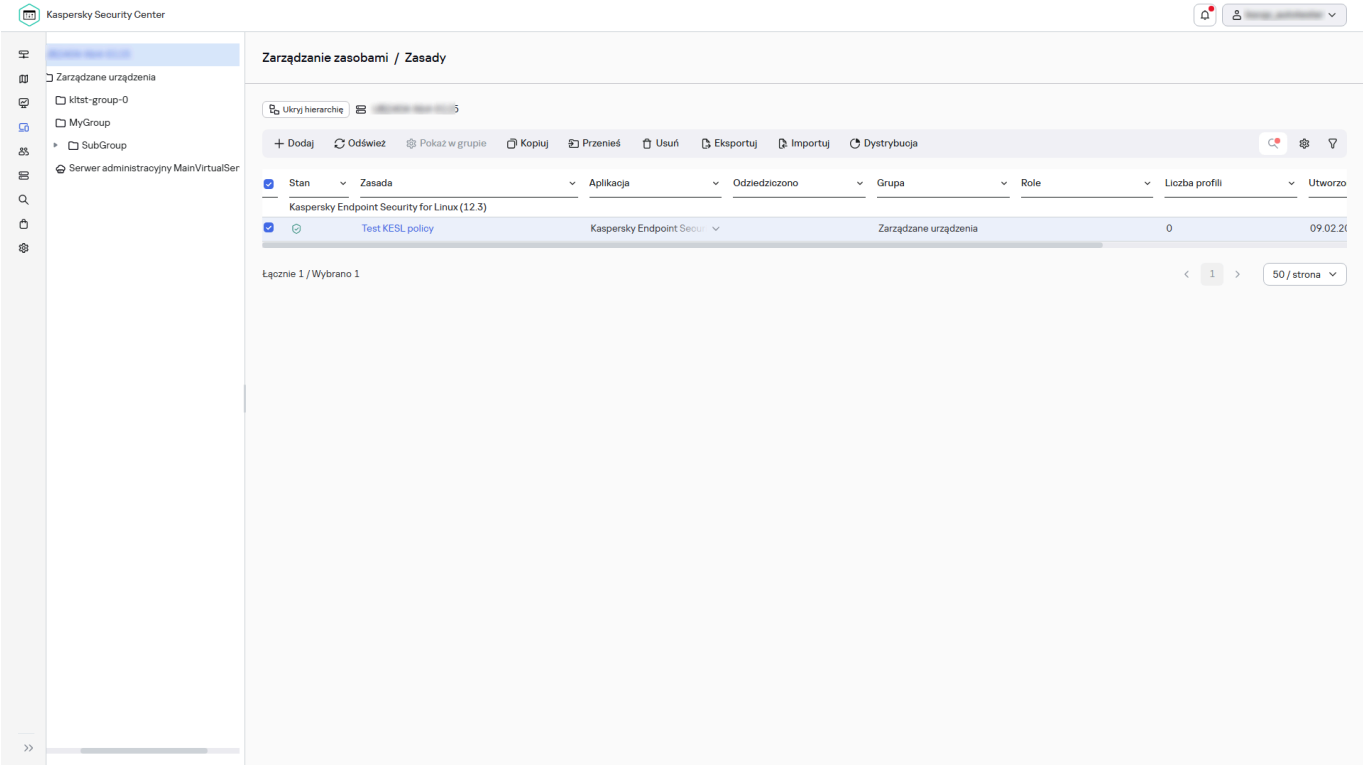
Możesz przenieść zasady z jednej grupy administracyjnej do innej. Na przykład, chcesz usunąć grupę, ale chcesz używać jej zasad dla innej grupy. W tym przypadku można przenieść zasadę ze starszej grupy do nowej zanim usuniesz starszą grupę.

> Podczas przenoszenia zasady do innej grupy administracyjnej historia rewizji zasady jest usuwana. Karta **Historia rewizji** wyświetla informacje tylko o ostatniej zmianie.

W celu przeniesienia zasady do innej grupy administracyjnej:

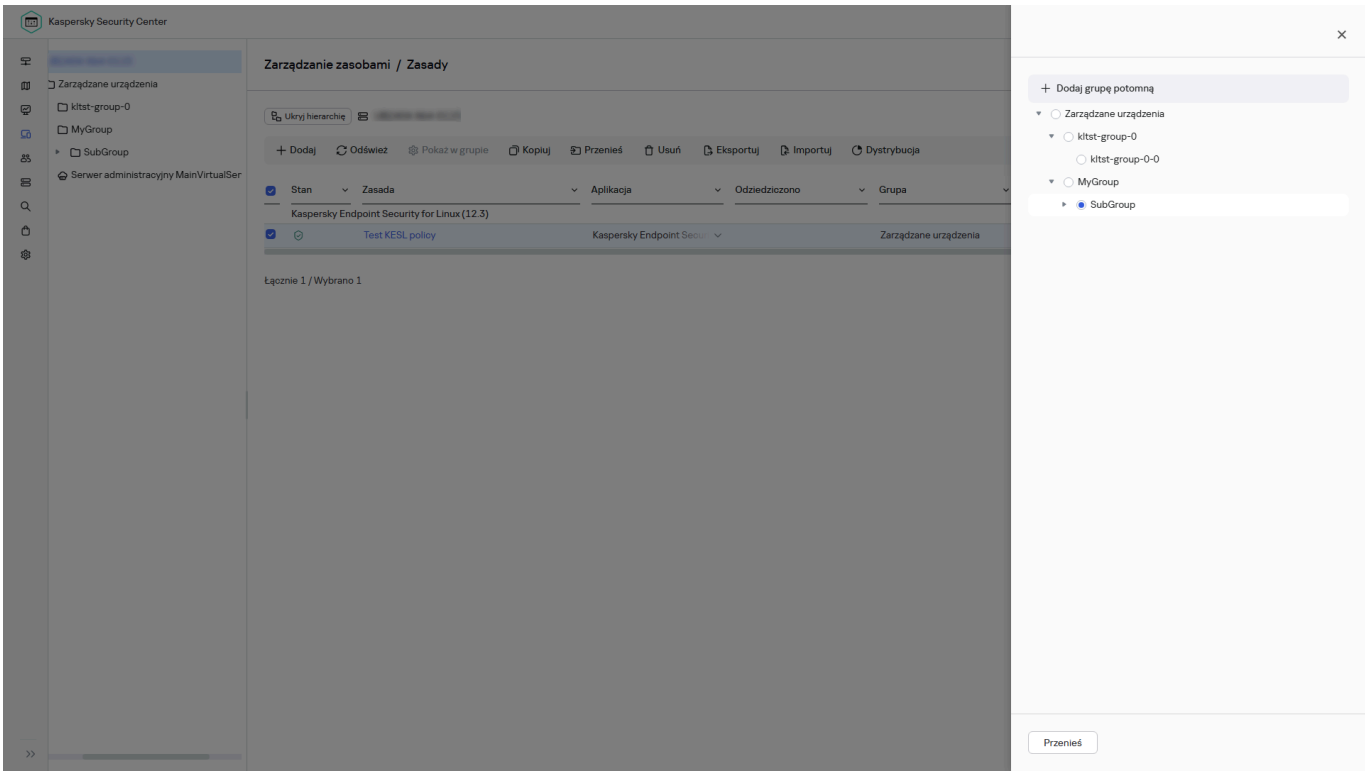
1. W menu głównym przejdź do **Zarządzanie zasobami** → **Zasady**.

2. Zaznacz pole obok zasady (lub zasad), którą (które) chcesz przenieść.



3. Kliknij przycisk **Przenieś**.

   W prawej części okna pojawi się drzewo grup administracyjnych.



4. Z drzewa wybierz grupę docelową, czyli grupę, do której chcesz przenieść zasadę (lub zasady).

5. W dolnej części okna kliknij przycisk **Przenieś**.

6. Kliknij **OK**, aby potwierdzić działanie.

   Jeśli zasada nie jest dziedziczona z grupy źródłowej, zostaje przeniesiona do grupy docelowej ze wszystkimi swoimi profilami. Stan zasady w grupie docelowej będzie **Nieaktywny**. W dowolnym momencie możesz zmienić stan na **Aktywny**.

   Jeśli zasada jest dziedziczona z grupy źródłowej, pozostanie w grupie źródłowej. Zostanie skopiowana do grupy docelowej ze wszystkimi swoimi profilami. Stan zasady w grupie docelowej będzie **Nieaktywny**. W dowolnym momencie możesz zmienić stan na **Aktywny**.

Jeżeli zasada z nazwą podobną do nazwy nowo przeniesionej zasady znajduje się już w grupie docelowej, do nazwy nowo przeniesionej zasady zostanie dodany przyrostek (<kolejny numer>), na przykład: (1).

Eksportowanie zasady

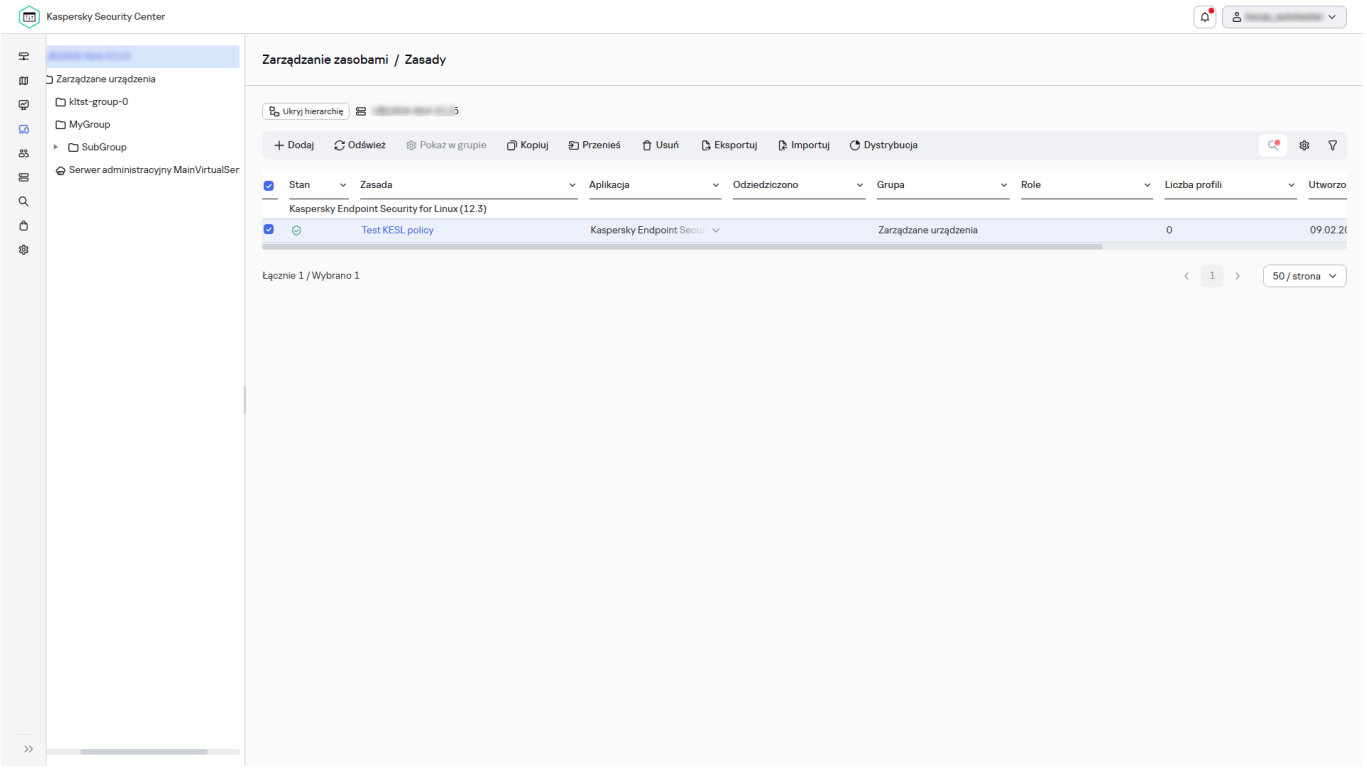
Kaspersky Security Center Linux umożliwia zapisanie zasady, jej ustawień i profili zasad w pliku KLP. Możesz użyć tego pliku KLP do zaimportowania zapisanej zasady zarówno do Kaspersky Security Center Windows, jak i Kaspersky Security Center Linux.

W celu wyeksportowania zasady:

1. W menu głównym przejdź do **Zarządzanie zasobami** → **Zasady**.

2. Zaznacz pole obok zasady, którą chcesz wyeliminować.

Nie można jednocześnie eksportować wielu zasad. Jeśli wybierzesz więcej niż jedną zasadę, przycisk **Eksportuj** będzie nieaktywny.



Wybór zasady do eksportu

3. Kliknij przycisk **Eksportuj**.

4. W otwartym oknie **Zapisz jako** określ nazwę i ścieżkę dostępu pliku zasady. Kliknij przycisk **Zapisz**.

   Okno **Zapisz jako** jest wyświetlane tylko wtedy, gdy korzystasz z przeglądarki Google Chrome, Microsoft Edge lub Opera. Jeśli używasz innej przeglądarki, plik zasady jest automatycznie zapisywany w folderze **Pobrane**.

Importowanie zasady

Kaspersky Security Center Linux umożliwia importowanie zasady z pliku KLP. Plik KLP zawiera wyeksportowaną zasadę, jej ustawienia oraz profile zasad.

W celu zaimportowania zasady:

1. W menu głównym przejdź do **Zarządzanie zasobami** → **Zasady**.

2. Kliknij przycisk **Importuj**.

3. Kliknij przycisk **Przeglądaj**, aby wybrać plik zasad, który chcesz zaimportować.

4. W otwartym oknie określ ścieżkę do pliku zasady KLP, a następnie kliknij przycisk **Otwórz**. Pamiętaj, że możesz wybrać tylko jeden plik zasady.

   Rozpoczyna się przetwarzanie zasady.

5. Po pomyślnym przetworzeniu zasady wybierz Grupa administracyjna, do których chcesz przypisać zasadę.

6. Kliknij przycisk **Zakończone**, aby zakończyć import zasad.

Pojawi się powiadomienie z wynikami importu. Jeśli zasada została pomyślnie zaimportowana, możesz kliknąć łącze **Szczegóły**, aby wyświetlić właściwości zasady.

Po pomyślnym imporcie zasada zostanie wyświetlona na liście zasad. Importowane są również ustawienia i profile zasad. Niezależnie od statusu zasady, który został wybrany podczas eksportu, importowana zasada jest nieaktywna. Możesz zmienić stan zasady we właściwościach zasady.

> Jeżeli nowo importowana zasada ma nazwę identyczną z nazwą istniejącej zasady, nazwa importowanej zasady jest rozszerzana o indeks **(<następny numer kolejny>)**, na przykład: **(1)**, **(2)**.

Wymuszona synchronizacja

Chociaż Kaspersky Security Center Linux automatycznie synchronizuje stan, ustawienia, zadania i zasady dla zarządzanych urządzeń, to w niektórych przypadkach administrator musi dokładnie wiedzieć, czy w danym momencie dla określonego urządzenia została już przeprowadzona synchronizacja.

Synchronizowanie pojedynczego urządzenia

W celu wymuszenia synchronizacji między Serwerem administracyjnym a zarządzanym urządzeniem:

1. W menu głównym przejdź do **Zarządzanie zasobami** → **Zasoby (urządzenia)**.
2. Kliknij nazwę urządzenia, które chcesz zsynchronizować z Serwerem administracyjnym.

   Zostanie otwarte okno właściwości na wybranej sekcji **Ogólne**.
3. Kliknij przycisk **Wymuś synchronizację**.

Aplikacja synchronizuje wybrane urządzenie z Serwerem administracyjnym.

Synchronizowanie kilku urządzeń

W celu wymuszenia synchronizacji między Serwerem administracyjnym a kilkoma zarządzanymi urządzeniami:

1. Otwórz listę urządzeń grupy administracyjnej lub wyboru urządzeń:
   - Uruchom wybór urządzeń, aby przejrzeć listę urządzeń.
   - W menu głównym przejdź do **Zarządzanie zasobami** → **Zasoby (urządzenia)**, a następnie wybierz grupę administracyjną zawierającą urządzenia do synchronizacji:
     - W przypadku grupy głównej możesz przejść do następnego kroku.
     - Aby dodać podgrupę, kliknij przycisk **Pokaż hierarchię** u góry strony, a następnie w oknie, które zostanie otwarte, kliknij nazwę podgrupy.

       Ścieżka do wybranej grupy jest wyświetlana na górze strony. W razie potrzeby możesz kliknąć odnośnik z nazwą grupy administracyjnej, aby do niej przejść. Domyślnie ostatni odnośnik na ścieżce jest nieaktywny. Można również zamknąć okno hierarchii, klikając przycisk **Ukryj hierarchię**.

2. Zaznacz pola obok urządzeń, które chcesz zsynchronizować z Serwerem administracyjnym.

3. Nad listą zarządzanych urządzeń kliknij przycisk wielokropka (...), a następnie kliknij przycisk **Wymuś synchronizację**.

   Aplikacja synchronizuje wybrane urządzenia z Serwerem administracyjnym.

4. Na liście urządzeń sprawdź, czy czas ostatniego połączenia z Serwerem administracyjnym uległ zmianie dla wybranych urządzeń na bieżący czas. Jeśli czas nie został zmieniony, wówczas zmień zawartość strony, klikając przycisk **Odśwież**.

Wybrane urządzenia zostaną zsynchronizowane z Serwerem administracyjnym.

Przeglądanie czasu dostarczenia zasady

Po zmianie zasady dla aplikacji Kaspersky na Serwerze administracyjnym, administrator może sprawdzić, czy zmieniona zasada została dostarczona do określonego zarządzanego urządzenia. Zasada może zostać dostarczona podczas regularnej synchronizacji lub wymuszonej synchronizacji.

W celu sprawdzenia daty i godziny dostarczenia zasady aplikacji na zarządzane urządzenie:

1. W menu głównym przejdź do **Zarządzanie zasobami** → **Zasoby (urządzenia)**.

2. Kliknij nazwę urządzenia, które chcesz zsynchronizować z Serwerem administracyjnym.

   Zostanie otwarte okno właściwości na wybranej sekcji **Ogólne**.

3. Wybierz zakładkę **Aplikacje**.

4. Wybierz aplikację, dla której chcesz sprawdzić datę synchronizacji zasady.

   Zostanie otwarte okno zasady aplikacji na sekcji **Ogólne** i z wyświetloną datą i godziną dostarczenia zasady.

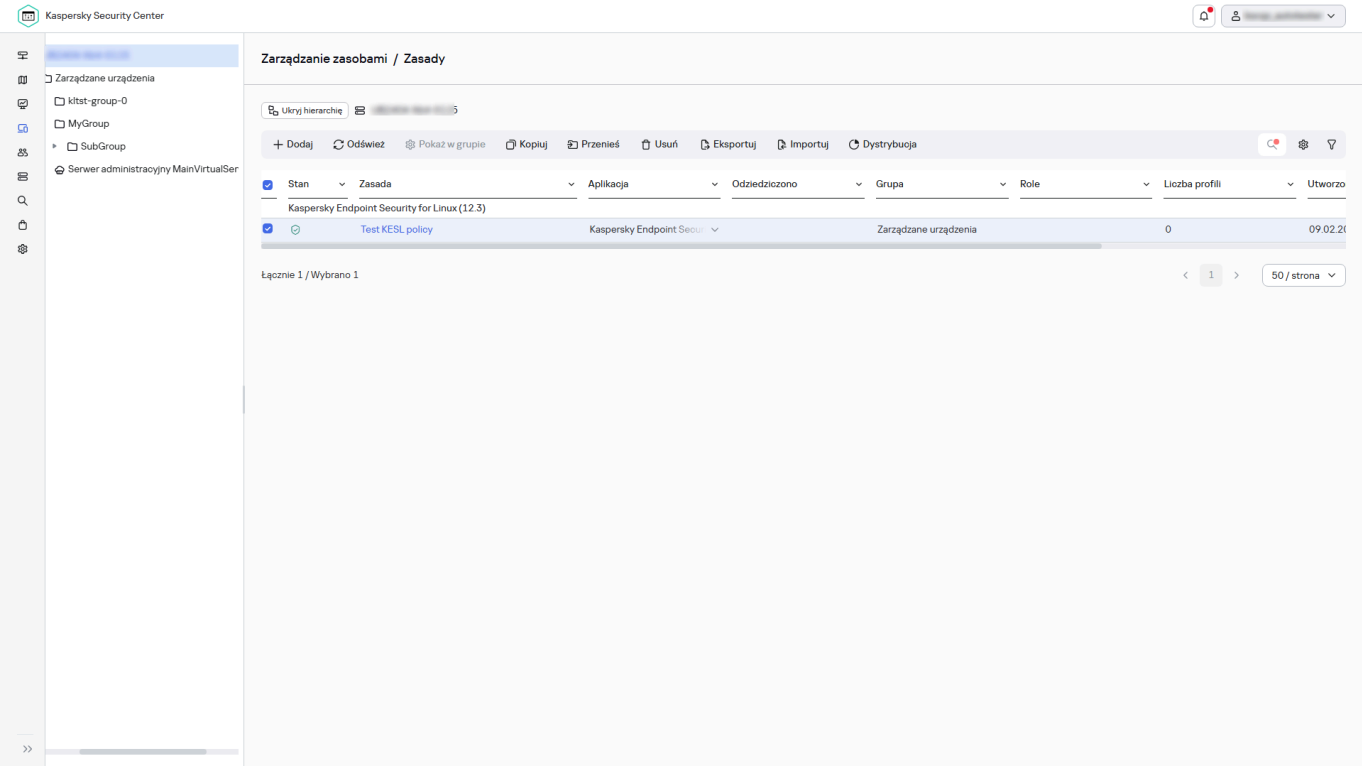
Przeglądanie wykresu stanu dystrybucji zasad

W Kaspersky Security Center Linux możesz przejrzeć stan zastosowania zasady na każdym urządzeniu w wykresie stanu dystrybucji zasady.

W celu wyświetlenia stanu dystrybucji zasady na każdym urządzeniu:

1. W menu głównym przejdź do **Zarządzanie zasobami** → **Zasady**.

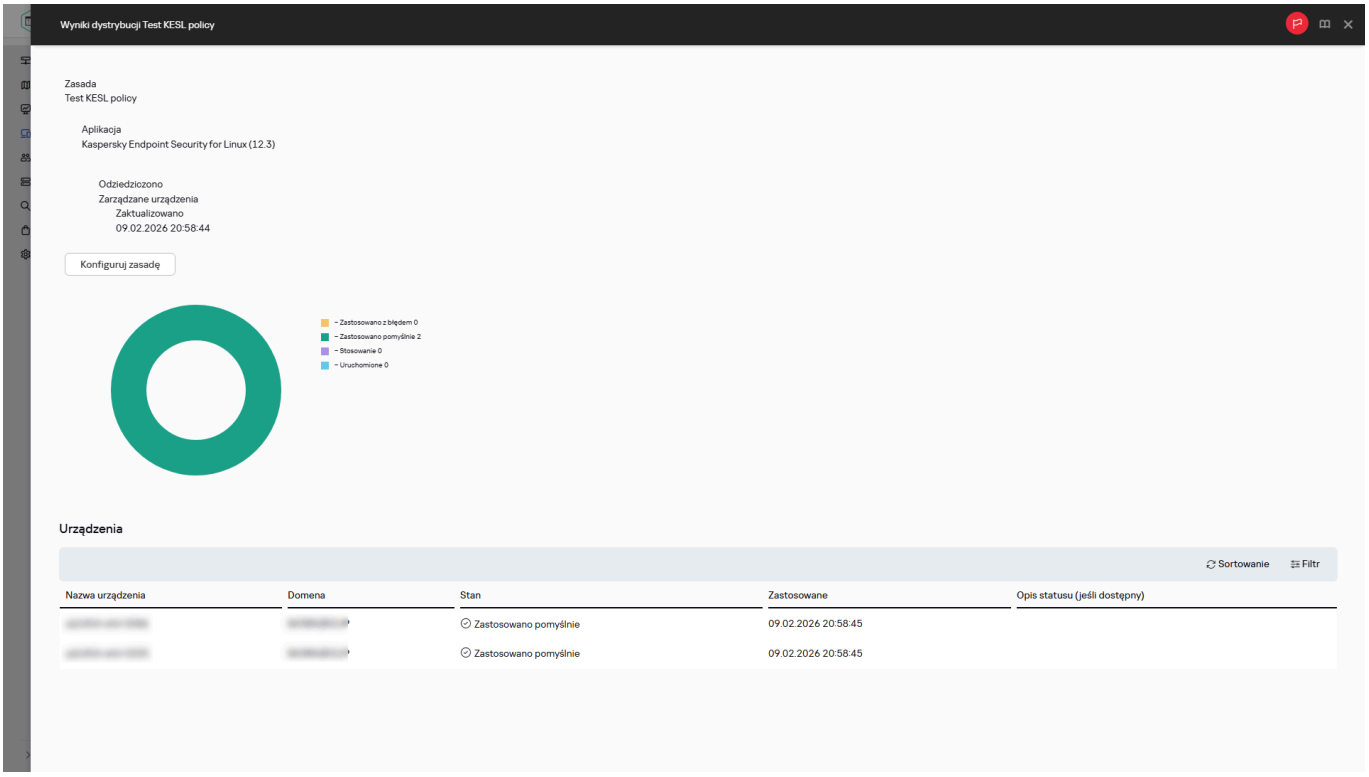
2. Zaznacz pole obok nazwy zasady, dla której chcesz przejrzeć stan dystrybucji na urządzeniach.



Lista zasad

3. W wyświetlonym menu wybierz odnośnik **Dystrybucja**.

   Zostanie otwarte okno **Wyniki dystrybucji <nazwa zasady>**.



Wyniki dystrybucji zasady

4. W otwartym oknie **Wyniki dystrybucji <nazwa zasady>** zostanie wyświetlony **Opis stanu** zasady.

Możesz zmienić liczbę wyników wyświetlanych na liście z dystrybucją zasady. Maksymalna liczba urządzeń to 100 000.

W celu zmiany liczby urządzeń wyświetlanych na liście z wynikami dystrybucji zasady:

1. W menu głównym przejdź do sekcji **Ustawienia** → **Opcje interfejsu**.
2. W sekcji **Ogranicz urządzenia wyświetlane w wynikach dystrybucji zasady** wprowadź liczbę urządzeń (do 100 000).

   Domyślnie ustawiona jest liczba 5000.
3. Kliknij **Zapisz**.

   Ustawienia zostaną zapisane i zastosowane.

Aktywowanie zasady automatycznie po wystąpieniu zdarzenia Ataku wirusa

W celu skonfigurowania zasady tak, aby była aktywowana automatycznie po wystąpieniu Ataku wirusa:

1. W menu głównym kliknij nazwę Serwera administracyjnego.

   Okno właściwości Serwera administracyjnego zostanie otwarte na zakładce **Ogólne**.
2. Wybierz sekcję **Atak wirusa**.
3. W prawej części okna kliknij odnośnik **Skonfiguruj zasady, które zostaną aktywowane po wystąpieniu ataku wirusa**.

   Zostanie otwarte okno **Aktywacja zasady**.
4. W sekcji dotyczącej komponentu, który wykrywa atak wirusa—Ochrona antywirusowa stacji roboczych i serwerów plików, Ochrona antywirusowa dla serwerów pocztowych lub Ochrona antywirusowa bram internetowych—wybierz przycisk opcji obok żądanego wpisu, a następnie kliknij **Dodaj**.

   Zostanie otwarte okno z grupą administracyjną **Zarządzane urządzenia**.
5. Kliknij ikonę strzałki (>) obok **Zarządzane urządzenia**.

   Zostanie wyświetlona hierarchia grup administracyjnych i ich zasad.
6. W hierarchii grup administracyjnych i ich zasad kliknij nazwę zasady lub zasad, które są aktywowane w przypadku wykrycia ataku wirusa.

   Aby wybrać wszystkie zasady na liście lub w grupie, zaznacz pole obok żądanej nazwy.
7. Kliknij przycisk **Zapisz**.

   Okno z hierarchią grup administracyjnych i ich zasad zostało zamknięte.

Wybrane zasady są dodawane do listy zasad, które są aktywowane po wykryciu ataku wirusa. Wybrane zasady są aktywowane w momencie wystąpienia ataku wirusa, niezależnie od tego, czy są aktywne czy nie.

Jeśli zasada została aktywowana po wystąpieniu zdarzenia Atak wirusa, możesz wrócić do poprzedniej zasady tylko przy użyciu trybu ręcznego.

Usuwanie zasady

Możesz usunąć zasadę, jeśli już jej nie potrzebujesz. Możesz usunąć tylko tą zasadę, która nie jest dziedziczona w określonej grupie administracyjnej. Jeśli zasada została odziedziczona, możesz ją usunąć tylko w grupie wyższego poziomu, dla której została utworzona.

W celu usunięcia zasady:

1. W menu głównym przejdź do **Zarządzanie zasobami** → **Zasady**.
2. Zaznacz pole obok zasady, który chcesz usunąć, a następnie kliknij **Usuń**.

   Przycisk **Usuń** stanie się niedostępny (przyciemniony), jeśli wybierzesz zasadę dziedziczoną.
3. Kliknij **OK**, aby potwierdzić działanie.

Zasada jest usuwana ze wszystkimi swoimi profilami. Po usunięciu zasady zdarzenia zmiany zasady są eksportowane do systemu SIEM, jeśli ta opcja jest włączona.

Zarządzanie profilami zasad

Ta sekcja opisuje zarządzanie profilami zasad i zawiera informacje o przeglądaniu profili zasad, zmienianiu priorytetu profilu zasad, tworzeniu profilu zasad, kopiowaniu profilu zasad, tworzeniu reguły aktywacji profilu zasad, usuwaniu, eksportowaniu i importowaniu profilu zasad.

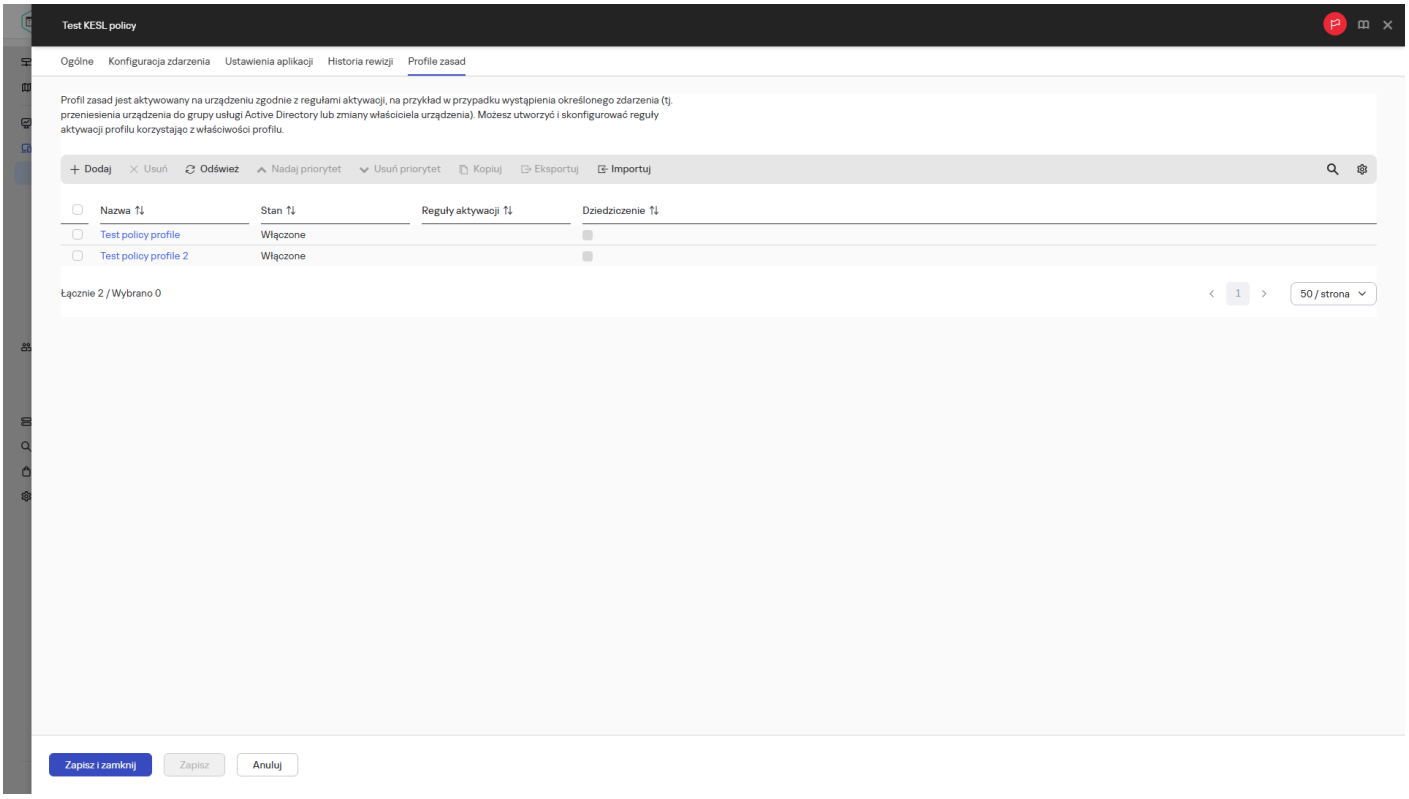
Przeglądanie profili zasad

W celu przejrzenia profili zasad:

1. W menu głównym przejdź do **Zarządzanie zasobami** → **Zasady**.
2. Kliknij nazwę zasady, której profile chcesz przejrzeć.

   Okno właściwości zasady zostanie otwarte na wybranej zakładce **Ogólne**.
3. Otwórz zakładke **Profile zasad**.

Lista profili zasad zostanie wyświetlona w postaci tabeli. Jeśli zasada nie zawiera profili, pojawi się pusta tabela.



Lista profili zasad

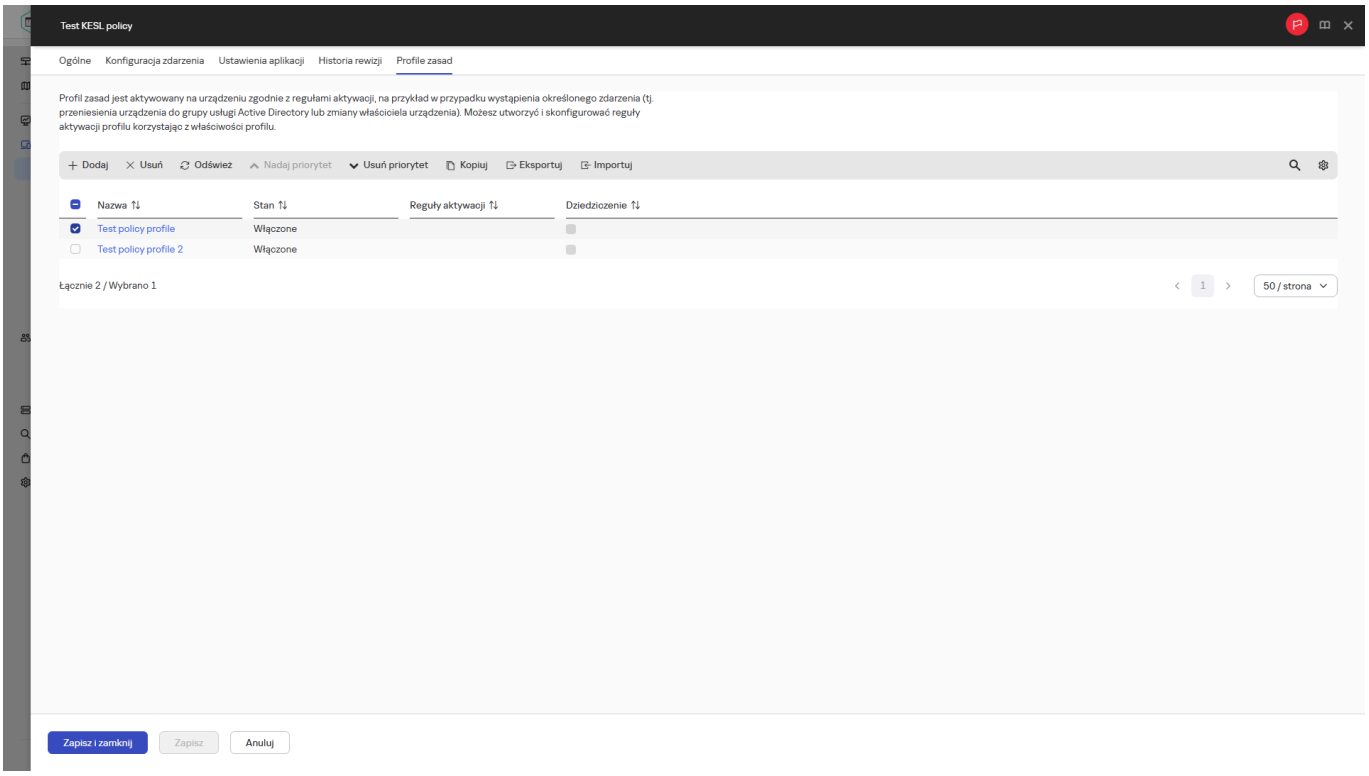
Zmiana priorytetu profilu zasad

W celu zmiany priorytetu profilu zasad:

1. Przejdź do listy profili zasady, której potrzebujesz.

   Zostanie otwarta lista profili zasad.
2. Na zakładce **Profile zasad** zaznacz pole obok profilu zasad, dla którego chcesz zmienić priorytet.
3. Ustaw nową pozycję profilu zasad na liście, klikając **Nadaj priorytet** lub **Usuń priorytet**.

   Im wyżej profil zasad znajduje się na liście, tym wyższy jego priorytet.



4. Kliknij przycisk **Zapisz**.

   Priorytet wybranego profilu zasad zostanie zmieniony i zastosowany.

Tworzenie profilu zasad

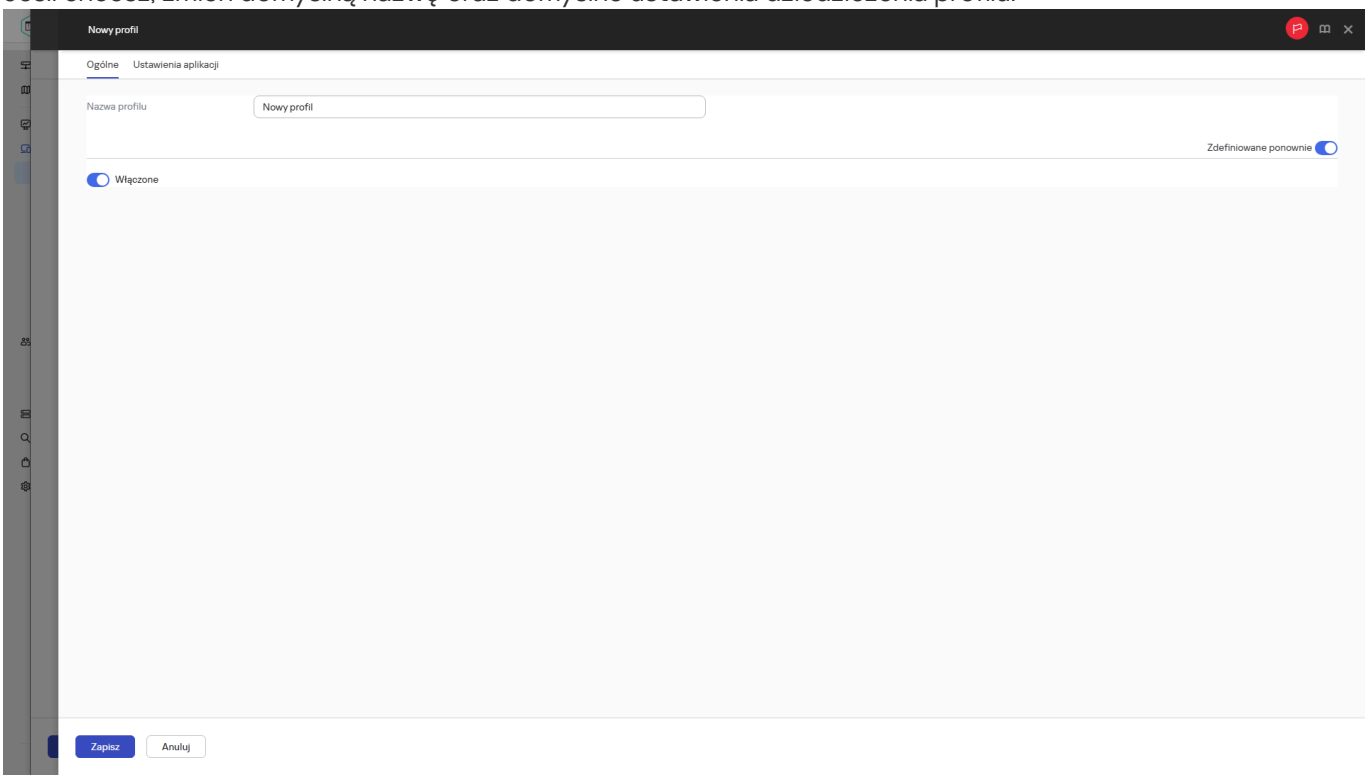
W celu utworzenia profilu zasad:

1. Przejdź do listy profili zasady, której potrzebujesz.

   Zostanie otwarta lista profili zasad. Jeśli zasada nie zawiera profili, pojawi się pusta tabela.

2. Kliknij **Dodaj**.

3. Jeśli chcesz, zmień domyślną nazwę oraz domyślne ustawienia dziedziczenia profilu.



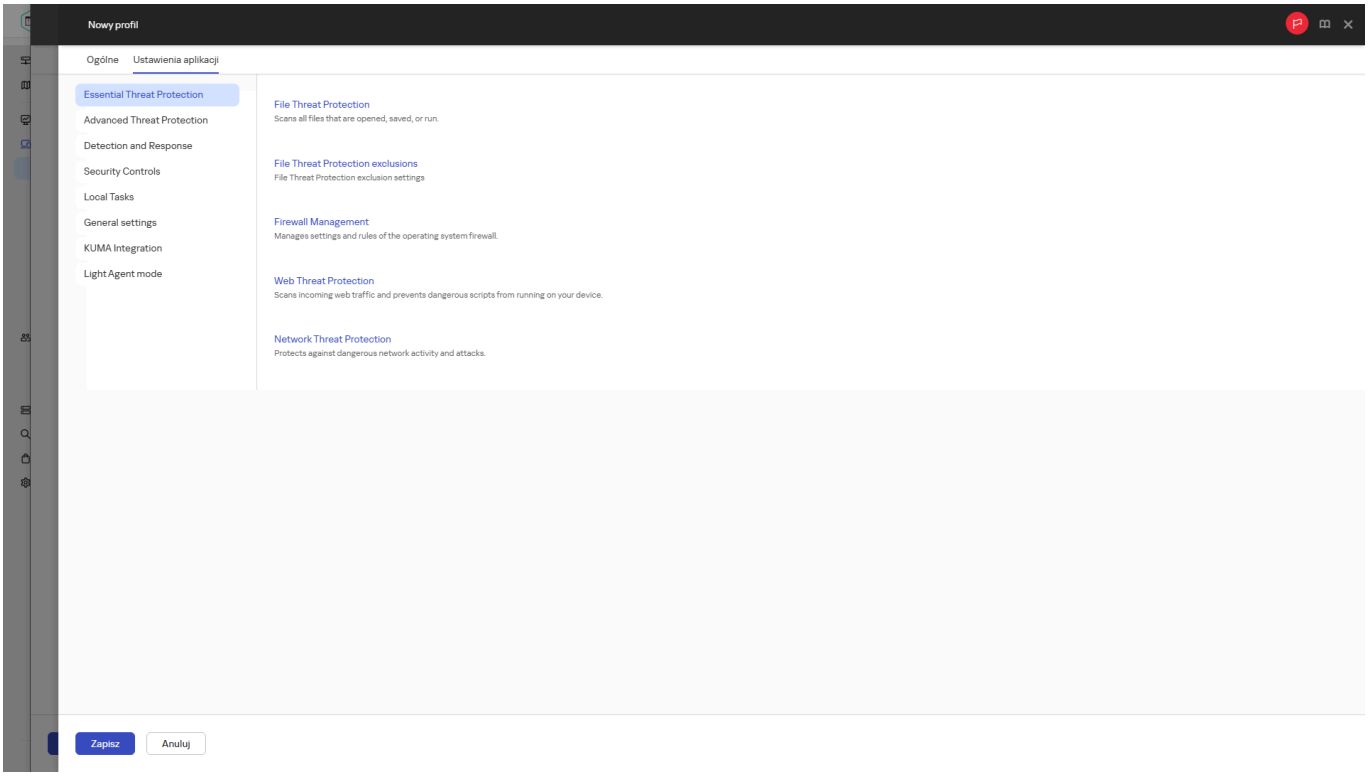
Tworzenie nowego profilu zasad

4. Wybierz zakładkę **Ustawienia aplikacji**.

   Lub kliknij **Zapisz** i zakończ działanie. Utworzony profil pojawia się na liście profili zasad i będzie można w późniejszym czasie zmienić ustawienia.

5. Na zakładce **Ustawienia aplikacji**, w lewej części okna wybierz żądaną kategorię, a w prawej części okna zmień ustawienia profilu. Możesz zmienić ustawienia profilu zasad w każdej kategorii (sekcja).

Podczas edytowania ustawień możesz kliknąć **Anuluj**, aby anulować ostatnie działanie.



Określanie ustawień profilu zasad

6. Kliknij **Zapisz**, aby zapisać profil.

   Profil pojawi się na liście profili zasad.

Kopiowanie profilu zasad

Możesz skopiować profil zasad do bieżącego profilu lub do innego profilu, na przykład, jeśli chcesz mieć identyczne profile dla różnych zasad. Kopiowania możesz użyć także, jeśli chcesz mieć dwa lub więcej profili, które różnią się tylko małą liczbą ustawień.

W celu skopiowania profilu zasad:

1. Przejdź do listy profili zasady, której potrzebujesz.

   Zostanie otwarta lista profili zasad. Jeśli zasada nie zawiera profili, pojawi się pusta tabela.

2. Na zakładce **Profile zasad** wybierz profil zasady, który chcesz skopiować.

3. Kliknij **Kopiuj**.

4. W otwartym oknie wybierz zasadę, do której chcesz skopiować profil.

   Profil zasady możesz skopiować do tej samej zasady lub do zasady, którą określiłeś.

5. Kliknij **Kopiuj**.

   Profil zasad został skopiowany do wybranej zasady. Nowo skopiowany profil uzyskuje najniższy priorytet. Jeśli skopiujesz profil do tej samej zasady, nazwa nowo skopiowanego profilu zostanie poszerzona o indeks (), na przykład: (1), (2).

Później będziesz mógł zmienić ustawienia profilu, w tym jego nazwę i priorytet; w tym przypadku oryginalny profil zasady nie zostanie zmieniony.

Tworzenie reguły aktywacji profilu zasad

W celu utworzenia reguły aktywacji profilu zasad:

1. Przejdź do listy profili zasady, której potrzebujesz.

   Zostanie otwarta lista profili zasad.

2. Na zakładce **Profile zasad** kliknij profil zasad, dla którego chcesz utworzyć regułę aktywacji.

   Jeśli lista profili zasad jest pusta, możesz utworzyć profil zasad.

3. Na zakładce **Reguły aktywacji** kliknij przycisk **Dodaj**.

   Zostanie otwarte okno z regułami aktywacji profilu zasad.

4. Określ nazwę reguły.

5. Zaznacz pola obok warunków, które mają wpływać na aktywację tworzonego profilu zasad:

   - **Główne reguły dotyczące aktywacji profilu zasad**

     Zaznacz to pole, aby skonfigurować reguły aktywacji profilu zasad na urządzeniu w zależności od stanu trybu offline urządzenia, regułę połączenia z Serwerem administracyjnym, a także znaczniki przypisywane do urządzenia.

     Dla tej opcji, w następnym kroku określ:

     - **Stan urządzenia**

       Określ warunek obecności urządzenia w sieci:

       - **Online**— Urządzenie jest w sieci, więc Serwer administracyjny jest dostępny.
       - **Offline**— Urządzenie jest w sieci zewnętrznej, co oznacza, że Serwer administracyjny nie jest dostępny.
       - **N/D**—Kryterium nie będzie stosowane.

     - **Lokalizacja sieciowa urządzenia**

       Wybierz warunek aktywacji profilu zasad (czy reguła jest wykonywana) i wybierz nazwę reguły.

       Reguła definiuje lokalizację sieciową urządzenia dla połączenia z Serwerem administracyjnym, którego warunki muszą być spełnione (lub nie muszą być spełnione) dla aktywacji profilu zasad.

       Opis lokalizacji sieciowej urządzeń dla połączenia z Serwerem administracyjnym może zostać utworzony lub skonfigurowany w regule przełączania Agenta sieciowego.

   - **Reguły dla określonego właściciela urządzenia**

Dla tej opcji, w następnym kroku określ:

- **Właściciel urządzenia**

  Włącz tę opcję, aby skonfigurować i włączyć regułę aktywacji profilu na urządzeniu zgodnie z jego właścicielem. Z listy rozwijalnej, znajdującej się pod tym polem, możesz wybrać kryterium aktywacji profilu:

  - Urządzenie należy do określonego właściciela (znak „=”).
  - Urządzenie nie należy do określonego właściciela (znak „#”).

    Jeśli ta opcja jest włączona, profil zostanie aktywowany na urządzeniu zgodnie ze skonfigurowanym kryterium. Możesz określić właściciela urządzenia, gdy opcja jest włączona. Jeśli ta opcja jest wyłączona, kryterium aktywacji profilu nie jest stosowane. Domyślnie opcja ta jest wyłączona.

- **Właściciel urządzenia należy do wewnętrznej grupy bezpieczeństwa**

  Włącz tę opcję, aby skonfigurować i włączyć regułę aktywacji profilu na urządzeniu według przynależności właściciela do wewnętrznej grupy zabezpieczeń Kaspersky Security Center Linux. Z listy rozwijalnej, znajdującej się pod tym polem, możesz wybrać kryterium aktywacji profilu:

  - Właściciel urządzenia jest członkiem określonej grupy bezpieczeństwa (znak „=”).
  - Właściciel urządzenia nie jest członkiem określonej grupy bezpieczeństwa (znak „#”).

    Jeśli ta opcja jest włączona, profil zostanie aktywowany na urządzeniu zgodnie ze skonfigurowanym kryterium. Możesz określić grupę zabezpieczeń Kaspersky Security Center Linux. Jeśli ta opcja jest wyłączona, kryterium aktywacji profilu nie jest stosowane. Domyślnie opcja ta jest wyłączona.

- **Reguły dla specyfikacji sprzętowej**

  Zaznacz to pole, aby skonfigurować reguły aktywacji profilu zasad na urządzeniu w zależności od ilości pamięci oraz liczby procesów logicznych.

  Dla tej opcji, w następnym kroku określ:

  - **Rozmiar pamięci RAM, w MB**

    Włącz tę opcję, aby skonfigurować i włączyć regułę aktywacji profilu według ilości pamięci RAM dostępnej na tym urządzeniu. Z listy rozwijalnej, znajdującej się pod tym polem, możesz wybrać kryterium aktywacji profilu:

    - Rozmiar pamięci RAM jest mniejszy niż określona wartość (znak „<”).
    - Rozmiar pamięci RAM jest większy niż określona wartość (znak „>”).

    Jeśli ta opcja jest włączona, profil zostanie aktywowany na urządzeniu zgodnie ze skonfigurowanym kryterium. Możesz określić ilość pamięci RAM na urządzeniu. Jeśli ta opcja jest wyłączona, kryterium aktywacji profilu nie jest stosowane. Domyślnie opcja ta jest wyłączona.

  - **Liczba procesorów logicznych**

    Włącz tę opcję, aby skonfigurować i włączyć regułę aktywacji profilu na urządzeniu według liczby procesorów logicznych na tym urządzeniu. Z listy rozwijalnej, znajdującej się pod tym polem, możesz wybrać kryterium aktywacji profilu:

    - Liczba procesorów logicznych na urządzeniu jest mniejsza niż lub równa określonej wartości (znak „<”).
    - Liczba procesorów logicznych na urządzeniu jest większa niż lub równa określonej wartości (znak „>”).

Jeśli ta opcja jest włączona, profil zostanie aktywowany na urządzeniu zgodnie ze skonfigurowanym kryterium. Możesz określić liczbę procesorów logicznych na urządzeniu. Jeśli ta opcja jest wyłączona, kryterium aktywacji profilu nie jest stosowane. Domyślnie opcja ta jest wyłączona.

- **Reguły dla przypisywania roli**

  Dla tej opcji, w następnym kroku określ:

  - **Aktywuj profil zasad określoną rolą właściciela urządzenia**

    Wybierz te opcję, aby skonfigurować i włączyć regułę aktywacji profilu na urządzeniu w zależności od roli właściciela. Dodaj rolę ręcznie z listy istniejących ról.

    Jeśli ta opcja jest włączona, profil zostanie aktywowany na urządzeniu zgodnie ze skonfigurowanym kryterium.

- **Reguły dla użycia znaczników**

  Zaznacz to pole, aby skonfigurować reguły aktywacji profilu zasad na urządzeniu w zależności od znaczników przypisanych do urządzenia. Możesz aktywować profil zasad dla urządzeń, które posiadają znaczniki lub które ich nie posiadają.

  Dla tej opcji, w następnym kroku określ:

  - **Lista znaczników**

    Na liście znaczników możesz określić regułę uwzględniania urządzenia w profilu zasad, zaznaczając pola obok odpowiednich znaczników.

    Możesz dodać nowe znaczniki do listy, wprowadzając je w polu nad listą i klikając przycisk **Dodaj**.

    Profil zasad obejmuje urządzenia z opisami zawierającymi wszystkie zaznaczone tagi. Jeśli pola nie są zaznaczone, kryterium nie jest stosowane. Domyślnie pola te nie są zaznaczone.

  - **Zastosuj do urządzeń bez określonych znaczników**

    Włącz tę opcje, jeśli musisz odwrócić wybór znaczników.

    Jeśli ta opcja jest włączona, profil zasad obejmuje urządzenia z opisami, które nie zawierają żadnego z wybranych znaczników. Jeśli ta opcja jest wyłączona, kryterium nie zostanie zastosowane.

    Domyślnie opcja ta jest wyłączona.

- **Reguły dotyczące używania Active Directory**

  Zaznacz to pole, aby skonfigurować reguły aktywacji profilu zasad na urządzeniu w zależności od obecności urządzenia w jednostce organizacyjnej Active Directory (OU) lub członkostwa urządzenia (lub jego właściciela) w grupie zabezpieczeń Active Directory.

  Dla tej opcji, w następnym kroku określ:

  - **Członkostwo właściciela urządzenia w grupie zabezpieczeń Active Directory**

    Jeśli ta opcja jest włączona, profil zasad jest aktywowany na urządzeniu, którego właściciel jest członkiem określonej grupy zabezpieczeń. Jeśli ta opcja jest wyłączona, kryterium aktywacji profilu nie jest stosowane. Domyślnie opcja ta jest wyłączona.

  - **Członkostwo urządzenia w grupie zabezpieczeń Active Directory**

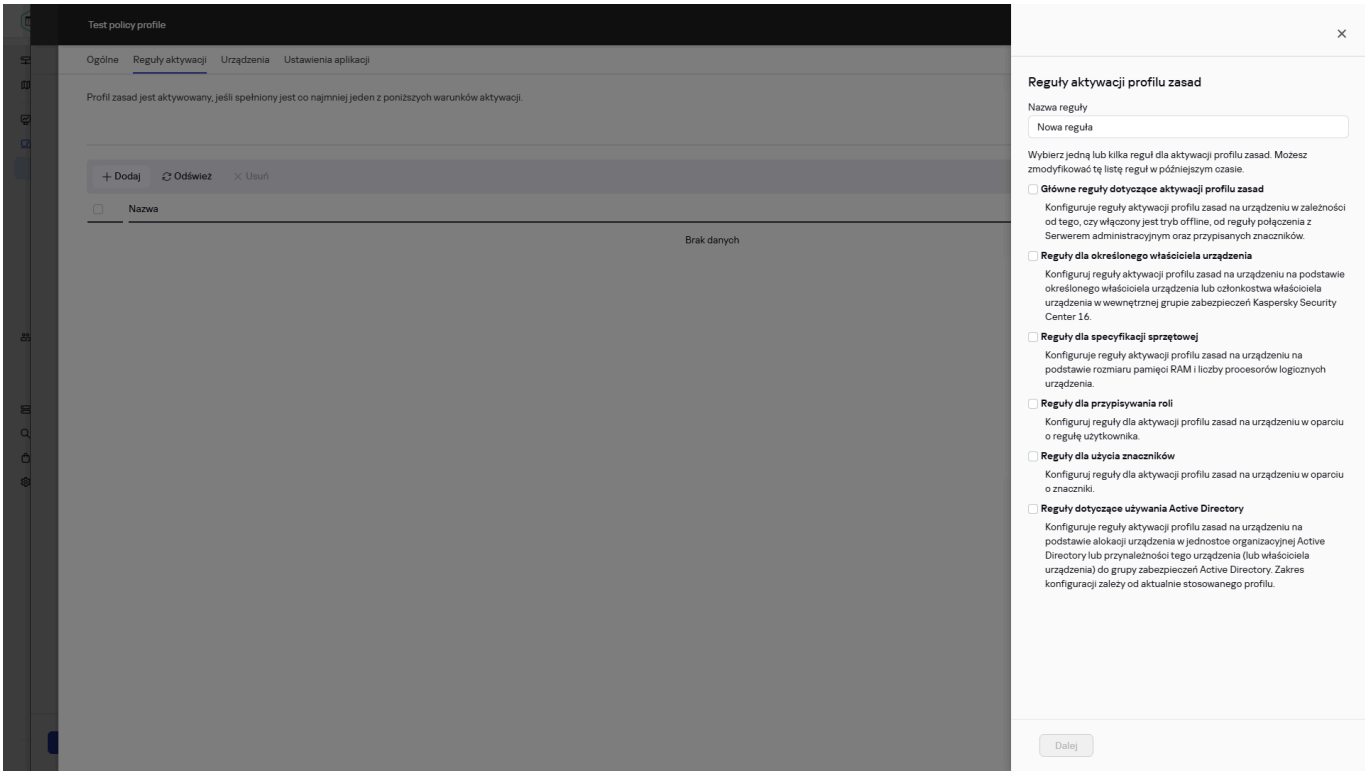
    Jeśli ta opcja jest włączona, profil zasad jest aktywowany na urządzeniu. Jeśli ta opcja jest wyłączona, kryterium aktywacji profilu nie jest stosowane. Domyślnie opcja ta jest wyłączona.

- **Alokacja urządzenia w jednostce organizacyjnej Active Directory**

  Jeśli ta opcja jest włączona, profil zasad jest aktywowany na urządzeniu, które jest uwzględnione w określonej jednostce organizacyjnej Active Directory. Jeśli ta opcja jest wyłączona, kryterium aktywacji profilu nie jest stosowane.

  Domyślnie opcja ta jest wyłączona.

Liczba dodatkowych okien w kreatorze zależy od ustawień wybranych w pierwszym kroku. Reguły aktywacji profili zasad można zmodyfikować w późniejszym czasie.



Tworzenie reguły aktywacji profilu zasad

6. Sprawdź listę skonfigurowanych parametrów. Jeśli lista jest poprawna, kliknij **Utwórz**.

   Profil zostanie zapisany. Profil zostanie aktywowany na urządzeniu po wyzwoleniu reguł aktywacji.

Reguły aktywacji profilu zasad utworzone dla profilu będą wyświetlone we właściwościach profilu zasad, na zakładce **Reguły aktywacji**. Możesz zmodyfikować lub usunąć dowolną regułę aktywacji profilu zasad.

Jednocześnie może być wyzwolonych kilka reguł aktywacji.

Usuwanie profilu zasad

W celu usunięcia profilu zasad:

1. Przejdź do listy profili zasady, której potrzebujesz.

   Zostanie otwarta lista profili zasad.

2. Na zakładce **Profile zasad** zaznacz pole obok profilu zasady, którą chcesz usunąć, a następnie kliknij **Usuń**.

3. W otwartym oknie ponownie kliknij **Usuń**.

   Profil zasad został usunięty. Jeśli zasada jest dziedziczona przez grupę niskiego poziomu, profil pozostanie w tej grupie, ale stanie się profilem zasady tej grupy. Odbywa się to w celu wyeliminowania znaczących zmian w ustawieniach zarządzanych aplikacji zainstalowanych na urządzeniach grup niskiego poziomu.

Eksportowanie i importowanie profilu zasad

Możesz zapisać profil zasad w pliku KLPROF bez eksportowania zasad, a następnie użyć tego pliku KLPROF do zaimportowania zapisanego profilu do zasad.

Umożliwia to szybkie przywrócenie ustawień profilu zasad zamiast ich ponownej konfiguracji.

Profil zasad jest importowany do zasad tej samej wersji aplikacji, z której wyeksportowano profil. W przypadku aplikacji obsługujących wsteczną zgodność zasad (na przykład Kaspersky Endpoint Security for Windows)), możesz importować profile zasad do różnych wersji zasad.

W celu wyeksportowania profilu zasady:

1. Przejdź do listy profili zasady, której potrzebujesz.

   Zostanie otwarta lista profili zasad.

2. Na zakładce **Profile zasad** kliknij profil zasady, który chcesz wyeksportować.

3. Na pasku narzędzi kliknij przycisk **Eksportuj**.

4. W otwartym oknie określ katalog, w którym chcesz zapisać plik z profilem zasad.

   W razie potrzeby możesz zmienić nazwę pliku.

5. Kliknij przycisk **Zapisz**.

   Jeśli operacja zakończy się pomyślnie, na ekranie wyświetli się odpowiedni komunikat. W przeciwnym razie pojawi się komunikat o błędzie.

W celu zaimportowania profilu zasady:

1. Przejdź do listy profili zasady, której potrzebujesz.

   Zostanie otwarta lista profili zasad.

2. Na pasku narzędzi kliknij przycisk **Importuj**.

3. W otwartym oknie wybierz plik KLPROF z wymaganym profilem zasad, a następnie kliknij przycisk **Otwórz**.

   Maksymalny rozmiar pliku raportu wynosi 4 MB.

Jeśli operacja zakończy się pomyślnie, na ekranie wyświetli się odpowiedni komunikat. W przeciwnym razie pojawi się komunikat o błędzie.

Profil zasad jest importowany pod nazwą, którą miał w chwili eksportu, a nie pod nazwą pliku KLPROF.
Plik jest importowany ze stanem **Wyłączone** i najniższym priorytetem, niezależnie od priorytetu profilu zasady przed eksportem.

Nie można wykonać importu:

- Jeśli zasada ma już profil o tej samej nazwie.
- Jeśli liczba profili w zasadzie wynosi 100.

Ustawienia zasady Agenta sieciowego

W celu skonfigurowania zasady Agenta sieciowego:

1. W menu głównym przejdź do **Zarządzanie zasobami** → **Zasady**.
2. Kliknij nazwę zasady Agenta sieciowego.

   Zostanie otwarte okno właściwości zasady Agenta sieciowego. Okno właściwości zawiera zakładki i ustawienia opisane poniżej.

Zobacz tabelę porównawczą, w której szczegółowo opisano, jak poniższe ustawienia mają zastosowanie w zależności od używanego systemu operacyjnego.

Ogólne

Na tej zakładce możesz zmodyfikować nazwę zasady, stan zasady oraz określić dziedziczenie ustawień zasady:

- W polu **Nazwa** możesz zmodyfikować nazwę zasady.
- W sekcji **Stan zasady** możesz wybrać jeden z trybów zasady:
  - **Aktywny**

    Jeśli wybrano tę opcję, zasada jest aktywna.

    Domyślnie opcja ta jest zaznaczona.
  - **Nieaktywny**

    Jeśli ta opcja jest zaznaczona, zasada stanie się nieaktywna, ale wciąż będzie przechowywana w folderze **Zasady**. Jeśli jest to wymagane, zasadę można aktywować.

- W grupie ustawień **Dziedziczenie ustawień** możesz skonfigurować dziedziczenie zasady:
  - **Dziedzicz ustawienia z zasady nadrzędnej**

    Jeśli ta opcja jest włączona, wartości ustawień zasady są dziedziczone z zasady grupy najwyższego poziomu, są więc zablokowane.

    Domyślnie opcja ta jest włączona.
  - **Wymuś dziedziczenie ustawień w zasadach podrzędnych**

    Jeśli ta opcja jest włączona, po zastosowaniu zmian w zasadzie zostaną wykonane następujące czynności:
    - Wartości ustawień zasady zostaną rozesłane do zasad podgrup administracyjnych, czyli do zasad podrzędnych.
    - Opcja **Dziedzicz ustawienia z zasady nadrzędnej** będzie automatycznie włączona w podsekcji **Dziedziczenie ustawień** sekcji **Ogólne** okna właściwości każdej zasady podrzędnej.

    Jeśli ta opcja jest włączona, ustawienia zasad podrzędnych są zablokowane.

    Domyślnie opcja ta jest wyłączona.

Konfiguracja zdarzenia

Na tej zakładce możesz skonfigurować rejestrowania zdarzeń oraz powiadamianie o zdarzeniach. Wydarzenia są dystrybuowane według istotności w następujących sekcjach:

- **Błąd funkcjonalny**
- **Ostrzeżenie**
- **Informacja**

W każdej sekcji, lista wyświetla typy zdarzeń oraz domyślny czas przechowywania zdarzeń na Serwerze administracyjnym (w dniach). Po kliknięciu typu zdarzenia możesz określić ustawienia zapisywania zdarzeń oraz powiadomień o zdarzeniach wybranych z listy. Domyślnie typowe ustawienia powiadamiania, określone dla całego Serwera administracyjnego, są używane dla wszystkich typów zdarzeń. Jednakże możesz zmienić określone ustawienia dla żądanych typów zdarzeń.

Na przykład, w sekcji **Ostrzeżenie** możesz skonfigurować typ zdarzenia **Wystąpił incydent związany z bezpieczeństwem**. Takie zdarzenia mogą mieć miejsce, na przykład, gdy wolne miejsce na dysku punktu dystrybucji jest mniejsze niż 2 GB (co najmniej 4 GB są wymagane do zdalnego instalowania aplikacji i pobierania aktualizacji). Aby skonfigurować zdarzenie **Wystąpił incydent związany z bezpieczeństwem**, kliknij je i określ, gdzie mają być przechowywane zdarzenia i jak powiadamiać o nich.

> Jeśli Agent sieciowy wykrywa problem bezpieczeństwa, możesz nim zarządzać za pomocą ustawień zarządzanego urządzenia.

Ustawienia

W sekcji **Ustawienia** możesz skonfigurować zasadę Agenta sieciowego:

- **Rozsyłaj pliki tylko poprzez punkty dystrybucji**

  Jeśli ta opcja jest włączona, Agenty sieciowe na zarządzanych urządzeniach pobierają uaktualnienia tylko z punktów dystrybucji.

  Jeśli ta opcja jest wyłączona, Agenty sieciowe na zarządzanych urządzeniach pobierają uaktualnienia z punktów dystrybucji lub z Serwera administracyjnego.

  > Należy pamiętać, że aplikacje zabezpieczające na zarządzanych urządzeniach pobierają uaktualnienia ze źródła ustawionego w zadaniu aktualizacji dla każdej aplikacji zabezpieczającej. Jeśli włączysz opcję **Rozsyłaj pliki tylko poprzez punkty dystrybucji**, upewnij się, że Kaspersky Security Center Linux jest ustawiony jako źródło aktualizacji w zadaniach aktualizacji.

  Domyślnie opcja ta jest wyłączona.

- **Maksymalny rozmiar kolejki zdarzeń, w MB**

  W tym polu możesz określić maksymalny rozmiar przestrzeni dyskowej zajmowanej przez kolejkę zdarzenia.

  Domyślna wartość to 2 megabajty (MB).

- **Aplikacja może pobierać rozszerzone dane zasad na urządzenie**

  Agent sieciowy zainstalowany na zarządzanym urządzeniu przesyła informacje o zastosowanej zasadzie aplikacji zabezpieczającej (na przykład Kaspersky Endpoint Security for Linux). Przesłane informacje możesz przejrzeć w interfejsie aplikacji zabezpieczającej.

  Agent sieciowy przesyła następujące informacje:

  - Czas dostarczenia zasady na zarządzane urządzenie.
  - Nazwę aktywnej zasady w momencie dostarczenia zasady na zarządzane urządzenie.
  - Nazwę zasady użytkowania mobilnego w momencie dostarczenia jej do zarządzanego urządzenia (niedostępna dla Agenta sieciowego dla systemu Linux).
  - Nazwę i pełną ścieżkę do grupy administracyjnej, która zawierała zarządzane urządzenie w momencie dostarczenia zasady na zarządzane urządzenie.
  - Listę aktywnych profili zasad wraz z ich nazwami i priorytetami w momencie dostarczenia zasad do zarządzanego urządzenia.

  Możesz użyć informacji, aby zapewnić, że poprawna zasada zostanie zastosowana do urządzenia oraz aby rozwiązać problemy. Domyślnie opcja ta jest wyłączona.

- **Chroń usługę Agenta sieciowego przed nieuprawnionym usuwaniem, zatrzymywaniem i zmianami ustawień**

  Gdy ta opcja pozostaje aktywna, po zainstalowaniu Agenta sieciowego na zarządzanym urządzeniu, składnik nie może zostać usunięty ani ponownie skonfigurowany bez wymaganych uprawnień. Usługa Agenta sieciowego nie może zostać zatrzymana. Ta opcja nie ma wpływu na kontrolery domeny.

  Włącz tę opcję, aby chronić Agenta sieciowego na stacjach roboczych obsługiwanych z uprawnieniami lokalnego administratora.

  Domyślnie opcja ta jest wyłączona.

- **Użyj hasła dezinstalacyjnego**

  Jeśli ta opcja jest włączona, klikając przycisk **Modyfikuj**, można określić hasło do narzędzia klmover i zdalnej dezinstalacji Agenta sieciowego na urządzeniach opartych na systemie Windows.

  Domyślnie opcja ta jest wyłączona.

Repozytoria

W sekcji **Repozytoria** możesz wybrać typy obiektów, których szczegóły zostaną wysłane z Agenta sieciowego na Serwer administracyjny:

- **Szczegóły zainstalowanych aplikacji**

  Jeśli ta opcja jest włączona, informacje o aplikacjach zainstalowanych na urządzeniach klienckich są przesyłane do Serwera administracyjnego.

  Domyślnie opcja ta jest włączona.

- **Dołącz informacje o poprawkach**

  Informacje o poprawkach aplikacji zainstalowanych na urządzeniach klienckich są wysyłane do Serwera administracyjnego. Włączenie tej opcji może zwiększyć obciążenie na Serwerze administracyjnym oraz DBMS, a także spowodować zwiększenie rozmiaru bazy danych.

  Domyślnie opcja ta jest włączona. Jest dostępny tylko dla systemu Windows.

- **Szczegóły aktualizacji Windows Update**

  Jeśli ta opcja jest włączona, informacje o aktualizacjach Microsoft Windows Update, które powinny zostać zainstalowane na urządzeniach klienckich, są przesyłane do Serwera administracyjnego.

  Domyślnie opcja ta jest włączona. Jest dostępny tylko dla systemu Windows.

  Informacje o opcjonalnych aktualizacjach Microsoft Windows nie są wysyłane do Serwera administracyjnego.

- **Szczegóły luk w oprogramowaniu oraz odpowiednich aktualizacji**

  Jeśli ta opcja jest włączona, informacje o lukach w oprogramowaniu innej firmy (w tym oprogramowaniu firmy Microsoft), wykrytych na zarządzanych urządzeniach, oraz o aktualizacjach oprogramowania, które eliminują luki innych firm (nie dotyczy oprogramowania firmy Microsoft) są wysyłane do Serwera administracyjnego.

  Wybranie tej opcji (**Szczegóły luk w oprogramowaniu oraz odpowiednich aktualizacji**) zwiększy obciążenie sieci, obciążenie dysku Serwera administracyjnego oraz zużycie zasobów Agenta sieciowego.

  Domyślnie opcja ta jest włączona. Jest dostępny tylko dla systemu Windows.

  Aby zarządzać aktualizacjami oprogramowania firmy Microsoft, użyj opcji **Szczegóły aktualizacji Windows Update**.

- **Szczegóły rejestru sprzętu**

  Agent sieciowy zainstalowany na urządzeniu wysyła informacje o sprzęcie urządzenia do Serwera administracyjnego. Możesz przejrzeć szczegóły sprzętu we właściwościach urządzenia.

  Upewnij się, że narzędzie lshw jest zainstalowane na urządzeniach z systemem Linux, z których chcesz pobrać szczegółowe informacje o sprzęcie. Szczegóły dot. sprzętu przechwycone z maszyn wirtualnych mogą być niekompletne, w zależności od używanego hiperwizora.

Jeśli modyfikacja niektórych ustawień w tej sekcji jest zablokowana przez zasadę Agenta sieciowego, nie można ich modyfikować.

Aktualizacje oprogramowania i luki

W sekcji **Aktualizacje oprogramowania i luki** możesz włączyć skanowanie plików wykonywalnych w poszukiwaniu luk:

- **Skanuj pliki wykonywalne w poszukiwaniu luk podczas ich uruchamiania**

  Jeśli ta opcja jest włączona, pliki wykonywalne są skanowane w poszukiwaniu luk podczas ich uruchamiania.

  Domyślnie opcja ta jest włączona.

Zarządzanie ponownym uruchamianiem

W sekcji **Zarządzanie ponownym uruchamianiem** możesz określić działanie, jakie zostanie wykonane, jeśli system operacyjny urządzenia zarządzanego musi być uruchomiony ponownie, gdy korzystasz, instalujesz lub dezinstalujesz aplikację:

- **Nie uruchamiaj ponownie systemu operacyjnego**

  Urządzenia klienckie nie są automatycznie uruchamiane ponownie po działaniu. Aby zakończyć działanie, należy uruchomić urządzenie ponownie (na przykład ręcznie lub przy użyciu zadania zarządzania urządzeniem). Informacje o wymaganym ponownym uruchomieniu zostaną zapisane w wynikach zadania oraz w statusie urządzenia. Opcja ta jest odpowiednia dla zadań na serwerach i innych urządzeniach, na których działanie ciągłe jest krytyczne.

- **Jeżeli będzie to wymagane, automatycznie uruchom ponownie system operacyjny**

  Urządzenia klienckie są zawsze automatycznie uruchamiane ponownie, jeśli jest to wymagane do zakończenia działania. Opcja jest przydatna, gdy zadania są uruchamiane na urządzeniach, na których możliwe są regularne przerwy w działaniu (wyłączenie lub ponowne uruchomienie).

- **Pytaj użytkownika o akcję**

  Na urządzeniu klienckim wyświetlane jest przypomnienie o ręcznym ponownym uruchomieniu urządzenia. Dla tej opcji można zdefiniować pewne ustawienia zaawansowane: treść wyświetlanego komunikatu, częstotliwość wyświetlania wiadomości oraz przedział czasu, po upływie którego ponowne uruchomienie zostanie wymuszone (bez potwierdzenia ze strony użytkownika). Ta opcja jest najodpowiedniejsza dla stacji roboczych, na których użytkownicy muszą mieć możliwość wyboru odpowiedniej godziny ponownego uruchomienia.

Domyślnie opcja ta jest zaznaczona.

- **Ponawiaj pytanie co (min)**

  Jeśli ta opcja jest włączona, aplikacja wyświetli pytanie o ponowne uruchomienie systemu operacyjnego z określoną częstotliwością.

  Domyślnie opcja ta jest włączona. Domyślnie przedział czasu wynosi 5 minut. Dostępne wartości znajdują się w zakresie od 1 do 1440 minut.

  Jeśli ta opcja jest wyłączona, monit zostaje wyświetlony tylko raz.

- **Wymuś restart po (min)**

  Po wyświetleniu monitu, aplikacja wymusza ponowne uruchomienie systemu operacyjnego po minięciu określonego przedziału czasu.

  Domyślnie opcja ta jest włączona. Domyślne opóźnienie wynosi 30 minut. Dostępne wartości znajdują się w zakresie od 1 do 1440 minut.

- **Wymuś zamknięcie aplikacji dla zablokowanych sesji**

  Uruchomione aplikacje mogą uniemożliwić ponowne uruchomienie urządzenia klienckiego. Na przykład, jeśli dokument jest edytowany w edytorze tekstu i nie zostanie zapisany, aplikacja nie zezwoli na ponowne uruchomienie urządzenia.

  Jeśli ta opcja jest włączona, zostaje wymuszone zamknięcie takich aplikacji na zablokowanym urządzeniu przed jego ponownym uruchomieniem. W wyniku tego działania użytkownicy mogą utracić niezapisane zmiany.

  Jeśli ta opcja jest wyłączona, zablokowane urządzenie nie zostanie uruchomione ponownie. Stan zadania na tym urządzeniu informuje, że wymagane jest ponowne uruchomienie urządzenia. Użytkownicy muszą ręcznie zamknąć wszystkie aplikacje uruchomione na zablokowanych urządzeniach i uruchomić ponownie te urządzenia.

  Domyślnie opcja ta jest wyłączona.

Zarządzaj poprawkami i aktualizacjami

W sekcji Zarządzaj poprawkami i aktualizacjami możesz skonfigurować pobieranie i dystrybucję uaktualnień oraz instalację poprawek na zarządzanych urządzeniach:

- **Automatycznie instaluj możliwe do zainstalowania aktualizacje i poprawki dla składników ze stanem Niezdefiniowany**

  Jeśli ta opcja jest włączona, poprawki Kaspersky ze stanem zatwierdzenia *Niezdefiniowane* będą automatycznie instalowane na zarządzanych urządzeniach natychmiast po pobraniu z serwerów aktualizacji.

  Jeśli ta opcja jest wyłączona, poprawki Kaspersky, które zostały pobrane i oznaczone jako *Niezdefiniowane*, zostaną zainstalowane dopiero po zmianie ich stanu na *Zatwierdzone*.

  Domyślnie opcja ta jest włączona.

- **Pobierz aktualizacje i antywirusowe bazy danych z Serwera administracyjnego z wyprzedzeniem (zalecane)**

  Jeśli ta opcja jest włączona, tryb offline pobierania aktualizacji jest używany. Jeśli Serwer administracyjny pobierze uaktualnienia, powiadomi Agenta sieciowego (na urządzeniach, na których jest zainstalowany) o uaktualnieniach, które będą wymagane dla zarządzanych aplikacji. Jeśli Agent sieciowy otrzyma informacje o tych uaktualnieniach, pobierze odpowiednie pliki z Serwera administracyjnego z wyprzedzeniem. Przy pierwszym nawiązaniu połączenia z Agentem sieciowym, Serwer administracyjny inicjuje pobranie aktualizacji. Jeśli Agent sieciowy pobierze wszystkie uaktualnienia na urządzenie klienckie, staną się one dostępne dla aplikacji na tym urządzeniu.

  Jeśli zarządzana aplikacja na urządzeniu klienckim spróbuje uzyskać dostęp do Agenta sieciowego w celu uzyskania uaktualnień, Agent sieciowy sprawdzi, czy posiada wszystkie wymagane uaktualnienia. Jeśli uaktualnienia zostały pobrane z Serwera administracyjnego nie więcej niż 25 godzin przed zażądaniem ich przez zarządzaną aplikację, Agent sieciowy nie nawiąże połączenia z Serwerem administracyjnym, ale dostarczy zarządzanej aplikacji uaktualnienia z lokalnej pamięci podręcznej. Połączenie z Serwerem administracyjnym może nie zostać nawiązane, gdy Agent sieciowy dostarcza uaktualnienia aplikacji na urządzeniach klienckich, ale połączenie nie jest wymagane w celu przeprowadzenia aktualizacji.

  Jeśli ta opcja jest wyłączona, tryb offline pobierania aktualizacji nie jest używany. Uaktualnienia są rozsyłane zgodnie z terminarzem zadania pobierania aktualizacji.

  Domyślnie opcja ta jest włączona.

Łączność

Sekcja **Łączność** zawiera trzy podsekcje:

- **Sieć**
- **Profile połączenia**
- **Terminarz połączeń**

W podsekcji **Sieć** możesz skonfigurować połączenie z Serwerem administracyjnym, włączyć korzystanie z portu UDP oraz określić numer UDP.

- W grupie ustawień **Połącz z Serwerem administracyjnym** możesz skonfigurować połączenie z serwerem administracyjnym oraz określić przedziału czasu dla synchronizacji pomiędzy urządzeniami klienckimi a serwerem administracyjnym:

  - **Okres synchronizacji (min)**

    Agent sieciowy synchronizuje zarządzane urządzenie z Serwerem administracyjnym. Zalecane jest ustawienie okresu synchronizacji (zwanego także puls) na 15 minut dla 10 000 zarządzanych urządzeń.

  - **Kompresuj ruch sieciowy**

    Jeżeli ta opcja jest włączona, prędkość transferu danych przez Agenta sieciowego zostaje zwiększona poprzez zmniejszenie ilości przesyłanych informacji i tym samym zmniejszenie obciążenia Serwera administracyjnego.

    > Obciążenie procesora komputera klienckiego może się zwiększyć.

    Domyślnie pole to jest zaznaczone.

- **Otwórz porty dla Agenta sieciowego w Zaporze sieciowej systemu Windows**

  Jeżeli ta opcja jest włączona, porty niezbędne do pracy Agenta sieciowego, zostaną dodane do listy wykluczeń Zapory sieciowej systemu Microsoft Windows.

  Domyślnie opcja ta jest włączona.

- **Użyj połączenia SSL**

  Jeśli ta opcja jest włączona, połączenie z Serwerem administracyjnym jest nawiązywane poprzez bezpieczny port przy użyciu protokołu SSL.

  Domyślnie opcja ta jest włączona.

- **Użyj bramy połączenia na punkcie dystrybucji (jeśli jest dostępny) w domyślnych ustawieniach połączenia**

  Jeśli ta opcja jest włączona, brama połączenia na punkcie dystrybucji jest używana z ustawieniami określonymi we właściwościach grupy administracyjnej.

  Domyślnie opcja ta jest włączona.

- **Użyj portu UDP**

  Jeśli chcesz, żeby Agent Sieciowy nawiązywał połączenie z Serwerem administracyjnym poprzez port UDP, włącz opcję **Użyj portu UDP** i określ **Numer portu UDP**. Domyślnie opcja ta jest włączona. Domyślny port UDP do nawiązywania połączenia z Serwerem administracyjnym to 15000.

- **Numer portu UDP**

  W tym polu możesz wprowadzić numer portu UDP. Domyślny numer portu to 15000.

  Używany jest system dziesiętny.

- **Użyj punktu dystrybucji, aby wymusić połączenie z Serwerem administracyjnym**

  Wybierz tę opcję, jeśli w oknie ustawień punktu dystrybucji zaznaczyłeś opcję **Użyj tego punktu dystrybucji jako serwera push**. W przeciwnym razie punkt dystrybucji nie będzie działał jako serwer push.

W podsekcji **Profile połączenia** możesz określić ustawienia lokalizacji sieciowej i włączyć tryb użytkownika mobilnego, gdy Serwer administracyjny nie jest dostępny:

- **Ustawienia lokalizacji sieciowej**

  Ustawienia lokalizacji sieciowej definiują cechy sieci, do której podłączone jest urządzenie klienckie, i określają reguły przełączania Agenta sieciowego z jednego profilu połączenia Serwera administracyjnego do innego, gdy te cechy sieci zostaną zmienione.

- **Profile połączeń Serwera administracyjnego**

  Możesz dodawać i wyświetlać profile połączenia Agenta sieciowego z Serwerem administracyjnym. W tej sekcji możesz także utworzyć reguły przełączania Agenta sieciowego na inne Serwery administracyjne, gdy wystąpią następujące zdarzenia:

  - Gdy urządzenie klienckie zostanie podłączone do innej sieci lokalnej
  - Gdy zostanie zerwane połączenie między urządzeniem a siecią lokalną organizacji
  - Gdy adres bramy połączenia zostanie zmieniony lub adres serwera DNS zostanie zmodyfikowany

- **Włącz tryb użytkownika mobilnego, gdy Serwer administracyjny nie jest dostępny**

  Jeśli ta opcja jest włączona, w przypadku połączenia przez ten profil, aplikacje zainstalowane na urządzeniu klienckim będą używać profili zasad dla urządzeń w trybie użytkownika mobilnego, a także zasad użytkownika mobilnego. Jeżeli dla aplikacji nie określono zasady użytkownika mobilnego, zostanie użyta zasada aktywna.

  Jeżeli ta opcja jest wyłączona, aplikacje będą używać zasad aktywnych.

  Domyślnie opcja ta jest wyłączona.

W podsekcji **Terminarz połączeń** możesz określić przedziały czasu, w trakcie których Agent sieciowy wysyła dane do Serwera administracyjnego:

- **Połącz, gdy jest to konieczne**

  Jeśli ta opcja jest zaznaczona, połączenie jest nawiązywane, gdy Agent sieciowy musi wysłać dane na Serwer administracyjny.

  Domyślnie opcja ta jest zaznaczona.

- **Połącz w określonych przedziałach czasu**

  Jeśli ta opcja jest zaznaczona, Agent sieciowy łączy się z Serwerem administracyjnym w określonym czasie. Możesz dodać kilka przedziałów czasu.

Przeszukiwanie sieci według punktów dystrybucji

W sekcji **Przeszukiwanie sieci według punktów dystrybucji** możesz skonfigurować automatyczne przeszukiwanie sieci. W celu włączenia przeszukiwania sieci i skonfigurowania jego częstotliwości możesz użyć następujących opcji:

- **Sieć Windows**

  Opcja ta jest dostępna tylko dla punktów dystrybucji opartych na systemie Windows.

  Jeśli ta opcja jest włączona, Serwer administracyjny automatycznie przeszuka sieć zgodnie z terminarzem skonfigurowanym po kliknięciu odnośników **Ustaw terminarz szybkiego przeszukiwania** i **Ustaw terminarz pełnego przeszukiwania**.

  Jeżeli ta opcja jest wyłączona, Serwer administracyjny przeszukuje sieć z częstotliwością określoną w polu **Częstotliwość przeszukiwania sieci (min)**.

  Interwał wykrywania urządzeń dla wersji Agenta sieciowego można skonfigurować w polach **Częstotliwość pobierania informacji z domen Windows (min)** (w przypadku szybkiego przeszukiwania sieci z domen Windows) i **Częstotliwość przeszukiwania sieci (min)** (w przypadku pełnego przeszukiwania sieci z domen Windows).

  Domyślnie opcja ta jest wyłączona.

- **Zakresy IP**

  Jeśli opcja jest włączona, punkt dystrybucji automatycznie przeszuka zakresy IP zgodnie z terminarzem skonfigurowanym po kliknięciu przycisku **Ustaw terminarz przeszukiwania**.

  Jeśli ta opcja jest wyłączona, Serwer punkt dystrybucji nie będzie przeszukiwał zakresów IP.

  Częstotliwość przeszukiwania zakresu IP dla Agenta sieciowego w wersjach poprzedzających 10.2 może być skonfigurowana w polu **Interwał przeszukiwania (min)**. Pole jest dostępne, jeśli opcja jest włączona.

  Domyślnie opcja ta jest wyłączona.

- **Zeroconf**

  Jeśli ta opcja jest włączona, punkt dystrybucji automatycznie przeszukuje sieć za pomocą urządzeń IPv6, używając zero-configuration networking (zwany również *Zeroconf*). W takim przypadku włączone przeszukiwanie zakresu adresów IP jest ignorowane, ponieważ punkt dystrybucji przeszukuje całą sieć.

  W celu rozpoczęcia korzystania z Zeroconf, muszą być spełnione następujące warunki:

  - Punkt dystrybucji musi działać pod systemem Linux.
  - Musisz zainstalować narzędzie avahi-browse na punkcie dystrybucji.

  Jeśli ta opcja jest wyłączona, punkt dystrybucji nie przeszukuje sieci z urządzeniami IPv6.

  Domyślnie opcja ta jest wyłączona.

- **Sterowniki domeny**

  Jeśli opcja jest włączona, punkt dystrybucji automatycznie przeszuka kontrolery domeny zgodnie z terminarzem skonfigurowanym po kliknięciu przycisku **Ustaw terminarz przeszukiwania**.

  Jeśli ta opcja jest wyłączona, punkt dystrybucji nie będzie przeszukiwał kontrolerów domeny.

  Częstotliwość przeszukiwania kontrolera domeny dla Agenta sieciowego w wersjach poprzedzających 10.2 może być skonfigurowana w polu **Interwał przeszukiwania (min)**. Pole jest dostępne, jeśli ta opcja jest włączona.

  Domyślnie opcja ta jest wyłączona.

Ustawienia sieci dla punktów dystrybucji

W sekcji **Ustawienia sieci dla punktów dystrybucji** możesz określić ustawienia dostępu do internetu:

- **Użyj serwera proxy**
- **Adres**
- **Numer portu**
- **Pomiń serwer proxy dla adresów lokalnych**

  Jeśli ta opcja jest włączona, żaden serwer proxy nie będzie używany do nawiązywania połączenia z urządzeniami w sieci lokalnej.

  Domyślnie opcja ta jest wyłączona.

- **Uwierzytelnianie na serwerze proxy**

  Jeśli to pole jest zaznaczone, w polach wejściowych możesz określić dane uwierzytelniające do autoryzacji na serwerze proxy.

  Domyślnie pole to nie jest zaznaczone.

KSN Proxy (punkty dystrybucji)

W sekcji **KSN Proxy (punkty dystrybucji)** możesz skonfigurować aplikację tak, aby używała punktu dystrybucji do przekazywania żądań Kaspersky Security Network (KSN) z zarządzanych urządzeń:

- **Włącz KSN Proxy po stronie punktu dystrybucji**

  Usługa KSN proxy jest uruchamiana na urządzeniu, które jest używane jako punkt dystrybucji. Użyj tej funkcji do redystrybucji i optymalizacji ruchu w sieci.

  Punkt dystrybucji wysyła statystyki KSN, które zostały wymienione w Oświadczeniu Kaspersky Security Network, do Kaspersky.

  Domyślnie opcja ta jest wyłączona. Włączenie tej opcji działa, jeśli opcje **Użyj Serwera administracyjnego jako serwera proxy** i **Zgadzam się na korzystanie z Kaspersky Security Network** zostały włączone w oknie właściwości Serwera administracyjnego.

  Możesz przypisać węzeł klastra aktywny-pasywny do punktu dystrybucji i włączyć serwer proxy KSN na tym węźle.

- **Przesyłaj żądania KSN do Serwera administracyjnego**

  Punkt dystrybucji przesyła żądania KSN z zarządzanych urządzeń do Serwera administracyjnego.

  Domyślnie opcja ta jest włączona.

- **Dostęp do KSN Cloud/KPSN bezpośrednio przez Internet**

  Punkt dystrybucji przesyła żądania KSN z zarządzanych urządzeń do chmury KSN lub KPSN. Żądania KSN wygenerowane na samym punkcie dystrybucji są także wysyłane bezpośrednio do chmury KSN lub KPSN.

- **Port TCP**

  Numer portu TCP, którego zarządzane urządzenia będą używały do nawiązywania połączenia z serwerem KSN proxy. Domyślny numer portu to 13111.

- **Port UDP**

  Jeśli chcesz, żeby Agent Sieciowy nawiązywał połączenie z Serwerem administracyjnym poprzez port UDP, włącz opcję **Użyj portu UDP** i określ **Numer portu UDP**. Domyślnie opcja ta jest włączona. Domyślny port UDP do nawiązywania połączenia z Serwerem administracyjnym to 15000.

- **Port HTTPS**

  Jeżeli chcesz, aby zarządzane urządzenia łączyły się z serwerem proxy KSN poprzez port HTTPS, włącz opcję **Użyj HTTPS**, a następnie w polu **Port HTTPS** podaj numer portu. Domyślnie opcja ta jest wyłączona. Domyślny port HTTPS do nawiązywania połączenia z serwerem KSN Proxy to 17111.

Aktualizacje (punkty dystrybucji)

W sekcji **Aktualizacje (punkty dystrybucji)** możesz włączyć funkcję pobierania plików diff, dzięki czemu punkty dystrybucji pobierają aktualizacje w postaci plików diff z serwerów aktualizacji firmy Kaspersky.

Zarządzanie kontem lokalnym (tylko Linux)

Sekcja **Zarządzanie kontem lokalnym (tylko Linux)** zawiera trzy podsekcje:

- **Zarządzanie certyfikatami użytkowników**
- **Dodaj lub edytuj odpowiednie lokalne grupy administratorów**
- **Prześlij plik referencyjny, aby chronić plik sudoers na urządzeniu użytkownika przed zmianami**

W podsekcji **Zarządzanie certyfikatami użytkowników** możesz określić, które certyfikaty główne mają zostać zainstalowane. Certyfikaty te mogą służyć np. do weryfikacji autentyczności stron internetowych czy serwerów internetowych.

- **Zainstaluj certyfikaty główne**

  Jeżeli opcja jest włączona, certyfikaty dodane do tabeli zostaną zainstalowane na określonych urządzeniach.

  Jeśli ta opcja jest wyłączona, na określonych urządzeniach nie zostaną zainstalowane żadne certyfikaty.

  Domyślnie opcja ta jest wyłączona.

- **Dodaj**

  Kliknięcie tego przycisku powoduje otwarcie okna, w którym możesz dodać certyfikat.

  Certyfikat musi mieć mniej niż 10 MB.

  Kaspersky Security Center obsługuje certyfikaty z rozszerzeniami CER, CRT, CERT, PEM i KEY.

W podsekcji **Dodaj lub edytuj odpowiednie lokalne grupy administratorów** możesz zarządzać grupami administratorów lokalnych. Grupy te są wykorzystywane, na przykład, podczas wycofywania uprawnień administratora lokalnego. Możesz także sprawdzić listę kont użytkowników uprzywilejowanych, korzystając z **Raport o uprzywilejowanych użytkownikach urządzenia (tylko Linux)**.

- **Add**

  Kliknięcie tego przycisku otwiera okno, w którym możesz dodać grupę administratorów lokalnych.

- **Edit**

  Kliknięcie tego przycisku powoduje otwarcie okna, w którym możesz edytować grupę administratorów lokalnych.

  Przycisk ten jest dostępny, jeśli zaznaczone jest pole wyboru obok grupy administratorów lokalnych.

- **Delete**

  Kliknięcie tego przycisku powoduje usunięcie wybranej grupy administratorów lokalnych z tabeli.

  Przycisk ten jest dostępny, jeśli zaznaczone jest pole wyboru obok grupy administratorów lokalnych.

W podsekcji **Prześlij plik referencyjny, aby chronić plik sudoers na urządzeniu użytkownika przed zmianami**, możesz skonfigurować kontrolę nad plikiem sudoers. Grupy uprzywilejowane i użytkownicy urządzeń są definiowani w pliku sudoers na urządzeniu. Plik sudoers znajduje się w folderze `/etc/sudoers`. Możesz przesłać referencyjny plik sudoers, aby chronić plik sudoers przed zmianami. Zapobiegnie to niepożądanym zmianom w pliku sudoers.

Nieprawidłowy plik referencyjny sudoers może spowodować nieprawidłowe działanie urządzenia użytkownika.

- **Plik kontrolny sudoers**

  Jeśli ta opcja jest włączona, plik sudoers zostanie zastąpiony bieżącym plikiem referencyjnym sudoers.

  Jeśli ta opcja jest wyłączona, plik sudoers pozostanie niezmieniony.

  Domyślnie opcja ta jest wyłączona.

- **Plik referencyjny sudoers**

  W tym polu wyświetlana jest nazwa przesłanego pliku referencyjnego sudoers.

- **Prześlij**

  Kliknięcie tego przycisku powoduje otwarcie okna, w którym możesz przesłać referencyjny plik sudoers.

- **Bieżący plik referencyjny sudoers**

  Kliknięcie tego przycisku powoduje wyświetlenie zawartości bieżącego pliku sudoers.

Historia rewizji

W zakładce **Historia rewizji** możesz:

- Wyświetl i zapisz historię rewizji zasad.
- Wróć do wersji zasad.
- Dodaj i edytuj opisy wersji zasad.
- Porównaj rewizje zasad.

Korzystanie z Agenta sieciowego dla systemu Windows, Linux i macOS: Porównanie

Korzystanie z Agenta sieciowego różni się w zależności od systemu operacyjnego urządzenia. Ustawienia zasady Agenta sieciowego i pakietu instalacyjnego także różnią się w zależności od systemu operacyjnego. W poniższej tabeli porównano funkcje Agenta sieciowego i scenariusze użycia dostępne dla systemów operacyjnych Windows, Linux i macOS.

Funkcja Agenta sieciowego	Windows	Linux	macOS
Instalacja			
Instalacja poprzez sklonowanie obrazu dysku twardego administratora z systemem operacyjnym i Agentem sieciowym przy użyciu narzędzi innych firm	✓ Ograniczenie: Nieobsługiwane przez Agenta sieciowego dla systemu Microsoft Windows opartego na architekturze Arm.	✓	✓
Instalowanie przy użyciu narzędzi firm trzecich dla zdalnej instalacji aplikacji	✓	✓	✓
Ręczne instalowanie poprzez uruchomienie instalatorów aplikacji na urządzeniach	✓	✓	✓
Instalowanie Agenta sieciowego w trybie cichym	✓	✓	✓
Ręczne łączenie urządzenia klienckiego z Serwerem administracyjnym. Narzędzie klmover	✓	✓	✓
Automatyczne instalowanie aktualizacji i poprawek dla komponentów Kaspersky Security Center	✓	✓	—
Automatyczne rozsyłanie kluczy	✓	✓	✓
Wymuszona synchronizacja	✓	✓	✓ Za wyjątkiem serwera push
Punkt dystrybucji			
Przy użyciu punktu dystrybucji	✓ Ograniczenie: Nieobsługiwane przez Agenta sieciowego dla systemu Microsoft Windows opartego na architekturze Arm.	✓	✓
Obliczanie liczby i konfigurowanie punktów dystrybucji	✓ Ograniczenie: Nieobsługiwane przez Agenta sieciowego dla systemu Microsoft Windows opartego na architekturze Arm.	✓ Bez korzystania z funkcji rozpoznawania lokalizacji w sieci (NLA).	✓ Bez korzystania z funkcji rozpoznawania lokalizacji w sieci (NLA).
Tryb offline pobierania aktualizacji	✓ Ograniczenie: Nieobsługiwane przez Agenta sieciowego dla systemu Microsoft Windows opartego na architekturze Arm.	✓	✓

Funkcja Agenta sieciowego	Windows	Linux	macOS
Przeszukiwanie sieci	✓ • Przeszukiwanie zakresu IP • Przeszukiwanie kontrolera domeny (Microsoft Active Directory) Ograniczenie: Nieobsługiwane przez Agenta sieciowego dla systemu Microsoft Windows opartego na architekturze Arm.	✓ Przeszukiwanie zakresu IP Przeszukiwanie Zeroconf Przeszukiwanie kontrolera domeny (Microsoft Active Directory, Samba 4 Active Directory, FreeIPA, ALD Pro)	—
Uruchamianie usługi KSN proxy po stronie punktu dystrybucji	✓ Ograniczenie: Nieobsługiwane przez Agenta sieciowego dla systemu Microsoft Windows opartego na architekturze Arm.	✓	—
Pobieranie aktualizacji za pośrednictwem serwerów aktualizacji Kaspersky do repozytoriów punktów dystrybucji, które dystrybuują aktualizacje do zarządzanych urządzeń	✓ Ograniczenie: Nieobsługiwane przez Agenta sieciowego dla systemu Microsoft Windows opartego na architekturze Arm.	✓	— (jeśli co najmniej jedno urządzenie działające pod kontrolą systemu operacyjnego Linux lub macOS znajduje się w zakresie zadania Pobierz aktualizacje do repozytoriów punktów dystrybucji, zadanie zostanie zakończone ze stanem Niepowodzenie nawet wtedy, gdy zostało zakończone pomyślnie na wszystkich urządzeniach z systemem Windows).
Instalowanie aplikacji w trybie push	✓ Ograniczenie: Nieobsługiwane przez Agenta sieciowego dla systemu Microsoft Windows opartego na architekturze Arm.	Ograniczone: nie można przeprowadzić instalacji w trybie push na urządzeniach z systemem Windows przy użyciu punktów dystrybucji systemu Linux.	Ograniczone: nie można przeprowadzić instalacji w trybie push na urządzeniach z systemem Windows przy użyciu punktów dystrybucji systemu macOS.
Używanie serwera push	✓ Ograniczenie: Nieobsługiwane przez Agenta sieciowego dla systemu Microsoft Windows opartego na architekturze Arm.	✓	—
Informacje o aplikacjach innych firm			
Zdalne instalowanie aplikacji na urządzeniach	✓	✓	✓ Więcej szczegółów znajdziesz w poniższym artykule: Instalacja zdalna aplikacji na urządzeniach macOS.
Konfigurowanie aktualizacji systemu operacyjnego w zasadzie Agenta sieciowego	✓ Ograniczenie: Nieobsługiwane przez Agenta sieciowego dla systemu Microsoft Windows opartego na architekturze Arm.	—	—
Przeglądanie informacji o lukach w oprogramowaniu	✓ Ograniczenie: Nieobsługiwane przez Agenta sieciowego dla systemu Microsoft Windows opartego na architekturze Arm.	—	—

Funkcja Agenta sieciowego	Windows	Linux	macOS
Skanowanie aplikacji w poszukiwaniu luk	✓ Ograniczenie: Nieobsługiwane przez Agenta sieciowego dla systemu Microsoft Windows opartego na architekturze Arm.	—	—
Aktualizacje oprogramowania	✓ Ograniczenie: Nieobsługiwane przez Agenta sieciowego dla systemu Microsoft Windows opartego na architekturze Arm.	—	—
Inwentaryzacja oprogramowania zainstalowanego na urządzeniach	✓	✓	—
Maszyny wirtualne			
Instalowanie Agenta sieciowego na maszynie wirtualnej	✓	✓	✓
Ustawienia optymalizacji dla Virtual Desktop Infrastructure (VDI)	✓ Ograniczenie: Nieobsługiwane przez Agenta sieciowego dla systemu Microsoft Windows opartego na architekturze Arm.	✓	✓
Obsługa dynamicznych maszyn wirtualnych	✓ Ograniczenie: Nieobsługiwane przez Agenta sieciowego dla systemu Microsoft Windows opartego na architekturze Arm.	✓	✓
Inne			
Audyt działań na zdalnym urządzeniu klienckim przy użyciu Udostępniania pulpitu Windows	✓	—	—
Monitorowanie stanu ochrony antywirusowej	✓	✓	✓
Zarządzanie ponownymi uruchomieniami urządzenia	✓	—	—
Obsługa przywracania systemu plików	✓	✓	✓
Używanie Agenta sieciowego jako bramy połączenia	✓	✓	✓
Menedżer połączeń	✓	✓	✓
Profile połączenia dla użytkowników mobilnych	✓	✓	✓
Przełączanie Agenta sieciowego z jednego Serwera administracyjnego na inny (automatycznie według lokalizacji sieciowej)	✓	✓	✓

Funkcja Agenta sieciowego	Windows	Linux	macOS
Sprawdzanie połączenia pomiędzy urządzeniem klienckim a Serwerem administracyjnym. Narzędzie klnagchk	✓	✓	✓
Zdalne połączenie z pulpitem urządzenia klienckiego	✓	✓	✓ Korzystając z systemu Virtual Network Computing (VNC).
Pobieranie autonomicznego pakietu instalacyjnego poprzez kreator migracji	✓	✓	✓
Wyświetlanie informacji o sprzęcie urządzeń klienckich	✓	✓ Informacje o sprzęcie urządzeń Linux wysyłane do Serwera administracyjnego przez Agenta sieciowego zainstalowanego na tych urządzeniach ograniczają się do informacji określonych w opisie ustawień zarządzanego urządzenia.	✓ Informacje o sprzęcie urządzeń z systemem macOS wysyłane do Serwera administracyjnego przez Agenta sieciowego zainstalowanego na tych urządzeniach ograniczają się do informacji określonych w opisie ustawień zarządzanego urządzenia.

Porównanie ustawień Agenta sieciowego według systemów operacyjnych

Poniższa tabela pokazuje, które ustawienia zasady Agenta sieciowego są dostępne w zależności od systemu operacyjnego zarządzanego urządzenia, na którym został zainstalowany Agent sieciowy.

Ustawienia Agenta sieciowego: porównanie według systemów operacyjnych

Sekcja Ustawienia	Windows	Linux	macOS
Ogólne	✓	✓	✓
Konfiguracja zdarzenia	✓	✓	✓
Ustawienia	✓	✓ Dostępne są następujące opcje: • **Rozsyłaj pliki tylko poprzez punkty dystrybucji** • **Maksymalny rozmiar kolejki zdarzeń, w MB** • **Aplikacja może pobierać rozszerzone dane zasad na urządzenie**	✓
Repozytoria	✓	✓ Dostępne są następujące opcje: • **Szczegóły zainstalowanych aplikacji** • **Szczegóły rejestru sprzętu**	✓ Dostępna jest opcja **Szczegóły rejestru sprzętu**.
Łączność → Sieć	✓	✓ Za wyjątkiem opcji **Otwórz porty dla Agenta sieciowego w Zaporze sieciowej systemu Windows**.	✓
Łączność → Profile połączenia	✓	✓	✓
Łączność → Terminarz połączeń	✓	✓	✓

Sekcja Ustawienia	Windows	Linux	macOS
Przeszukiwanie sieci według punktów dystrybucji	✓ Dostępne są następujące opcje: • **Sieć Windows** • **Zakresy IP** • **Sterowniki domeny**	✓ Dostępne są następujące opcje: • **Zeroconf** • **Zakresy IP** • **Sterowniki domeny**	—
Ustawienia sieci dla punktów dystrybucji	✓	✓	✓
KSN Proxy (punkty dystrybucji)	✓	✓	—
Aktualizacje (punkty dystrybucji)	✓	✓	—
Historia rewizji	✓	✓	✓

Włączanie i wyłączanie trybu niskiego zużycia zasobów dla Agenta sieciowego

Tryb niskiego zużycia zasobów umożliwia ograniczenie zużycia pamięci RAM przez Agenta sieciowego zainstalowanego na urządzeniu klienckim. Domyślnie tryb niskiego zużycia zasobów jest wyłączony.

W trybie niskiego zużycia zasobów nie są realizowane następujące funkcje:

- Agenta sieciowego nie można przypisać do działania jako punkt dystrybucji (ręcznie lub automatycznie).
- Agent sieciowy nie rejestruje informacji o stanie Agenta sieciowego w osobnym pliku tekstowym.
- Agent sieciowy nie obsługuje modelu pobierania aktualizacji w trybie offline.
- Następujące komponenty i procesy są wyłączone:
  - Uzyskiwanie informacji o aktualizacjach i lukach w zabezpieczeniach innych firm.
  - Uruchamianie KSN Proxy po stronie punktu dystrybucyjnego.
  - Przesyłanie aktualizacji do repozytorium punktu dystrybucji.
  - Ominięcie blokady serwera DNS.
  - Uzyskiwanie informacji o wolnej przestrzeni dyskowej.

Komponenty i procesy wznawiają działanie po wyłączeniu trybu niskiego zużycia zasobów.

Aby włączyć tryb niskiego zużycia zasobów:

1. Na urządzeniu klienckim wykonaj następujące polecenie w wierszu poleceń:

```
sudo /opt/kaspersky/klnagent64/sbin/klscflag -fset -pv klnagent -n
KLNAG_FLAG_TEST_VM_PERF -t d -v 1
```

2. Uruchom ponownie Agenta sieciowego za pomocą następującego polecenia:

```
sudo service klnagent64 restart
```

3. W dzienniku systemu operacyjnego sprawdź, czy wyświetlany jest wpis **Agent sieciowy Kaspersky Security Center działa w trybie niskiego zużycia zasobów**.

Tryb niskiego zużycia zasobów jest włączony.

Aby wyłączyć tryb niskiego zużycia zasobów:

1. Na urządzeniu klienckim wykonaj następujące polecenie w wierszu poleceń:

```
sudo /opt/kaspersky/klnagent64/sbin/klscflag -fset -pv klnagent -n
KLNAG_FLAG_TEST_VM_PERF -t d -v 0
```

2. Uruchom ponownie Agenta sieciowego za pomocą następującego polecenia:

```
sudo service klnagent64 restart
```

Tryb niskiego zużycia zasobów jest wyłączony.

Tryb niskiego zużycia zasobów można także włączyć zdalnie, korzystając z zadania *Zdalne wykonywanie skryptów*.

Konfigurowanie ustawień ochrony aplikacji zarządzanych

Aby skonfigurować ustawienia ochrony aplikacji zarządzanych firmy Kaspersky, możesz użyć zasad.

Więcej informacji na temat konfigurowania zasad programu Kaspersky Endpoint Security można znaleźć w odpowiedniej pomocy:

- Pomoc Kaspersky Endpoint Security for Windows
- Pomoc Kaspersky Endpoint Security for Linux
- Pomoc dotycząca programu Kaspersky Endpoint Security for Mac

Ręczna konfiguracja grupowego zadania aktualizacji dla Kaspersky Endpoint Security

Optymalną i zalecaną opcją terminarza dla Kaspersky Endpoint Security jest **Po pobraniu nowych aktualizacji do repozytorium**, gdy zaznaczone jest pole **Używaj automatycznie losowego opóźnienia dla uruchamiania zadań**.

Ręczna konfiguracja grupowego zadania skanowania urządzeń z zainstalowanym programem Kaspersky Endpoint Security

Kreator wstępnej konfiguracji tworzy grupowe zadanie skanowania urządzeń. Jeżeli automatycznie określony harmonogram zadania skanowania grupowego nie jest odpowiedni dla Twojej organizacji, musisz ręcznie ustawić najdogodniejszy harmonogram tego zadania na podstawie zasad przyjętych w organizacji.

Domyślnie skonfigurowano terminarz **uruchamiania zadania we wtorki o godzinie 19:00** z automatyczną randomizacją i zaznaczonym polem **Uruchom pominięte zadania**. Oznacza to, że jeśli urządzenia w organizacji są wyłączone w piątki, na przykład o godzinie 18:30, zadanie skanowania urządzeń nigdy nie zostanie uruchomione. W takim przypadku musisz ręcznie skonfigurować zadanie skanowania grupowego.

Kaspersky Security Network (KSN)

Ta sekcja opisuje sposób korzystania z infrastruktury usług online o nazwie Kaspersky Security Network (KSN). Sekcja zawiera szczegóły dotyczące KSN, a także instrukcje związane z włączaniem KSN, konfiguracją dostępu do KSN oraz wyświetlaniem statystyk korzystania z serwera proxy KSN.

Aktualizuje funkcje (obejmuje aktualizacje sygnatur wirusów oraz aktualizacje bazy kodu), przy czym funkcja KSN może nie być dostępna w oprogramowaniu na terytorium Stanów Zjednoczonych.

Informacje o KSN

Kaspersky Security Network (KSN) jest to usługa sieciowa oferująca dostęp do internetowej Bazy Wiedzy firmy Kaspersky, zawierającej informacje o reputacji plików, zasobach sieciowych oraz oprogramowaniu. Korzystanie z danych z Kaspersky Security Network zapewnia przyspieszenie czasu odpowiedzi aplikacji Kaspersky po wykryciu zagrożeń, ulepszenie działania niektórych składników ochrony oraz zmniejszenie ryzyka fałszywych alarmów. KSN umożliwia korzystanie z baz danych reputacji firmy Kaspersky, z których pobierane są informacje o aplikacjach zainstalowanych na zarządzanych urządzeniach.

Uczestnicząc w KSN, wyrażasz zgodę na wysyłanie do Kaspersky w trybie automatycznym informacji dotyczących działania aplikacji firmy Kaspersky, zainstalowanych na urządzeniach klienckich, które są zarządzane przez Kaspersky Security Center Linux. Informacje są wysyłane zgodnie z bieżącymi ustawieniami dostępu KSN.

Kaspersky Security Center Linux obsługuje następujące rozwiązania infrastrukturalne KSN:

- *Globalna sieć KSN* to rozwiązanie umożliwiające wymianę informacji z Kaspersky Security Network. Uczestnicząc w KSN, wyrażasz zgodę na wysyłanie do Kaspersky w trybie automatycznym informacji dotyczących działania aplikacji firmy Kaspersky, zainstalowanych na urządzeniach klienckich, które są zarządzane przez Kaspersky Security Center Linux. Informacje są wysyłane zgodnie z bieżącymi ustawieniami dostępu KSN. Analitycy firmy Kaspersky dodatkowo analizują otrzymane informacje i umieszczają je w reputacyjnych i statystycznych bazach danych Kaspersky Security Network. Kaspersky Security Center Linux domyślnie korzysta z tego rozwiązania.

- *Kaspersky Private Security Network (KPSN)* to rozwiązanie, które umożliwia użytkownikom urządzeń z zainstalowanymi aplikacjami Kaspersky uzyskanie dostępu do baz danych reputacji Kaspersky Security Network oraz innych danych statystycznych bez wysyłania danych do Globalnej sieci KSN z ich własnych urządzeń. Sieć KPSN została zaprojektowana dla klientów korporacyjnych, którzy nie mogą uczestniczyć w Kaspersky Security Network z jednego z następujących powodów:

  - Urządzenia użytkowników nie są podłączone do internetu.

  - Przekazywanie jakichkolwiek danych poza granice kraju lub poza korporacyjną sieć LAN jest zabronione przez prawo lub ograniczone przez korporacyjną politykę bezpieczeństwa.

  Możesz skonfigurować ustawienia dostępu do Kaspersky Private Security Network w sekcji **KSN Proxy** w oknie właściwości Serwera administracyjnego.

Aplikacja wyświetla pytanie o przyłączenie się do KSN podczas działania kreatora wstępnej konfiguracji. Można rozpocząć lub zakończyć korzystanie z KSN w dowolnym momencie, podczas korzystania z aplikacji.

Korzystasz z KSN zgodnie z Oświadczeniem KSN, które czytasz i akceptujesz, gdy włączasz KSN. Jeśli Oświadczenie KSN zostanie zaktualizowane, zostanie wyświetlone podczas aktualizacji Serwera administracyjnego. Możesz zaakceptować zaktualizowane Oświadczenie KSN lub odrzucić je. Jeśli odrzucisz Oświadczenie, będziesz nadal korzystać z KSN zgodnie z poprzednią wersją Oświadczenia KSN, które zaakceptowałeś wcześniej.

Gdy KSN jest włączone, Kaspersky Security Center Linux sprawdza, czy serwery KSN są dostępne, aby upewnić się, że poziom bezpieczeństwa zarządzanych urządzeń jest utrzymany. Jeżeli dostęp do serwerów za pomocą systemowego DNS nie jest możliwy, aplikacja korzysta z publicznych serwerów DNS.

Urządzenia klienckie zarządzane przez Serwer administracyjny wchodzą w interakcję z KSN poprzez serwer proxy KSN. Serwer proxy KSN posiada następujące cechy:

- Urządzenia klienckie mogą wysyłać żądania do KSN, otrzymywać informacje z KSN oraz przesyłać informacje do KSN nawet wtedy, gdy nie mają bezpośredniego dostępu do internetu.

- Serwer KSN proxy buforuje przetwarzane dane, ograniczając obciążenie połączenia wychodzącego i czas oczekiwania na informacje żądane przez urządzenie klienckie.

Serwer KSN Proxy można skonfigurować w sekcji **KSN Proxy** dostępnej w oknie właściwości Serwera administracyjnego.

Konfigurowanie dostępu do KSN

Możesz skonfigurować dostęp do Kaspersky Security Network (KSN) na Serwerze administracyjnym i na punkcie dystrybucji.

W celu skonfigurowania dostępu Serwera administracyjnego do KSN:

1. W menu głównym kliknij nazwę Serwera administracyjnego.

   Zostanie otwarte okno właściwości Serwera administracyjnego.

2. Na zakładce **Ogólne** wybierz sekcję **KSN Proxy**.

3. Ustaw przycisk przełącznika w pozycji **Włącz KSN Proxy na Serwerze administracyjnym Włączono**.

   Jeśli ta opcja jest włączona, serwer proxy KSN wysyła dane do KSN w celu zwiększenia efektywności działania komponentów Kaspersky Security Center i poprawienia działania aplikacji Kaspersky. Dane są wysyłane z urządzeń klienckich do KSN zgodnie z zasadą Kaspersky Endpoint Security, która jest aktywna na tych urządzeniach klienckich. Jeśli to pole jest odznaczone, żadne dane nie będą wysyłane do KSN z Serwera administracyjnego i urządzeń klienckich poprzez Kaspersky Security Center Linux. Jednakże urządzenia klienckie mogą wysyłać dane bezpośrednio do KSN (z pominięciem Kaspersky Security Center Linux) zgodnie z ich ustawieniami. Zasada Kaspersky Endpoint Security, aktywna na urządzeniach klienckich, określa, które dane będą wysyłane bezpośrednio z tych urządzeń do KSN (z pominięciem Kaspersky Security Center Linux).

4. Wybierz Rozwiązanie infrastrukturalne KSN.

   W podsekcji **Uczestnictwo w KSN** wykonaj jedną z następujących czynności:

   - Jeśli korzystasz z Globalnej sieci KSN, ustaw przycisk przełącznika w pozycji **Użyj Kaspersky Security Network Włączono**.

     Przed włączeniem tej opcji należy przeczytać i zaakceptować warunki Oświadczenia KSN.

   - Jeśli używasz sieci KPSN, ustaw przycisk przełącznika opcji **Oświadczenie Kaspersky Private Security Network Włączone** i kliknij przycisk **Określ plik z ustawieniami KSN**, aby pobrać ustawienia prywatnej sieci KPSN (pliki z rozszerzeniami pkcs7 i pem). Po pobraniu ustawień, interfejs wyświetla kontakty i nazwę dostawcy, a także datę utworzenia pliku z ustawieniami prywatnej sieci KPSN.

   Po ustawieniu przycisku przełącznika opcji **Oświadczenie Kaspersky Private Security Network Włączone**, pojawi się komunikat ze szczegółami dotyczącymi sieci KPSN.

   Sieć KPSN jest obsługiwane przez następujące aplikacje Kaspersky:

   - Kaspersky Security Center Linux
   - Kaspersky Endpoint Security for Linux
   - Kaspersky Endpoint Security for Windows

   Jeśli włączysz sieć KPSN w Kaspersky Security Center Linux, te aplikacje otrzymają informację o obsłudze sieci KPSN. W oknie ustawień aplikacji, w podsekcji **Kaspersky Security Network** sekcji **Zaawansowana ochrona przed zagrożeniami** wyświetlana jest informacja dotycząca wybranego dostawcy sieci KSN – KSN lub KPSN.

   > Kaspersky Security Center Linux nie wysyła żadnych danych statystycznych do Kaspersky Security Network, jeśli sieć KPSN została skonfigurowana w sekcji **KSN Proxy** okna właściwości Serwera administracyjnego.

5. Jeśli skonfigurowałeś ustawienia serwera proxy we właściwościach Serwera administracyjnego, ale Twoja sieć wymaga, abyś korzystał bezpośrednio z prywatnej sieci KSN, włącz opcję **Ignoruj ustawienia serwera proxy w przypadku łączenia z KPSN**. W przeciwnym razie, żądania z zarządzanych aplikacji nie będą mogły dotrzeć do KPSN.

6. Skonfiguruj połączenie Serwera administracyjnego z usługą KSN proxy:

   - W sekcji **Ustawienia połączenia**, w polu **Port TCP** określ numer portu TCP, który będzie używany do nawiązywania połączenia z serwerem proxy KSN. Domyślny port do nawiązywania połączenia z serwerem KSN proxy to 13111.

   - Jeśli chcesz, żeby Serwer administracyjny nawiązywał połączenie z serwerem proxy KSN poprzez port UDP, włącz opcję **Użyj portu UDP** i w polu **Port UDP** określ numer portu. Domyślnie opcja ta jest wyłączona i używany jest port TCP. Jeśli ta opcja jest włączona, domyślny port UDP do nawiązywania połączenia z serwerem KSN proxy to 15111.

   - Jeśli chcesz, żeby Serwer administracyjny nawiązywał połączenie z serwerem proxy KSN poprzez port HTTPS, włącz opcję **Użyj HTTPS** i w polu **Port HTTPS** określ numer portu. Domyślnie opcja ta jest wyłączona i używany jest port TCP. Jeśli ta opcja jest włączona, domyślny port HTTPS do nawiązywania połączenia z serwerem KSN proxy to 17111.

7. Przełącz przycisk przełącznika na pozycję **Połącz podrzędne Serwery administracyjne z KSN przez główny Serwer administracyjny Włączone**.

   Jeśli ta opcja jest włączona, podrzędne Serwery administracyjne używają głównego Serwera administracyjnego jako serwera KSN proxy. Jeśli ta opcja jest wyłączona, podrzędne Serwery administracyjne same łączą się z KSN. W tym przypadku zarządzane urządzenia używają podrzędnych Serwerów administracyjnych jako serwerów KSN proxy.

   > Podrzędne Serwery administracyjne używają głównego Serwera administracyjnego jako serwera proxy, jeśli w prawej części sekcji **KSN Proxy**, dostępnej we właściwościach podrzędnych Serwerów administracyjnych, przycisk przełącznika jest ustawiony w pozycji **Włącz KSN Proxy na Serwerze administracyjnym Włączono**.

8. Kliknij przycisk **Zapisz**.

Ustawienia dostępu do KSN zostaną zapisane.

Możesz także skonfigurować dostęp punktu dystrybucji do KSN, na przykład, jeśli chcesz zmniejszyć obciążenie na Serwerze administracyjnym. Punkt dystrybucji działający jako serwer KSN proxy wysyła żądania KSN z zarządzanych urządzeń bezpośrednio do Kaspersky, bez używania Serwera administracyjnego.

W celu skonfigurowania dostępu punktu dystrybucji do Kaspersky Security Network (KSN):

1. Upewnij się, że punkt dystrybucji został przypisany ręcznie.

2. W menu głównym kliknij nazwę Serwera administracyjnego.

   Zostanie otwarte okno właściwości Serwera administracyjnego.

3. Na zakładce **Ogólne** wybierz sekcję **Punkty dystrybucji**.

4. Kliknij nazwę punktu dystrybucji, aby otworzyć okno właściwości.

5. W oknie właściwości punktu dystrybucji, w sekcji **KSN Proxy** włącz opcję **Włącz KSN Proxy po stronie punktu dystrybucji**, a następnie włącz opcję **Dostęp do KSN Cloud/KPSN bezpośrednio przez Internet**.

6. Kliknij **OK**.

Punkt dystrybucji będzie działał jako serwer KSN proxy.

Należy pamiętać, że punkt dystrybucji nie obsługuje uwierzytelniania urządzeń zarządzanych przy użyciu protokołu NTLM.

Włączanie i wyłączanie korzystania z KSN

Aby umożliwić korzystanie z KSN:

1. W menu głównym kliknij nazwę Serwera administracyjnego.

   Zostanie otwarte okno właściwości Serwera administracyjnego.

2. Na zakładce **Ogólne** wybierz sekcję **KSN Proxy**.

3. Ustaw przycisk przełącznika w pozycji **Włącz KSN Proxy na Serwerze administracyjnym Włączono**.

Serwer proxy KSN jest włączony i wysyła dane do KSN w celu zwiększenia efektywności działania komponentów Kaspersky Security Center i usprawnienia działania aplikacji Kaspersky.

1. W zależności od używanego rozwiązania infrastruktury KSN włącz odpowiednie przyciski przełączające.

   - Jeśli korzystasz z Globalnej sieci KSN, ustaw przycisk przełącznika w pozycji **Użyj Kaspersky Security Network Włączono**.

     Wysyłanie danych do KSN jest już możliwe. Przed włączeniem tej opcji należy przeczytać i zaakceptować warunki Oświadczenia KSN.

   - Jeśli używasz sieci KPSN, ustaw przycisk przełącznika w pozycji **Oświadczenie Kaspersky Private Security Network Włączone** i kliknij przycisk ustawień **Określ plik z ustawieniami KSN**, aby pobrać ustawienia sieci KPSN (pliki z rozszerzeniami pkcs7 i pem). Po pobraniu ustawień, interfejs wyświetla kontakty i nazwę dostawcy, a także datę utworzenia pliku z ustawieniami prywatnej sieci KPSN.

     Po ustawieniu przycisku przełącznika w pozycji **Oświadczenie Kaspersky Private Security Network Włączone**, pojawi się komunikat ze szczegółami dotyczącymi sieci KPSN.

2. Kliknij przycisk **Zapisz**.

Aby wyłączyć korzystanie z KSN:

1. W menu głównym kliknij nazwę Serwera administracyjnego.

   Zostanie otwarte okno właściwości Serwera administracyjnego.

2. Na zakładce **Ogólne** wybierz sekcję **KSN Proxy**.

3. Ustaw przycisk przełącznika w pozycji **Włącz KSN Proxy na Serwerze administracyjnym Wyłączono**, aby wyłączyć usługę KSN Proxy.

4. Kliknij przycisk **Zapisz**.

Przeglądanie zaakceptowanego Oświadczenia KSN

Po włączeniu Kaspersky Security Network (KSN) musisz przeczytać i zaakceptować Oświadczenie KSN. W każdej chwili możesz przejrzeć zaakceptowane Oświadczenie KSN.

W celu przejrzenia zaakceptowanego Oświadczenia KSN:

1. W menu głównym kliknij nazwę Serwera administracyjnego.

   Zostanie otwarte okno właściwości Serwera administracyjnego.

2. Na zakładce **Ogólne** wybierz sekcję **KSN Proxy**.

3. Kliknij odnośnik **Zobacz Oświadczenie Kaspersky Security Network**.

W otwartym oknie możesz przejrzeć treść zaakceptowanego Oświadczenia KSN.

Akceptowanie zaktualizowanego Oświadczenia KSN

Korzystasz z KSN zgodnie z Oświadczeniem KSN, które czytasz i akceptujesz, gdy włączasz KSN. Jeśli Oświadczenie KSN zostanie zaktualizowane, zostanie wyświetlone podczas aktualizacji Serwera administracyjnego. Możesz zaakceptować zaktualizowane Oświadczenie KSN lub odrzucić je. Jeśli odrzucisz Oświadczenie, będziesz kontynuować korzystanie z KSN zgodnie z wersją Oświadczenia KSN, którą zaakceptowałeś wcześniej.

Po uaktualnieniu wersji Serwera administracyjnego zaktualizowane Oświadczenie KSN zostanie wyświetlona automatycznie. Jeśli odrzucisz zaktualizowane Oświadczenie KSN, nadal możesz je przejrzeć i zaakceptować później.

W celu wyświetlenia, a następnie zaakceptowania lub odrzucenia zaktualizowanego Oświadczenia KSN:

1. Kliknij odnośnik **Wyświetl powiadomienia** znajdujący się w prawym górnym rogu okna głównego aplikacji.

   Zostanie otwarte okno **Powiadomienia**.

2. Kliknij odnośnik **Wyświetl zaktualizowane Oświadczenie KSN**.

   Zostanie otwarte okno **Aktualizacja Oświadczenia Kaspersky Security Network**.

3. Przeczytaj Oświadczenie KSN, a następnie podejmij decyzję, klikając jeden z następujących przycisków:

   - **Akceptuję zaktualizowane Oświadczenie KSN**
   - **Użyj KSN w ramach starego Oświadczenia**

W zależności od Twojego wyboru KSN działa zgodnie z warunkami aktualnego lub zaktualizowanego Oświadczenia KSN. Możesz wyświetlić tekst zaakceptowanego Oświadczenia KSN we właściwościach Serwera administracyjnego w dowolnym momencie.

Sprawdzanie, czy punkt dystrybucji działa jako serwer proxy KSN

Na zarządzanym urządzeniu przypisanym do pracy jako punkt dystrybucji możesz włączyć Kaspersky Security Network (KSN) Proxy. Zarządzane urządzenie działa jako serwer proxy KSN, gdy usługa ksnproxy jest uruchomiona na urządzeniu. Możesz lokalnie sprawdzić, włączyć lub wyłączyć tę usługę na urządzeniu.

Jako punkt dystrybucji można przypisać urządzenie z systemem Windows lub Linux. Metoda sprawdzania punktu dystrybucji zależy od systemu operacyjnego tego punktu dystrybucji.

Aby sprawdzić, czy punkt dystrybucji oparty na systemie Linux działa jako serwer proxy KSN:

1. Na urządzeniu będącym punktem dystrybucji uruchom polecenie `ps aux`, aby wyświetlić listę uruchomionych procesów.

2. Na liście uruchomionych procesów sprawdź, czy proces `/opt/kaspersky/klnagent64/sbin/ksnproxy` jest uruchomiony.

Jeśli proces `/opt/kaspersky/klnagent64/sbin/ksnproxy` jest uruchomiony, Agent sieciowy na urządzeniu uczestniczy w Kaspersky Security Network i działa jako serwer proxy KSN dla zarządzanych urządzeń należących do obszaru punktu dystrybucji.

Aby sprawdzić, czy punkt dystrybucji oparty na systemie Windows działa jako serwer proxy KSN:

1. Na urządzeniu punktu dystrybucji, w systemie Windows otwórz **Usługi** (**Wszystkie programy** → **Narzędzia administracyjne** → **Usługi**).

2. Na liście usług sprawdź, czy usługa ksnproxy jest uruchomiona.

   Jeśli usługa ksnproxy jest uruchomiona, Agent sieciowy na urządzeniu uczestniczy w Kaspersky Security Network i działa jako serwer proxy KSN dla zarządzanych urządzeń należących do obszaru punktu dystrybucji.

Jeśli chcesz, możesz wyłączyć usługę ksnproxy. W takim przypadku Agent sieciowy w punkcie dystrybucji przestaje uczestniczyć w Kaspersky Security Network. To działanie wymaga uprawnień administratora lokalnego.

Przeglądanie statystyk dotyczących serwera proxy KSN

Kaspersky Security Center Web Console umożliwia przeglądanie statystyk użycia serwera proxy KSN.

Statystyki obejmują następujące parametry:

- Stan połączenia z KSN
- Liczba rekordów pamięci podręcznej
- Liczba pakietów przetworzonych w pamięci podręcznej
- Liczba otrzymanych pakietów

Jeśli używasz KPSN jako rozwiązania infrastrukturalnego, zostaną wyświetlone statystyki użycia KPSN.

Aby wyświetlić statystyki:

1. W menu głównym kliknij nazwę Serwera administracyjnego.

   Zostanie otwarte okno właściwości Serwera administracyjnego.

2. Na karcie **Ogólne** wybierz sekcję **KSN Proxy**, a następnie otwórz kartę **Statystyki**.

   Na tej karcie wyświetlane są aktualne statystyki użycia serwera proxy KSN. Statystyki odświeżają się co 15 sekund.

Statystyki można skopiować, klikając przycisk **Kopiuj do schowka**.

Zarządzanie zadaniami

Ta sekcja opisuje zadania używane przez Kaspersky Security Center Linux.

Informacje o zadaniach

Kaspersky Security Center Linux zarządza aplikacjami zabezpieczającymi Kaspersky, zainstalowanymi na urządzeniach poprzez tworzenie i uruchamianie *zadań*. Zadania są potrzebne do instalowania, uruchamiania i zatrzymywania działania aplikacji, skanowania plików, aktualizowania baz danych i modułów aplikacji, a także wykonywania innych działań na aplikacjach.

Zadania dla określonej aplikacji można utworzyć przy użyciu Kaspersky Security Center Web Console tylko wtedy, gdy wtyczka administracyjna dla tej aplikacji jest zainstalowana na serwerze Kaspersky Security Center Web Console Server.

Zadania mogą być wykonywane na Serwerze administracyjnym i na urządzeniach.

Zadania, które są wykonywane na Serwerze administracyjnym, obejmują:

- Automatyczne rozsyłanie raportów
- Pobieranie uaktualnień do repozytorium
- Tworzenie kopii zapasowych danych Serwera administracyjnego
- Obsługa baz danych

Na urządzeniach wykonywane są następujące typy zadań:

- *Zadania lokalne*—zadania wykonywane na określonym urządzeniu

  Zadania lokalne mogą zostać zmodyfikowane przez administratora przy użyciu narzędzi Kaspersky Security Center Web Console lub przez użytkownika zdalnego urządzenia (na przykład z poziomu interfejsu aplikacji zabezpieczającej). Jeśli zadanie lokalne zostało zmodyfikowane jednocześnie przez administratora i użytkownika zarządzanego urządzenia, zostaną zastosowane zmiany wprowadzone przez administratora, ponieważ mają wyższy priorytet.

- *Zadania grupowe*—zadania wykonywane na wszystkich urządzeniach określonej grupy

  Dopóki nie określono inaczej we właściwościach zadania, zadanie grupowe także wpływa na wszystkie podgrupy wybranej grupy. Zadanie grupowe także może wpływać (opcjonalnie) na urządzenia, które zostały podłączone do podrzędnych i wirtualnych Serwerów administracyjnych zainstalowanych w grupie lub w jej dowolnej podgrupie.

- *Zadania globalne*—zadania wykonywane na zbiorze urządzeń, niezależnie od tego, czy znajdują się w jakiejkolwiek grupie.

Dla każdej aplikacji można utworzyć dowolną liczbę zadań grupowych, zadań globalnych lub zadań lokalnych.

Możesz wprowadzać zmiany w ustawieniach zadań, przeglądać postęp ich wykonywania, a także kopiować, eksportować, importować i usuwać zadania.

Zadanie jest uruchamiane na urządzeniu tylko wtedy, gdy uruchomiona jest aplikacja, dla której utworzono zadanie.

Wyniki wykonania zadań są zapisywane w dzienniku zdarzeń systemu operacyjnego na każdym urządzeniu, w dzienniku zdarzeń systemu operacyjnego na Serwerze administracyjnym, a także w bazie danych Serwera administracyjnego.

Nie używaj prywatnych danych w ustawieniach zadania. Na przykład, unikaj określania hasła administratora domeny.

Informacje o obszarze zadania

Obszar zadania to zestaw urządzeń, na których wykonywane jest zadanie. Typy obszaru to:

- Dla *zadania lokalnego* obszarem jest samo urządzenie.

- Dla *zadania Serwera administracyjnego* obszarem jest Serwer administracyjny.

- Dla *zadania grupowego* obszarem jest lista urządzeń znajdujących się w grupie.

Podczas tworzenia *zadania globalnego* możesz użyć następujących metod do określenia jego obszaru:

- Ręcznie określ pewne urządzenia.

  Jako adresu urządzenia możesz użyć adresu IP (lub zakresu adresów IP) lub nazwy DNS. Możesz również wybrać urządzenia wykryte w sieci przez Serwer administracyjny.

- Zaimportuj listę urządzeń z pliku .txt zawierającego adresy dodawanych urządzeń (każdy adres powinien znajdować się w pojedynczej linii).

  Jeśli lista urządzeń jest importowana z pliku lub jest tworzona ręcznie, a urządzenia są identyfikowane po nazwie, lista może zawierać tylko urządzenia, o których informacje zostały już dodane do bazy danych Serwera administracyjnego. Co więcej, informacje musiały zostać wprowadzone, gdy te urządzenia były podłączone lub podczas wyszukiwania urządzeń.

- Utwórz wybór urządzeń.

Obszar zadania zmienia się, gdy zmienia się zbiór urządzeń zawartych w wyborze. Wybór urządzeń można utworzyć w oparciu o atrybuty urządzeń, włączając w to oprogramowanie zainstalowane na urządzeniach, a także w oparciu o znaczniki przydzielone do urządzeń. Wybór urządzeń to najbardziej elastyczny sposób określania obszaru zadania.

Zadania dla wyborów urządzeń są zawsze uruchamiane przez Serwer administracyjny zgodnie z terminarzem. Te zadania nie mogą zostać uruchomione na urządzeniach, które nie są połączone z Serwerem administracyjnym. Zadania, których obszar jest określony przy użyciu innych metod, są uruchamiane bezpośrednio na urządzeniach i dlatego nie zależą od połączenia urządzenia z Serwerem administracyjnym.

Zadania dla wyborów urządzeń nie są uruchamiane zgodnie z czasem lokalnym urządzenia tylko z czasem lokalnym Serwera administracyjnego. Zadania, których obszar jest określony przy użyciu innych metod, są uruchamiane zgodnie z czasem lokalnym urządzenia.

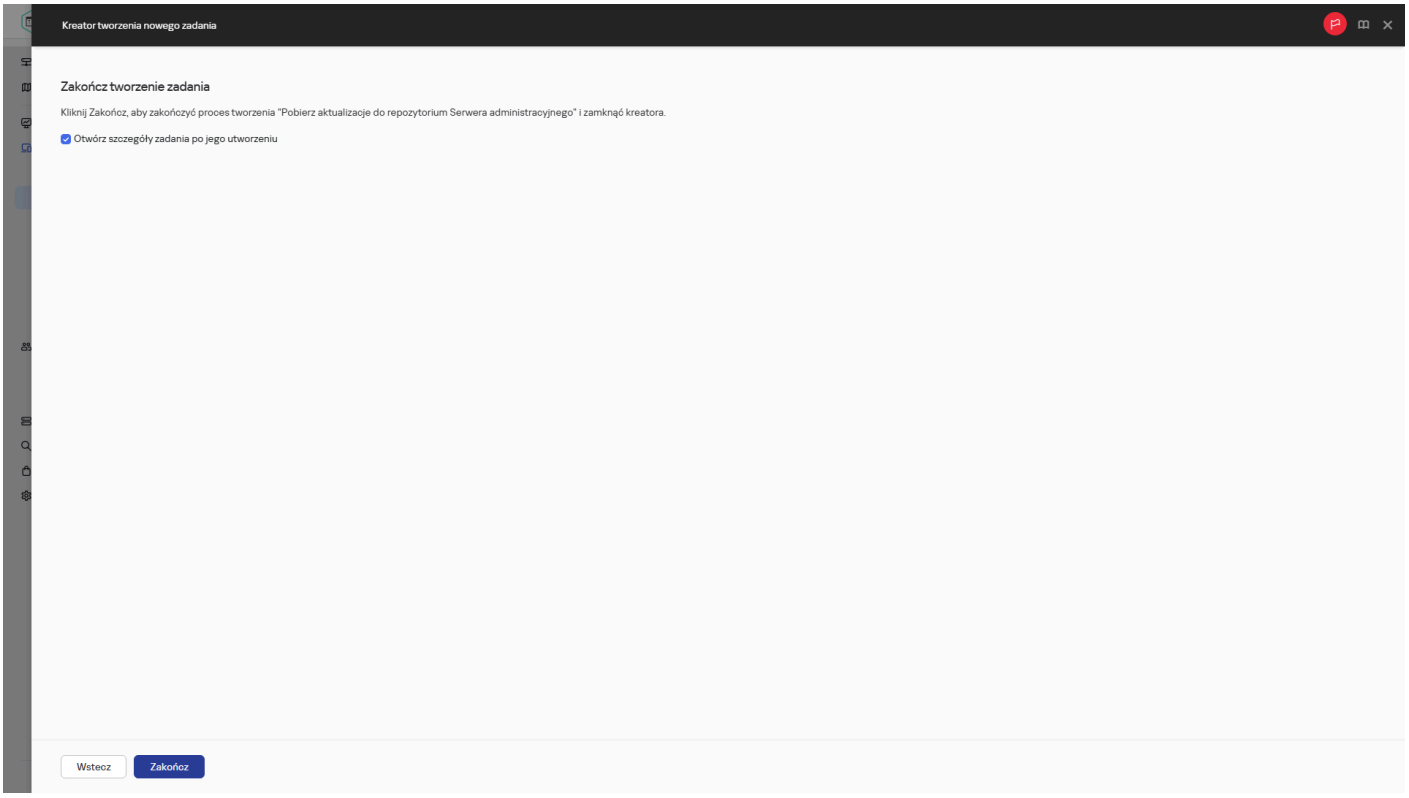
Tworzenie zadania

W celu utworzenia zadania:

1. W menu głównym przejdź do **Zadania**.
2. Kliknij **Dodaj**.

   Zostanie uruchomiony Kreator tworzenia nowego zadania. Postępuj zgodnie z jego instrukcjami.
3. Jeśli chcesz zmodyfikować domyślne ustawienia zadania, włącz opcję **Otwórz szczegóły zadania po jego utworzeniu** na stronie **Zakończ tworzenie zadania**. Jeśli nie włączysz tej opcji, zadanie zostanie utworzone z domyślnymi ustawieniami. Możesz zmodyfikować domyślne ustawienia później w dowolnym momencie.
4. Kliknij przycisk **Zakończ**.

Zadanie zostanie utworzone i będzie wyświetlane na liście zadań.



Zakończenie tworzenia zadania

Aby utworzyć nowe zadanie przypisane do wybranych urządzeń:

1. W menu głównym przejdź do **Zarządzanie zasobami** → **Zasoby (urządzenia)**.

   Zostanie wyświetlona lista zarządzanych urządzeń.

2. Aby uruchomić zadanie dla danych urządzeń, zaznacz znajdujące się obok nich pola wyboru na liście zarządzanych urządzeń. Aby znaleźć urządzenia, których szukasz, możesz skorzystać z funkcji wyszukiwania i filtrowania.

3. Kliknij przycisk **Uruchom zadanie**, a następnie wybierz opcję **Dodaj nowe zadanie**.

   Zostanie uruchomiony Kreator tworzenia nowego zadania.

   W pierwszym kroku kreatora możesz usunąć wybrane urządzenia, które chcesz uwzględnić w zakresie zadania. Postępuj zgodnie z instrukcjami kreatora.

4. Kliknij przycisk **Zakończ**.

Zadanie zostanie utworzone dla wybranych urządzeń.

Ręczne uruchamianie zadania

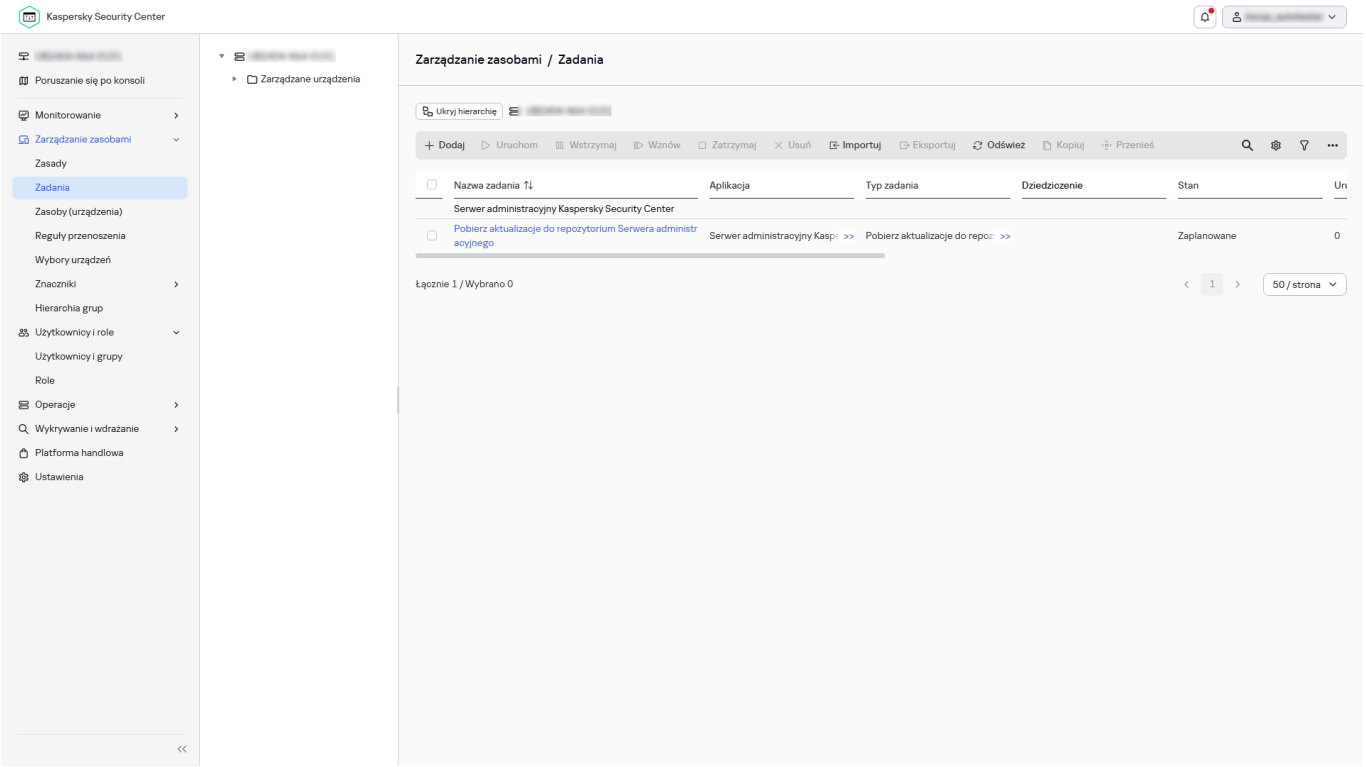
Aplikacja jest uruchamiana zgodnie z ustawieniami terminarza, określonymi we właściwościach każdego zadania. Możesz ręcznie uruchomić zadanie w dowolnym momencie poziomu listy zadań. Alternatywnie możesz wybrać urządzenia na liście **Zasoby (urządzenia)**, a następnie rozpocząć dla nich istniejące zadanie.

W celu ręcznego uruchomienia zadania:

1. W menu głównym przejdź do **Zadania**.

2. Na liście zadań zaznacz pole obok zadania, które chcesz uruchomić.

3. Kliknij przycisk **Uruchom**.



Rozpoczęcie zadania z listy zadań

Zadanie zostanie uruchomione. Możesz sprawdzić stan zadania w kolumnie **Stan** lub klikając przycisk **Wynik**.

Rozpoczęcie zadania dla wybranych urządzeń

Na liście urządzeń możesz wybrać jedno lub więcej urządzeń klienckich, a następnie uruchomić dla nich wcześniej utworzone zadanie. Dzięki temu możesz uruchamiać zadania utworzone wcześniej dla konkretnego zestawu urządzeń.

Spowoduje to zmianę urządzeń, do których przydzielono zadanie na listę urządzeń wybieraną podczas uruchamiania zadania.

W celu rozpoczęcia zadania dla wybranych urządzeń:

1. W menu głównym przejdź do **Zarządzanie zasobami** → **Zasoby (urządzenia)**. Zostanie wyświetlona lista zarządzanych urządzeń.

2. Aby uruchomić zadanie dla zarządzanych urządzeń, użyj znajdującego się obok nich pola wyboru na ich liście. Aby znaleźć urządzenia, których szukasz, możesz skorzystać z funkcji wyszukiwania i filtrowania.

3. Kliknij przycisk **Uruchom zadanie**, a następnie wybierz opcję **Zastosuj istniejące zadanie**.

   Zostanie wyświetlona lista istniejących zadań.

4. Wybrane urządzenia zostaną wyświetlone nad listą zadań. W razie potrzeby możesz usunąć urządzenie z tej listy. Możesz usunąć wszystkie urządzenia oprócz jednego.

5. Wybierz żądane zadanie z listy. Możesz użyć pola wyszukiwania nad listą, aby wyszukać żądane zadanie według nazwy. Można wybrać tylko jedno zadanie.

6. Kliknij **Zapisz i uruchom zadanie**.

   Wybrane zadanie zostanie natychmiast uruchomione dla wybranych urządzeń. Ustawienia zaplanowanego uruchomienia w zadaniu nie ulegają zmianie.

Przeglądanie listy zadań

Możesz przejrzeć listę zadań, które zostały utworzone w Kaspersky Security Center Linux.

W celu przejrzenia listy zadań,

W menu głównym przejdź do **Zadania**.

Zostanie wyświetlona lista zadań. Zadania są grupowane według nazw aplikacji, których dotyczą. Na przykład zadanie *Zdalna instalacja aplikacji* dotyczy Serwera administracyjnego, a zadanie *Aktualizacja* odnosi się do Kaspersky Endpoint Security.

W celu przejrzenia właściwości zadania:

Kliknij nazwę zadania.

Okno właściwości zadania zostanie wyświetlone z kilkoma nazwanymi zakładkami. Na przykład, **Typ zadania** jest wyświetlany na zakładce **Ogólne**, a terminarz zadania na zakładce **Terminarz**.

Ogólne ustawienia zadania

Ta sekcja zawiera ustawienia, które możesz przeglądać i konfigurować dla większości swoich zadań. Lista dostępnych ustawień zależy od konfigurowanego zadania.

Ustawienia określone podczas tworzenia zadania

Podczas tworzenia zadania możesz określić następujące ustawienia. Niektóre z tych ustawień mogą także zostać zmodyfikowane we właściwościach utworzonego zadania.

- Ustawienia ponownego uruchamiania systemu operacyjnego:

  - **Nie uruchamiaj ponownie urządzenia**

    Urządzenia klienckie nie są automatycznie uruchamiane ponownie po działaniu. Aby zakończyć działanie, należy uruchomić urządzenie ponownie (na przykład ręcznie lub przy użyciu zadania zarządzania urządzeniem). Informacje o wymaganym ponownym uruchomieniu zostaną zapisane w wynikach zadania oraz w statusie urządzenia. Opcja ta jest odpowiednia dla zadań na serwerach i innych urządzeniach, na których działanie ciągłe jest krytyczne.

- **Uruchom urządzenie ponownie**

  Urządzenia klienckie są zawsze automatycznie uruchamiane ponownie, jeśli jest to wymagane do zakończenia działania. Opcja jest przydatna, gdy zadania są uruchamiane na urządzeniach, na których możliwe są regularne przerwy w działaniu (wyłączenie lub ponowne uruchomienie).

- **Wymuś zamknięcie aplikacji dla zablokowanych sesji**

  Uruchomione aplikacje mogą uniemożliwić ponowne uruchomienie urządzenia klienckiego. Na przykład, jeśli dokument jest edytowany w edytorze tekstu i nie zostanie zapisany, aplikacja nie zezwoli na ponowne uruchomienie urządzenia.

  Jeśli ta opcja jest włączona, zostaje wymuszone zamknięcie takich aplikacji na zablokowanym urządzeniu przed jego ponownym uruchomieniem. W wyniku tego działania użytkownicy mogą utracić niezapisane zmiany.

  Jeśli ta opcja jest wyłączona, zablokowane urządzenie nie zostanie uruchomione ponownie. Stan zadania na tym urządzeniu informuje, że wymagane jest ponowne uruchomienie urządzenia. Użytkownicy muszą ręcznie zamknąć wszystkie aplikacje uruchomione na zablokowanych urządzeniach i uruchomić ponownie te urządzenia.

  Domyślnie opcja ta jest wyłączona.

- Ustawienia terminarza zadania:

  Rodzaje harmonogramów mogą się różnić w zależności od zadania.

  Niektóre rodzaje harmonogramów mogą być niedostępne dla innych aplikacji Kaspersky.

  - **Ustawienie Uruchom zadanie:**

    - **Co N godzin**

      Zadanie jest uruchamiane regularnie, w określonych przedziałach czasu, począwszy od określonego dnia i godziny.

      Domyślnie, zadanie jest uruchamiane co 6 godzin, począwszy od bieżącej daty i godziny systemowej.

    - **Co N dni**

      Zadanie jest uruchamiane regularnie, w określonych przedziałach czasu. Dodatkowo, możesz określić datę i godzinę pierwszego uruchomienia zadania. Te dodatkowe opcje staną się dostępne, jeśli są obsługiwane przez aplikację, dla której tworzysz zadanie.

      Domyślnie, zadanie jest uruchamiane codziennie, począwszy od bieżącej daty i godziny systemowej.

    - **Co N minut**

      Zadanie jest uruchamiane regularnie, w określonych przedziałach czasu, począwszy od określonej godziny w dniu utworzenia zadania.

      Domyślnie, zadanie jest uruchamiane co 30 minut, począwszy od bieżącego czasu systemowego.

    - **Według dni tygodnia**

      Zadanie jest uruchamiane regularnie, w określone dni tygodnia i o określonej godzinie.

      Domyślnie zadanie jest uruchamiane w każdy piątek o godzinie 18:00:00.

- **Co miesiąc**

  Zadanie jest uruchamiane regularnie, w określonym dniu miesiąca i o określonej godzinie.

  W miesiącach, w które nie ma określonego dnia, zadanie jest uruchamiane w ostatnim dniu.

  Domyślnie, zadanie jest uruchamiane w pierwszym dniu każdego miesiąca, o godzinie zgodnej z bieżącym czasem systemowym.

- **Ręcznie**

  Zadanie nie jest uruchamiane automatycznie. Możesz je uruchomić tylko ręcznie.

  Domyślnie opcja ta jest zaznaczona.

- **Raz**

  Zadanie zostanie uruchomione raz, w określonym dniu i o określonej godzinie (domyślnie w dniu utworzenia zadania).

- **Natychmiast**

  Zadanie uruchamia się natychmiast po zapisaniu ustawień.

- **Miesięcznie wybranego dnia tygodnia**

  Zadanie jest uruchamiane regularnie, w określone dni każdego miesiąca i o określonej godzinie.

  Domyślnie godzina rozpoczęcia to 18:00, a żadne dni miesiąca nie są wybrane.

  > Należy pamiętać, że nie wybiera się konkretnej daty w miesiącu ani numeru tygodnia (pierwszy, drugi tydzień miesiąca), ale kolejny numer dnia tygodnia w miesiącu. Na przykład, jeśli ustawisz kursor w komórce **Wt** w **Pierwszy** wierszu, oznacza to, że zadanie będzie uruchamiane w każdy pierwszy wtorek każdego nowego miesiąca.

  Można wybrać kilka dni tygodnia.

- **Po pobraniu nowych aktualizacji do repozytorium**

  Zadanie jest uruchamiane po pobraniu uaktualnień do repozytorium. Na przykład możesz użyć tego terminarza dla zadania *Aktualizacja*.

- **Po zakończeniu wykonywania innego zadania**

  Bieżące zadanie jest uruchamiane po zakończeniu innego zadania. Opcja ta działa tylko wtedy, gdy oba zadania są przypisane do tych samych urządzeń. Na przykład możesz chcieć uruchomić zadanie *Zarządzaj urządzeniami* z opcją **Włącz urządzenie** i, po zakończeniu jego wykonywania, uruchomić zadanie *Skanowanie antywirusowe*, jako zadanie wyzwalające.

  Musisz wybrać z tabeli zadanie wyzwalające i status, z jakim to zadanie musi zostać ukończone (**Pomyślnie zakończone** lub **Niepowodzenie**).

W razie potrzeby możesz wyszukiwać, sortować i filtrować zadania w tabeli w następujący sposób:

- Wpisz nazwę zadania w polu wyszukiwania, aby wyszukać zadanie na podstawie jego nazwy.
- Kliknij ikonę sortowania, aby posortować zadania według nazwy.

  Domyślnie zadania są sortowane alfabetycznie, w porządku rosnącym.
- Kliknij ikonę filtra i w oknie, które zostanie otwarte, przefiltruj zadania według grupy, a następnie kliknij przycisk **Zastosuj**.

- **Uruchom pominięte zadania**

  Ta opcja określa zachowanie zadania, jeśli urządzenie klienckie nie jest widoczne w sieci, gdy zadanie ma zostać uruchomione.

  Jeżeli ta opcja jest włączona, system podejmie próbę uruchomienia zadania podczas kolejnego uruchomienia aplikacji Kaspersky na urządzeniu klienckim. Jeśli terminarz uruchamiania zadania jest ustawiony na **Ręcznie**, **Raz** lub **Natychmiast**, zadanie jest uruchamiane, gdy urządzenie stanie się widoczne w sieci lub od razu po uwzględnieniu urządzenia w obszarze zadania.

  Jeśli ta opcja jest wyłączona, na urządzeniach klienckich będą uruchamiane tylko zaplanowane zadania. W przypadku harmonogramu **Ręcznie**, **Raz** i **Natychmiast** zadania są uruchamiane tylko na tych urządzeniach klienckich, które są widoczne w sieci. Na przykład, możesz chcieć wyłączyć tę opcję dla zadań zużywających duże ilości zasobów, które chcesz uruchamiać tylko poza godzinami pracy.

  Domyślnie opcja ta jest wyłączona.

- **Używaj automatycznie losowego opóźnienia dla uruchamiania zadań**

  Jeśli ta opcja jest włączona, zadanie jest uruchamiane na urządzeniach klienckich losowo, w określonym przedziale czasu, czyli z *rozproszonym uruchomieniem zadania*. Opcja ta pozwala uniknąć dużej liczby równoczesnych żądań wysyłanych przez urządzenia klienckie do Serwera administracyjnego, gdy uruchomione jest zaplanowane zadanie.

  Czas rozpoczęcia podjęcia próby uzyskania dostępu jest wyliczany automatycznie podczas tworzenia zadania, w zależności od liczby urządzeń klienckich, do których zadanie jest przypisane. Później zadanie będzie zawsze uruchamiane o wyliczonej godzinie uruchomienia. Jednakże, jeśli ustawienia zadania zostaną zmienione lub zadanie zostanie uruchomione ręcznie, zmieni się wyliczona wartość czasu uruchomienia zadania.

  Jeśli ta opcja jest wyłączona, zadanie jest uruchamiane na urządzeniach klienckich zgodnie z terminarzem.

- **Użyj automatycznego losowego opóźnienia dla zadań uruchamianych w przedziale**

  Jeśli ta opcja jest włączona, zadanie jest uruchamiane na urządzeniach klienckich losowo, w określonym przedziale czasu. Opcja ta pozwala uniknąć dużej liczby równoczesnych żądań wysyłanych przez urządzenia klienckie do Serwera administracyjnego, gdy uruchomione jest zaplanowane zadanie.

  Jeśli ta opcja jest wyłączona, zadanie jest uruchamiane na urządzeniach klienckich zgodnie z terminarzem.

  Domyślnie opcja ta jest wyłączona. Domyślny przedział czasu wynosi 1 minutę.

- Urządzenia, do których zadanie zostanie przypisane:

  - **Wybierz urządzenia wykryte w sieci przez Serwer administracyjny**

    Zadanie jest przydzielane do określonych urządzeń. Określone urządzenia mogą obejmować urządzenia z grup administracyjnych oraz nieprzypisane urządzenia.

    Na przykład, możesz chcieć użyć tej opcji w zadaniu instalowania Agenta sieciowego na nieprzypisanych urządzeniach.

- **Określ adresy urządzeń ręcznie lub zaimportuj adresy z listy**

  Możesz określić nazwy NetBIOS, nazwy DNS, adresy IP oraz podsieci IP urządzeń, do których chcesz przydzielić zadanie.

  Możesz użyć tej opcji do wykonania zadania dla określonej podsieci. Na przykład, możesz chcieć zainstalować pewną aplikację na urządzeniach księgowych lub przeskanować urządzenia w podsieci, która jest prawdopodobnie zainfekowana.

- **Przypisz zadanie do wyboru urządzeń**

  Zadanie jest przypisywane do urządzeń znajdujących się w wyborze urządzeń. Możesz określić jeden z istniejących wyborów.

  Na przykład, możesz chcieć użyć tej opcji do uruchomienia zadania na urządzeniach z określoną wersją systemu operacyjnego.

- **Przypisz zadanie do grupy administracyjnej**

  Zadanie jest przypisywane do urządzeń znajdujących się w grupie administracyjnej. Możesz określić jedną z istniejących grup lub utworzyć nową grupę.

  Na przykład, możesz chcieć użyć tej opcji do uruchomienia zadania wysyłania wiadomości do użytkowników, jeśli wiadomość jest specyficzna dla urządzeń znajdujących się w określonej grupie administracyjnej.

  Jeśli zadanie jest przypisane do grupy administracyjnej, zakładka **Zabezpieczenia** nie jest wyświetlana w oknie właściwości zadania, ponieważ zadania grupowe podlegają ustawieniom zabezpieczeń grup, do których się odnoszą.

- Ustawienia konta:

  - **Konto domyślne**

    Zadanie zostanie uruchomione z poziomu tego samego konta co aplikacja, która wykonuje to zadanie.

    Domyślnie opcja ta jest zaznaczona.

  - **Określ konto**

    Uzupełnij pola **Konto** i **Hasło**, aby określić szczegóły konta, z poziomu którego uruchamiane jest zadanie. Konto musi posiadać wystarczające uprawnienia dla tego zadania.

  - **Konto**

    Konto, z poziomu którego zadanie jest uruchamiane.

  - **Hasło**

    Hasło do konta, z poziomu którego zadanie będzie uruchamiane.

Ustawienia określone po utworzeniu zadania

Następujące ustawienia możesz określić tylko po utworzeniu zadania.

- Ustawienia zadań grupowych:

  - **Roześlij do podgrup**

    Ta opcja jest dostępna tylko w ustawieniach zadań grupowych.

Kiedy ta opcja jest włączona, zakres zadania obejmuje:

- Grupa administracyjna, którą wybrano podczas tworzenia zadania.
- Grupy administracyjne podporządkowane wybranej grupie administracyjnej na dowolnym poziomie niżej w hierarchii grup.

Gdy ta opcja jest wyłączona, zakres zadania obejmuje tylko grupę administracyjną wybraną podczas tworzenia zadania.

Domyślnie opcja ta jest włączona.

- **Wyślij do podrzędnych i wirtualnych Serwerów administracyjnych**

  Gdy ta opcja jest włączona, zadanie działające na głównym serwerze administracyjnym jest również stosowane na drugorzędnych serwerach administracyjnych (w tym wirtualnych). Jeżeli zadanie tego samego typu już istnieje na drugorzędnym serwerze administracyjnym, oba zadania są stosowane na drugorzędnym serwerze administracyjnym — istniejące i odziedziczone z głównego serwera administracyjnego.

  Ta opcja jest dostępna tylko wtedy, gdy włączona jest opcja **Roześlij do podgrup**.

  Domyślnie opcja ta jest wyłączona.

- Zaawansowane ustawienia terminarza:

  - **Włącz urządzenia przed uruchomieniem zadania przy użyciu funkcji Wake-on-LAN**

    System operacyjny na urządzeniu zostanie uruchomiony o określonym czasie przed uruchomieniem zadania. Domyślnie czas ten wynosi pięć minut.

    Włącz tę opcję, jeśli chcesz, aby zadanie było uruchamiane na wszystkich urządzeniach klienckich z obszaru zadania, w tym tych urządzeniach, które są wyłączone, gdy zadanie ma zostać uruchomione.

    Jeśli chcesz, żeby urządzenie było automatycznie wyłączane po zakończeniu zadania, włącz opcję **Wyłącz urządzenia po zakończeniu zadania**. Ta opcja znajduje się w tym samym oknie.

    Domyślnie opcja ta jest wyłączona.

  - **Wyłącz urządzenia po zakończeniu zadania**

    Na przykład, możesz chcieć włączyć tę opcję dla zadania instalacji aktualizacji, które instaluje uaktualnienia na urządzeniach klienckich w każdy piątek w godzinach pracy, a następnie wyłącza te urządzenia w weekend.

    Domyślnie opcja ta jest wyłączona.

  - **Zatrzymaj zadanie, jeżeli jest wykonywane dłużej niż**

    Po minięciu określonego czasu, zadanie jest zatrzymywane automatycznie, niezależnie od tego, czy zostało zakończone.

    Włącz tę opcję, jeśli chcesz przerwać (lub zatrzymać) zadania, których wykonanie zajmuje zbyt dużo czasu.

    Domyślnie opcja ta jest wyłączona. Domyślny czas wykonania zadania to 120 minut.

- Ustawienia powiadomień:
  - Sekcja **Przechowywanie historii zadania**:
    - **Przechowuj w bazie danych Serwera administracyjnego przez (dni)**

      Zdarzenia aplikacji związane z wykonaniem zadania na wszystkich urządzeniach klienckich z obszaru zadania są przechowywane na Serwerze administracyjnym przez określoną liczbę dni. Po upłynięciu tego okresu, informacje są usuwane z Serwera administracyjnego.

      Domyślnie opcja ta jest włączona.

    - **Przechowuj w systemowym dzienniku zdarzeń urządzenia**

      Zdarzenia aplikacji związane z wykonaniem zadania są przechowywane lokalnie w dzienniku zdarzeń Syslog każdego urządzenia klienckiego.

      Domyślnie opcja ta jest wyłączona.

    - **Przechowuj w systemowym dzienniku zdarzeń Serwera administracyjnego**

      Zdarzenia aplikacji związane z wykonaniem zadania na wszystkich urządzeniach klienckich z obszaru zadania są przechowywane w sposób scentralizowany w dzienniku zdarzeń Syslog systemu operacyjnego Serwera administracyjnego (OS).

      Domyślnie opcja ta jest wyłączona.

    - **Zapisz wszystkie zdarzenia**

      Jeśli ta opcja jest zaznaczona, wszystkie zdarzenia dotyczące zadania zostaną zapisane w dziennikach zdarzeń.

    - **Zapisz zdarzenia dotyczące postępu zadania**

      Jeśli ta opcja jest zaznaczona, tylko zdarzenia dotyczące wykonania zadania zostaną zapisane w dziennikach zdarzeń.

    - **Zapisz jedynie wyniki wykonywania zadania**

      Jeśli ta opcja jest zaznaczona, tylko zdarzenia dotyczące wyników zadania zostaną zapisane w dziennikach zdarzeń.

  - **Powiadom administratora o wynikach wykonywania zadania**

    Możesz wybrać metody, przy użyciu których administratorzy otrzymają powiadomienia o wynikach wykonania zadań: za pośrednictwem poczty elektronicznej, przez SMS oraz poprzez uruchomienie pliku wykonywalnego. Aby skonfigurować powiadomienie, kliknij odnośnik **Ustawienia**.

    Domyślnie, wszystkie metody powiadamiania są wyłączone.

  - **Powiadom tylko o błędach**

    Jeśli ta opcja jest włączona, administratorzy są powiadamiani tylko wtedy, gdy wykonanie zadania zakończy się błędem.

    Jeśli ta opcja jest wyłączona, administratorzy są powiadamiania po każdym zakończeniu wykonywania zadania.

Domyślnie opcja ta jest włączona.

- Ustawienia zabezpieczeń.
- Ustawienia obszaru zadania.

  W zależności od sposobu określenia obszaru zadania, dostępne są następujące ustawienia:

  - **Urządzenia**

    Jeśli obszar zadania jest określany przez grupę administracyjną, możesz przejrzeć tę grupę. Nie ma tutaj dostępnych zmian. Jednakże możesz ustawić **Wykluczenia z zakresu zadania**.

    Jeśli obszar zadania jest określany przez listę urządzeń, możesz zmodyfikować tę listę poprzez dodanie i usunięcie urządzeń.

  - **Wybór urządzeń**

    Możesz zmienić wybór urządzeń, do którego zadanie jest stosowane.

  - **Wykluczenia z zakresu zadania**

    Możesz określić grupę urządzeń, do których zadanie nie jest stosowane. Grupy, które mają zostać wykluczone, mogą być tylko podgrupami grupami administracyjnej, do której zadanie jest stosowane.

- **Historia rewizji**.

Eksportowanie zadania

Kaspersky Security Center Linux umożliwia zapisanie zadania i jego ustawień w pliku KLT. Możesz użyć tego pliku KLT do zaimportowania zapisanego zadania zarówno do Kaspersky Security Center Windows, jak i Kaspersky Security Center Linux.

W celu wyeksportowania zadania:

1. W menu głównym przejdź do **Zadania**.
2. Zaznacz pole obok zadania, które chcesz wyeliminować.

   Nie można jednocześnie eksportować wielu zadań. Jeśli wybierzesz więcej niż jedno zadanie, przycisk **Eksportuj** będzie nieaktywny. Zadania Serwera administracyjnego są również niedostępne do eksportu.
3. Kliknij przycisk **Eksportuj**.
4. W otwartym oknie **Zapisz jako** określ nazwę i ścieżkę pliku zadania. Kliknij przycisk **Zapisz**.

   Okno **Zapisz jako** jest wyświetlane tylko wtedy, gdy korzystasz z przeglądarki Google Chrome, Microsoft Edge lub Opera. Jeśli używasz innej przeglądarki, plik zadania jest automatycznie zapisywany w folderze **Pobrane**.

Importowanie zadania

Kaspersky Security Center Linux umożliwia import zadania z pliku KLT. Plik KLT zawiera wyeksportowane zadanie i jego ustawienia.

Aby importowanie zadań aplikacji Kaspersky przebiegało prawidłowo, należy zainstalować odpowiednią wtyczkę zarządzającą.

W celu zaimportowania zadania:

1. W menu głównym przejdź do **Zadania**.
2. Kliknij przycisk **Importuj**.
3. Kliknij przycisk **Przeglądaj**, aby wybrać plik zadania, który chcesz zaimportować.
4. W otwartym oknie określ ścieżkę do pliku zadania KLT, a następnie kliknij przycisk **Otwórz**. Pamiętaj, że możesz wybrać tylko jeden plik zadania.

   Zadanie zostanie uruchomione.
5. Po pomyślnym przetworzeniu zadania wybierz urządzenia, do których chcesz przypisać zadanie. W tym celu wykonaj jedną z następujących czynności:

   - **Przypisz zadanie do grupy administracyjnej**

     Zadanie jest przypisywane do urządzeń znajdujących się w grupie administracyjnej. Możesz określić jedną z istniejących grup lub utworzyć nową grupę.

     Na przykład, możesz chcieć użyć tej opcji do uruchomienia zadania wysyłania wiadomości do użytkowników, jeśli wiadomość jest specyficzna dla urządzeń znajdujących się w określonej grupie administracyjnej.

     Jeśli zadanie jest przypisane do grupy administracyjnej, zakładka **Zabezpieczenia** nie jest wyświetlana w oknie właściwości zadania, ponieważ zadania grupowe podlegają ustawieniom zabezpieczeń grup, do których się odnoszą.

   - **Określ adresy urządzeń ręcznie lub zaimportuj adresy z listy**

     Możesz określić nazwy NetBIOS, nazwy DNS, adresy IP oraz podsieci IP urządzeń, do których chcesz przydzielić zadanie.

     Możesz użyć tej opcji do wykonania zadania dla określonej podsieci. Na przykład, możesz chcieć zainstalować pewną aplikację na urządzeniach księgowych lub przeskanować urządzenia w podsieci, która jest prawdopodobnie zainfekowana.

   - **Przypisz zadanie do wyboru urządzeń**

     Zadanie jest przypisywane do urządzeń znajdujących się w wyborze urządzeń. Możesz określić jeden z istniejących wyborów.

     Na przykład, możesz chcieć użyć tej opcji do uruchomienia zadania na urządzeniach z określoną wersją systemu operacyjnego.
6. Wybierz obszar zadania.
7. Kliknij przycisk **Zakończone**, aby zakończyć import zadania.

Pojawi się powiadomienie z wynikami importu. Jeśli zadanie zostało pomyślnie zaimportowane, możesz kliknąć łącze **Szczegóły**, aby wyświetlić właściwości zadania.

Po pomyślnym imporcie zadanie zostanie wyświetlone na liście zadań. Importowane są również ustawienia zadania i harmonogram. Zadanie zostanie uruchomione zgodnie z harmonogramem.

> Jeśli nowo importowane zadanie ma identyczną nazwę jak istniejące zadanie, nazwa importowanego zadania jest rozszerzana o indeks **(<następny numer porządkowy>)**, na przykład: **(1)**, **(2)**.

Uruchamianie kreatora zmiany haseł w zadaniach

Dla zadania, które nie jest lokalne, możesz określić konto, z poziomu którego zadanie musi być uruchomione. Konto może zostać określone podczas tworzenia zadania lub we właściwościach istniejącego zadania. Jeśli określone konto jest używane zgodnie z instrukcjami bezpieczeństwa organizacji, te instrukcje mogą wymagać zmiany hasła do konta od czasu do czasu. Jeśli hasło do konta wygaśnie i ustawisz nowe, nie powiedzie się uruchomienie zadań, aż do momentu, gdy określisz nowe ważne hasło we właściwościach zadania.

Kreator zmiany haseł w zadaniach umożliwia automatyczne zastąpienie starego hasła nowym we wszystkich zadaniach, w których konto jest określone. Alternatywnie, możesz ręcznie zmienić to hasło we właściwościach każdego zadania.

W celu uruchomienia kreatora zmiany haseł w zadaniach:

1. W menu głównym przejdź do **Zadania**.
2. Kliknij **Zarządzaj poświadczeniami kont do uruchamiania zadań**.

   Postępuj zgodnie z instrukcjami kreatora.

Krok 1. Określanie danych uwierzytelniających

Określ nowe poświadczenia, które są aktualnie ważne w Twoim systemie. Jeśli przejdziesz do następnego kroku kreatora, Kaspersky Security Center Linux sprawdzi, czy nazwa określonego konta odpowiada nazwie konta we właściwościach każdego zadania, które nie jest lokalne. Jeśli nazwy kont pasują do siebie, hasło we właściwościach zadania zostanie automatycznie zastąpione nowym.

W celu określenia nowego konta, wybierz opcję:

- **Użyj bieżącego konta**

  Kreator używa nazwy konta, na którym aktualnie zalogowano się do Kaspersky Security Center Web Console. Następnie ręcznie podaj hasło do konta w polu **Aktualne hasło do użycia w zadaniach**.

- **Określ inne konto**

  Określ nazwę konta, z poziomu którego zadania muszą być uruchamiane. Następnie określ hasło do konta w polu **Aktualne hasło do użycia w zadaniach**.

Jeśli uzupełnisz pole **Poprzednie hasło (opcjonalnie; jeśli chcesz zastąpić je obecnym)**, Kaspersky Security Center Linux zastępuje hasło tylko dla tych zadań, w których zostanie wykryta nazwa konta oraz stare hasło. Zastępowanie odbywa się automatycznie. We wszystkich pozostałych przypadkach musisz wybrać działanie, jakie ma zostać podjęte w kolejnym kroku kreatora.

Krok 2. Wybieranie działania, jakie ma zostać podjęte

Jeśli nie określiłeś poprzedniego hasła w pierwszym kroku kreatora lub jeśli stare hasło nie odpowiada hasłom we właściwościach zadań, powinieneś wybrać działanie, jakie ma zostać wykonane na wykrytych zadaniach.

W celu wybrania akcji dla zadania:

1. Zaznacz pole obok zadania, dla której chcesz wybrać działanie.
2. Wykonaj jedną z następujących czynności:
   - Aby usunąć hasło we właściwościach zadania, kliknij **Usuń poświadczenia**.

     Zadanie zostanie przełączone do działania na koncie domyślnym.
   - Aby zastąpić hasło nowym, kliknij **Wymuszaj zmianę hasła, nawet jeśli stare hasło jest niepoprawne lub nie zostało podane**.
   - Aby anulować zmianę hasła, kliknij **Nie wybrano akcji**.

Wybrane akcje zostaną zastosowane po przejściu do następnego kroku kreatora.

Krok 3. Sprawdzanie wyników

W ostatnim kroku kreatora przejrzyj wyniki dla każdego wykrytego zadania. Aby zakończyć działanie kreatora, kliknij przycisk **Zakończ**.

Przeglądanie wyników wykonywania zadań przechowywanych na Serwerze administracyjnym

Kaspersky Security Center Linux umożliwia przeglądanie wyników wykonywania zadań grupowych, zadań dla określonych urządzeń oraz zadań Serwera administracyjnego.

W celu przejrzenia wyników wykonania zadania:

1. W oknie właściwości zadania wybierz sekcję **Ogólne**.
2. Kliknij odnośnik **Wyniki**, aby otworzyć okno **Wyniki zadania**.

Aby wyświetlić wyniki zadania dla podrzędnego Serwera administracyjnego:

1. W oknie właściwości zadania wybierz sekcję **Ogólne**.
2. Kliknij odnośnik **Wyniki**, aby otworzyć okno **Wyniki zadania**.
3. Kliknij **Statystyki z serwerów dodatkowych**.
4. Wybierz serwer dodatkowy, dla którego chcesz wyświetlić okno **Wyniki zadania**.

Znaczniki aplikacji

Ta sekcja opisuje znaczniki aplikacji oraz zawiera instrukcje ich tworzenia i modyfikowania oraz znakowania aplikacji firm trzecich.

Znaczniki aplikacji

Kaspersky Security Center Linux umożliwia oznaczenie aplikacji z rejestru aplikacji. Znacznik to etykieta aplikacji, która może zostać użyta do grupowania lub wyszukiwania aplikacji. Znacznik przypisany do aplikacji może służyć jako warunek w wyborach urządzeń.

Na przykład, możesz utworzyć znacznik `[Browsers]` i przypisać go do wszystkich przeglądarek Microsoft Internet Explorer, Google Chrome, Mozilla Firefox.

Tworzenie znacznika aplikacji

W celu utworzenia znacznika aplikacji:

1. W menu głównym przejdź do **Zarządzanie oprogramowaniem** → **Aplikacje innych firm** → **Znaczniki aplikacji**.
2. Kliknij **Dodaj**.

   Zostanie otwarte okno nowego znacznika.
3. Wprowadź nazwę znacznika.
4. Kliknij **OK**, aby zachować zmiany.

Nowy znacznik pojawi się na liście znaczników aplikacji.

Zmienianie nazwy znacznika aplikacji

W celu zmiany nazwy znacznika aplikacji:

1. W menu głównym przejdź do **Zarządzanie oprogramowaniem** → **Aplikacje innych firm** → **Znaczniki aplikacji**.
2. Zaznacz pole obok znacznika, którego nazwę chcesz zmienić, a następnie kliknij **Edytuj**.

   Zostanie otwarte okno właściwości znacznika.
3. Zmień nazwę znacznika.
4. Kliknij **OK**, aby zachować zmiany.

Zaktualizowany znacznik pojawi się na liście znaczników aplikacji.

Przydzielanie znaczników do aplikacji

W celu przydzielenia jednego lub kilku znaczników do aplikacji:

1. W menu głównym przejdź do sekcji **Zarządzanie oprogramowaniem** → **Aplikacje innych firm** → **Rejestr aplikacji**.
2. Kliknij nazwę aplikacji, do której chcesz przydzielić znaczniki.
3. Wybierz zakładkę **Znaczniki**.

   Zakładka wyświetla wszystkie znaczniki aplikacji, które istnieją na Serwerze administracyjnym. Dla znaczników przypisanych do wybranej aplikacji, w kolumnie **Przypisany znacznik** zaznaczone jest pole.
4. Dla znaczników, które chcesz przypisać, w kolumnie **Przypisany znacznik** zaznacz pola.
5. Kliknij **Zapisz**, aby zachować zmiany.

Znaczniki zostają przypisane do aplikacji.

Usuwanie przydzielonych znaczników z aplikacji

W celu usunięcia jednego lub kilku znaczników z aplikacji:

1. W menu głównym przejdź do sekcji **Zarządzanie oprogramowaniem** → **Aplikacje innych firm** → **Rejestr aplikacji**.
2. Kliknij nazwę aplikacji, z której chcesz usunąć znaczniki.
3. Wybierz zakładkę **Znaczniki**.

   Zakładka wyświetla wszystkie znaczniki aplikacji, które istnieją na Serwerze administracyjnym. Dla znaczników przypisanych do wybranej aplikacji, w kolumnie **Przypisany znacznik** zaznaczone jest pole.

4. Dla znaczników, które chcesz usunąć, w kolumnie **Przypisany znacznik** odznacz pola.

5. Kliknij **Zapisz**, aby zachować zmiany.

Znaczniki zostają usunięte z aplikacji.

Usunięte znaczniki aplikacji nie zostają całkowicie usunięte. Jeśli chcesz, możesz usunąć je ręcznie.

Usuwanie znacznika aplikacji

W celu usunięcia znacznika aplikacji:

1. W menu głównym przejdź do **Zarządzanie oprogramowaniem** → **Aplikacje innych firm** → **Znaczniki aplikacji**.

2. Z listy wybierz znacznik aplikacji, który chcesz usunąć.

3. Kliknij przycisk **Usuń**.

4. W otwartym oknie potwierdzenia kliknij **OK**.

Znacznik aplikacji zostanie usunięty. Usunięty znacznik jest automatycznie usuwany ze wszystkich aplikacji, do których został przydzielony.

Użycie narzędzia klscflag do otwarcia portu 13291

Możesz zautomatyzować działanie Kaspersky Security Center Linux przy użyciu narzędzia klakaut. Narzędzie klakaut i jego system pomocy znajdują się w folderze instalacyjnym Kaspersky Security Center Linux. Jeśli chcesz użyć narzędzia klakaut, otwórz port 13291 za pomocą narzędzia klscflag.

Narzędzie klscflag zmienia wartość parametru KLSRV_SP_SERVER_SSL_PORT_GUI_OPEN.

Aby otworzyć port 13291:

1. Wykonaj następujące polecenie w wierszu poleceń:
```
/opt/kaspersky/ksc64/sbin/klscflag -ssvset -pv klserver -s 87 -n
KLSRV_SP_SERVER_SSL_PORT_GUI_OPEN -sv true -svt BOOL_T -ss "|ss_type =
\"SS_SETTINGS\";"
```

2. Uruchom ponownie usługę Serwer administracyjny Kaspersky Security Center, wykonując następujące polecenie:
```
sudo systemctl restart kladminserver_srv
```

Port 13291 jest otwarty.

Aby sprawdzić, czy port 13291 został pomyślnie otwarty:

Wykonaj następujące polecenie w wierszu poleceń:

```
/opt/kaspersky/ksc64/sbin/klscflag -ssvget -pv klserver -s 87 -n
KLSRV_SP_SERVER_SSL_PORT_GUI_OPEN -svt BOOL_T -ss "|ss_type = \"SS_SETTINGS\";"
```

To polecenie zwraca następujący wynik:

```
+--- (PARAMS_T)
+---KLSRV_SP_SERVER_SSL_PORT_GUI_OPEN = (BOOL_T)true
```

Wartość `true` oznacza, że port jest otwarty. W przeciwnym razie wyświetlana jest wartość `false`.

Rejestrowanie interfejsu aplikacji Kaspersky Industrial CyberSecurity for Networks w Kaspersky Security Center Web Console

Aby rozpocząć pracę z aplikacją Kaspersky Industrial CyberSecurity for Networks za pośrednictwem konsoli Kaspersky Security Center Web Console, musisz najpierw zarejestrować go w konsoli Kaspersky Security Center Web Console.

W celu zarejestrowania aplikacji Kaspersky Industrial CyberSecurity for Networks:

1. Upewnij się, że wykonano następujące czynności:

   - Pobrałeś i zainstalowałeś wtyczkę webową Kaspersky Industrial CyberSecurity for Networks.

     Możesz to zrobić później, czekając na synchronizację Kaspersky Industrial CyberSecurity for Networks Server z Serwerem administracyjnym. Po pobraniu i zainstalowaniu wtyczki sekcja **KICS for Networks** zostanie wyświetlona w menu głównym Kaspersky Security Center Web Console.

   - W interfejsie internetowym Kaspersky Industrial CyberSecurity for Networks można skonfigurować i włączyć interakcję z Kaspersky Security Center Linux. Aby uzyskać szczegółowe informacje, zapoznaj się z pomocą online do Kaspersky Industrial CyberSecurity for Networks.

2. Przenieś urządzenie, na którym zainstalowano Kaspersky Industrial CyberSecurity for Networks Server, z grupy Urządzenia nieprzypisane do grupy Zarządzane urządzenia:

   a. W menu głównym przejdź do **Zarządzanie zasobami** → **Urządzenia nieprzypisane**.

   b. Zaznacz pole wyboru obok urządzenia, na którym jest zainstalowany Kaspersky Industrial CyberSecurity for Networks Server.

   c. Kliknij przycisk **Przenieś do grupy**.

   d. W hierarchii grup administracyjnych zaznacz pole wyboru obok grupy **Zarządzane urządzenia**.

   e. Kliknij przycisk **Przenieś**.

3. Przejdź do okna właściwości urządzenia, na którym jest zainstalowany Kaspersky Industrial CyberSecurity for Networks Server.

4. Na stronie właściwości urządzenia, w sekcji **General** wybierz opcję **Nie odłączaj od Serwera administracyjnego**, a następnie kliknij przycisk **Zapisz**.

5. W oknie właściwości urządzenia wybierz sekcję **Applications**.

6. W sekcji **Applications** wybierz Agent sieciowy Kaspersky Security Center.

7. Jeśli aktualny stan aplikacji to *Zatrzymana*, poczekaj, aż zmieni się na *Uruchomiona*.

   Ten proces trwa do 15 minut. Jeśli nie jest jeszcze zainstalowana wtyczka webowa Kaspersky Industrial CyberSecurity for Networks, możesz to zrobić teraz.

8. Jeśli chcesz przeglądać statystyki Kaspersky Industrial CyberSecurity for Networks, możesz dodać widżety na pulpicie nawigacyjnym. Aby dodać widżety, wykonaj następujące czynności:

   a. W menu głównym przejdź do **Monitorowanie** → **Dashboard**.

   b. Na pulpicie nawigacyjnym kliknij przycisk **Add or restore web widget**.

   c. W otwartym menu widżetu wybierz **Inne**.

   d. Wybierz widżety, które chcesz dodać:

      - Mapa wdrożenia KICS for Networks
      - Informacje o KICS dla serwerów sieciowych
      - Aktualne wydarzenia KICS for Networks
      - Urządzenia, na których występują problemy w KICS for Networks
      - Krytyczne wydarzenia w KICS for Networks
      - Statusy w KICS for Networks

9. Aby przejść do interfejsu internetowego Kaspersky Industrial CyberSecurity for Networks, wykonaj następujące czynności:

   a. W menu głównym przejdź do **KICS for Networks** → **Search**.

   b. Kliknij przycisk **Find events or devices**.

   c. W otwartym oknie **Parametry zapytania** kliknij pole **Serwer**.

   d. Z rozwijanej listy serwerów zintegrowanych z Kaspersky Security Center Linux wybierz Kaspersky Industrial CyberSecurity for Networks Server, a następnie kliknij przycisk **Znajdź**.

   e. Kliknij odnośnik **Przejdź do serwera** znajdujący się obok nazwy Kaspersky Industrial CyberSecurity for Networks Server.

      Zostanie wyświetlona strona logowania do Kaspersky Industrial CyberSecurity for Networks.

      Aby zalogować się do interfejsu sieciowego Kaspersky Industrial CyberSecurity for Networks, musisz podać dane uwierzytelniające konta użytkownika aplikacji.

Zarządzanie użytkownikami i rolami użytkowników

Ta sekcja opisuje użytkowników i role użytkownika, a także zawiera instrukcje ich tworzenia i modyfikowania, przydzielania ról i grup do użytkowników, a także kojarzenia profili zasad z rolami.

Informacje o kontach użytkowników

Kaspersky Security Center Linux umożliwia zarządzanie kontami użytkowników i grupami bezpieczeństwa. Aplikacja obsługuje trzy typy kont:

- Konta pracowników firmy. Serwer administracyjny pobiera dane kont tych użytkowników domeny podczas przeszukiwania kontrolera domeny organizacji.
- Konta lokalnych użytkowników. Konta lokalne na zarządzanych urządzeniach, a także konta lokalne na urządzeniu, na którym zainstalowany jest Serwer administracyjny.
- Konta użytkowników wewnętrznych Kaspersky Security Center Linux. Możesz tworzyć konta użytkowników wewnętrznych. Konta te są używane wyłącznie w Kaspersky Security Center Linux.

Grupy kladmins nie można użyć w celu uzyskania dostępu do Kaspersky Security Center Web Console w Kaspersky Security Center Linux. Grupa kladmins może zawierać wyłącznie konta służące do uruchamiania usług Kaspersky Security Center Linux.

Aby wyświetlić tabele kont użytkowników i grup bezpieczeństwa:

1. W menu głównym przejdź do **Użytkownicy i role** → **Użytkownicy i grupy**.
2. Wybierz zakładkę **Użytkownicy** lub **Grupy**.

Zostanie otwarta tabela użytkowników lub grup bezpieczeństwa. Jeśli chcesz wyświetlić tabelę tylko z wewnętrznymi użytkownikami lub grupami albo tylko z lokalnymi użytkownikami lub grupami, ustaw kryteria filtra **Typ konta** odpowiednio na **Wewnętrzny** lub **Lokalny**.

Jeśli tabela użytkowników znajduje się w kontenerze zawierającym ponad 50 000 użytkowników, wyświetlanych jest tylko pierwszych 50 000 użytkowników, a pozostali użytkownicy nie są widoczni.

Informacje o rolach użytkowników

Rola użytkownika (zwana dalej *rolą*) to obiekt zawierający zestaw praw i uprawnień. Rola może zostać skojarzona z ustawieniami aplikacji Kaspersky zainstalowanych na urządzeniu użytkownika. Możesz przypisać rolę do zestawu użytkowników lub do zestawu grup bezpieczeństwa na dowolnym poziomie w hierarchii grup administracyjnych, Serwerów administracyjnych lub na poziomie określonych obiektów.

Jeśli zarządzasz urządzeniami poprzez hierarchię Serwerów administracyjnych, która obejmuje wirtualne Serwery administracyjne, pamiętaj, że możesz tworzyć, modyfikować lub usuwać role użytkowników tylko z fizycznego Serwera administracyjnego. Następnie możesz propagować role użytkowników na podrzędne Serwery administracyjne, w tym wirtualne.

Możesz skojarzyć role użytkownika z profilami zasad. Jeśli użytkownikowi przydzielono rolę, ten użytkownik uzyska ustawienia zabezpieczeń niezbędne do pełnienia funkcji związanych z jego stanowiskiem pracy.

Rola użytkownika może zostać skojarzona z użytkownikami urządzeń w określonej grupie administracyjnej.

Obszar roli użytkownika

Obszar roli użytkownika to połączenie użytkowników i grup administracyjnych. Ustawienia skojarzone z rolą użytkownika są stosowane tylko do urządzeń, które należą do użytkowników posiadających tę rolę i tylko wtedy, gdy te urządzenia należą do grup skojarzonych z tą rolą, w tym grup podrzędnych.

Korzyści korzystania z ról

Korzyścią korzystania z ról jest brak konieczności określenia ustawień zabezpieczeń dla każdego z zarządzanych urządzeń lub dla każdego z użytkowników oddzielnie. Liczba użytkowników i urządzeń w firmie może być całkiem duża, ale liczba różnych stanowisk pracy, które wymagają różnych ustawień zabezpieczeń jest znacząco mała.

Różnice wynikające z używania profili zasad

Profile zasad to właściwości zasady tworzone dla każdej aplikacji Kaspersky oddzielnie. Rola jest skojarzona z wieloma profilami zasad utworzonymi dla różnych aplikacji. Dlatego też rola jest metodą zebrania ustawień dla określonego typu użytkownika w jednym miejscu.

Konfigurowanie praw dostępu do funkcji aplikacji. Kontrola dostępu oparta o rolę

Kaspersky Security Center Linux oferuje możliwości dla dostępu opartego na roli do funkcji Kaspersky Security Center Linux i zarządzanych aplikacji firmy Kaspersky.

Możesz skonfigurować uprawnienia dostępu do funkcji aplikacji dla użytkowników Kaspersky Security Center Linux w jeden z następujących sposobów:

- Konfigurując uprawnienia dla każdego użytkownika lub grupy użytkowników indywidualnie.
- Tworząc standardowe role użytkownika z predefiniowanym zestawem uprawnień i przypisując te role do użytkowników w zależności od ich zakresu obowiązków.

Stosowanie ról użytkownika jest przeznaczone do uproszczenia i skrócenia rutynowych procedur konfigurowania uprawnień dostępu użytkowników do funkcji aplikacji. Uprawnienia dostępu w obrębie roli są konfigurowane zgodnie ze 'standardowymi' zadaniami i zakresem obowiązków użytkowników.

Rolom użytkownika można przypisać nazwy, które odpowiadają ich przeznaczeniu. Możesz utworzyć nieograniczoną liczbę ról w aplikacji.

Możesz użyć predefiniowanych ról użytkownika z już skonfigurowanym zestawem uprawnień lub utworzyć nowe role i samodzielnie skonfigurować wymagane uprawnienia.

Prawa dostępu do funkcji aplikacji

Poniższa tabela przedstawia funkcje Kaspersky Security Center Linux wraz z prawami dostępu do zarządzania powiązanymi zadaniami, raportami, ustawieniami i wykonywania powiązanych działań użytkownika.

Aby wykonać czynności użytkownika wymienione w tabeli, użytkownik musi mieć określone uprawnienia obok akcji.

Prawa do **odczytu**, **wpisywania** i **wykonywania** mają zastosowanie do każdego zadania, raportu lub ustawienia. Oprócz tych praw użytkownik musi mieć uprawnienie **Wykonaj operacje na wyborach urządzeń**, aby zarządzać zadaniami, raportami lub ustawieniami wyborów urządzeń.

> Wszystkie zadania, raporty, ustawienia i pakiety instalacyjne, których brakuje w tabeli, należą do obszaru funkcjonalnego **Funkcje ogólne: Podstawowa funkcjonalność**.

Obszar funkcjonalny	Uprawnienie	Akcja użytkownika: uprawnienia wymagane do wykonania akcji	Zadanie	Raport	Inne
Funkcje ogólne: **Zarządzanie grupami administracyjnymi**	**Wpisz**	• Dodaj urządzenie do grupy administracyjnej: **Wpisz** • Usuń urządzenie z grupy administracyjnej: **Wpisz** • Dodaj grupę administracyjną do innej grupy administracyjnej: **Wpisz** • Usuń grupę administracyjną z innej grupy administracyjnej: **Wpisz**	Brak	Brak	Brak

Obszar funkcjonalny	Uprawnienie	Akcja użytkownika: uprawnienia wymagane do wykonania akcji	Zadanie	Raport	Inne
Funkcje ogólne: **Uzyskuj dostęp do obiektów bez względu na ich listy ACL**	**Odczyt**	Uzyskaj dostęp do odczytu do wszystkich obiektów: **Odczyt**	Brak	Brak	**Funkcje ogólne: Uzyskuj dostęp do obiektów bez względu na ich listy ACL** są przeznaczone do celów audytu. Gdy użytkownikom zostan przyznane prawa **Odczyt** w tym obszarze funkcjonalnym, uzyskają pełny dostęp do **Odczyt** do wszystkich obiektów będą mogli wykonywać dowolne utworzone zadania na wybranych urządzeniach podłączonych do Serwera administracyjnego poprzez Agenta sieciowego z uprawnieniami administratora lokalnego (root w przypadku systemu Linux). Zalecamy ostrożne przyznanie tych praw ograniczonej grupie użytkowników, którzy potrzebują ich do wykonywania swoich obowiązków służbowych. Dostęp jest przyznawany niezależnie od innych praw, nawet jeśli zabraniają one dostępu do odczytu określonych obiektów
Cechy ogólne: **Podstawowa funkcjonalność**	• **Odczyt** • **Wpisz** • **Wykonaj** • **Wykonaj operacje na wyborach urządzeń**	• Reguły przenoszenia urządzeń (tworzenie, modyfikowanie lub usuwanie) dla Serwera wirtualnego: **Wpisz**, **Wykonuj** operacje na wybranych urządzeniach • Uzyskaj niestandardowy certyfikat protokołu Mobile (LWNGT): **Odczytaj** • Ustaw certyfikat niestandardowy protokołu Mobile (LWNGT): **Zapisz** • Uzyskaj listę sieci zdefiniowaną przez NLA: **Odczytaj** • Dodaj, zmodyfikuj lub usuń listę sieci zdefiniowaną przez NLA: **Wpisz**	• „Pobierz aktualizacje do repozytorium serwera administracyjnego" • „Dostarczaj raporty" • „Roześlij pakiet instalacyjny" • „Zdalnie zainstaluj aplikację na podrzędnych Serwerach administracyjnych"	• „Raport o stanie ochrony" • „Raport o zagrożeniach" • „Raport o najbardziej zainfekowanych urządzeniach" • „Raport o stanie antywirusowych baz danych" • „Raport o błędach" • „Raport o atakach sieciowych" • „Raport podsumowujący o zainstalowanych aplikacjach zabezpieczających systemy pocztowe"	Brak

Obszar funkcjonalny	Uprawnienie	Akcja użytkownika: uprawnienia wymagane do wykonania akcji	Zadanie	Raport	Inne
		• Wyświetl listę kontroli dostępu grup: **Odczytaj** • Wyświetl dziennik systemu operacyjnego: **Przeczytaj** • Wyświetl klucz odzyskiwania, aby przywrócić dostęp do dysku twardego zaszyfrowanego za pomocą Szyfrowania dysków funkcją BitLocker: **Wykonaj**		• „Raport podsumowujący o zainstalowanej ochronie stacji roboczych oraz o zainstalowanych aplikacjach chroniących system Windows Server” • „Raport podsumowujący o aplikacjach zabezpieczających styk sieci z internetem” • „Raport podsumowujący o typach zainstalowanych aplikacji” • „Raport o użytkownikach zainfekowanych urządzeń” • „Raport o incydentach związanych z bezpieczeństwem” • „Raport o zdarzeniach” • „Raport aktywności punktów dystrybucji” • „Raport o podrzędnych Serwerach administracyjnych” • „Raport zdarzeń Kontroli urządzeń” • „Raport o lukach” • „Raport o zabronionych aplikacjach” • „Raport Kontroli sieci” • „Raport o stanie szyfrowania zarządzanych urządzeń” • „Raport o stanie szyfrowania urządzeń pamięci masowej” • „Raport o prawach dostępu do zaszyfrowanych dysków” • „Raport o błędach podczas szyfrowania plików” • „Raport o zablokowanym dostępie do zaszyfrowanych plików” • „Raport o obowiązujących uprawnieniach użytkowników” • „Raport na temat praw”	

Obszar funkcjonalny	Uprawnienie	Akcja użytkownika: uprawnienia wymagane do wykonania akcji	Zadanie	Raport	Inne
Funkcje ogólne: **Obiekty usunięte**	• **Odczyt** • **Wpisz**	• Wyświetl usunięte obiekty w Koszu: **Odczytaj** • Usuń obiekty z Kosza: **Wpisz**	Brak	Brak	Brak
Funkcje ogólne: **Przetwarzanie zdarzeń**	• **Usuń zdarzenia** • **Edytuj ustawienia powiadomień o zdarzeniach** • **Edytuj ustawienia rejestrowania zdarzeń** • **Wpisz**	• Zmień ustawienia rejestracji zdarzeń: **Edytuj ustawienia rejestrowania zdarzeń** • Zmień ustawienia powiadomień o zdarzeniach: **Edytuj ustawienia powiadomień o zdarzeniach** • Usuń zdarzenia: **Usuń zdarzenia**	Brak	Brak	Ustawienia: • Maksymalna liczb zdarzeń przechowywanyc w bazie danych • Okres przechowywania zdarzeń z usuniętych urządzeń
Funkcje ogólne: **Operacje na Serwerze administracyjnym**	• **Odczyt** • **Wpisz** • **Wykonaj** • **Modyfikuj listy ACL obiektów** • **Wykonaj operacje na wyborach urządzeń**	• Określ porty Serwera administracyjnego dla połączenia agenta sieciowego: **Wpisz** • Określ porty Serwera proxy aktywacji uruchomionego na serwerze administracyjnym Serwer administracyjny: **Wpisz** • Określ porty serwera proxy aktywacji dla urządzeń przenośnych uruchomionych na Serwerze administracyjnym: **Wpisz** • Określ porty serwera sieciowego do dystrybucji samodzielnych pakietów: **Wpisz** • Określ porty serwera sieciowego do dystrybucji profili MDM: **Wpisz** • Określ porty SSL Serwera administracyjnego do połączenia przez Web Console: **Wpisz** • Określ porty serwera administracyjnego Serwer administracyjny dla połączenia mobilnego: **Wpisz**	• „Tworzenie kopii zapasowych danych Serwera administracyjnego" • „Konserwacja baz danych"	Brak	Brak

Obszar funkcjonalny	Uprawnienie	Akcja użytkownika: uprawnienia wymagane do wykonania akcji	Zadanie	Raport	Inne
		• Zmienianie maksymalnej liczby zdarzeń przechowywanych w bazie danych Serwera administracyjnego: **Wpisz** • Określ maksymalną liczbę zdarzeń, które mogą być wysłane przez Serwer administracyjny: **Wpisz** • Określ przedział czasu, w którym zdarzenia mogą być wysyłane przez Serwer administracyjny: **Wpisz**			
Funkcje ogólne: **Wdrażanie oprogramowania Kaspersky**	• **Zarządzaj poprawkami Kaspersky** • **Odczyt** • **Wpisz** • **Wykonaj** • **Wykonaj operacje na wyborach urządzeń**	Zaakceptuj lub odrzuć instalację poprawki: **Zarządzaj poprawkami Kaspersky**	Brak	• „Raport użycia klucza licencyjnego przez wirtualny Serwer administracyjny" • „Raport o wersjach oprogramowania Kaspersky" • „Raport o niekompatybilnych aplikacjach" • „Raport o wersjach aktualizacji modułu oprogramowania Kaspersky" • „Raport wdrażania ochrony"	Pakiet instalacyjny „Kaspersky"
Cechy ogólne: **Zarządzanie kluczami**	• **Eksportuj plik klucza** • **Wpisz**	• Eksportuj plik klucza: **Eksportuj plik klucza** • Zmodyfikuj ustawienia klucza licencyjnego Serwera administracyjnego: **Wpisz**	Brak	Brak	Brak
Funkcje ogólne: **Wymuszone zarządzanie raportami**	• **Odczyt** • **Wpisz**	• Twórz raporty niezależnie od ich list ACL: **Zapisz** • Wykonywanie raportów niezależnie od ich list ACL: **Odczytaj**	Brak	Brak	Brak
Funkcje ogólne: **Hierarchia serwerów administracyjnych**	**Skonfiguruj hierarchię Serwerów administracyjnych**	• Zarejestruj, zaktualizuj lub usuń podrzędne Serwery administracyjne: **Skonfiguruj hierarchię Serwerów administracyjnych**	Brak	Brak	Brak
Cechy ogólne: **Uprawnienia użytkownika**	**Modyfikuj listy ACL obiektów**	• Zmień właściwości Zabezpieczenia dowolnego obiektu: **Modyfikuj**	Brak	Brak	Brak

Obszar funkcjonalny	Uprawnienie	Akcja użytkownika: uprawnienia wymagane do wykonania akcji	Zadanie	Raport	Inne
		listy ACL obiektów • Zarządzaj rolami użytkowników: **Modyfikuj listy ACL obiektów** • Zarządzaj użytkownikami wewnętrznymi: **Modyfikuj listy ACL obiektów** • Zarządzaj grupami zabezpieczeń: **Modyfikuj listy ACL obiektów** • Zarządzaj aliasami: **Modyfikuj listy ACL obiektów**			
Funkcje ogólne: **Wirtualne serwery administracyjne**	• **Zarządzaj wirtualnym serwerem administracyjnym Serwery administracyjne** • **Odczyt** • **Wpisz** • **Wykonaj** • **Wykonaj operacje na wyborach urządzeń**	• Pobierz listę wirtualnych serwerów administracyjnych Serwery administracyjne: **Odczytaj** • Uzyskaj informacje na temat wirtualnego Serwera administracyjnego: **Odczytaj** • Utwórz, zaktualizuj lub usuń wirtualny Serwer administracyjny: **Zarządzaj wirtualnymi serwerami administracyjnymi** • Przenieś wirtualny Serwer administracyjny do innej grupy: **Zarządzaj wirtualnymi serwerami administracyjnymi** • Ustaw uprawnienia do administracyjnego Serwera wirtualnego: **Zarządzaj wirtualnymi serwerami administracyjnymi**	Brak	Brak	Brak

Obszar funkcjonalny	Uprawnienie	Akcja użytkownika: uprawnienia wymagane do wykonania akcji	Zadanie	Raport	Inne
Funkcje ogólne: **Zarządzanie kluczami szyfrowania**	**Wpisz**	Zaimportuj klucze szyfrowania: **Wpisz**	Brak	Brak	Brak
Zarządzanie urządzeniami mobilnymi: **Ogólne**	• **Podłączanie nowych urządzeń** • **Wysyłaj tylko polecenia informacyjne na urządzenia mobilne** • **Wysyłanie poleceń na urządzenia mobilne** • **Zarządzaj certyfikatami** • **Odczyt** • **Wpisz**	• Uzyskaj dane przywracania Usługi zarządzania kluczami: **Odczytaj** • Usuń certyfikaty użytkownika: **Zarządzaj certyfikatami** • Uzyskaj część publiczną certyfikatu użytkownika: **Odczytaj** • Sprawdź, czy infrastruktura klucza publicznego jest włączona: **Odczytaj** • Sprawdź konto infrastruktury klucza publicznego: **Odczytaj** • Uzyskaj szablony infrastruktury klucza publicznego: **Odczytaj** • Uzyskaj szablony infrastruktury klucza publicznego za pomocą certyfikatu rozszerzonego użycia klucza: **Odczytaj** • Sprawdź, czy certyfikat infrastruktury klucza publicznego został odwołany: **Odczytaj** • Zaktualizuj ustawienia wydawania certyfikatów użytkownika: **Zarządzaj certyfikatami** • Uzyskaj ustawienia wydawania certyfikatu użytkownika: **Odczytaj** • Pobierz pakiety według nazwy i wersji aplikacji: **Odczytaj** • Ustaw lub anuluj certyfikat użytkownika: **Zarządzaj certyfikatami** • Odnów certyfikat użytkownika: **Zarządzaj certyfikatami**	Brak	Brak	Brak

Obszar funkcjonalny	Uprawnienie	Akcja użytkownika: uprawnienia wymagane do wykonania akcji	Zadanie	Raport	Inne
		• Ustaw tag certyfikatu użytkownika: **Zarządzaj certyfikatami** • Uruchom generację pakietu instalacyjnego MDM; anuluj generowanie pakietu instalacyjnego MDM: **Podłącz nowe urządzenia**			
Zarządzanie systemem: **Łączność**	• **Rozpocznij sesje RDP** • **Połącz się z istniejącymi sesjami RDP** • **Rozpocznij tunelowanie** • **Zapisz pliki z urządzeń na stacji roboczej administratora** • **Odczyt** • **Wpisz** • **Wykonaj** • **Wykonaj operacje na wyborach urządzeń**	• Utwórz sesję udostępniania pulpitu: **Prawo do tworzenia sesji udostępniania pulpitu** • Utwórz sesję RDP: **Połącz się z istniejącymi sesjami RDP** • Utwórz tunel: **Zainicjuj tunelowanie** • Zapisz listę sieci partnerskiej: **Zapisz pliki z urządzeń na stacji roboczej administratora**	Brak	„Raport o użytkownikach urządzenia”	Brak
Zarządzanie systemem: **zarządzanie lukami i poprawkami**	• **Odczyt** • **Wpisz** • **Wykonaj** • **Wykonaj operacje na wyborach urządzeń**	• Wyświetl właściwości poprawki trzeciej firmy: **Odczytaj** • Zmień właściwości poprawki trzeciej firmy: **Wpisz**	• „Napraw luki” • „Zainstaluj wymagane aktualizacje i napraw luki”	„Raport o aktualizacjach oprogramowania”	Brak
Zarządzanie systemem: **Zdalne wykonywanie skryptów**	• **Odczyt** • **Wpisz** • **Wykonaj** • **Wykonaj operacje na wyborach urządzeń**	Użytkownik może przeglądać właściwości zadania: **Odczyt** Użytkownik może utworzyć, usunąć lub zmodyfikować pakiet instalacyjny: **Zapis** Użytkownik może uruchomić zadanie: **Wpisz**. Na urządzeniach klienckich z systemem Linux skrypty są wykonywane z uprawnieniami roota. Użytkownik może uruchomić zadanie lub zaplanować jego uruchomienie: **Wykonanie**	„Zdalne wykonywanie skryptów”	Brak	Brak

Obszar funkcjonalny	Uprawnienie	Akcja użytkownika: uprawnienia wymagane do wykonania akcji	Zadanie	Raport	Inne
		Użytkownik może uruchomić zadanie na wybranych urządzeniach: **Wykonaj operacje na wybranych urządzeniach**			

Informacje o rolach użytkowników

Role użytkowników przypisane do użytkowników Kaspersky Security Center Linux zapewniają im zestawy praw dostępu do funkcji aplikacji.

Użytkownikom utworzonym na Serwerze wirtualnym nie można przypisać roli na Serwerze administracyjnym.

Możesz użyć predefiniowanych ról użytkownika z już skonfigurowanym zestawem uprawnień lub utworzyć nowe role. W takim przypadku należy samodzielnie ustawić zakres roli i przypisać uprawnienia dostępu do funkcji Kaspersky Security Center Linux. Niektóre predefiniowane role użytkownika dostępne w Kaspersky Security Center Linux mogą być powiązane z określonymi stanowiskami pracy, na przykład **Audytor**, **Pracownik ochrony**, **Nadzorca**. Prawa dostępu do tych ról są wstępnie skonfigurowane zgodnie ze standardowymi zadaniami i zakresem obowiązków powiązanych stanowisk. Poniższa tabela pokazuje jak role mogą zostać powiązane z określonymi stanowiskami pracy:

Przykłady ról dla określonych stanowisk pracy

Rola	Komentarz
Audytor	Zezwala na wszystkie operacje przeglądania i wykonywania wszelkich utworzonych zadań na wybranych urządzeniach podłączonych do Serwera administracyjnego za pośrednictwem Agenta sieciowego z uprawnieniami administratora lokalnego (root w przypadku Linux). Zalecamy ostrożne przyznawanie tych praw ograniczonej grupie użytkowników, którzy potrzebują ich do wykonywania swoich obowiązków służbowych.
Opiekun	Zezwala na wszystkie działania przeglądania, ale nie zezwala na pozostałe działania. Możesz przypisać tę rolę do specjalisty ds. zabezpieczeń i innych menadżerów zarządzających bezpieczeństwem IT w Twojej firmie.
Specjalista ds. zabezpieczeń	Zezwala na wszystkie działania przeglądania, zezwala na zarządzanie raportami; przydziela ograniczone uprawnienia w obszarze **Zarządzanie systemami**: **Łączność**. Możesz przypisać tę rolę do specjalisty zarządzającego bezpieczeństwem IT w Twojej firmie.

Poniższa tabela przedstawia prawa dostępu przypisane do każdej predefiniowanej roli użytkownika.

Prawa dostępu do predefiniowanych ról użytkowników

Rola	Opis

Administrator serwera administracyjnego	Zezwala na wszystkie operacje w następujących obszarach funkcjonalnych:
	• **Funkcje ogólne**:
	  • **Podstawowa funkcjonalność**
	  • **Zarządzanie kluczami szyfrowania**
	  • **Przetwarzanie zdarzeń**
	  • **Hierarchia Serwerów administracyjnych**
	  • **Wirtualne Serwery administracyjne**
	• **Zarządzanie poprawkami i lukami**:
	  • **Łączność**
	  • **Inwentaryzacja sprzętu**
	  • **Inwentaryzacja oprogramowania**

Operator serwera administracyjnego	Przyznaje prawa **odczytu** i **wykonywania** (w stosownych przypadkach) we wszystkich następujących obszarach funkcjonalnych:
	• **Funkcje ogólne**:
	  • **Podstawowa funkcjonalność**
	  • **Zarządzanie kluczami szyfrowania**
	  • **Wirtualne Serwery administracyjne**
	• **Zarządzanie poprawkami i lukami**:
	  • **Łączność**
	  • **Inwentaryzacja sprzętu**
	  • **Inwentaryzacja oprogramowania**

Audytor	Zezwala na następujące operacje w obszarach funkcjonalnych, w **Cechach ogólnych**: • **Uzyskuj dostęp do obiektów bez względu na ich listy ACL** • **Usunięte obiekty** • **Wymuszone zarządzanie raportami** Tę rolę można przypisać do osoby, która przeprowadza audyt w Twojej organizacji.

Administrator instalacji	Zezwala na wszystkie operacje w następujących obszarach funkcjonalnych:
	• **Funkcje ogólne:**
	  • **Podstawowa funkcjonalność**
	  • **Wdrażanie aplikacji Kaspersky**
	  • **Zarządzanie kluczami licencyjnymi**
	• **Zarządzanie systemem:**
	  • **Wdrażanie systemu operacyjnego**
	  • **Zarządzanie lukami i poprawkami**
	  • **Instalacja zdalna**
	  • **Inwentaryzacja oprogramowania**
	Przyznaje uprawnienia do **odczytu** i **wykonywania** w obszarze funkcjonalnym **Funkcje ogólne: Wirtualne serwery administracyjne**.

Rola	Opis

Operator instalacji	Przyznaje prawa **odczytu** i **wykonywania** (w stosownych przypadkach) we wszystkich następujących obszarach funkcjonalnych:
	• **Funkcje ogólne:**
	  • **Podstawowa funkcjonalność**
	  • **Wdrażanie aplikacji Kaspersky** (przyznaje również prawa do **Zarządzania poprawkami Kaspersky** bezpośrednio w tym obszarze)
	  • **Wirtualne Serwery administracyjne**
	• **Zarządzanie systemem:**
	  • **Wdrażanie systemu operacyjnego**
	  • **Zarządzanie lukami i poprawkami**
	  • **Instalacja zdalna**
	  • **Inwentaryzacja oprogramowania**

Administrator Kaspersky Endpoint Security	Zezwala na wszystkie operacje w następujących obszarach funkcjonalnych: • **Cechy ogólne: Podstawowa funkcjonalność** • **Funkcje ogólne: Zarządzanie kluczami szyfrowania** • Obszar **Kaspersky Endpoint Security** zawierający wszystkie funkcje
Operator Kaspersky Endpoint Security	Przyznaje prawa **odczytu** i **wykonywania** (w stosownych przypadkach) we wszystkich następujących obszarach funkcjonalnych: • **Cechy ogólne: Podstawowa funkcjonalność** • **Funkcje ogólne: Zarządzanie kluczami szyfrowania** • Obszar **Kaspersky Endpoint Security** zawierający wszystkie funkcje
Główny administrator	Zezwala na wszystkie operacje w obszarach funkcjonalnych, z *wyjątkiem* następujących obszarów w **Cechach ogólnych**: • **Uzyskuj dostęp do obiektów bez względu na ich listy ACL** • **Wymuszone zarządzanie raportami**

Główny operator	Przyznaje prawa **odczytu** i **wykonywania** (w stosownych przypadkach) we wszystkich następujących obszarach funkcjonalnych:
	• **Funkcje ogólne**:
	  • **Podstawowa funkcjonalność**
	  • **Usunięte obiekty**
	  • **Zarządzanie kluczami szyfrowania**
	  • **Operacje na Serwerze administracyjnym**
	  • **Znaczniki urządzeń**
	  • **Wdrażanie aplikacji Kaspersky**
	  • **Integracja aplikacji**
	  • **Wirtualne Serwery administracyjne**
	• Obszar **Zarządzanie urządzeniami mobilnymi** zawierający wszystkie funkcje
	• Obszar **Zarządzanie systemem** zawierający wszystkie funkcje
	• Obszar **Kaspersky Endpoint Security** zawierający wszystkie funkcje

Administrator zarządzania urządzeniami mobilnymi	Zezwala na wszystkie operacje w następujących obszarach funkcjonalnych: • **Cechy ogólne: Podstawowa funkcjonalność** • Obszar **Zarządzanie urządzeniami mobilnymi** zawierający wszystkie funkcje Przyznaje prawa **Eksportowania pliku klucza** w **Funkcje ogólne: Zarządzanie kluczami licencyjnymi**. Przyznaje prawa **odczytu** w **Zarządzanie systemem: Zarządzanie lukami i poprawkami**.
Operator zarządzania urządzeniami mobilnymi	Przyznaje prawa **odczytu** i **wykonywania** w **Funkcje ogólne: Podstawowa funkcjonalność**. Przyznaje prawa **odczytu** i **wysyłania tylko poleceń informacyjnych na urządzenia mobilne** w **Zarządzanie urządzeniami mobilnymi**: • **Ogólne** • **Portal Self Service Portal**

Rola	Opis
Specjalista ds. zabezpieczeń	Zezwala na następujące operacje w obszarach funkcjonalnych, w **Cechach ogólnych**: • **Uzyskuj dostęp do obiektów bez względu na ich listy ACL** • **Wymuszone zarządzanie raportami** Przyznaje następujące uprawnienia w obszarze funkcjonalnym **Zarządzanie systemem: Łączność**: **Odczyt**, **Zapis**, **Wykonywanie**, **Zapisywanie plików z urządzeń na stacji roboczej administratora** oraz **Wykonywanie operacji na wybranych urządzeniach**. Możesz przypisać tę rolę do specjalisty zarządzającego bezpieczeństwem IT w Twojej firmie.
Użytkownik portalu Self Service Portal	Zezwala na wszystkie operacje w obszarze funkcjonalnym **Zarządzanie urządzeniami mobilnymi: Self Service Portal**.
Opiekun	Przyznaje prawo do **Odczytu** w obszarach funkcjonalnych **Funkcje ogólne**: **Dostęp do obiektów, niezależnie od ich list ACL** i **Funkcje ogólne**: **Wymuszone zarządzanie raportami**. Możesz przypisać tę rolę do specjalisty ds. zabezpieczeń i innych menadżerów zarządzających bezpieczeństwem IT w Twojej firmie.
Administrator zarządzania lukami i poprawkami	Zezwala na wszystkie operacje w obszarach funkcjonalnych **Funkcje ogólne**: **Podstawowa funkcjonalność** i **Zarządzanie systemem** (w tym wszystkie funkcje, *za wyjątkiem* funkcji **Zdalne wykonywanie skryptu**).
Operator zarządzania lukami i poprawkami	Przyznaje prawa **odczytu** i **wykonywania** (w stosownych przypadkach) w obszarach funkcjonalnych **Funkcje ogólne**: **Podstawowa funkcjonalność** i **Zarządzanie systemem** (w tym wszystkie funkcje, *za wyjątkiem* funkcji **Zdalne wykonywanie skryptu**).

Nadawanie praw dostępu do określonych obiektów

Oprócz nadawania praw dostępu na poziomie serwera, możesz skonfigurować dostęp do konkretnych obiektów, np. do konkretnego zadania. Aplikacja umożliwia określenie praw dostępu do następujących typów obiektów:

- Grupy administracyjne
- Zadania
- Raporty
- Wybory urządzeń
- Wybory zdarzeń

Aby przypisać prawa dostępu do określonego obiektu:

1. W zależności od typu obiektu, w menu głównym przejdź do odpowiedniej sekcji:
   - **Zarządzanie zasobami** → **Hierarchia grup**
   - **Zadania**
   - **Monitorowanie** → **Raporty**
   - **Zarządzanie zasobami** → **Wybory urządzeń**
   - **Monitorowanie** → **Wybory zdarzeń**
2. Otwórz właściwości obiektu, do którego chcesz skonfigurować prawa dostępu.

   Aby otworzyć okno właściwości grupy administracyjnej lub zadania, kliknij nazwę obiektu. Właściwości innych obiektów można otworzyć za pomocą przycisku na pasku narzędzi.

3. W oknie właściwości otwórz sekcję **Prawa dostępu**.

   Zostanie otwarta lista użytkowników. Wymienieni użytkownicy i podane grupy zabezpieczeń mają prawa dostępu do obiektu. Domyślnie, jeśli używasz hierarchii grup administracyjnych lub Serwerów, lista i prawa dostępu są dziedziczone z nadrzędnej grupy administracyjnej lub Serwera podstawowego.

4. Aby móc modyfikować listę, włącz opcję **Użyj uprawnień niestandardowych**.

5. Skonfiguruj prawa dostępu:

   - Użyj przycisków **Dodaj** i **Usuń**, aby zmodyfikować listę.

   - Określ prawa dostępu dla użytkownika lub grupy zabezpieczeń. Wykonaj jedną z poniższych czynności:

     - Jeśli chcesz ręcznie określić prawa dostępu, wybierz użytkownika lub grupę zabezpieczeń, kliknij przycisk **Prawa dostępu**, a następnie określ prawa dostępu.

     - Jeśli chcesz przypisać rolę użytkownika do użytkownika lub grupy zabezpieczeń, wybierz użytkownika lub grupę zabezpieczeń, kliknij przycisk **Role**, a następnie wybierz rolę do przypisania.

6. Kliknij przycisk **Zapisz**.

Prawa dostępu do obiektu zostały skonfigurowane.

Przydzielanie praw dostępu użytkownikom i grupom bezpieczeństwa

Użytkownikom i grupom bezpieczeństwa można przyznać prawa dostępu do różnych funkcji Serwera administracyjnego, na przykład Kaspersky Endpoint Security for Linux.

Aby przypisać prawa dostępu do użytkownika lub grupy bezpieczeństwa:

1. W menu głównym kliknij nazwę Serwera administracyjnego.

   Zostanie otwarte okno właściwości Serwera administracyjnego.

2. Na zakładce **Prawa dostępu** zaznacz pole wyboru obok nazwy użytkownika lub grupy bezpieczeństwa, której chcesz przypisać prawa, a następnie kliknij przycisk **Prawa dostępu**.

   Nie można jednocześnie wybrać wielu użytkowników lub grup bezpieczeństwa. Jeśli wybierzesz więcej niż jeden element, przycisk **Prawa dostępu** będzie nieaktywny.

3. Skonfiguruj zestaw uprawnień dla użytkownika lub grupy:

   a. Rozwiń węzeł o funkcje Serwera administracyjnego lub innej aplikacji Kaspersky.

   b. Zaznacz pole wyboru **Zezwól** lub **Odmów** obok żądanej funkcji lub uprawnienia dostępu.

      Przykład 1: Zaznacz pole wyboru **Zezwól** obok węzła **Integracja aplikacji**, aby przyznać użytkownikowi lub grupie wszystkie dostępne uprawnienia dostępu do funkcji Integracja aplikacji (**Odczyt**, **Zapis** i **Wykonanie**).

Przykład 2: Rozwiń węzeł **Zarządzanie kluczami szyfrowania**, a następnie zaznacz pole wyboru **Zezwalaj** obok uprawnienia **Zapis**, aby przyznać użytkownikowi lub grupie uprawnienia dostępu **Zapis** do funkcji zarządzania kluczami szyfrowania.

4. Po skonfigurowaniu zestawu uprawnień dostępu kliknij przycisk **OK**.

Zestaw uprawnień dla użytkownika lub grupy użytkowników zostanie skonfigurowany.

Uprawnienia Serwera administracyjnego (lub grupy administracyjnej) są podzielone na następujące obszary:

- Funkcje ogólne:
  - Zarządzanie grupami administracyjnymi
  - Uzyskuj dostęp do obiektów bez względu na ich listy ACL
  - Podstawowa funkcjonalność
  - Usunięte obiekty
  - Zarządzanie kluczem szyfrowania
  - Przetwarzanie zdarzeń
  - Operacje na Serwerze administracyjnym (tylko w oknie właściwości Serwera administracyjnego)
  - Znaczniki urządzenia
  - Wdrażanie aplikacji Kaspersky
  - Zarządzanie kluczami licencyjnymi
  - Integracja aplikacji
  - Wymuszone zarządzanie raportami
  - Hierarchia Serwerów administracyjnych
  - Uprawnienia użytkownika
  - Wirtualne Serwery administracyjne
- Zarządzanie urządzeniami mobilnymi:
  - Ogólne
  - Self Service Portal
- Zarządzanie systemami:
  - Łączność
  - Zdalne wykonanie skryptu
  - Inwentarz sprzętu

- Network Access Control
- Wdrażanie systemu operacyjnego
- Zarządzanie lukami i poprawkami
- Zdalna instalacja
- Inwentaryzacja oprogramowania

Jeśli dla uprawnienia dostępu nie wybrano opcji **Zezwól** ani **Odmów**, wówczas uprawnienie dostępu jest uznawane za *niezdefiniowane*: zostaje odrzucone, dopóki wyraźnie nie zostanie dozwolone lub odrzucone dla użytkownika.

Uprawnienia użytkownika są sumą:

- Własnych uprawnień użytkownika
- Uprawnień wszystkich ról przypisanych do tego użytkownika
- Uprawnień wszystkich grup bezpieczeństwa, do których należy użytkownik
- Uprawnień wszystkich ról przypisanych do grupy bezpieczeństwa, do których należy użytkownik

Jeśli przynajmniej jeden z tych zestawów uprawnień posiada opcję **Odmów** dla uprawnienia, wówczas dla użytkownika zostaje zabronione to uprawnienie nawet wtedy, gdy inne zestawy zezwalają na nie lub pozostawiają je niezdefiniowane.

Można również dodać użytkowników i grupy zabezpieczeń do obszaru roli użytkownika, aby korzystać z różnych funkcji Serwera administracyjnego. Ustawienia skojarzone z rolą użytkownika są stosowane tylko do urządzeń, które należą do użytkowników posiadających tę rolę i tylko wtedy, gdy te urządzenia należą do grup skojarzonych z tą rolą, w tym grup podrzędnych.

Dodawanie konta użytkownika wewnętrznego

Jeśli chcesz dodać konto użytkownika, upewnij się, że Twoje konto ma uprawnienie Modyfikuj listy ACL obiektów w obszarze funkcjonalnym Funkcje ogólne: Uprawnienia użytkownika.

W celu dodania nowego konta użytkownika wewnętrznego do Kaspersky Security Center Linux:

1. W menu głównym przejdź do opcji **Użytkownicy i role** → **Użytkownicy i grupy**, a następnie wybierz zakładkę **Użytkownicy**.
2. Kliknij **Dodaj**.
3. W otwartym oknie **Dodaj użytkownika** określ ustawienia nowego konta użytkownika:
   - **Nazwa**.
   - **Hasło** dla połączenia użytkownika z Kaspersky Security Center Linux.

Hasło musi być zgodne z następującymi regułami:

- Hasło musi zawierać od 8 do 256 znaków.
- Hasło musi zawierać znaki z przynajmniej trzech z poniższych grup:
  - Wielkie litery (A-Z)
  - Małe litery (a-z)
  - Cyfry (0-9)
  - Znaki specjalne (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)
- Hasło nie może zawierać spacji, znaków Unicode lub kombinacji znaków "." i "@", gdy "." jest umieszczane przed "@".

Aby zobaczyć wprowadzone hasło kliknij 👁.

Możesz włączyć opcję **Użytkownik musi zmienić hasło przy pierwszym logowaniu** aby wymusić zmianę hasła przy pierwszym uwierzytelnieniu użytkownika.

4. Zapisz zmiany, aby dokończyć tworzenie nowego konta użytkownika.

Nowe konto użytkownika zostanie dodane do listy użytkowników.

Aby zalogować się przy użyciu utworzonego wewnętrznego konta użytkownika w Kaspersky Security Center Web Console, należy przypisać rolę do konta. Przed zalogowaniem upewnij się, że domena lub konto użytkownika wewnętrznego mają przypisaną rolę. W przeciwnym razie wystąpi błąd logowania.

Tworzenie grupy bezpieczeństwa

W celu utworzenia grupy bezpieczeństwa:

1. W menu głównym przejdź do opcji **Użytkownicy i role** → **Użytkownicy i grupy**, a następnie wybierz kartę **Grupy**.
2. Kliknij **Dodaj**.
3. W otwartym oknie **Utwórz grupę bezpieczeństwa** określ następujące ustawienia dla nowej grupy bezpieczeństwa:
   - **Nazwa grupy**
   - **Opis**
4. Kliknij **Zapisz**, aby zachować zmiany.

Nowa grupa bezpieczeństwa zostanie dodana do listy grup.

Edytowanie konta użytkownika wewnętrznego

Jeśli chcesz edytować konto użytkownika, upewnij się, że Twoje konto ma uprawnienie Modyfikuj listy ACL obiektów w obszarze funkcjonalnym Funkcje ogólne: Uprawnienia użytkownika.

W celu edytowania konta użytkownika wewnętrznego w Kaspersky Security Center Linux:

1. W menu głównym przejdź do opcji **Użytkownicy i role** → **Użytkownicy i grupy**, a następnie wybierz zakładkę **Użytkownicy**.

2. Kliknij nazwę konta użytkowników, które chcesz edytować.

3. W otwartym oknie ustawień użytkownika, na zakładce **Ogólne** zmień ustawienia konta użytkownika:

   - **Konto użytkownika**

     Jeśli to konieczne, przesuń przełącznik na **Nieaktywny**, aby zabronić użytkownikowi możliwość łączenia z aplikacją. Możesz wyłączyć konto, na przykład, gdy pracownik opuści teren firmy.

   - Opis

   - **Pełna nazwa**

   - **Adres e-mail**

   - **Główny numer telefonu**

   - **Hasło**

     W razie potrzeby możesz ustawić nowe hasło dla połączenia użytkownika z Kaspersky Security Center Linux w następujący sposób:

     a. Kliknij przycisk **Zmień hasło**, a następnie ustaw nowe hasło dla konta użytkownika.

     Hasło musi być zgodne z następującymi regułami:

     - Hasło musi zawierać od 8 do 256 znaków.

     - Hasło musi zawierać znaki z przynajmniej trzech z poniższych grup:

       - Wielkie litery (A-Z)

       - Małe litery (a-z)

       - Cyfry (0-9)

       - Znaki specjalne (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)

     - Hasło nie może zawierać spacji, znaków Unicode lub kombinacji znaków "." i "@", gdy "." jest umieszczane przed "@".

     Aby zobaczyć wprowadzone hasło kliknij 👁.

b. W razie potrzeby włącz opcję **Użytkownik musi zmienić hasło przy pierwszym logowaniu** aby wymusić zmianę hasła przy kolejnym uwierzytelnieniu użytkownika.

c. Jeśli konto użytkownika jest chronione przed nieautoryzowaną modyfikacją, musisz potwierdzić, że masz uprawnienia do wprowadzania zmian na tym koncie. W oknie **Ochrona konta** określ dane uwierzytelniające konta, które ma uprawnienie Modyfikuj listy ACL obiektów w obszarze funkcjonalnym Funkcje ogólne: Uprawnienia użytkownika.

4. Na zakładce **Uwierzytelnianie dwuskładnikowe** możesz określić ustawienia zabezpieczeń dla tego konta.

5. Na zakładce **Grupy** możesz dodać użytkownika do grup zabezpieczeń.

6. Na zakładce **Urządzenia** możesz przypisać urządzenia do użytkownika.

7. Na zakładce **Role** możesz przypisać role do użytkownika.

8. Zapisz zmiany, aby zakończyć edycję konta użytkownika.

Zaktualizowane konto użytkownika pojawi się na liście użytkowników.

Edytowanie grupy bezpieczeństwa

W celu edytowania grupy bezpieczeństwa:

1. W menu głównym przejdź do opcji **Użytkownicy i role** → **Użytkownicy i grupy**, a następnie wybierz kartę **Grupy**.

2. Kliknij nazwę grupy bezpieczeństwa, którą chcesz edytować.

3. W otwartym oknie ustawień grupy zmień ustawienia grupy bezpieczeństwa:

   - Na zakładce **Ogólne** możesz zmienić ustawienia **Nazwa** i **Opis**. Te ustawienia są dostępne tylko dla wewnętrznych grup bezpieczeństwa.

   - Na zakładce **Użytkownicy** możesz dodać użytkownika do grup zabezpieczeń. To ustawienie jest dostępne tylko dla użytkowników wewnętrznych i wewnętrznych grup bezpieczeństwa.

   - Na zakładce **Role** możesz przypisać rolę do grupy bezpieczeństwa.

4. Kliknij **Zapisz**, aby zachować zmiany.

Zmiany zostaną zastosowane do grupy bezpieczeństwa.

Przypisywanie roli do użytkownika lub grupy bezpieczeństwa

Aby przypisać rolę do użytkownika lub grupy bezpieczeństwa:

1. W menu głównym przejdź do opcji **Użytkownicy i role** → **Użytkownicy i grupy**, a następnie wybierz kartę **Użytkownicy** lub **Grupy**.

2. Wybierz nazwę użytkownika lub grupy bezpieczeństwa, do których chcesz przypisać rolę.

   Można wybrać kilka nazw.

3. W wierszu menu kliknij przycisk **Przypisz rolę**.

   Zostanie uruchomiony Kreator przypisywania roli.

4. Postępuj zgodnie z instrukcjami kreatora: wybierz rolę, którą chcesz przypisać wybranym użytkownikom lub grupom bezpieczeństwa, a następnie wybierz zakres roli.

   Obszar roli użytkownika to połączenie użytkowników i grup administracyjnych. Ustawienia skojarzone z rolą użytkownika są stosowane tylko do urządzeń, które należą do użytkowników posiadających tę rolę i tylko wtedy, gdy te urządzenia należą do grup skojarzonych z tą rolą, w tym grup podrzędnych.

Rola z zestawem uprawnień do pracy z Serwerem administracyjnym zostanie przypisana do użytkownika (lub użytkowników lub grupy bezpieczeństwa). Na liście użytkowników lub grup bezpieczeństwa w kolumnie **Ma przypisane role** pojawia się pole wyboru.

Dodawanie kont użytkowników do wewnętrznej grupy bezpieczeństwa

Do wewnętrznej grupy bezpieczeństwa możesz dodać tylko konta użytkowników wewnętrznych.

W celu dodania kont użytkowników do wewnętrznej grupy bezpieczeństwa:

1. W menu głównym przejdź do opcji **Użytkownicy i role** → **Użytkownicy i grupy**, a następnie wybierz zakładkę **Użytkownicy**.

2. Zaznacz pola obok kont użytkowników, które chcesz dodać do grupy bezpieczeństwa.

3. Kliknij przycisk **Przypisz grupę**.

4. W oknie **Przypisz grupę**, które zostanie otwarte, wybierz grupę, do której chcesz dodać konta użytkowników.

5. Kliknij przycisk **Zapisz**.

Konta użytkowników zostaną dodane do grupy bezpieczeństwa. Możesz także dodać użytkowników wewnętrznych do grupy bezpieczeństwa, korzystając z ustawień grupy.

Wskazywanie użytkownika jako właściciela urządzenia

Aby uzyskać informacje na temat przypisywania użytkownika jako właściciela urządzenia mobilnego, zobacz pomoc dla Kaspersky Secure Mobility Management.

W celu wskazania użytkownika jako właściciela urządzenia:

1. Jeżeli chcesz przypisać właściciela urządzenia podłączonego do wirtualnego Serwera administracyjnego, najpierw przełącz się na wirtualny Serwer administracyjny:

   a. W menu głównym kliknij ikonę jodełki (▸) po prawej stronie bieżącej nazwy Serwera administracyjnego.

   b. Wybierz wymagany Serwer administracyjny.

2. W menu głównym przejdź do opcji **Użytkownicy i role** → **Użytkownicy i grupy**, a następnie wybierz zakładkę **Użytkownicy**.

   Zostanie otwarta lista użytkowników. Jeśli jesteś aktualnie połączony z wirtualnym Serwerem administracyjnym, lista zawiera użytkowników z bieżącego wirtualnego Serwera administracyjnego oraz głównego Serwera administracyjnego.

3. Kliknij nazwę konta użytkownika, które chcesz przypisać jako właściciel urządzenia.

4. W otwartym oknie ustawień użytkownika kliknij zakładkę **Urządzenia**.

5. Kliknij **Dodaj**.

6. Z listy urządzeń wybierz urządzenie, które chcesz przypisać do użytkownika.

7. Kliknij **OK**.

   Wybrane urządzenie zostanie dodane do listy urządzeń przypisanych do użytkownika.

To samo działanie możesz wykonać w **Zarządzanie zasobami** → **Zasoby (urządzenia)**, klikając nazwę urządzenia, które chcesz przypisać, a następnie klikając odnośnik **Zarządzaj właścicielem urządzenia**.

Przypisywanie użytkownika jako właściciela urządzenia podczas instalacji Agenta sieciowego

Aby przypisać użytkownika, jako właściciela urządzenia podczas instalacji Agenta sieciowego za pośrednictwem pakietu instalacyjnego, dodaj zmienne określone w poniższej tabeli do ustawień pakietu instalacyjnego Agenta sieciowego.

Nazwa zmiennej	Wymagane	Opis	Możliwe wartości
KLNAGENT_DEVICEOWNER_REGISTRATION_START	Nie	Umożliwia uruchomienie narzędzia służącego do rejestracji użytkownika jako właściciela urządzenia po zainstalowaniu Agenta sieciowego. Jeśli opcja jest wyłączona, rejestracja jako właściciela urządzenia nie jest dostępna dla użytkownika.	1 — Narzędzie do rejestracji użytkownika jako właściciela urządzenia uruchomi się po zainstalowaniu Agenta sieciowego. Inne — narzędzie jest niedostępne.
KLNAGENT_DEVICEOWNER_LOGIN	Nie Tak, jeśli wpiszesz hasło	Zawiera login użytkownika, który zostanie zarejestrowany jako właściciel urządzenia.	Login użytkownika określony na liście użytkowników w Kaspersky Security Center Linux.
KLNAGENT_DEVICEOWNER_PASSWORD	Nie Tak, jeśli podasz login	Zawiera zaszyfrowane hasło użytkownika, który zostanie zarejestrowany jako właściciel urządzenia.	Hasło użytkownika.

Agent sieciowy odszyfruje podany login i hasło podczas instalacji Kaspersky Security Center Linux, a użytkownik zostanie zarejestrowany jako właściciel urządzenia.

Możesz także przypisać użytkownika jako właściciela urządzenia podczas instalowania Agenta sieciowego w trybie cichym za pomocą pliku odpowiedzi.

Aby przypisać użytkownika jako właściciela urządzenia podczas instalowania Agenta sieciowego w trybie cichym z plikiem odpowiedzi:

1. Dodaj parametr KLNAGENT_DEVICEOWNER_REGISTRATION_START do pliku odpowiedzi i ustaw go na 1.

   Narzędzie do rejestracji użytkownika jako właściciela urządzenia uruchomi się po zainstalowaniu Agenta sieciowego.

2. Wpisz login i hasło w wierszu poleceń na urządzeniu klienckim.

   Użytkownik zostanie przypisany jako właściciel urządzenia.

Jeśli użytkownik należy do wewnętrznej grupy zabezpieczeń, login musi zawierać nazwę użytkownika.

Jeżeli użytkownik należy do grupy zabezpieczeń Active Directory, login musi zawierać nazwę użytkownika i nazwę domeny.

Aby skorzystać z uwierzytelniania dwuskładnikowego, musisz wprowadzić jednorazowe hasło czasowe (TOTP) z aplikacji.

Przypisywanie użytkownika jako właściciela urządzenia z systemem Linux po instalacji Agenta sieciowego

Aby umożliwić użytkownikowi zarejestrowanie się jako właściciel urządzenia z systemem Linux:

1. W Kaspersky Security Center Web Console przejdź do sekcji **Zarządzanie oprogramowaniem** → **Pakiety instalacyjne**.

   Otworzy się lista pakietów instalacyjnych.

2. Kliknij pakiet instalacyjny Agenta sieciowego.

   Zostanie otwarte okno właściwości pakietu instalacyjnego.

3. W oknie właściwości pakietu instalacyjnego kliknij **Ustawienia** → **Zaawansowane**.

4. W sekcji **Rejestracja użytkownika jako właściciela urządzenia (tylko Linux)** włącz opcję **Zezwól na uruchomienie narzędzia rejestracji użytkownika po instalacji agenta sieciowego** i kliknij **Zapisz**.

Narzędzie do rejestracji użytkownika jako właściciela urządzenia można uruchomić z wiersza poleceń na urządzeniu klienckim.

Aby zarejestrować użytkownika jako właściciela urządzenia z systemem Linux na urządzeniu klienckim:

1. Wykonaj następujące polecenie w wierszu poleceń na urządzeniu klienckim:
   ```
   $ /opt/kaspersky/klnagent64/bin/nagregister -set_owner
   ```

2. Wprowadź login i hasło, jeśli zostanie wyświetlony taki monit.

   Jeśli login i hasło znajdują się w pliku odpowiedzi lub pakiecie instalacyjnym Agenta sieciowego, wykonaj następujące polecenie w wierszu poleceń na urządzeniu klienckim:
   ```
   $ /opt/kaspersky/klnagent64/bin/nagregister -set_owner -unattended
   ```

Jeśli użytkownik należy do wewnętrznej grupy zabezpieczeń, login musi zawierać nazwę użytkownika.

Jeżeli użytkownik należy do grupy zabezpieczeń Active Directory, login musi zawierać nazwę użytkownika i nazwę domeny.

Aby skorzystać z uwierzytelniania dwuskładnikowego, musisz wprowadzić jednorazowe hasło czasowe (TOTP) z aplikacji.

Użytkownik zostanie zarejestrowany jako właściciel urządzenia.

Usuwanie użytkownika jako właściciela urządzenia

Aby usunąć użytkownika jako właściciela urządzenia na urządzeniu klienckim:

1. Na urządzeniu klienckim wykonaj następujące polecenie w wierszu poleceń:
   ```
   $ /opt/kaspersky/klnagent64/bin/nagregister -remove_owner
   ```

2. Wprowadź nazwę użytkownika i hasło.

Jeśli użytkownik należy do wewnętrznej grupy zabezpieczeń, login musi zawierać nazwę użytkownika.

Jeżeli użytkownik należy do grupy zabezpieczeń Active Directory, login musi zawierać nazwę użytkownika i nazwę domeny.

Aby skorzystać z uwierzytelniania dwuskładnikowego, musisz wprowadzić jednorazowe hasło czasowe (TOTP) z aplikacji.

Użytkownik zostanie usunięty jako właściciel urządzenia.

Włączanie ochrony konta przed nieautoryzowaną modyfikacją

Możesz włączyć dodatkową opcję ochrony konta użytkownika przed nieautoryzowaną modyfikacją. Jeżeli opcja jest włączona, modyfikowanie ustawień konta użytkownika wymaga autoryzacji przez użytkownika z uprawnieniami do modyfikacji.

W celu włączenia lub wyłączenia ochrony konta przed nieautoryzowaną modyfikacją:

1. W menu głównym przejdź do opcji **Użytkownicy i role** → **Użytkownicy i grupy**, a następnie wybierz zakładkę **Użytkownicy**.
2. Kliknij nazwę wewnętrznego konta użytkownika, dla którego chcesz określić ochronę konta przed nieautoryzowaną modyfikacją.
3. W otwartym oknie ustawień użytkownika wybierz zakładkę **Uwierzytelnianie dwuskładnikowe**.
4. Na zakładce **Uwierzytelnianie dwuskładnikowe** wybierz opcję **Żądaj uwierzytelnienia w celu weryfikacji uprawnień do modyfikacji kont użytkowników**, jeśli chcesz żądać poświadczeń i jednorazowego kodu zabezpieczającego do uwierzytelniania dwuskładnikowego za każdym razem, gdy ustawienia konta są zmieniane lub modyfikowane. W przeciwnym razie wybierz opcję **Zezwól użytkownikom na modyfikowanie tego konta bez dodatkowego uwierzytelniania**.
5. Zapisz zmiany.

Konfigurowanie uwierzytelniania dwuskładnikowego

Począwszy od wersji 16.1 Serwera administracyjnego uwierzytelnianie dwuskładnikowe jest włączane automatycznie. Globalna opcja wyłączenia uwierzytelniania dwuskładnikowego nie jest obsługiwana. Ten scenariusz przedstawia kroki konfiguracji uwierzytelniania dwuetapowego przy pierwszym logowaniu oraz konfigurację ustawień uwierzytelniania dwuskładnikowego na Serwerze administracyjnym.

Etapy

Konfigurowanie uwierzytelniania dwuskładnikowego przebiega etapami:

1. **Instalacja aplikacji uwierzytelniającej na urządzeniu**

   Można zainstalować dowolną aplikację obsługującą algorytm czasowego hasła jednorazowego (TOTP).

   Dostępne w Rosji:

   - Kaspersky Password Manager for Business (zalecany)
   - Bitrix24 OTP
   - Yandex ID

- Avanpost Authenticator
- Aladdin 2FA
- Rutoken OTP

Dostępne na całym świecie (w tym w Rosji):

- Google Authenticator
- Microsoft Authenticator

Aby sprawdzić, czy Kaspersky Security Center Linux obsługuje aplikację uwierzytelniającą, której chcesz użyć, włącz uwierzytelnianie dwuskładnikowe dla wszystkich użytkowników lub dla określonego użytkownika.

Jeden z kroków sugeruje podanie kodu zabezpieczającego wygenerowanego przez aplikację uwierzytelniającą. Jeśli się powiedzie, Kaspersky Security Center Linux obsługuje wybrany token uwierzytelniający.

> Zdecydowanie nie zalecamy instalowania aplikacji uwierzytelniającej na tym samym urządzeniu, z którego nawiązywane jest połączenie z Serwerem administracyjnym.

2. **Synchronizacja czasu na urządzeniu z aplikacją uwierzytelniającą z czasem urządzenia, na którym zainstalowany jest Serwer administracyjny**

   Upewnij się, że czas na urządzeniu z aplikacją uwierzytelniającą i czas na urządzeniu z Serwerem administracyjnym są zsynchronizowane z czasem UTC. Aby zapewnić większą dokładność, zalecamy korzystanie z tych samych serwerów NTP w całej infrastrukturze. W przeciwnym razie mogą wystąpić błędy podczas konfigurowania uwierzytelniania dwuskładnikowego.

3. **Konfigurowanie uwierzytelniania dwuskładnikowego dla kont użytkowników podczas logowania do Web Console**

   Zaloguj się do Web Console i skonfiguruj uwierzytelnianie dwuskładnikowe.

   Jeśli konfiguracja uwierzytelniania dwuskładnikowego nie jest dla Ciebie dostępna, skontaktuj się z użytkownikiem mającym uprawnienie Modyfikuj listy ACL obiektów w obszarze funkcjonalnym **Funkcje ogólne: Uprawnienia użytkownika** i skonfigurowane uwierzytelnianie dwuskładnikowe, aby dodać swoje konto do listy dozwolonych uwierzytelniania dwuskładnikowego.

4. **Konfigurowanie ustawień uwierzytelniania dwuskładnikowego na Serwerze administracyjnym**

   Jeśli skonfigurowano uwierzytelnianie dwuskładnikowe oraz opcję Modyfikuj listy ACL obiektów po prawej stronie obszaru funkcjonalnego **Funkcje ogólne**: **Uprawnienia użytkownika**, możesz skonfigurować ustawienia uwierzytelniania dwuskładnikowego na Serwerze administracyjnym w następujący sposób:

   1. Przeglądanie listy użytkowników, którzy mogą konfigurować uwierzytelnianie dwuskładnikowe podczas logowania:

      - Aby zainstalować serwer administracyjny 16.1 od podstaw: Dodaj wymaganych użytkowników do listy dozwolonych użytkowników uwierzytelniania dwuskładnikowego, aby umożliwić im skonfigurowanie uwierzytelniania dwuskładnikowego podczas pierwszego logowania.
      - Aby zaktualizować lub przywrócić Serwer administracyjny 16.1: Przejrzyj listę dozwolonych kont uwierzytelniania dwuskładnikowego i usuń konta, które nie mogą mieć dostępu do Serwera administracyjnego.

2. Wykluczenie kont użytkowników, dla których nie musisz włączać uwierzytelniania dwuskładnikowego (opcjonalne)

   W razie potrzeby wyklucz konta użytkowników z weryfikacji dwuetapowej, aby umożliwić im logowanie się do Serwera administracyjnego, nawet jeśli nie skonfigurowali uwierzytelniania dwuskładnikowego. Wykluczenie kont z uwierzytelniania dwuskładnikowego może być konieczne w przypadku kont integracji, które nie mogą przekazać kodu zabezpieczającego podczas uwierzytelniania. Konta integracji służą do uruchamiania skryptów za pośrednictwem OpenAPI.

3. Resetowanie lub usuwanie klucza tajnego uwierzytelniania dwuskładnikowego (opcjonalne)

   Klucz tajny uwierzytelniania dwuskładnikowego można zresetować, gdy użytkownik utraci dostęp do swojego urządzenia do uwierzytelniania dwuskładnikowego lub gdy konieczne jest skonfigurowanie uwierzytelniania dwuskładnikowego na nowym urządzeniu. Można również zresetować klucz tajny dla własnego konta.

   Można usunąć klucz tajny, aby całkowicie zablokować użytkownikowi możliwość logowania się do Web Console i uniemożliwić mu dostęp do Serwera administracyjnego.

4. Edytowanie nazwy wystawcy kodu zabezpieczającego (opcjonalne)

   Jeśli masz kilka Serwerów administracyjnych o podobnych nazwach, konieczna może być zmiana nazw wystawców kodów zabezpieczających w celu lepszego rozpoznawania różnych Serwerów administracyjnych.

Wyniki

Po zakończeniu tego scenariusza:

- Uwierzytelnianie dwuskładnikowe jest skonfigurowane dla Twojego konta oraz dla konta innego użytkownika, który potrzebuje dostępu do Serwera administracyjnego.
- Wybrane konta integracji są wykluczone z uwierzytelniania dwuskładnikowego.

Informacje o uwierzytelnianiu dwuskładnikowym konta

Kaspersky Security Center Linux zapewnia uwierzytelnianie dwuskładnikowe dla użytkowników Kaspersky Security Center Web Console. Uwierzytelnianie dwuskładnikowe opiera się na standardzie RFC 6238 (TOTP: Algorytm czasowego hasła jednorazowego).

Za każdym razem, gdy logujesz się do Kaspersky Security Center Web Console, wprowadzasz swoją nazwę użytkownika, hasło i dodatkowy jednorazowy kod bezpieczeństwa. Aby otrzymać jednorazowy kod zabezpieczający, musisz mieć aplikację uwierzytelniającą na komputerze lub urządzeniu mobilnym.

> Każde oprogramowanie uwierzytelniające, które obsługuje algorytm czasowego hasła jednorazowego (TOTP), może być używane jako aplikacja uwierzytelniająca, na przykład Google Authenticator. Aby wygenerować jednorazowy kod zabezpieczający, musisz zsynchronizować czas ustawiony na urządzeniu z aplikacją uwierzytelniającą z czasem ustawionym na urządzeniu z Serwerem administracyjnym. Aby zapewnić większą dokładność, zalecamy korzystanie z tych samych serwerów NTP w całej infrastrukturze.

Aby sprawdzić, czy Kaspersky Security Center Linux obsługuje aplikację uwierzytelniającą, której chcesz użyć, spróbuj skonfigurować uwierzytelnianie dwuskładnikowe za pomocą tej aplikacji.

Jeden z kroków sugeruje podanie jednorazowego kodu zabezpieczającego wygenerowanego przez aplikację uwierzytelniającą. Jeśli się powiedzie, Kaspersky Security Center Linux obsługuje wybrany token uwierzytelniający.

Generowanie tajnego kodu za pomocą aplikacji uwierzytelniającej

Aplikacja uwierzytelniająca generuje kod zabezpieczający w następujący sposób:

1. Serwer administracyjny generuje specjalny tajny klucz i kod QR.
2. Przekazujesz wygenerowany klucz tajny lub kod QR do aplikacji uwierzytelniającej.
3. Aplikacja uwierzytelniająca generuje jednorazowy kod zabezpieczający, który należy przekazać do okna uwierzytelniania Serwera administracyjnego.

Kod zabezpieczający posiada identyfikator, o którym mowa w *nazwie wystawcy*. Nazwa wystawcy kodu zabezpieczającego jest używana jako identyfikator Serwera administracyjnego w aplikacji uwierzytelniającej. Możesz zmienić nazwę wystawcy kodu zabezpieczającego. Nazwa wystawcy kodu zabezpieczającego ma domyślną wartość, która jest taka sama, jak nazwa Serwera administracyjnego. Nowa nazwa wystawcy kodu zabezpieczającego jest przypisywana do Serwera administracyjnego po następnym zalogowaniu. Kod zabezpieczający jest jednorazowy i ważny do 30 sekund (dokładny czas może się różnić).

Zdecydowanie zalecamy, aby zapisać klucz tajny (lub kod QR) i przechowywać go w bezpiecznym miejscu. Pomoże to w przywróceniu dostępu do Kaspersky Security Center Web Console w przypadku utraty dostępu do urządzenia z aplikacją uwierzytelniającą.

Uwierzytelnianie dwuskładnikowe ma następujące funkcje:

- Począwszy od wersji 16.1 Serwera administracyjnego, uwierzytelnianie dwuskładnikowe jest włączane automatycznie, a opcja konfiguracji uwierzytelniania dwuskładnikowego podczas logowania jest domyślnie wyłączona. Konfigurowanie uwierzytelniania dwuskładnikowego podczas logowania jest dostępne tylko dla użytkowników, którzy znajdują się na liście dozwolonych uwierzytelniania dwuskładnikowego.
- Użytkownik może włączyć uwierzytelnianie dwuskładnikowe tylko dla swojego konta.
- Użytkownik może wykluczyć konta z uwierzytelniania dwuskładnikowego. Może to być konieczne w przypadku kont usług, które nie mogą otrzymać kodu zabezpieczającego dla uwierzytelnienia. Konta integracji służą do uruchamiania skryptów za pośrednictwem OpenAPI.
- Aby ponownie wygenerować klucz tajny uwierzytelniania dwuskładnikowego, użytkownik musi zresetować klucz tajny dla swojego konta.
- Aby zresetować lub usunąć klucz tajny uwierzytelniania dwuskładnikowego dla konta innego użytkownika, użytkownik musi posiadać konto ze skonfigurowanym uwierzytelnianiem dwuskładnikowym i uprawnieniem Modyfikuj listy ACL obiektów w obszarze funkcjonalnym **Funkcje ogólne**: **Uprawnienia użytkownika**.
- Aby wykluczyć konta innych użytkowników z uwierzytelniania dwuskładnikowego lub zmodyfikować listę dozwolonych uwierzytelniania dwuskładnikowego, użytkownik musi posiadać konto ze skonfigurowanym uwierzytelnianiem dwuskładnikowym i uprawnieniem Modyfikuj listy ACL obiektów w obszarze funkcjonalnym **Funkcje ogólne**: **Uprawnienia użytkownika**.
- Zawsze powinien być co najmniej jeden użytkownik ze skonfigurowanym uwierzytelnianiem dwuskładnikowym, aby ten użytkownik mógł zarządzać listą dozwolonych uwierzytelniania dwuskładnikowego i listą wykluczeń.
- Uwierzytelnianie dwuskładnikowe jest włączane automatycznie tylko w wersji 16.1 Serwera administracyjnego. Jeśli inne główne lub podrzędne Serwery administracyjne korzystają z wersji 16 lub starszej, ich ustawienia uwierzytelniania dwuskładnikowego pozostaną niezmienione.

- Wirtualny Serwer administracyjny dziedziczy ustawienia uwierzytelniania dwuskładnikowego z fizycznego Serwera administracyjnego, dzięki czemu jeśli uwierzytelnianie dwuskładnikowe jest włączone na fizycznym Serwerze administracyjnym, jest ono również włączone na wirtualnym Serwerze administracyjnym. Nie można skonfigurować ustawień uwierzytelniania dwuskładnikowego na wirtualnym Serwerze administracyjnym.

- Aby uwierzytelnianie dwuskładnikowe działało poprawnie, należy uaktualnić Serwer administracyjny i Web Console do wersji 16.1 lub nowszej.

Aby zapewnić kompleksową ochronę przy użyciu uwierzytelniania dwuskładnikowego, konieczne jest zabezpieczenie nie tylko Serwera administracyjnego, ale także urządzenia, na którym jest zainstalowany. W tym celu należy zapoznać się z zaleceniami Przewodnika po zwiększaniu odporności.

Konfigurowanie klucza tajnego uwierzytelniania dwuskładnikowego podczas logowania do Kaspersky Security Center Web Console

Po pierwszym zalogowaniu do Kaspersky Security Center Linux 16.1 lub nowszej wersji otwiera się okno konfiguracji uwierzytelniania dwuskładnikowego.

W celu skonfigurować uwierzytelniania dwuskładnikowego na swoim koncie:

1. Zainstaluj na urządzeniu mobilnym lub komputerze dowolną aplikację obsługującą Algorytm czasowego hasła jednorazowego (TOTP), taką jak:

   - Google Authenticator
   - Microsoft Authenticator
   - Bitrix24 OTP
   - Yandex ID
   - Avanpost Authenticator
   - Aladdin 2FA
   - Rutoken OTP

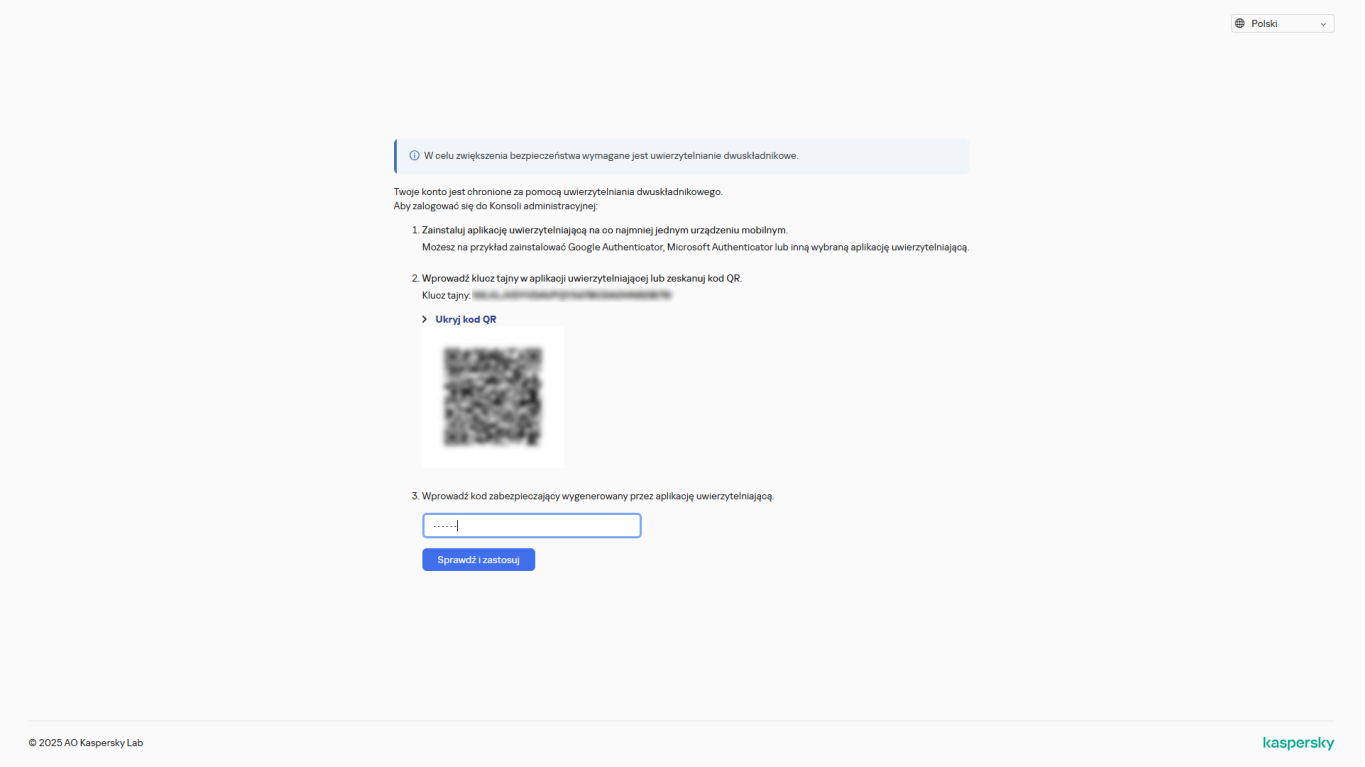
   Zdecydowanie nie zalecamy instalowania aplikacji uwierzytelniającej na tym samym urządzeniu, z którego nawiązywane jest połączenie z Serwerem administracyjnym.

2. Upewnij się, że czas na urządzeniu z aplikacją uwierzytelniającą i czas na urządzeniu z Serwerem administracyjnym są zsynchronizowane z czasem UTC. Aby zapewnić większą dokładność, zalecamy korzystanie z tych samych serwerów NTP w całej infrastrukturze.

3. Wygeneruj jednorazowy kod bezpieczeństwa z użyciem aplikacji uwierzytelniającej na urządzeniu mobilnym. W tym celu wykonaj jedną z następujących czynności:

   - Wprowadź ręcznie klucz tajny uwierzytelniania dwuskładnikowego w aplikacji uwierzytelniającej.
   - Kliknij opcję **Wyświetl kod QR** i zeskanuj kod QR za pomocą aplikacji uwierzytelniającej.

   Na urządzeniu mobilnym wyświetli się jednorazowy 6-cyfrowy kod bezpieczeństwa.



Konfigurowanie klucza tajnego uwierzytelniania dwuskładnikowego podczas logowania do Kaspersky Security Center Web Console

4. W oknie **Uwierzytelnianie dwuskładnikowe** określ jednorazowy kod bezpieczeństwa, wygenerowany przez aplikację uwierzytelniającą, a następnie kliknij przycisk **Sprawdź i zastosuj**.

   Konfiguracja Rutoken OTP

   Jeśli używasz Rutoken OTP, potrzebujesz urządzenia mobilnego z systemem Android z zainstalowaną aplikacją Rutoken OTP. Urządzenie mobilne z systemem Android musi spełniać następujące wymagania:

   - System operacyjny Android 7 lub nowszy.
   - Moduł NFC jest dostępny i włączony.

   W aplikacji Rutoken OTP musisz skonfigurować następujące parametry:

   - Wykonaj skanowanie kodu QR wyświetlonego w kreatorze konfiguracji dwuetapowej.
   - Ustaw odstęp czasu na 30 sekund.
   - Wybierz SHA1 jako algorytm.

   Aby skonfigurować Rutoken OTP:

   1. Umieść urządzenie Rutoken OTP obok urządzenia mobilnego z modułem NFC.
   2. W aplikacji Rutoken OTP naciśnij przycisk **Połącz token**.

3. W aplikacji Rutoken OTP naciśnij przycisk **Konfiguruj ustawienia**, a następnie naciśnij przycisk **Zapisz klucz tajny.**

   Jeśli token zostanie pomyślnie połączony z urządzeniem mobilnym, aplikacja Rutoken OTP wyświetli następujące komunikaty o stanie:

   - **Token jest połączony.**
   - **Ustawienia zostały skonfigurowane.**
   - **Klucz tajny został zapisany.**

4. Na urządzeniu Rutoken OTP naciśnij przycisk.

   Na urządzeniu zostanie wyświetlony kod bezpieczeństwa.

5. W Kaspersky Security Center Web Console, w oknie weryfikacji dwuetapowej, wprowadź kod zabezpieczający.

Uwierzytelnianie dwuskładnikowe jest skonfigurowany na Twoim koncie. Możesz uzyskać dostęp do Serwera administracyjnego zgodnie ze swoimi uprawnieniami.

Jeśli konfiguracja uwierzytelniania dwuskładnikowego nie jest dla Ciebie dostępna, skontaktuj się z użytkownikiem, który ma uprawnienie Modyfikuj listy ACL obiektów w obszarze funkcjonalnym **Funkcje ogólne**: **Uprawnienia użytkownika** i skonfigurował uwierzytelnianie dwuskładnikowe, aby dodać swoje konto do listy dozwolonych uwierzytelniania dwuskładnikowego.

Zezwalanie użytkownikom na konfigurowanie uwierzytelniania dwuskładnikowego

Lista dozwolonych uwierzytelniania dwuskładnikowego to lista użytkowników, którzy mają uprawnienia do początkowej konfiguracji uwierzytelniania dwuskładnikowego podczas logowania się do Web Console. Ta lista zawiera konta użytkowników bez skonfigurowanego uwierzytelniania dwuskładnikowego. Domyślnie nowe konta użytkowników nie są uwzględniane na liście dozwolonych kont uwierzytelniania dwuskładnikowego i muszą zostać dodane do listy przez administratora. Jeśli nowe konto jest kontem integracji używanym do uruchamiania skryptów OpenAPI, musi zostać wykluczone z uwierzytelniania dwuskładnikowego.

Konto użytkownika zostanie automatycznie usunięte z listy dozwolonych kont uwierzytelniania dwuskładnikowego, gdy skonfigurowano dla niego uwierzytelnianie dwuskładnikowe lub gdy zostanie z niego wykluczone.

Ręczna modyfikacja listy dozwolonych kont uwierzytelniania dwuskładnikowego jest dostępna dla kont, które mają skonfigurowane uwierzytelnianie dwuskładnikowe i mają uprawnienie Modyfikuj listy ACL obiektów w obszarze funkcjonalnym **Funkcje ogólne**: **Uprawnienia użytkownika**.

Aby ręcznie dodać konto użytkownika do listy zezwolonych uwierzytelniania dwuskładnikowego:

1. W menu głównym kliknij nazwę Serwera administracyjnego.

   Zostanie otwarte okno właściwości Serwera administracyjnego.

2. Na karcie **Uwierzytelnianie dwuskładnikowe** okna właściwości, w tabeli **Użytkownicy, którzy mogą generować klucze tajne** kliknij przycisk **Dodaj**.

3. W oknie, które zostanie otwarte:

   a. Wybierz konta użytkowników, które chcesz dodać.

      Do listy zezwolonych uwierzytelniania dwuskładnikowego można dodać tylko użytkowników, którzy nie są wykluczeni z uwierzytelniania dwuskładnikowego i nie mają klucza tajnego uwierzytelniania dwuskładnikowego.

   b. Jeśli konto jest chronione przed nieautoryzowaną modyfikacją, musisz potwierdzić, że masz uprawnienia do wprowadzania zmian na tym koncie. W oknie **Ochrona konta** podaj dane logowania do swojego konta i jednorazowy kod bezpieczeństwa do uwierzytelniania dwuskładnikowego.

   c. Zapisz zmiany.

   Wybrane konto użytkownika zostanie dodane do listy dozwolonych kont uwierzytelniania dwuskładnikowego. Przy następnym logowaniu użytkownik będzie mógł wygenerować klucz tajny.

Konto użytkownika można usunąć z listy dozwolonych kont uwierzytelniania dwuskładnikowego, dopóki uwierzytelnianie dwuskładnikowe nie zostanie dla niego skonfigurowane.

Aby ręcznie usunąć konta użytkowników z listy dozwolonych kont uwierzytelniania dwuskładnikowego:

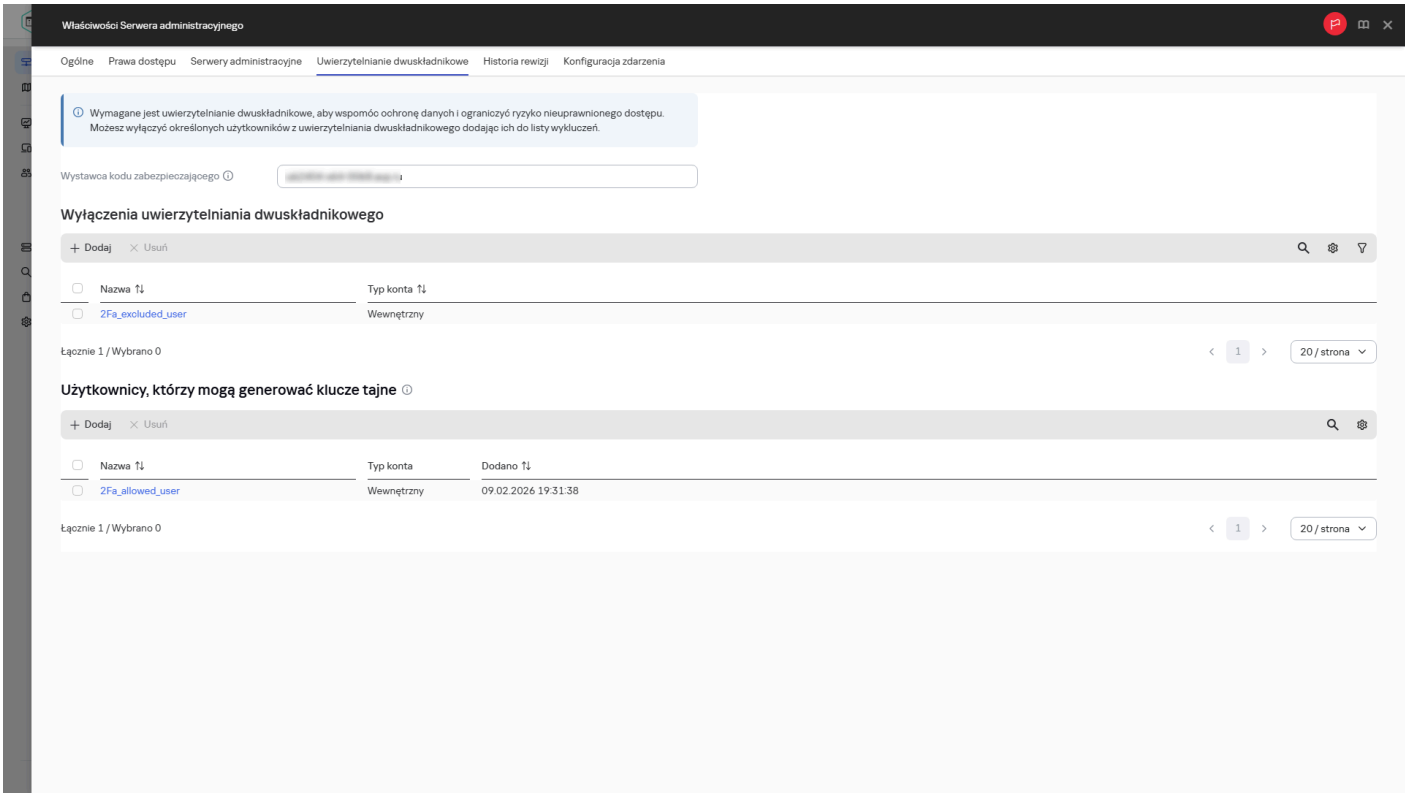
1. W menu głównym kliknij nazwę Serwera administracyjnego.

   Zostanie otwarte okno właściwości Serwera administracyjnego.

2. Na karcie **Uwierzytelnianie dwuskładnikowe** w oknie właściwości, w tabeli **Użytkownicy, którzy mogą generować klucze tajne**, wybierz konta użytkowników, które chcesz usunąć, a następnie kliknij przycisk **Usuń**.

3. Jeśli konto jest chronione przed nieautoryzowaną modyfikacją, musisz potwierdzić, że masz uprawnienia do wprowadzania zmian na tym koncie. W oknie **Ochrona konta** podaj dane logowania do swojego konta i jednorazowy kod bezpieczeństwa do uwierzytelniania dwuskładnikowego.

Wybrane konta użytkowników są wykluczone z listy zezwolonych uwierzytelniania dwuskładnikowego.



Konfigurowanie listy dozwolonych uwierzytelniania dwuskładnikowego

Jeśli podczas aktywnej sesji na Serwerze administracyjnym Twój klucz tajny uwierzytelniania dwuskładnikowego zostanie usunięty przez innego użytkownika lub samodzielnie zresetujesz klucz, ale nie utworzysz nowego, możliwość modyfikacji listy dozwolonych uwierzytelniania dwuskładnikowego.

Konta użytkowników mogą być również automatycznie dodawane i usuwane z listy zezwolonych uwierzytelniania dwuskładnikowego.

Podczas resetowania klucza tajnego uwierzytelniania dwuskładnikowego dla innych kont, ich konta są automatycznie dodawane do listy dozwolonych uwierzytelniania dwuskładnikowego, aby mogły wygenerować nowy klucz tajny.

Podczas aktualizacji Serwera administracyjnego z wersji 16 lub starszej do wersji 16.1 lub nowszej, a także podczas tworzenia kopii zapasowej danych na Serwerze administracyjnym w wersji 16 lub starszej i przywracania jej na Serwerze administracyjnym w wersji 16.1 lub nowszej, konta użytkowników zostaną automatycznie dodane do listy dozwolonych uwierzytelniania dwuskładnikowego, jeśli spełnione są wszystkie poniższe warunki:

- Użytkownik ma uprawnienie Odczyt w obszarze funkcyjnym *Funkcje ogólne: Podstawowa funkcjonalność* przypisane bezpośrednio do użytkownika (a nie przez grupę zabezpieczeń). Zakres roli użytkownika z tym uprawnieniem musi obejmować wszystkie zarządzane i nieprzypisane urządzenia i musi być ustawiony na poziomie Serwera administracyjnego.

- Użytkownik nie jest wykluczony z uwierzytelniania dwuskładnikowego.

- Użytkownik nie posiada klucza tajnego uwierzytelniania dwuskładnikowego.
- Uwierzytelnianie dwuskładnikowe nie zostało włączone dla wszystkich użytkowników na Serwerze administracyjnym w poprzedniej wersji.

Niespełnienie nawet jednego warunku spowoduje, że użytkownik nie zostanie dodany do listy dozwolonych uwierzytelniania dwuskładnikowego.

> Po uaktualnieniu lub przywróceniu zalecamy upewnienie się, że lista dozwolonych uwierzytelniania dwuskładnikowego zawiera tylko konta użytkowników, które muszą mieć dostęp do Serwera administracyjnego. Przejrzyj listę zezwolonych kont uwierzytelniania dwuskładnikowego i usuń z niej wszystkie inne konta. Dodaj konta integracji używane do uruchamiania skryptów przez OpenAPI do listy wykluczeń, aby zapobiec błędom skryptów.

Konta użytkowników utracą dostęp do Serwera administracyjnego po aktualizacji lub przywróceniu, jeśli spełnione zostaną wszystkie następujące warunki:

- Użytkownik ma uprawnienie Odczyt w obszarze funkcjonalnym *Funkcje ogólne: Podstawowa funkcjonalność* przypisane przez grupę zabezpieczeń (nie bezpośrednio użytkownikowi) lub nie ma tego uprawnienia w ogóle.
- Użytkownik nie jest wykluczony z uwierzytelniania dwuskładnikowego.
- Użytkownik nie posiada klucza tajnego uwierzytelniania dwuskładnikowego.
- Uwierzytelnianie dwuskładnikowe zostało włączone dla wszystkich użytkowników na Serwerze administracyjnym poprzedniej wersji.

W razie potrzeby te konta można ręcznie dodać do listy dozwolonych kont uwierzytelniania dwuskładnikowego.

Resetowanie i usuwanie klucza tajnego uwierzytelniania dwuskładnikowego

Możesz zresetować klucz tajny, gdy użytkownik utraci dostęp do swojego urządzenia do uwierzytelniania dwuskładnikowego lub będzie musiał skonfigurować uwierzytelnianie dwuskładnikowe na nowym urządzeniu. Zresetowanie klucza tajnego umożliwia użytkownikowi ponowne zalogowanie się do Web Console i wygenerowanie nowego klucza tajnego.

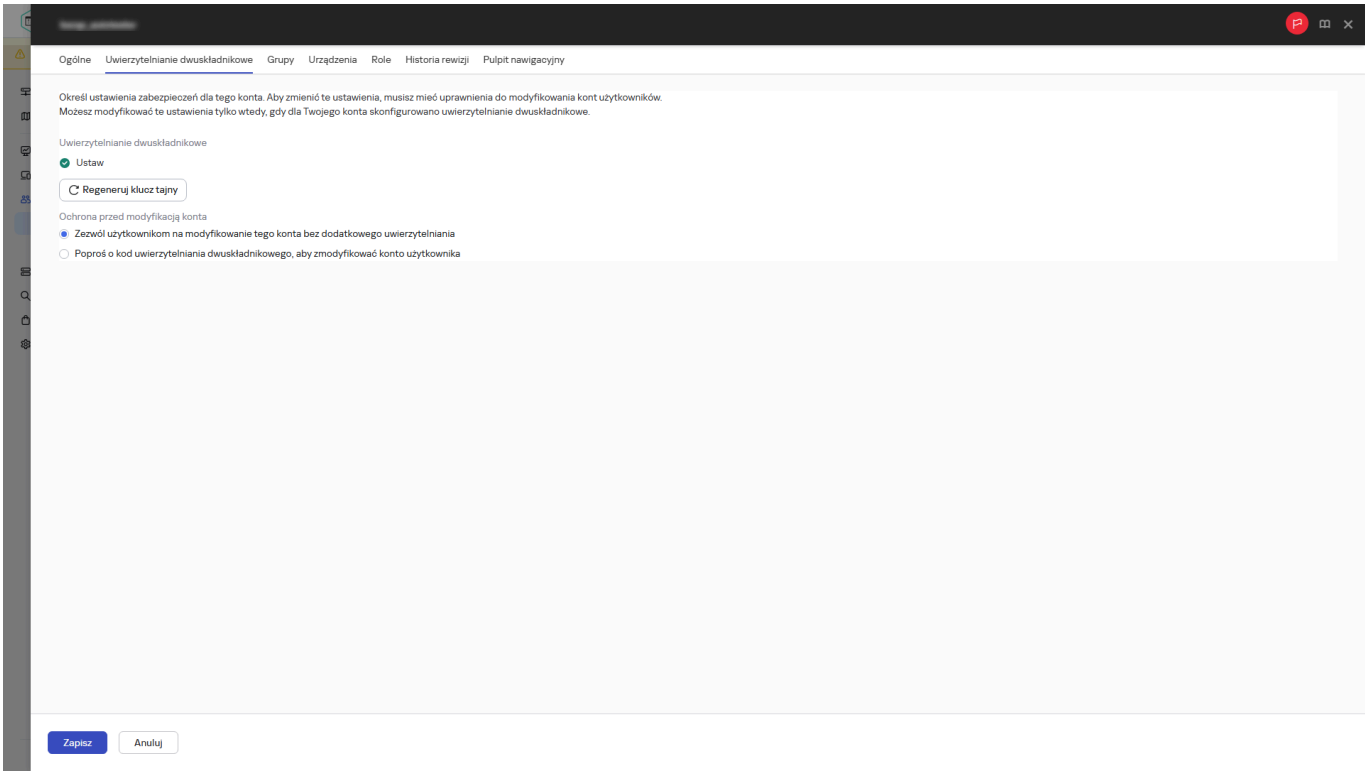
> Możesz zresetować lub usunąć klucz tajny uwierzytelniania dwuskładnikowego dla kont innych użytkowników tylko wtedy, gdy skonfigurowano uwierzytelnianie dwuskładnikowe i masz uprawnienie Modyfikuj listy ACL obiektów w obszarze funkcjonalnym **Funkcje ogólne**: **Uprawnienia użytkownika**. Możesz również ponownie wygenerować własny klucz tajny.

Aby zresetować klucz tajny dla konta:

1. W menu głównym przejdź do opcji **Użytkownicy i role** → **Użytkownicy i grupy**, a następnie wybierz zakładkę **Użytkownicy**.
2. Kliknij nazwę konta użytkownika, dla którego chcesz zresetować klucz tajny.

3. Jeśli chcesz zresetować klucz tajny dla swojego konta:

a. Na karcie **Uwierzytelnianie dwuskładnikowe** kliknij przycisk **Regeneruj klucz tajny**.

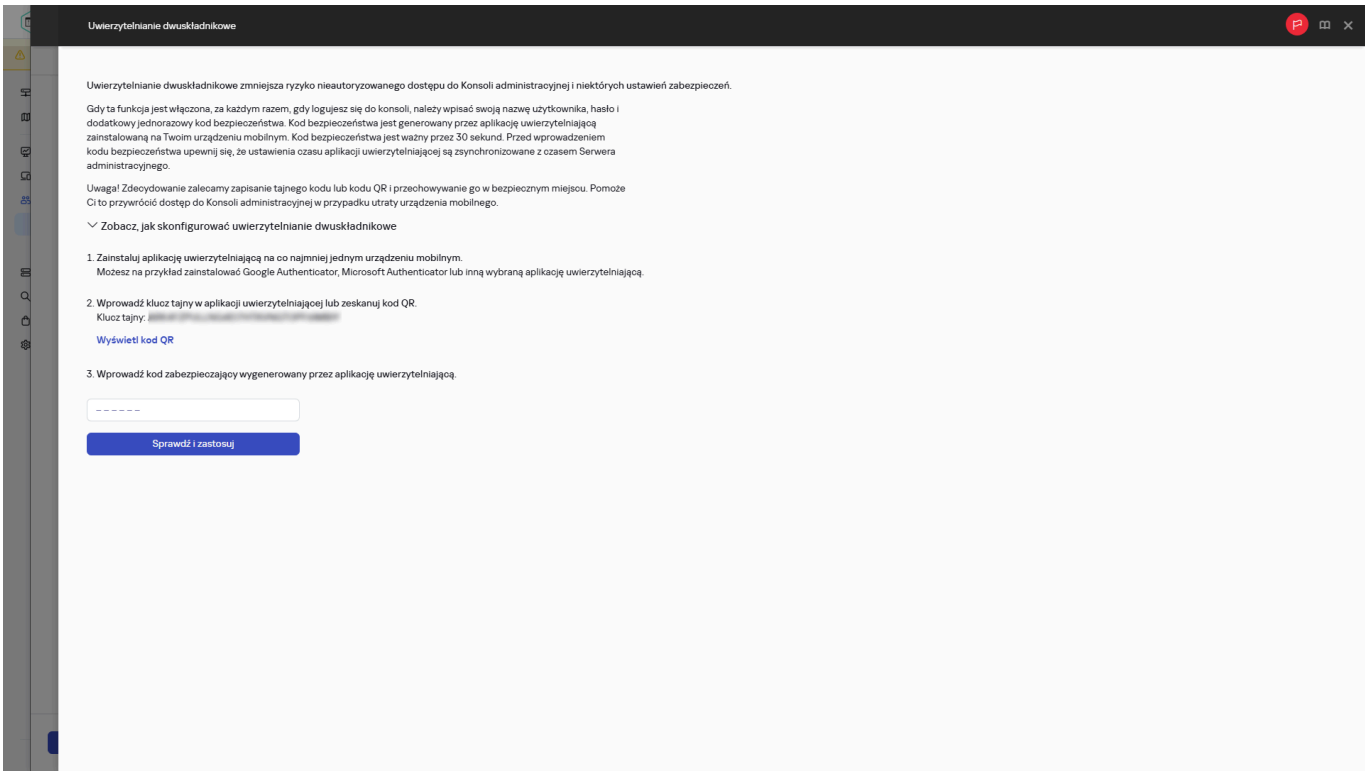


Ponowne generowanie klucza tajnego uwierzytelniania dwuskładnikowego dla bieżącego konta użytkownika

a. Jeśli Twoje konto jest chronione przed nieautoryzowaną modyfikacją, musisz potwierdzić, że masz uprawnienia do wprowadzania zmian na tym koncie. W oknie **Ochrona konta** określ dane uwierzytelniające własnego konta i kod uwierzytelniania dwuskładnikowego.

b. W oknie **Uwierzytelnianie dwuskładnikowe** kliknij **Zobacz, jak skonfigurować uwierzytelnianie dwuskładnikowe**, a następnie kliknij **Wyświetl kod QR**.

c. Użyj aplikacji uwierzytelniającej na urządzeniu mobilnym, aby przeprowadzić skanowanie kodu QR i otrzymać jednorazowy kod bezpieczeństwa.



Konfigurowanie nowego klucza tajnego uwierzytelniania dwuskładnikowego dla bieżącego konta użytkownika

a. W oknie **Uwierzytelnianie dwuskładnikowe** określ jednorazowy kod bezpieczeństwa, wygenerowany przez aplikację uwierzytelniającą, kliknij przycisk **Sprawdź i zastosuj**, a następnie zapisz zmiany.

Konfiguracja Rutoken OTP

Jeśli używasz Rutoken OTP, potrzebujesz urządzenia mobilnego z systemem Android z zainstalowaną aplikacją Rutoken OTP. Urządzenie mobilne z systemem Android musi spełniać następujące wymagania:

- System operacyjny Android 7 lub nowszy.
- Moduł NFC jest dostępny i włączony.

W aplikacji Rutoken OTP musisz skonfigurować następujące parametry:

- Wykonaj skanowanie kodu QR wyświetlonego w kreatorze konfiguracji dwuetapowej.
- Ustaw odstęp czasu na 30 sekund.
- Wybierz SHA1 jako algorytm.

Aby skonfigurować Rutoken OTP:

1. Umieść urządzenie Rutoken OTP obok urządzenia mobilnego z modułem NFC.
2. W aplikacji Rutoken OTP naciśnij przycisk **Połącz token**.
3. W aplikacji Rutoken OTP naciśnij przycisk **Konfiguruj ustawienia**, a następnie naciśnij przycisk **Zapisz klucz tajny.**

Jeśli token zostanie pomyślnie połączony z urządzeniem mobilnym, aplikacja Rutoken OTP wyświetli następujące komunikaty o stanie:

- **Token jest połączony.**
- **Ustawienia zostały skonfigurowane.**
- **Klucz tajny został zapisany.**

4. Na urządzeniu Rutoken OTP naciśnij przycisk.

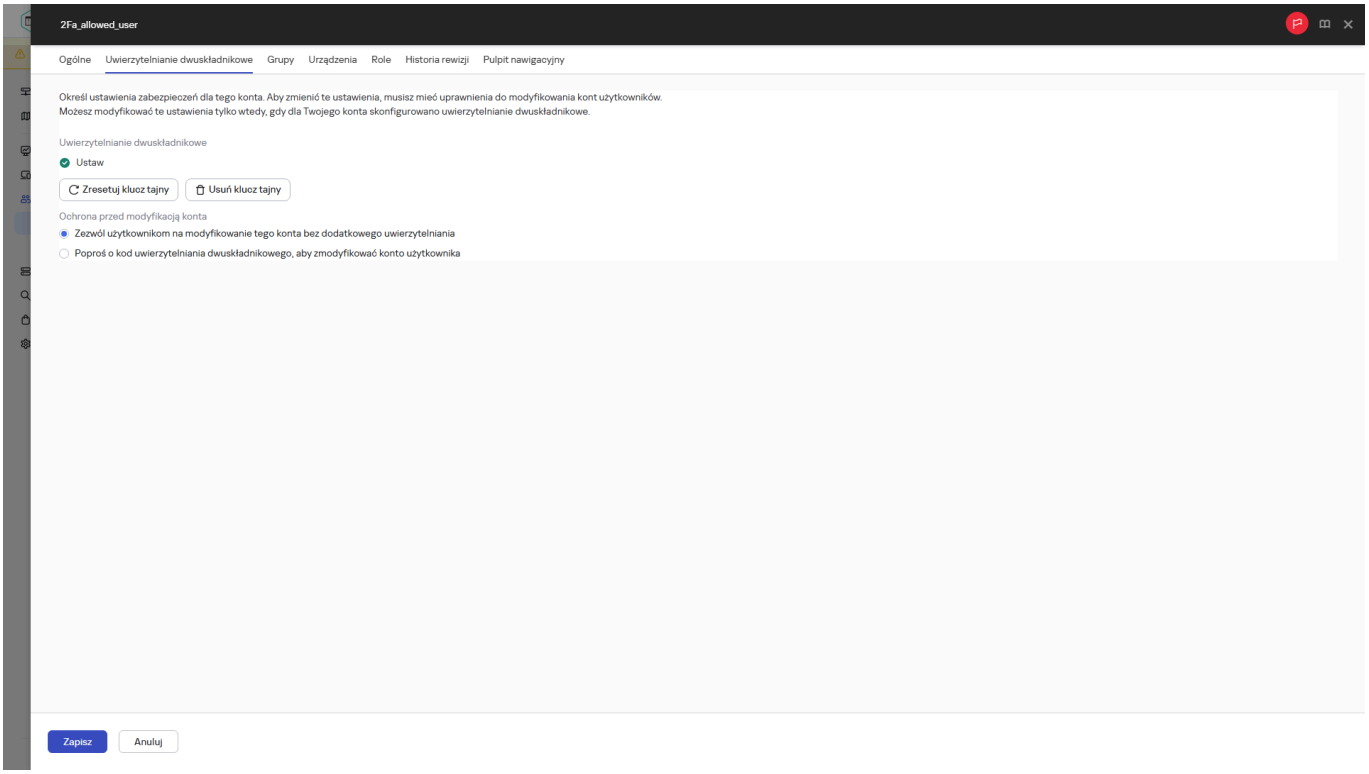
   Na urządzeniu zostanie wyświetlony kod bezpieczeństwa.

5. W Kaspersky Security Center Web Console, w oknie weryfikacji dwuetapowej, wprowadź kod zabezpieczający.

Klucz tajny dla Twojego konta został zmieniony.

4. Jeśli chcesz zresetować klucz tajny dla innego konta:

   a. Na karcie **Uwierzytelnianie dwuskładnikowe** kliknij przycisk **Zresetuj klucz tajny**.



Resetowanie klucza tajnego uwierzytelniania dwuskładnikowego dla innego konta użytkownika

   a. Jeśli konto jest chronione przed nieautoryzowaną modyfikacją, musisz potwierdzić, że masz uprawnienia do wprowadzania zmian na tym koncie. W oknie **Ochrona konta** określ dane uwierzytelniające własnego konta i jednorazowy kod bezpieczeństwa dla uwierzytelniania dwuskładnikowego.

   b. Potwierdź zresetowanie klucza tajnego, a następnie zapisz zmiany.

Po zresetowaniu klucza tajnego dla innego konta, istniejący klucz tajny zostanie usunięty, a konto użytkownika zostanie dodane do listy dozwolonych uwierzytelniania dwuskładnikowego we właściwościach Serwera administracyjnego. Przy następnym logowaniu użytkownik będzie mógł wygenerować nowy klucz tajny.

Klucz tajny konta użytkownika zostanie zresetowany.

Można usunąć klucz tajny, aby całkowicie zablokować użytkownikowi możliwość logowania się do Web Console i uniemożliwić mu dostęp do Serwera administracyjnego.

Aby usunąć klucz tajny:

1. W menu głównym przejdź do opcji **Użytkownicy i role** → **Użytkownicy i grupy**, a następnie wybierz zakładkę **Użytkownicy**.

2. Kliknij nazwę wewnętrznego konta użytkownika, dla którego chcesz usunąć klucz tajny.

   Nie możesz usunąć klucza tajnego dla swojego konta.

3. Na karcie **Uwierzytelnianie dwuskładnikowe** kliknij przycisk **Usuń klucz tajny**.

4. Jeśli konto jest chronione przed nieautoryzowaną modyfikacją, musisz potwierdzić, że masz uprawnienia do wprowadzania zmian na tym koncie. W oknie **Ochrona konta** określ dane uwierzytelniające własnego konta i jednorazowy kod bezpieczeństwa dla uwierzytelniania dwuskładnikowego.

5. Potwierdź usunięcie klucza tajnego, a następnie zapisz zmiany.

Klucz tajny konta użytkownika zostanie usunięty.

Możesz przywrócić dostęp, dodając użytkownika do listy dozwolonych uwierzytelniania dwuskładnikowego we właściwościach Serwera administracyjnego. W takim przypadku przy następnym logowaniu użytkownik będzie mógł wygenerować nowy klucz tajny.

Wykluczanie kont z uwierzytelniania dwuskładnikowego

W razie potrzeby wyklucz konta użytkowników z uwierzytelniania dwuskładnikowego, aby umożliwić im logowanie się do Serwera administracyjnego, nawet jeśli nie skonfigurowali uwierzytelniania dwuskładnikowego. Wykluczenie kont z uwierzytelniania dwuskładnikowego może być konieczne w przypadku kont integracji, które nie mogą przekazać kodu zabezpieczającego podczas uwierzytelniania. Konta integracji służą do uruchamiania skryptów za pośrednictwem OpenAPI.

Możesz zmodyfikować listę wykluczeń, jeśli dla Twojego konta skonfigurowano uwierzytelnianie dwuskładnikowe i masz uprawnienie Modyfikuj listy ACL obiektów w obszarze funkcjonalnym **Funkcje ogólne**: **Uprawnienia użytkownika**.

W celu wykluczenia konta użytkownika z uwierzytelniania dwuskładnikowego:

1. W menu głównym kliknij nazwę Serwera administracyjnego.

   Zostanie otwarte okno właściwości Serwera administracyjnego.

2. Na zakładce **Uwierzytelnianie dwuskładnikowe** w oknie właściwości, w tabeli **Wyłączenia uwierzytelniania dwuskładnikowego** kliknij przycisk **Dodaj**.

3. W oknie, które zostanie otwarte:

   a. Wybierz konto użytkownika, które chcesz wykluczyć.

   b. Jeśli konto jest chronione przed nieautoryzowaną modyfikacją, musisz potwierdzić, że masz uprawnienia do wprowadzania zmian na tym koncie. W oknie **Ochrona konta** podaj dane logowania do swojego konta i jednorazowy kod bezpieczeństwa do uwierzytelniania dwuskładnikowego.

   c. Zapisz zmiany.

   Wybrane konta użytkowników są wykluczane z uwierzytelniania dwuskładnikowego, a ich klucze tajne, jeśli istnieją, są usuwane. Lista wykluczonych kont nie ulega zmianie po przywróceniu kopii zapasowej na Serwerze administracyjnym 16.1 ani po uaktualnieniu Serwera administracyjnego do wersji 16.1 lub nowszej. Jeśli konta z listy wykluczeń miały klucze tajne w poprzedniej wersji Serwera administracyjnego, te klucze tajne zostaną usunięte w wersji 16.1.

Możesz usunąć konta użytkowników z listy wykluczeń, aby całkowicie zablokować użytkownikom możliwość logowania się do Web Console i uniemożliwić im dostęp do Serwera administracyjnego.

Aby usunąć konta użytkowników z listy wykluczeń:

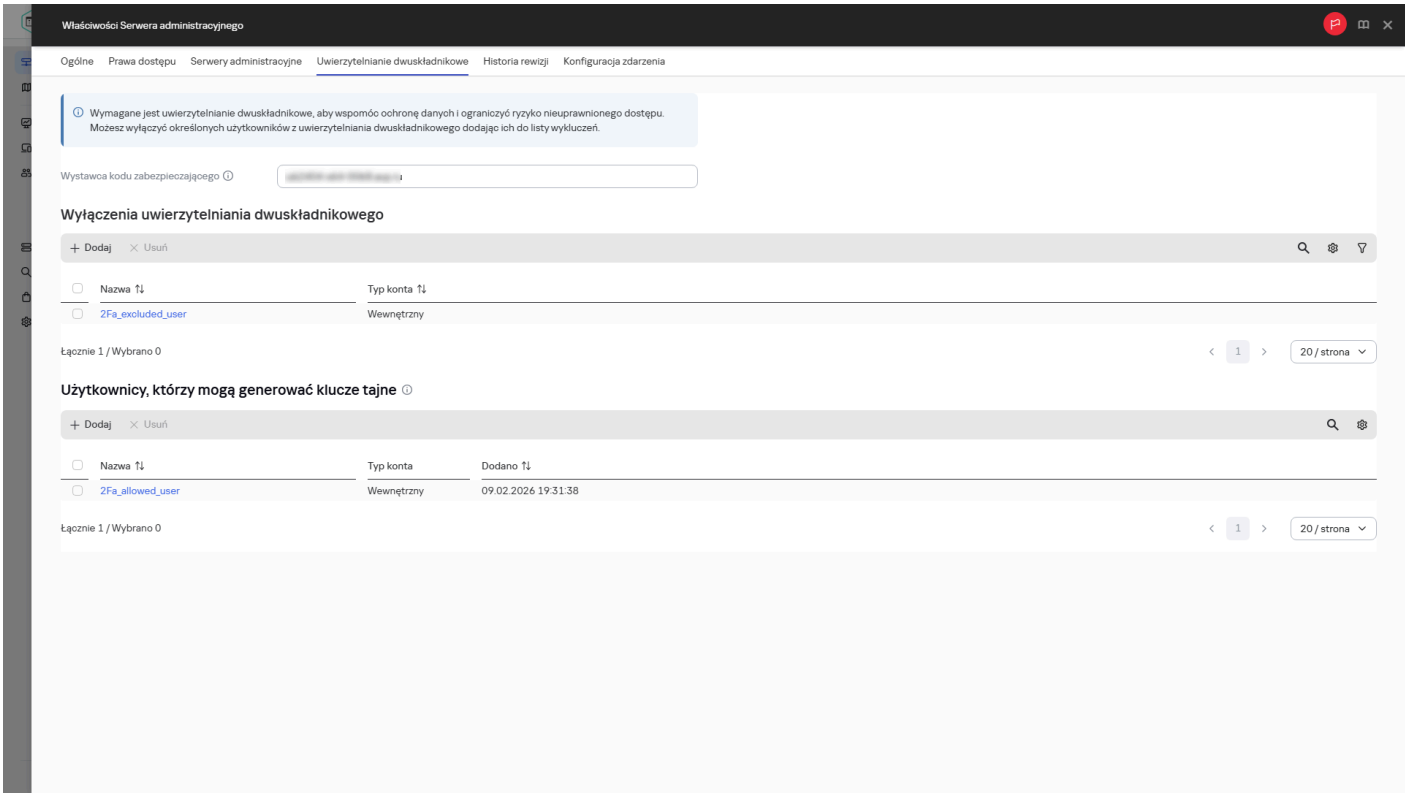
1. W menu głównym kliknij nazwę Serwera administracyjnego.

   Zostanie otwarte okno właściwości Serwera administracyjnego.

2. Na karcie **Uwierzytelnianie dwuskładnikowe** okna właściwości, w tabeli **Wyłączenia uwierzytelniania dwuskładnikowego** wybierz konta użytkowników, które chcesz usunąć, a następnie kliknij **Usuń**.

3. Jeśli konto jest chronione przed nieautoryzowaną modyfikacją, musisz potwierdzić, że masz uprawnienia do wprowadzania zmian na tym koncie. W oknie **Ochrona konta** podaj dane logowania do swojego konta i jednorazowy kod bezpieczeństwa do uwierzytelniania dwuskładnikowego.

Wybrane konta użytkowników zostaną usunięte z listy wykluczeń.



Konfigurowanie listy wykluczeń uwierzytelniania dwuskładnikowego

Edytowanie nazwy wystawcy kodu zabezpieczającego

Możesz mieć kilka identyfikatorów (nazywanych wystawcami) dla różnych Serwerów administracyjnych. Możesz zmienić nazwę wystawcy kodu zabezpieczającego w przypadku, gdy, na przykład, Serwer administracyjny już używa podobnej nazwy wystawcy kodu zabezpieczającego dla innego Serwera administracyjnego. Domyślnie, nazwa wystawcy kodu zabezpieczającego jest taka sama, jak nazwa Serwera administracyjnego.

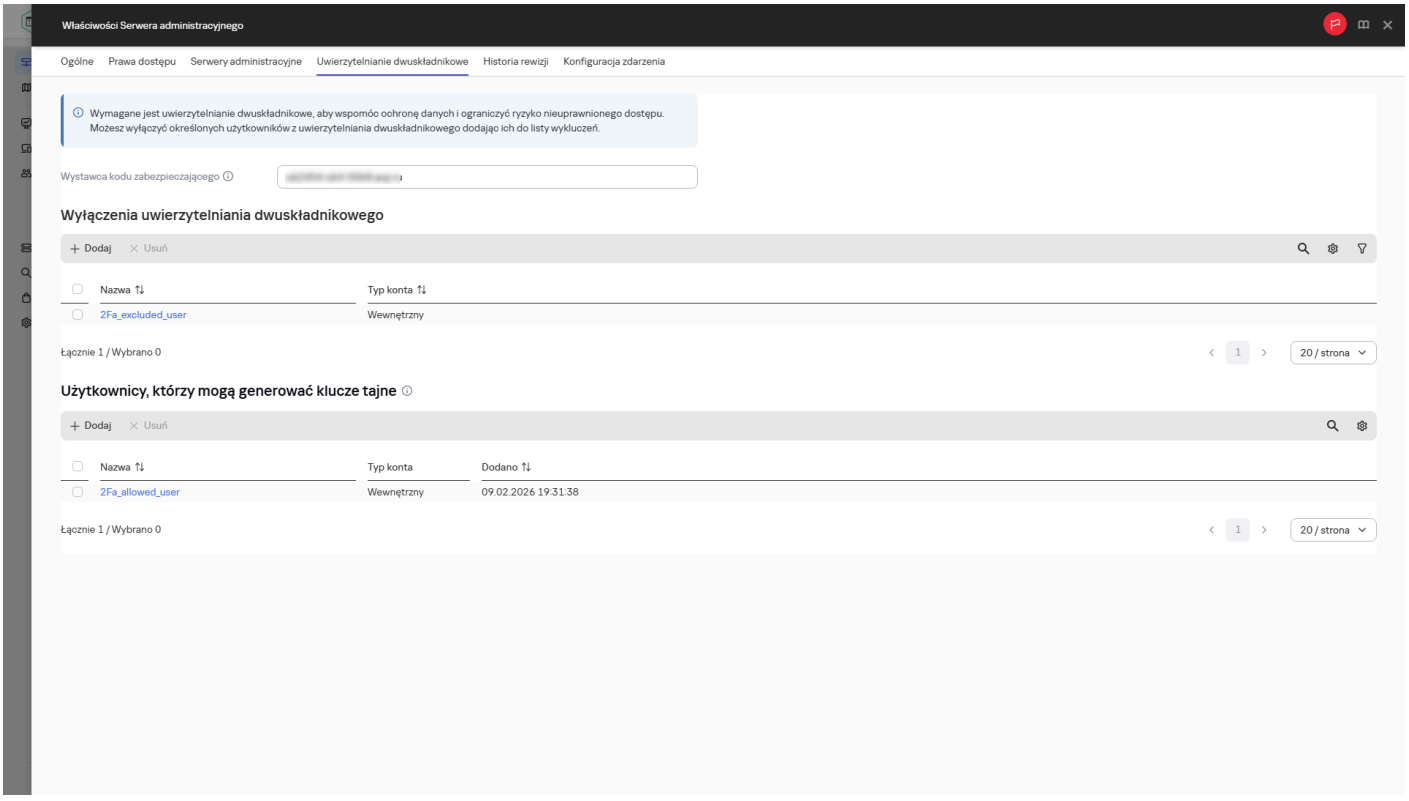
W celu określenia nowej nazwy wystawcy kodu zabezpieczającego:

1. W menu głównym kliknij nazwę Serwera administracyjnego.

   Zostanie otwarte okno właściwości Serwera administracyjnego.

2. Na karcie **Uwierzytelnianie dwuskładnikowe** w oknie właściwości wprowadź nową nazwę w polu **Wystawca kodu zabezpieczającego**, a następnie zapisz zmiany.

Nowa nazwa wystawcy kodu zabezpieczającego zostanie przypisana do Serwera administracyjnego po następnym zalogowaniu.



Określanie nazwy wystawcy kodu zabezpieczającego

Zmienianie liczby dozwolonych prób wprowadzenia hasła

Użytkownik Kaspersky Security Center Linux może wprowadzić niepoprawne hasło ograniczoną liczbę razy. Po osiągnięciu limitu, konto użytkownika zostaje zablokowane na godzinę.

Domyślnie, maksymalna liczba dozwolonych prób wprowadzenia hasła to 10. Możesz zmienić liczbę dozwolonych prób wprowadzenia hasła w sposób opisany w tej sekcji.

W celu zmiany liczny dozwolonych prób wprowadzenia hasła:

1. Na urządzeniu Serwera administracyjnego uruchom wiersz poleceń systemu Linux.

2. W przypadku narzędzia klscflag uruchom następujące polecenie:

   ```
   sudo /opt/kaspersky/ksc64/sbin/klscflag -fset -pv klserver -n SrvSplPpcLogonAttempts -t d -v N
   ```

gdzie N to liczba prób wprowadzenia hasła.

3. Aby zastosować zmiany, uruchom ponownie usługę Serwera administracyjnego.

Maksymalna liczba dozwolonych prób wprowadzenia hasła zostanie zmieniona.

Usuwanie użytkownika lub grupy bezpieczeństwa

Możesz usunąć tylko użytkowników wewnętrznych lub wewnętrzne grupy bezpieczeństwa.

W celu usunięcia użytkownika lub grupy bezpieczeństwa:

1. W menu głównym przejdź do opcji **Użytkownicy i role** → **Użytkownicy i grupy**, a następnie wybierz kartę **Użytkownicy** lub **Grupy**.

2. Zaznacz pole obok użytkownika lub grupy bezpieczeństwa, którą chcesz usunąć.

   Zawsze powinien być co najmniej jeden użytkownik ze skonfigurowanym uwierzytelnianiem dwuskładnikowym, aby ten użytkownik mógł zarządzać listą dozwolonych uwierzytelniania dwuskładnikowego i listą wykluczeń.

3. Kliknij **Usuń**.

4. W otwartym oknie potwierdzenia kliknij **OK**.

Użytkownik lub grupa bezpieczeństwa zostanie usunięta.

Zmiana hasła do konta użytkownika

Zmiana hasła do własnego konta lub konta innego użytkownika może być konieczna, jeśli obecne hasło wkrótce wygaśnie lub chcesz je zmienić na bezpieczniejsze.

Hasło musi być zgodne z następującymi regułami:

- Hasło musi zawierać od 8 do 256 znaków.
- Hasło musi zawierać znaki z przynajmniej trzech z poniższych grup:
  - Wielkie litery (A-Z)
  - Małe litery (a-z)

- Cyfry (0-9)
- Znaki specjalne (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)

- Hasło nie może zawierać spacji, znaków Unicode lub kombinacji znaków "." i "@", gdy "." jest umieszczane przed "@".

Zmiana hasła do własnego konta

Aby edytować hasło do swojego konta:

1. W górnym panelu przejdź do menu konta, klikając nazwę swojego konta.
2. Z listy rozwijalnej wybierz **Zmień hasło**.
3. W prawym panelu, który zostanie otwarty, wprowadź aktualne hasło, a następnie określ nowe hasło do połączenia z Kaspersky Security Center Linux.

   Aby zobaczyć wprowadzone hasło kliknij 👁.
4. Jeśli Twoje konto jest chronione przed nieautoryzowaną modyfikacją, musisz potwierdzić, że masz uprawnienia do wprowadzania zmian na tym koncie. W oknie **Ochrona konta** podaj dane uwierzytelniające własnego konta lub konta, które ma uprawnienie Modyfikowanie list ACL obiektów w obszarze funkcjonalnym **Funkcje ogólne**: **Uprawnienia użytkownika**.
5. Wprowadź jednorazowy kod bezpieczeństwa wygenerowany z użyciem aplikacji uwierzytelniającej na urządzeniu mobilnym.

Zmiana hasła do konta użytkownika wewnętrznego

Aby edytować hasło dla konta użytkownika wewnętrznego:

1. W menu głównym przejdź do opcji **Użytkownicy i role** → **Użytkownicy i grupy**, a następnie wybierz zakładkę **Użytkownicy**.
2. Kliknij nazwę konta użytkowników, które chcesz edytować.
3. W otwartym oknie ustawień użytkownika, na karcie **Ogólne** kliknij przycisk **Zmień hasło**.
4. Ustaw nowe hasło w celu połączenia użytkownika z Kaspersky Security Center Linux.

   Aby zobaczyć wprowadzone hasło kliknij 👁.
5. W razie potrzeby włącz opcję **Użytkownik musi zmienić hasło przy pierwszym logowaniu**, aby wymusić zmianę hasła przy kolejnym uwierzytelnieniu użytkownika.

6. Jeśli konto użytkownika jest chronione przed nieautoryzowaną modyfikacją, musisz potwierdzić, że masz uprawnienia do wprowadzania zmian na tym koncie. W oknie **Ochrona konta** określ dane uwierzytelniające konta, które ma uprawnienie Modyfikuj listy ACL obiektów w obszarze funkcjonalnym **Funkcje ogólne**: **Uprawnienia użytkownika**.

7. Wprowadź jednorazowy kod bezpieczeństwa wygenerowany z użyciem aplikacji uwierzytelniającej na urządzeniu mobilnym.

Konfigurowanie opcji zmiany hasła za pomocą flag serwera

Aby skonfigurować zmianę hasła, możesz użyć narzędzia klscflag, używając następujących poleceń:

- Konfigurowanie okresu rotacji hasła (flaga `LP_SplPwdChangePeriodDays`)

  ```
  klscflag -fset -pv .core/.independent -s KLLIM -n LP_SplPwdChangePeriodDays -t d -v
  < okres_rotacji >
  ```

  Gdzie `< okres_rotacji >` to okres czasu w dniach, po którym hasło użytkownika wygasa. Możliwe wartości: 0–730. Jeżeli wartość parametru wynosi 0, rotacja haseł jest wyłączona.

- Konfigurowanie czasu wstępnego ostrzeżenia o konieczności zmiany hasła (flaga `LP_SplPwdChangeNotificationHours`)

  ```
  klscflag -fset -pv .core/.independent -s KLLIM -n LP_SplPwdChangeNotificationHours -t
  d -v < czas_ostrzeżenia >
  ```

  Gdzie `< czas_ostrzeżenia >` to okres czasu w godzinach, po którym hasło użytkownika wygasa. W tym czasie wyświetla się powiadomienie o konieczności zmiany hasła. Możliwe wartości: 0–17520. Jeżeli wartość parametru wynosi 0, czas ostrzeżenia wynosi 25 procent okresu rotacji hasła.

- Określenie wartości domyślnej opcji **Użytkownik musi zmienić hasło przy pierwszym logowaniu** (flaga `LP_SplPwdForceChange`)

  ```
  klscflag -fset -pv .core/.independent -s KLLIM -n LP_SplPwdForceChange -t d -v
  < wartość >
  ```

  Gdzie możliwe wartości flagi `< wartość >` to:

  `1`—Opcja **Użytkownik musi zmienić hasło przy pierwszym logowaniu** jest włączona.

  `0`—Opcja **Użytkownik musi zmienić hasło przy pierwszym logowaniu** jest wyłączona.

Aby wyświetlić bieżącą wartość flagi, uruchom następujące polecenie:

```
klscflag -fget -pv .core/.independent -s KLLIM -n < flaga > -t d
```

Gdzie `< flaga >` jest flagą `LP_SplPwdChangePeriodDays`, `LP_SplPwdChangeNotificationHours` lub `LP_SplPwdForceChange`.

Tworzenie roli użytkownika

W celu utworzenia roli użytkownika:

1. W menu głównym przejdź do **Użytkownicy i role** → **Role**.
2. Kliknij **Dodaj**.
3. W oknie **Nazwa nowej roli**, które zostanie otwarte, wprowadź nazwę nowej roli.
4. Kliknij **OK**, aby zastosować zmiany.
5. W oknie właściwości roli, które zostanie otwarte, zmień ustawienia roli:
   - Na zakładce **Ogólne** edytuj nazwę roli.
     Nie możesz edytować nazwy predefiniowanej roli.
   - Na zakładce **Ustawienia** edytuj zakres roli oraz zasady i profile skojarzone z rolą.
   - Na zakładce **Prawa dostępu** edytuj uprawnienia dostępu do aplikacji firmy Kaspersky.
6. Kliknij **Zapisz**, aby zachować zmiany.

Nowa rola pojawi się na liście ról użytkownika.

Edytowanie roli użytkownika

W celu edytowania roli użytkownika:

1. W menu głównym przejdź do **Użytkownicy i role** → **Role**.
2. Kliknij nazwę roli, którą chcesz edytować.
3. W oknie właściwości roli, które zostanie otwarte, zmień ustawienia roli:
   - Na zakładce **Ogólne** edytuj nazwę roli.
     Nie możesz edytować nazwy predefiniowanej roli.
   - Na zakładce **Ustawienia** edytuj zakres roli oraz zasady i profile skojarzone z rolą.
   - Na zakładce **Prawa dostępu** edytuj uprawnienia dostępu do aplikacji firmy Kaspersky.
4. Kliknij **Zapisz**, aby zachować zmiany.

Zaktualizowana rola pojawi się na liście ról użytkownika.

Edytowanie obszaru roli użytkownika

Obszar roli użytkownika to połączenie użytkowników i grup administracyjnych. Ustawienia skojarzone z rolą użytkownika są stosowane tylko do urządzeń, które należą do użytkowników posiadających tę rolę i tylko wtedy, gdy te urządzenia należą do grup skojarzonych z tą rolą, w tym grup podrzędnych.

W celu dodania użytkowników, grup bezpieczeństwa i grup administracyjnych do obszaru roli użytkownika, możesz użyć jednej z następujących metod:

Metoda 1:

1. W menu głównym przejdź do opcji **Użytkownicy i role** → **Użytkownicy i grupy**, a następnie wybierz kartę **Użytkownicy** lub **Grupy**.
2. Zaznacz pola obok użytkowników lub grup bezpieczeństwa, które chcesz dodać do obszaru roli użytkownika.
3. Kliknij przycisk **Przypisz rolę**.

   Zostanie uruchomiony Kreator przypisywania roli. Przejdź przez kroki kreatora, korzystając z przycisku **Dalej**.
4. W kroku **Wybierz rolę** wybierz rolę użytkownika, którą chcesz przypisać.
5. W kroku **Zdefiniuj zakres** wybierz grupę administracyjną, którą chcesz dodać do obszaru roli użytkownika.
6. W celu zakończenia działania Kreatora kliknij przycisk **Przypisz rolę**.

Wybrani użytkownicy lub grupy bezpieczeństwa i wybrana grupa administracyjna zostaną dodane do obszaru roli użytkownika.

Metoda 2:

1. W menu głównym przejdź do **Użytkownicy i role** → **Role**.
2. Kliknij nazwę roli, dla której chcesz określić obszar.
3. W otwartym oknie właściwości roli wybierz zakładkę **Ustawienia**.
4. W sekcji **Zakres roli** kliknij **Dodaj**.

   Zostanie uruchomiony Kreator przypisywania roli. Przejdź przez kroki kreatora, korzystając z przycisku **Dalej**.
5. W kroku **Zdefiniuj zakres** wybierz grupę administracyjną, którą chcesz dodać do obszaru roli użytkownika.
6. W kroku **Wybierz użytkowników** wybierz użytkowników i grupy zabezpieczeń, które chcesz dodać do obszaru roli użytkownika.
7. W celu zakończenia działania Kreatora kliknij przycisk **Przypisz rolę**.
8. Kliknij przycisk **Zamknij** (×), aby zamknąć okno właściwości roli.

Wybrani użytkownicy lub grupy bezpieczeństwa i wybrana grupa administracyjna zostaną dodane do obszaru roli użytkownika.

Metoda 3:

1. W menu głównym kliknij nazwę Serwera administracyjnego.

   Zostanie otwarte okno właściwości Serwera administracyjnego.

2. Na zakładce **Prawa dostępu** zaznacz pole wyboru obok nazwy użytkownika lub grupy bezpieczeństwa, którą chcesz dodać do obszaru roli użytkownika, a następnie kliknij przycisk **Role**.

   Nie można jednocześnie wybrać wielu użytkowników lub grup bezpieczeństwa. Jeśli wybierzesz więcej niż jeden element, przycisk **Role** będzie nieaktywny.

3. W oknie **Role** wybierz rolę użytkownika, którą chcesz przypisać, a następnie zastosuj i zapisz zmiany.

   Wybrani użytkownicy lub grupy bezpieczeństwa zostaną dodani do obszaru roli użytkownika.

Usuwanie roli użytkownika

W celu usunięcia roli użytkownika:

1. W menu głównym przejdź do **Użytkownicy i role** → **Role**.

2. Zaznacz pole obok nazwy roli, którą chcesz usunąć.

3. Kliknij **Usuń**.

4. W otwartym oknie potwierdzenia kliknij **OK**.

Rola użytkownika zostanie usunięta.

Kojarzenie profili zasad z rolami

Możesz skojarzyć role użytkownika z profilami zasad. W tym przypadku reguła aktywacji dla tego profilu zasad jest oparta na roli: profil zasad staje się aktywny dla użytkownika, który posiada określoną rolę.

Na przykład, zasada zabrania wszelkich programów do nawigacji GPS na wszystkich urządzeniach w grupie administracyjnej. Program do nawigacji GPS jest wymagany tylko na jednym urządzeniu w grupie administracyjnej Użytkownicy—na urządzeniu, które należy do użytkownika zatrudnionego w charakterze kuriera. W tym przypadku możesz przypisać rolę „Kurier" do jego właściciela, a następnie utworzyć profil zasad zezwalający na uruchamianie programu do nawigacji GPS tylko na urządzeniach, których właściciele posiadają rolę „Kurier". Wszystkie pozostałe ustawienia zasady zostają zachowane. Tylko użytkownik z rolą „Kurier" będzie mógł uruchamiać program do nawigacji GPS. Później, jeśli innemu pracownikowi przypisano rolę „Kurier", nowy pracownik także może uruchomić program do nawigacji na urządzeniu należącym do organizacji. Uruchamianie programu do nawigacji GPS wciąż będzie zabronione na innych urządzeniach w tej samej grupie administracyjnej.

W celu skojarzenia roli z profilem zasad:

1. W menu głównym przejdź do **Użytkownicy i role** → **Role**.

2. Kliknij nazwę roli, którą chcesz skojarzyć z profilem zasad.

   Okno właściwości roli zostanie otwarte na wybranej zakładce **Ogólne**.

3. Wybierz zakładkę **Ustawienia** i przewiń w dół do sekcji **Zasady**.

4. Kliknij **Edytuj**.

5. W celu skojarzenia roli z:

   - **Istniejącym profilem zasad**—kliknij ikonę strzałki (>) obok nazwy żądanej zasady, a następnie zaznacz pole obok profilu, z którym chcesz skojarzyć rolę.

   - **Nowy profil zasad**:

     a. Zaznacz pole obok zasady, dla której chcesz utworzyć profil.

     b. Kliknij **Nowy profil zasad**.

     c. Określ nazwę dla nowego profilu i skonfiguruj ustawienia profilu.

     d. Kliknij przycisk **Zapisz**.

     e. Zaznacz pole obok nowego profilu.

6. Kliknij **Przypisz do roli**.

   Profil zostanie skojarzony z rolą i pojawi się we właściwościach roli. Profil jest stosowany automatycznie do dowolnego urządzenia, którego właścicielowi przypisano rolę.

Przydzielanie ról użytkownika do podrzędnych Serwerów administracyjnych

Domyślnie, listy ról użytkownika głównego i podrzędnego Serwera administracyjnego są niezależne. Możesz skonfigurować aplikację w taki sposób, aby automatycznie rozsyłała role użytkownika utworzone na głównym Serwerze administracyjnym do wszystkich podrzędnych Serwerów administracyjnych. Role użytkownika mogą także zostać rozesłane z podrzędnego Serwera administracyjnego na swoje własne podrzędne Serwery administracyjne.

W celu przesłania ról użytkownika z głównego Serwera administracyjnego na podrzędne Serwery administracyjne:

1. W menu głównym kliknij nazwę Serwera administracyjnego.

   Okno właściwości Serwera administracyjnego zostanie otwarte na zakładce **Ogólne**.

2. Przejdź do sekcji **Hierarchia Serwerów administracyjnych**.

3. Włącz opcję **Przekaż listę reguł do podrzędnych Serwerów administracyjnych**, a następnie kliknij przycisk **Zapisz**.

   Aplikacja kopiuje role użytkownika głównego Serwera administracyjnego na podrzędne Serwery administracyjne.

Jeśli opcja **Przekaż listę reguł do podrzędnych Serwerów administracyjnych** jest włączona, a role użytkownika są przesyłane, nie mogą być edytowane ani usuwane na podrzędnych Serwerach administracyjnych. Jeśli tworzysz nową rolę lub edytujesz już tę istniejącą na głównym Serwerze administracyjnym, zmiany są automatycznie kopiowane do podrzędnych Serwerów administracyjnych. Jeśli usuwasz rolę użytkownika na głównym Serwerze administracyjnym, ta rola pozostanie na podrzędnych Serwerach administracyjnych, ale może być edytowana lub zostać usunięta.

Role, które są przesyłane na podrzędny Serwer administracyjny z Serwera głównego, są wyświetlane z zielonymi znacznikami wyboru (✓). Nie możesz edytować tych ról na podrzędnym Serwerze administracyjnym.

Jeśli tworzysz rolę na głównym Serwerze administracyjnym i istnieje rola z tą samą nazwą na swoim podrzędnym Serwerze administracyjnym, nowa rola zostaje skopiowana do podrzędnego Serwera administracyjnego z indeksem dodanym do jego nazwy, na przykład: ~~1, ~~2 (indeks może być losowy).

Jeśli wyłączysz opcję **Przekaż listę reguł do podrzędnych Serwerów administracyjnych**, wszystkie role użytkownika pozostaną na podrzędnych Serwerach administracyjnych, ale staną się niezależne od tych na głównym Serwerze administracyjnym. Po tym, jak role użytkownika staną się niezależne, role użytkownika na podrzędnych Serwerach administracyjnych mogą być edytowane lub usuwane.

Zmiana hasła do konta

Hasło do konta lokalnego możesz zmienić na przykład wtedy, gdy użytkownik zapomni hasła do konta lokalnego lub w celu zaplanowanej zmiany hasła.

Zmiana hasła będzie obowiązywać nawet jeśli użytkownik nie zalogował się do konta. Możesz także zmienić hasło do lokalnego konta root.

To zadanie można wykonać tylko na urządzeniach z systemem Linux.

Aby zmienić hasło do konta lokalnego na określonych urządzeniach:

1. W menu głównym przejdź do **Zadania**.
2. Kliknij **Dodaj**.

   Zostanie uruchomiony Kreator tworzenia nowego zadania.
3. W polu **Typ zadania** wybierz opcję **Zmień hasło do konta (tylko Linux)**.
4. Wybierz jedną z następujących opcji:

   - **Przypisz zadanie do grupy administracyjnej**

     Zadanie jest przypisywane do urządzeń znajdujących się w grupie administracyjnej. Możesz określić jedną z istniejących grup lub utworzyć nową grupę.

     Na przykład, możesz chcieć użyć tej opcji do uruchomienia zadania wysyłania wiadomości do użytkowników, jeśli wiadomość jest specyficzna dla urządzeń znajdujących się w określonej grupie administracyjnej.

     Jeśli zadanie jest przypisane do grupy administracyjnej, zakładka **Zabezpieczenia** nie jest wyświetlana w oknie właściwości zadania, ponieważ zadania grupowe podlegają ustawieniom zabezpieczeń grup, do których się odnoszą.

- **Określ adresy urządzeń ręcznie lub zaimportuj adresy z listy**

  Możesz określić nazwy NetBIOS, nazwy DNS, adresy IP oraz podsieci IP urządzeń, do których chcesz przydzielić zadanie.

  Możesz użyć tej opcji do wykonania zadania dla określonej podsieci. Na przykład, możesz chcieć zainstalować pewną aplikację na urządzeniach księgowych lub przeskanować urządzenia w podsieci, która jest prawdopodobnie zainfekowana.

- **Przypisz zadanie do wyboru urządzeń**

  Zadanie jest przypisywane do urządzeń znajdujących się w wyborze urządzeń. Możesz określić jeden z istniejących wyborów.

  Na przykład, możesz chcieć użyć tej opcji do uruchomienia zadania na urządzeniach z określoną wersją systemu operacyjnego.

Dla określonych urządzeń tworzone jest zadanie *Zmień hasło do konta (tylko w przypadku systemu Linux)*. Jeśli wybrano opcję **Przypisz zadanie do grupy administracyjnej**, zadanie jest zadaniem grupowym.

5. W kroku **Zakres zadania** określ grupę administracyjną, urządzenia o określonych adresach lub wybór urządzeń.

   Dostępne ustawienia zależą od opcji wybranej w poprzednim kroku.

6. W kroku **Wprowadź nazwę użytkownika i nowe hasło** określ następujące ustawienia:

   - W polu **Nazwa konta** podaj nazwę konta, dla którego chcesz zmienić hasło.

   - W polu **Nowe hasło** podaj hasło, które zostanie ustawione dla konta podanego w poprzednim polu.

     Aby zobaczyć wprowadzony tajny klucz, kliknij i przytrzymaj przycisk **Pokaż**.

   - W razie potrzeby zaznacz pole wyboru **Ustaw jako hasło jednorazowe (użytkownik musi zmienić hasło po pierwszym zalogowaniu)**.

     - **Ustaw jako hasło jednorazowe (użytkownik musi zmienić hasło po pierwszym zalogowaniu)**

       Jeżeli to pole wyboru jest zaznaczone, użytkownik zostanie poproszony o ustawienie nowego hasła po pierwszym logowaniu.

       Jeśli to pole wyboru nie jest zaznaczone, użytkownik nie będzie proszony o ustawienie nowego hasła po pierwszym logowaniu.

       Domyślnie pole to nie jest zaznaczone.

7. Na etapie **Zakończ tworzenie zadania** kliknij przycisk **Zakończ**, aby utworzyć zadanie i zamknąć kreatora.

   Jeśli włączyłeś opcję **Otwórz szczegóły zadania po jego utworzeniu**, zostanie otwarte okno ustawień zadania. W tym oknie możesz sprawdzić parametry zadania, zmodyfikować je lub skonfigurować harmonogram uruchamiania zadania, jeśli to konieczne.

8. Na liście zadań wybierz utworzone zadanie, a następnie kliknij przycisk **Start**.

   Ewentualnie poczekaj na uruchomienie zadania zgodnie z harmonogramem określonym w ustawieniach zadania.

Po zakończeniu zadania zmiany hasła do konta hasło dla określonego konta lokalnego na określonych urządzeniach zostanie zmienione.

Aby zapewnić poprawne działanie zadań zmiany hasła do konta, opcja SELinux musi być wyłączona na urządzeniu użytkownika.

Wycofanie uprawnień lokalnego administratora

Możesz wycofać uprawnienia administratora lokalnego z kont. Zapewnia to dodatkową warstwę kontroli nad kontami użytkowników. Można na przykład wycofać uprawnienia administratora lokalnego po zakończeniu jednorazowego przypisania.

Po uruchomieniu tego zadania sprawdzane jest określone konto lokalne, czy należy do lokalnych grup administratorów. Grupy te są zdefiniowane w ustawieniach zasad Agenta sieciowego. Możesz dostosować listę lokalnych grup administratorów w ustawieniach zasad Agenta sieciowego. Możesz także sprawdzić listę kont użytkowników uprzywilejowanych, korzystając z **Raport o uprzywilejowanych użytkownikach urządzenia (tylko Linux)**.

To zadanie można wykonać tylko na urządzeniach z systemem Linux.

Aby wycofać uprawnienia administratora lokalnego z określonych urządzeń:

1. W menu głównym przejdź do **Zadania**.
2. Kliknij **Dodaj**.

   Zostanie uruchomiony Kreator tworzenia nowego zadania.
3. W polu **Typ zadania** wybierz opcję **Odbierz uprawnienia administratora lokalnego (tylko Linux)**.
4. Wybierz jedną z następujących opcji:

   - **Przypisz zadanie do grupy administracyjnej**

     Zadanie jest przypisywane do urządzeń znajdujących się w grupie administracyjnej. Możesz określić jedną z istniejących grup lub utworzyć nową grupę.

     Na przykład, możesz chcieć użyć tej opcji do uruchomienia zadania wysyłania wiadomości do użytkowników, jeśli wiadomość jest specyficzna dla urządzeń znajdujących się w określonej grupie administracyjnej.

     Jeśli zadanie jest przypisane do grupy administracyjnej, zakładka **Zabezpieczenia** nie jest wyświetlana w oknie właściwości zadania, ponieważ zadania grupowe podlegają ustawieniom zabezpieczeń grup, do których się odnoszą.

   - **Określ adresy urządzeń ręcznie lub zaimportuj adresy z listy**

     Możesz określić nazwy NetBIOS, nazwy DNS, adresy IP oraz podsieci IP urządzeń, do których chcesz przydzielić zadanie.

     Możesz użyć tej opcji do wykonania zadania dla określonej podsieci. Na przykład, możesz chcieć zainstalować pewną aplikację na urządzeniach księgowych lub przeskanować urządzenia w podsieci, która jest prawdopodobnie zainfekowana.

   - **Przypisz zadanie do wyboru urządzeń**

     Zadanie jest przypisywane do urządzeń znajdujących się w wyborze urządzeń. Możesz określić jeden z istniejących wyborów.

     Na przykład, możesz chcieć użyć tej opcji do uruchomienia zadania na urządzeniach z określoną wersją systemu operacyjnego.

Dla określonych urządzeń tworzone jest zadanie *Odbierz uprawnienia administratora lokalnego (tylko w przypadku systemu Linux)*. Jeśli wybrano opcję **Przypisz zadanie do grupy administracyjnej**, zadanie jest zadaniem grupowym.

5. W kroku **Zakres zadania** określ grupę administracyjną, urządzenia o określonych adresach lub wybór urządzeń.

   Dostępne ustawienia zależą od opcji wybranej w poprzednim kroku.

6. W tym kroku kreatora należy ustawić następujące ustawienia:

   - W grupie ustawień **Tryb pracy** wybierz tryb pracy:

     - **Cofnij uprawnienia administratora lokalnego wymienionym kontom**

       Jeśli ta opcja zostanie wybrana, uprawnienia administratora lokalnego zostaną wycofane z określonych kont lokalnych.

       Domyślnie opcja ta jest zaznaczona.

     - **Wyklucz wymienione konta z możliwości cofnięcia uprawnień administratora lokalnego**

       Jeśli ta opcja zostanie wybrana, uprawnienia administratora lokalnego zostaną odebrane wszystkim kontom lokalnym, z wyjątkiem określonych.

       Domyślnie ta opcja nie jest zaznaczona.

   - Określ konta lokalne:

     - Kliknij **Dodaj**.

     - W otwartym oknie wykonaj następujące czynności:

       - W polu **Nazwa konta** podaj nazwę nowego zadania.

       - Wybierz działanie w grupie ustawień **Działanie na koncie** (dostępnej tylko w przypadku zaznaczenia opcji **Cofnij uprawnienia administratora lokalnego wymienionym kontom**).

       - **Zachowaj konto**

         Jeżeli ta opcja jest zaznaczona, konto lokalne nie zostanie usunięte po odebraniu uprawnień administratora lokalnego.

         Domyślnie opcja ta jest zaznaczona.

       - **Usuń konto**

         W przypadku wybrania tej opcji konto lokalne zostanie usunięte niezależnie od tego, czy posiada uprawnienia administratora lokalnego.

         Domyślnie ta opcja nie jest zaznaczona.

7. Na etapie **Zakończ tworzenie zadania** kliknij przycisk **Zakończ**, aby utworzyć zadanie i zamknąć kreatora.

   Jeśli włączyłeś opcję **Otwórz szczegóły zadania po jego utworzeniu**, zostanie otwarte okno ustawień zadania. W tym oknie możesz sprawdzić parametry zadania, zmodyfikować je lub skonfigurować harmonogram uruchamiania zadania, jeśli to konieczne.

8. Na liście zadań wybierz utworzone zadanie, a następnie kliknij przycisk **Start**.

   Ewentualnie poczekaj na uruchomienie zadania zgodnie z harmonogramem określonym w ustawieniach zadania.

Po zakończeniu zadania wycofania uprawnień administratora lokalnego uprawnienia administratora lokalnego zostaną wycofane z określonych kont lokalnych na określonych urządzeniach.

Konfigurowanie uwierzytelniania domeny Kerberos

Kaspersky Security Center Linux umożliwia korzystanie z uwierzytelniania domeny przy użyciu protokołu Kerberos. Użycie uwierzytelniania domeny umożliwia użytkownikowi włączenie bezpiecznego uwierzytelniania w Kaspersky Security Center Web Console bez konieczności ponownego wprowadzania hasła w sieci firmowej (technologia pojedynczego logowania).

Najpierw musisz skonfigurować kontroler domeny do korzystania z protokołu Kerberos i wygenerować plik tabeli kluczy. Aby uzyskać więcej informacji, zapoznaj się z dokumentacją kontrolera domeny.

Protokół SCRIL (do logowania interaktywnego wymagana jest karta inteligentna) jest obsługiwany przez usługę Microsoft Active Directory.

Generowanie pliku tabeli kluczy dla FreeIPA i AldPro

Aby wygenerować plik tabeli kluczy:

1. Utwórz konto użytkownika, za pomocą którego IAM będzie uzyskiwać dostęp do kontrolera domeny.
2. Jeżeli serwer administracyjny znajduje się poza domeną FreeIPA/AldPro, dodaj wpis rekordu DNS i wpis hosta:

   ```
   ipa dnsrecord-add <zoneName> <recordName> --a-rec < adres IP Serwera administracyjnego >
   ipa host-add --password=<password> < adres hosta Serwera administracyjnego >
   ```

3. Określ typ PAC podczas tworzenia usługi HTTP dla Serwera administracyjnego:

   ```
   ipa service-add HTTP/< FQDN hosta Serwera administracyjnego >@< DOMENA WYPISANA WIELKIMI
   LITERAMI > --ok-to-auth-as-delegate=true --pac-type PAD
   ```

4. Określ konto użytkownika do uwierzytelniania:

   ```
   ipa service-allow-retrieve-keytab HTTP/< adres hosta Serwera
   administracyjnego >@< DOMENA WYPISANA WIELKIMI LITERAMI > --user=<user>
   ```

5. Eksportuj plik tabeli kluczy:

   ```
   ipa-getkeytab -s < adres kontrolera domeny > -p HTTP/< adres hosta Serwera
   administracyjnego >@< DOMENA WYPISANA WIELKIMI LITERAMI > -k /tmp/h.keytab
   ```

Generowanie pliku tabeli kluczy dla usługi Microsoft Active Directory

Aby wygenerować plik tabeli kluczy:

1. Utwórz konto użytkownika, które będzie używane przez IAM do komunikacji z kontrolerem domeny.

2. Włącz następujące opcje dla konta użytkownika:

   - **Użytkownik nie może zmienić hasła**

   - **Szyfrowanie Kerberos AES 256-bitowe**

   Możesz włączyć opcję **Hasło nigdy nie wygasa**, aby uniknąć ponownego generowania pliku tabeli kluczy po każdym wygaśnięciu hasła.

3. Dodaj główną nazwę usługi (SPN) do konta użytkownika:

   ```
   setspn -S HTTP/< FQDN hosta Serwera administracyjnego > < DOMENA WYPISANA WIELKIMI
   LITERAMI >\<user>
   ```

4. Eksportuj plik tabeli kluczy:

   ```
   ktpass -out C:\<folder>\< nazwa pliku tabeli kluczy > -princ HTTP/< FQDN hosta Serwera
   administracyjnego >@< DOMENA WYPISANA WIELKIMI LITERAMI > -mapuser < DOMENA WYPISANA
   WIELKIMI LITERAMI >\<user> -crypto AES256-SHA1 -ptype KRB5_NT_PRINCIPAL -pass
   <password> -mapop set
   ```

Generowanie pliku tabeli kluczy dla Samba

Aby wygenerować plik tabeli kluczy:

1. Utwórz konto użytkownika, które będzie używane przez IAM do komunikacji z kontrolerem domeny:

   ```
   samba-tool user add <user>
   ```

2. Dodaj nazwę SPN do konta użytkownika:

   ```
   samba-tool spn add HTTP/< FQDN hosta Serwera administracyjnego > <user>
   ```

3. Eksportuj plik tabeli kluczy:

   ```
   samba-tool domain exportkeytab /tmp/file.keytab --principal=HTTP/< FQDN hosta Serwera
   administracyjnego >
   ```

Konfigurowanie uwierzytelniania domeny Kerberos

Aby włączyć uwierzytelnianie domeny Kerberos:

1. Wykonaj przeszukiwanie kontrolera domeny.
2. W menu głównym przejdź do **Ustawienia** → **Pojedyncze logowanie**.
3. Włącz opcję **Uwierzytelnianie Kerberos**.
4. Prześlij plik tabeli kluczy.
5. Przypisz rolę użytkownikom domeny, która daje dostęp do Kaspersky Security Center Web Console.

   Uwierzytelnianie domeny Kerberos jest włączone dla użytkowników domeny.

Aktualizowanie baz danych i aplikacji Kaspersky

Ta sekcja opisuje kroki, które musisz podjąć, aby regularnie aktualizować następujące elementy:

- Baz danych i modułów oprogramowania firmy Kaspersky
- Zainstalowane aplikacje Kaspersky, w tym składniki Kaspersky Security Center Linux i aplikacje zabezpieczające

Aktualizuje funkcje (obejmuje aktualizacje sygnatur wirusów oraz aktualizacje bazy kodu), przy czym funkcja KSN może nie być dostępna w oprogramowaniu na terytorium Stanów Zjednoczonych.

Scenariusz: Regularne aktualizowanie baz danych i aplikacji Kaspersky

Ta sekcja oferuje scenariusz regularnego aktualizowania baz danych, modułów i aplikacji firmy Kaspersky. Po zakończeniu Konfigurowania scenariusza ochrony sieci, musisz zachować niezawodność systemu ochrony, aby upewnić się, że Serwery administracyjne i zarządzane urządzenia są chronione przed różnymi zagrożeniami, w tym wirusami, atakami sieciowymi i atakami phishingowymi.

Aktualność ochrony sieci jest zapewniana przez regularne aktualizacje:

- Baz danych i modułów oprogramowania firmy Kaspersky
- Zainstalowane aplikacje Kaspersky, w tym składniki Kaspersky Security Center Linux i aplikacje zabezpieczające

Po zakończeniu tego scenariusza, możesz być pewny, że:

- Twoja sieć jest chroniona przez najaktualniejsze oprogramowanie firmy Kaspersky, w tym komponenty Kaspersky Security Center Linux i aplikacje zabezpieczające.
- Antywirusowe bazy danych i inne bazy danych Kaspersky krytyczne dla bezpieczeństwa sieci są zawsze aktualne.

Wymagania wstępne

Zarządzane urządzenia muszą mieć połączenie z Serwerem administracyjnym. Jeśli nie mają połączenia, rozważ ręczne zaktualizowanie baz danych i modułów oprogramowania Kaspersky lub bezpośrednio z serwerów aktualizacji Kaspersky.

Serwer administracyjny musi mieć połączenie z Internetem.

Przed rozpoczęciem upewnij się, że:

1. Wdrożono aplikacje zabezpieczające Kaspersky na zarządzanych urządzeniach zgodnie ze scenariuszem wdrażania aplikacji Kaspersky poprzez Kaspersky Security Center Web Console.

2. Utworzyłeś i skonfigurowałeś wszystkie wymagane zasady, profile zasad i zadania zgodnie ze scenariuszem konfigurowania ochrony sieci.

3. Przydzieliłeś odpowiednią liczbę punktów dystrybucji zgodnie z liczbą zarządzanych urządzeń i topologią sieci.

Aktualizowanie baz danych i aplikacji Kaspersky odbywa się w etapach:

1. **Wybranie schematu aktualizacji**

   Istnieje kilka schematów, których można użyć do zainstalowania aktualizacji aplikacji zabezpieczających. Wybierz schemat lub kilka schematów, które najlepiej spełniają wymagania Twojej sieci.

2. **Tworzenie zadania pobierania aktualizacji do repozytorium Serwera administracyjnego**

   To zadanie jest tworzone automatycznie przez Kreator wstępnej konfiguracji Kaspersky Security Center. Jeśli nie uruchamiałeś kreatora, utwórz zadanie teraz.

   To zadanie jest wymagane w celu pobrania aktualizacji z serwerów aktualizacji Kaspersky do repozytorium Serwera administracyjnego, a także do zaktualizowania baz danych i modułów oprogramowania Kaspersky dla Kaspersky Security Center Linux. Po pobraniu uaktualnień, mogą one zostać przesłane na zarządzane urządzenia.

   Jeśli w Twojej sieci są przypisane punkty dystrybucji, uaktualnienia są automatycznie pobierane z repozytorium Serwera administracyjnego do repozytoriów punktów dystrybucji. W tym przypadku zarządzane urządzenia, znajdujące się w obszarze punktu dystrybucji, pobierają uaktualnienia z repozytorium punktu dystrybucji zamiast repozytorium Serwera administracyjnego.

   Dostępne instrukcje: Tworzenie zadania pobierania aktualizacji do repozytorium Serwera administracyjnego

3. **Tworzenie zadania pobierania aktualizacji do repozytoriów punktów dystrybucji (opcjonalne)**

   Domyślnie, uaktualnienia są pobierane do punktów dystrybucji z Serwera administracyjnego. Możesz skonfigurować Kaspersky Security Center Linux do pobierania uaktualnień do punktów dystrybucji bezpośrednio z serwerów aktualizacji Kaspersky. Pobranie do repozytoriów punktów dystrybucji jest preferowane, jeśli ruch sieciowy pomiędzy Serwerem administracyjnym a punktami dystrybucji jest droższy niż ruch sieciowy pomiędzy punktami dystrybucji a serwerami aktualizacji Kaspersky lub jeśli Twój Serwer administracyjny nie ma dostępu do internetu.

   Jeśli do Twojej sieci są przypisane punkty dystrybucji i utworzone jest zadanie *Pobierz aktualizacje do repozytoriów punktów dystrybucji*, punkty dystrybucji pobiorą uaktualnienia z serwerów aktualizacji Kaspersky, a nie z repozytorium Serwera administracyjnego.

   Jak to zrobić: Tworzenie zadania pobierania aktualizacji do repozytoriów punktów dystrybucji

4. **Konfigurowanie punktów dystrybucji**

   Jeśli w Twojej sieci są przypisane punkty dystrybucji, upewnij się, że opcja **Włączone** jest włączona we właściwościach wszystkich wymaganych punktów dystrybucji. Jeśli ta opcja jest włączona dla punktu dystrybucji, urządzenia znajdujące się w obszarze punktu dystrybucji pobierają uaktualnienia z repozytorium Serwera administracyjnego.

5. **Optymalizacja procesu aktualizacji przy użyciu plików diff (opcjonalnie)**

   Możesz zoptymalizować ruch pomiędzy Serwerem administracyjnym a zarządzanymi urządzeniami przy użyciu plików diff. Jeśli ta funkcja jest włączona, Serwer administracyjny lub punkt dystrybucji pobierze pliki diff zamiast całych plików baz danych lub modułów Kaspersky. Plik diff opisuje różnice między dwoma wersjami pliku bazy danych lub modułu programu. Dlatego też plik diff zajmuje mniej miejsca niż cały plik. Spowoduje to zmniejszenie ruchu sieciowego między Serwerem administracyjnym lub punktami dystrybucji a zarządzanymi urządzeniami. Aby użyć tej funkcji, włącz opcję **Pobierz pliki diff** we właściwościach zadania *Pobierz aktualizacje do repozytorium Serwera administracyjnego* i/lub zadania *Pobierz aktualizacje do repozytoriów punktów dystrybucji*.

   Dostępne instrukcje: Używanie plików diff do aktualizowania baz danych i modułów aplikacji Kaspersky

6. **Konfigurowanie automatycznej instalacji uaktualnień dla aplikacji zabezpieczających**

   Utwórz zadania *Aktualizacja* dla zarządzanych aplikacji, aby zapewnić najnowsze aktualizacje aplikacji, modułów oprogramowania i baz danych Kaspersky, w tym antywirusowych baz danych. Aby zapewnić dostarczanie aktualizacji na czas, zalecane jest włączenie opcji **Po pobraniu nowych uaktualnień do repozytorium** podczas konfigurowania terminarza zadania.

   Jeśli aktualizacja wymaga przejrzenia i zaakceptowania warunków Umowy licencyjnej użytkownika końcowego, następnie musisz najpierw zaakceptować warunki. Dopiero wtedy aktualizacja będzie mogła zostać przesłana na zarządzane urządzenia.

7. **Zatwierdzanie i odrzucanie aktualizacji zarządzanych aplikacji Kaspersky**

   Domyślnie pobrane aktualizacje oprogramowania posiadają stan *Niezdefiniowane*. Możesz zmienić stan na *Zatwierdzone* lub *Odrzucone*. Zatwierdzone aktualizacje są zawsze instalowane. Jeśli aktualizacja zarządzanej aplikacji Kaspersky wymaga przejrzenia i zaakceptowania warunków Umowy licencyjnej, następnie musisz najpierw zaakceptować warunki. Dopiero wtedy aktualizacja będzie mogła zostać przesłana na zarządzane urządzenia. Aktualizacje, dla których ustawiłeś stan *Odrzucone*, nie zostaną zainstalowane na urządzeniach. Jeśli odrzucona aktualizacja dla aplikacji zarządzanej została wcześniej zainstalowana, Kaspersky Security Center Linux spróbuje odinstalować aktualizację ze wszystkich urządzeń.

   Zatwierdzanie i odrzucanie aktualizacji jest dostępne tylko w przypadku Agenta sieciowego i aplikacji zarządzanych Kaspersky zainstalowanych na urządzeniach klienckich z systemem Windows i Linux. Bezproblemowa aktualizacja Serwera administracyjnego, Kaspersky Security Center Web Console i webowych wtyczek administracyjnych nie jest obsługiwana.

   Instrukcje: zatwierdzanie i odrzucanie aktualizacji oprogramowania

   Czasami po aktualizacji Agenta sieciowego może zostać wyświetlony monit o ponowne uruchomienie zarządzanych urządzeń. Jeśli zostanie wyświetlone powiadomienie o konieczności ponownego uruchomienia, kliknij łącze **Wyświetl urządzenia** w powiadomieniu, zaznacz pola wyboru obok urządzeń, które mają zostać ponownie uruchomione, a następnie kliknij przycisk **Uruchom ponownie**, aby zakończyć aktualizację Agenta sieciowego.

Wyniki

Po zakończeniu scenariusza Kaspersky Security Center Linux jest skonfigurowany do aktualizowania baz danych Kaspersky po pobraniu aktualizacji do repozytorium Serwera administracyjnego. Możesz przejść do monitorowania stanu sieci.

Informacje o aktualizowaniu baz danych, modułów i aplikacji Kaspersky

W celu upewnienia się, że ochrona Serwerów administracyjnych i zarządzanych urządzeń jest aktualna, w odpowiednim czasie należy dostarczać aktualizacje:

- Baz danych i modułów oprogramowania firmy Kaspersky

  Przed pobraniem baz danych i modułów oprogramowania Kaspersky oprogramowanie Kaspersky Security Center Linux sprawdza, czy serwery Kaspersky są dostępne. Jeżeli dostęp do serwerów za pomocą systemowego DNS nie jest możliwy, aplikacja korzysta z publicznych serwerów DNS. Jest to konieczne, aby zapewnić aktualizację antywirusowych baz danych oraz zachować poziom bezpieczeństwa zarządzanych urządzeń.

- Zainstalowane aplikacje Kaspersky, w tym składniki Kaspersky Security Center Linux i aplikacje zabezpieczające

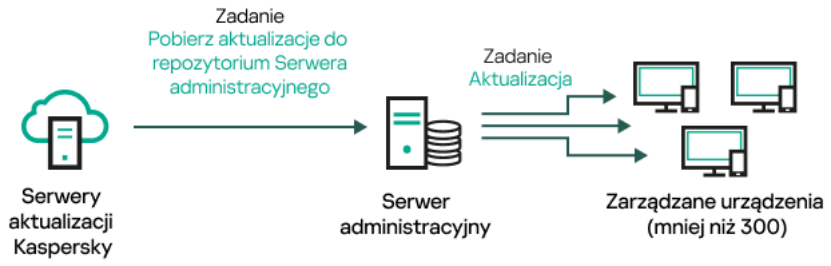
  Kaspersky Security Center Linux umożliwia automatyczną aktualizację aplikacji Agenta sieciowego i Kaspersky zainstalowanych na urządzeniach klienckich z systemem Windows i Linux. Bezproblemowa aktualizacja Serwera administracyjnego, Kaspersky Security Center Web Console i webowych wtyczek administracyjnych nie jest obsługiwana. Aby zaktualizować aplikacje, pobierz najnowsze wersje aplikacji z witryny internetowej Kaspersky, a następnie zainstaluj je ręcznie.

W zależności od konfiguracji sieci, możesz użyć następujących schematów pobierania i rozsyłania żądanych aktualizacji na zarządzane urządzenia:

- Za pomocą jednego zadania: *Pobierz aktualizacje do repozytorium Serwera administracyjnego*
- Używanie dwóch zadań:
  - Zadanie *Pobierz aktualizacje do repozytorium Serwera administracyjnego*
  - Zadanie *Pobierz aktualizacje do repozytoriów punktów dystrybucji*
- Ręcznie poprzez folder lokalny, folder współdzielony lub serwer FTP
- Bezpośrednio z serwerów aktualizacji Kaspersky do Kaspersky Endpoint Security na zarządzanych urządzeniach
- Poprzez folder lokalny lub sieciowy, jeśli Serwer administracyjny nie ma połączenia z Internetem

Używanie zadania Pobierz aktualizacje do repozytorium Serwera administracyjnego

W tym schemacie Kaspersky Security Center Linux pobiera aktualizacje za pośrednictwem zadania *Pobierz aktualizacje do repozytorium Serwera administracyjnego*. W małych sieciach, które zawierają mniej niż 300 zarządzanych urządzeń w jednym segmencie sieci lub mniej niż 10 zarządzanych urządzeń w każdym segmencie sieci, aktualizacje są rozsyłane na zarządzane urządzenia bezpośrednio z repozytorium Serwera administracyjnego (patrz rysunek poniżej).



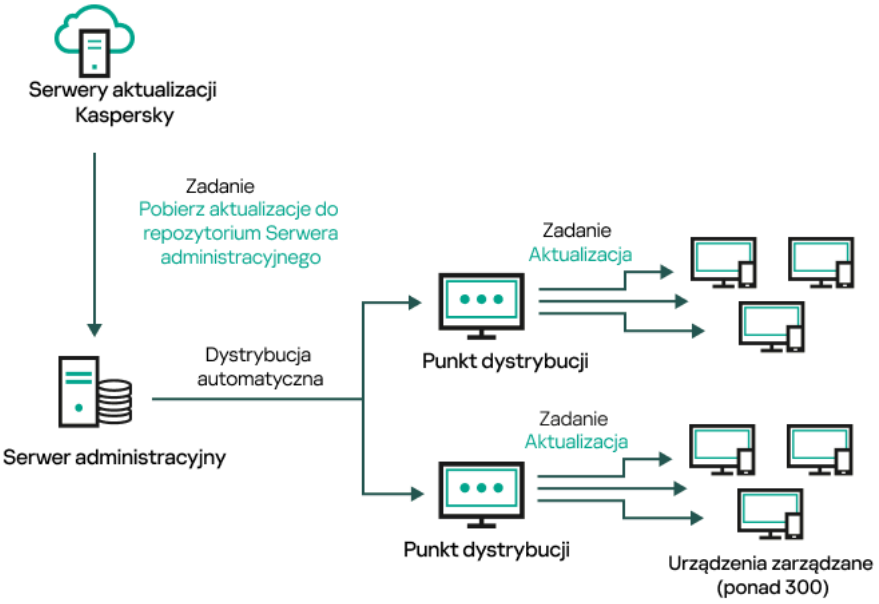
Aktualizowanie przy użyciu zadania *Pobierz aktualizacje do repozytorium Serwera administracyjnego* bez punktów dystrybucji

Jako źródło aktualizacji możesz użyć nie tylko serwerów aktualizacji Kaspersky, ale także folderu lokalnego lub sieciowego.

Domyślnie, Serwer administracyjny komunikuje się z serwerami aktualizacji Kaspersky i pobiera uaktualnienia, korzystając z protokołu HTTPS. Możesz skonfigurować Serwer administracyjny, aby używał protokołu HTTP zamiast HTTPS.

Jeśli sieć zawiera 300 zarządzanych urządzeń lub więcej w jednym segmencie sieci lub jeśli sieć zawiera kilka segmentów sieci z ponad 9 zarządzanymi urządzeniami w każdym segmencie sieci, zalecane jest użycie punktów dystrybucji do przesyłania aktualizacji na zarządzane urządzenia (patrz rysunek poniżej). Punkty dystrybucji zmniejszają obciążenie na Serwerze administracyjnym i optymalizują ruch sieciowy między Serwerem administracyjnym i zarządzanymi urządzeniami. Możesz obliczyć liczbę i konfigurację punktów dystrybucji wymaganych dla Twojej sieci.

W tym schemacie, uaktualnienia są automatycznie pobierane z repozytorium Serwera administracyjnego do repozytoriów punktów dystrybucji. Zarządzane urządzenia, znajdujące się w obszarze punktu dystrybucji, pobierają uaktualnienia z repozytorium punktu dystrybucji zamiast repozytorium Serwera administracyjnego.



Aktualizowanie przy użyciu zadania *Pobierz aktualizacje do repozytorium Serwera administracyjnego* z punktami dystrybucji

Po zakończeniu zadania *Pobierz aktualizacje do repozytorium Serwera administracyjnego* aktualizacje baz danych Kaspersky i modułów oprogramowania dla Kaspersky Endpoint Security są pobierane do repozytorium Serwera administracyjnego. Te aktualizacje są instalowane poprzez zadanie *Aktualizacja* dla Kaspersky Endpoint Security.

Zadanie *Pobierz uaktualnienia do repozytorium Serwera administracyjnego* nie jest dostępne na wirtualnych Serwerach administracyjnych. Repozytorium wirtualnego Serwera administracyjnego wyświetla uaktualnienia pobrane na główny Serwer administracyjny.

Możesz skonfigurować sprawdzanie aktualizacji pod kątem łatwości obsługi i błędów na zestawie urządzeń testowych. Jeśli weryfikacja zostanie zakończona pomyślnie, aktualizacje będą rozsyłane na inne zarządzane urządzenia.

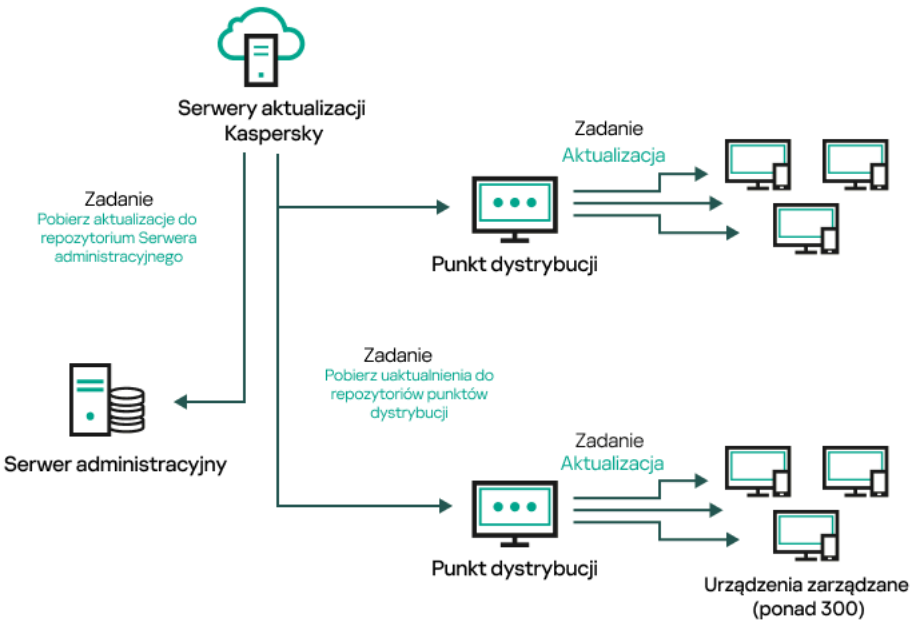
Każda aplikacja Kaspersky żąda wymaganych aktualizacji z Serwera administracyjnego. Serwer administracyjny gromadzi te żądania i pobiera tylko te uaktualnienia, które zostały zażądane przez aplikację. Dzięki temu te same uaktualnienia nie są pobierane kilka razy, a niepotrzebne uaktualnienia nie są pobierane wcale. Podczas wykonywania zadania *Pobierz aktualizacje do repozytorium Serwera administracyjnego*, Serwer administracyjny automatycznie wysyła następujące informacje do serwerów aktualizacji Kaspersky w celu zapewnienia pobrania najnowszych wersji baz danych i modułów aplikacji Kaspersky:

- Identyfikator i wersja aplikacji
- Identyfikator instalacji aplikacji
- Identyfikator aktywnego klucza
- ID uruchamiania zadania *Pobierz uaktualnienia do repozytorium Serwera administracyjnego*

Żadna z przesyłanych informacji nie zawiera danych osobowych ani innych poufnych danych. Firma AO Kaspersky Lab chroni informacje zgodnie z wymogami wynikającymi z przepisów prawa.

Używanie dwóch zadań: zadanie Pobierz aktualizacje do repozytorium Serwera administracyjnego oraz zadanie Pobierz aktualizacje do repozytoriów punktów dystrybucji

Możesz pobrać aktualizacje do repozytoriów punktów dystrybucji bezpośrednio z serwerów aktualizacji Kaspersky zamiast repozytorium Serwera administracyjnego, a następnie rozesłać aktualizacje na zarządzane urządzenia (patrz rysunek poniżej). Pobranie do repozytoriów punktów dystrybucji jest preferowane, jeśli ruch sieciowy pomiędzy Serwerem administracyjnym a punktami dystrybucji jest droższy niż ruch sieciowy pomiędzy punktami dystrybucji a serwerami aktualizacji Kaspersky lub jeśli Twój Serwer administracyjny nie ma dostępu do internetu.



Aktualizowanie przy użyciu zadania *Pobierz aktualizacje do repozytorium Serwera administracyjnego* oraz zadania *Pobierz aktualizacje do repozytoriów punktów dystrybucji*

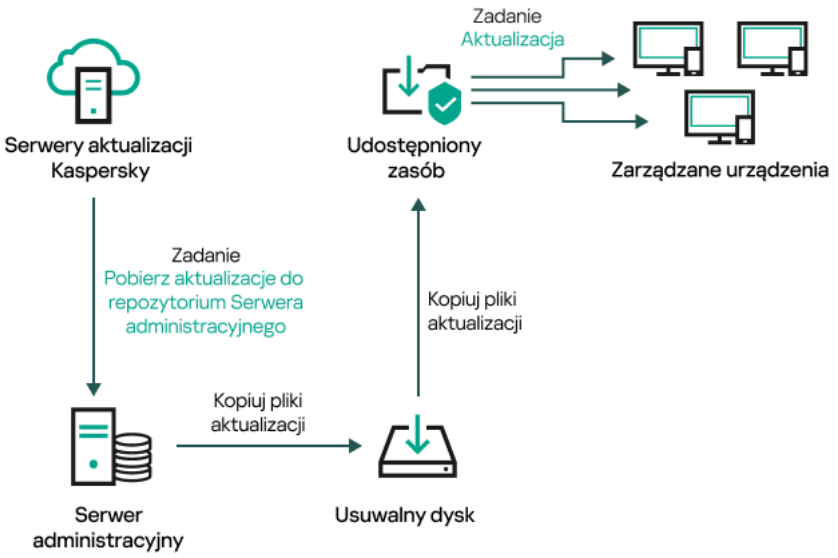
Domyślnie, Serwer administracyjny i punkty dystrybucji komunikują się z serwerami aktualizacji Kaspersky i pobierają uaktualnienia, korzystając z protokołu HTTPS. Możesz skonfigurować Serwer administracyjny i/lub punkty dystrybucji do używania protokołu HTTP zamiast HTTPS.

Aby zaimplementować ten schemat, utwórz zadanie *Pobierz aktualizacje do repozytoriów punktów dystrybucji* jako dodatek do zadania *Pobierz aktualizacje do repozytorium Serwera administracyjnego*. Po pobraniu przez punkty dystrybucji aktualizacji z serwerów aktualizacji Kaspersky, a nie z repozytorium Serwera administracyjnego.

Zadanie *Pobierz aktualizacje do repozytorium Serwera administracyjnego* jest także wymagane dla tego schematu, ponieważ to zadanie jest używane do pobrania baz danych i modułów Kaspersky dla Kaspersky Security Center Linux.

Ręcznie poprzez folder lokalny, folder współdzielony lub serwer FTP

Jeśli urządzenia klienckie nie mają połączenia z Serwerem administracyjnym, możesz użyć folderu lokalnego lub zasobu współdzielonego jako źródła dla aktualizacji baz danych, modułów i aplikacji Kaspersky. W tym schemacie możesz skopiować wymagane aktualizacje z repozytorium Serwera administracyjnego na dysk wymienny, a następnie skopiować aktualizacje do folderu lokalnego lub zasobu współdzielonego, określonego jako źródło uaktualnień w ustawieniach Kaspersky Endpoint Security (patrz rysunek poniżej).



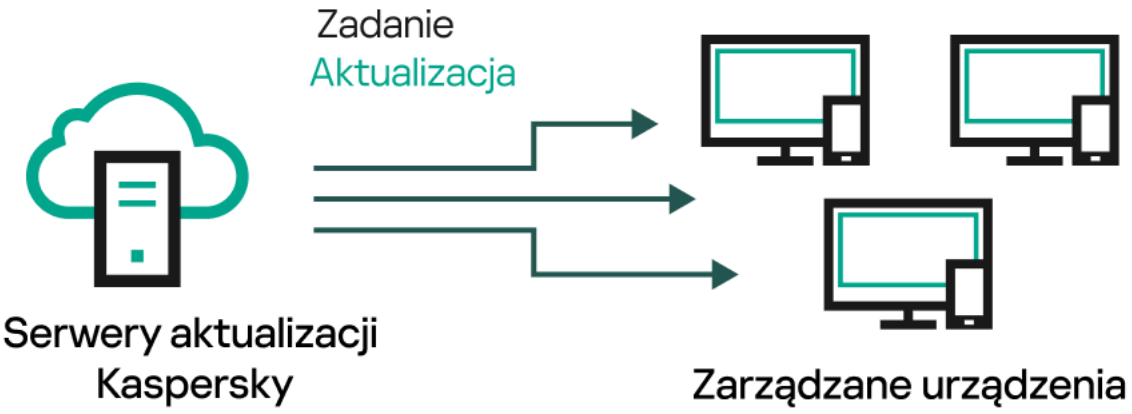
Aktualizowanie poprzez folder lokalny, folder współdzielony lub serwer FTP

Aby uzyskać więcej informacji na temat źródeł aktualizacji w Kaspersky Endpoint Security, zobacz następujące Pomoce:

- Pomoc Kaspersky Endpoint Security for Linux
- Pomoc Kaspersky Endpoint Security for Windows

Bezpośrednio z serwerów aktualizacji Kaspersky do Kaspersky Endpoint Security na zarządzanych urządzeniach

Na zarządzanych urządzeniach możesz skonfigurować Kaspersky Endpoint Security w celu pobierania aktualizacji bezpośrednio z serwerów aktualizacji Kaspersky (patrz rysunek poniżej).



Aktualizowanie aplikacji zabezpieczających bezpośrednio z serwerów aktualizacji Kaspersky

W tym schemacie aplikacja zabezpieczająca nie używa repozytoriów zapewnianych przez Kaspersky Security Center Linux. Aby pobierać aktualizacje bezpośrednio z serwerów aktualizacji Kaspersky, określ serwery aktualizacji Kaspersky jako źródło aktualizacji w aplikacji zabezpieczającej. Aby uzyskać więcej informacji na temat tych ustawień, zobacz następujące Pomoce:

- Pomoc Kaspersky Endpoint Security for Linux
- Pomoc Kaspersky Endpoint Security for Windows

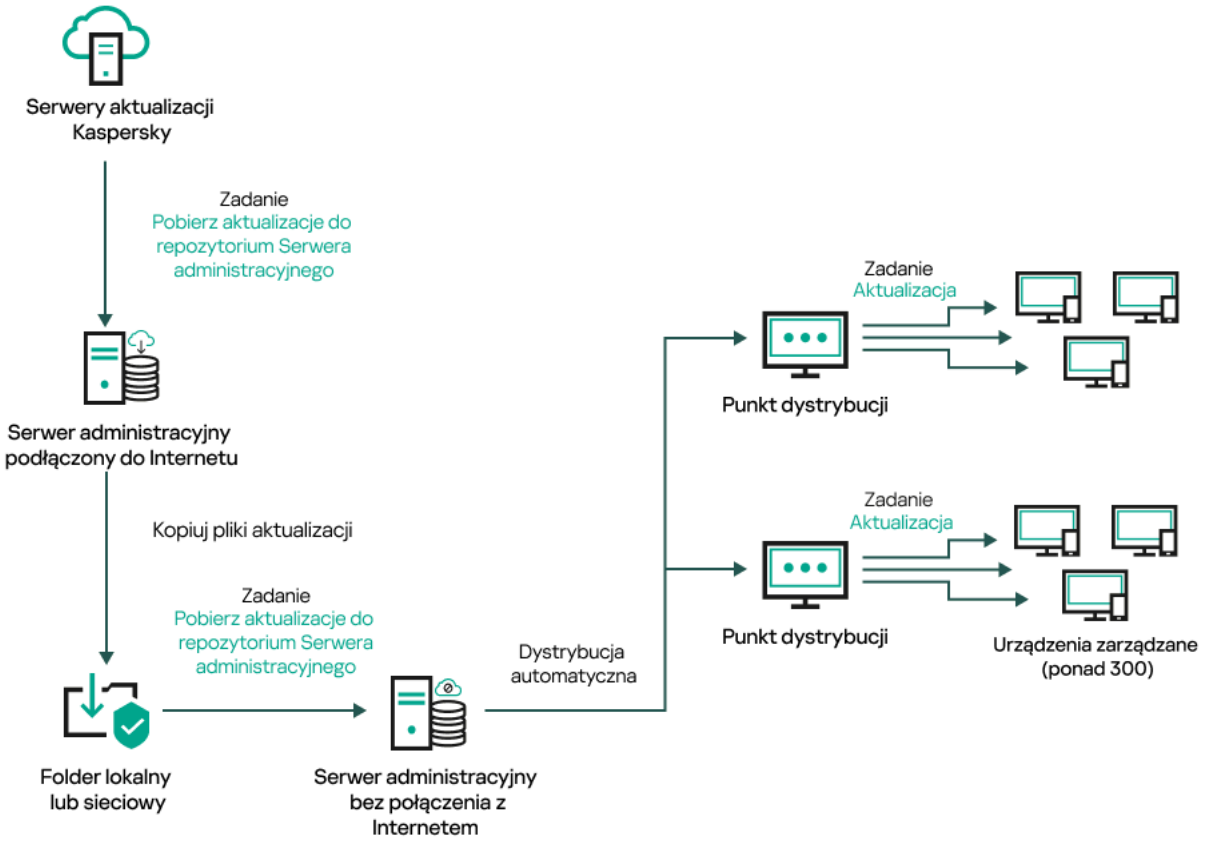
Poprzez folder lokalny lub sieciowy, jeśli Serwer administracyjny nie ma połączenia z Internetem

Jeżeli Serwer administracyjny nie ma połączenia z Internetem, możesz skonfigurować zadanie *Pobierz aktualizacje do repozytorium Serwera administracyjnego*, aby pobierać uaktualnienia z folderu lokalnego lub sieciowego. W takim przypadku należy od czasu do czasu kopiować wymagane pliki aktualizacji do określonego folderu. Na przykład możesz skopiować wymagane pliki aktualizacji z jednego z następujących źródeł:

- Serwer administracyjny z połączeniem internetowym (patrz rysunek poniżej)

  Ponieważ serwer administracyjny pobiera tylko aktualizacje wymagane przez aplikacje zabezpieczające, zestawy aplikacji zabezpieczających zarządzanych przez serwery administracyjne — ten, który ma połączenie z Internetem i ten, który go nie ma — muszą być zgodne.

  Jeżeli Serwer administracyjny, którego używasz do pobierania uaktualnień, ma wersję 13.2 lub wcześniejszą, otwórz właściwości zadania *Pobierz aktualizacje do repozytorium Serwera administracyjnego*, a następnie włącz opcję **Pobierz aktualizacje za pomocą starego schematu**.



Aktualizacja przez folder lokalny lub sieciowy, jeśli Serwer administracyjny nie ma połączenia z Internetem

- Kaspersky Update Utility

  Ponieważ narzędzie to wykorzystuje stary schemat do pobierania uaktualnień, otwórz właściwości zadania *Pobierz aktualizacje do repozytorium Serwera administracyjnego*, a następnie włącz opcję *Pobierz aktualizacje za pomocą starego schematu*. W razie potrzeby można także skonfigurować opcję *Pobierz automatycznie plik żądania aktualizacji*, tak aby Kaspersky Update Utility pobierało tylko wymagane aktualizacje.

Tworzenie zadania Pobierz aktualizacje do repozytorium serwera administracyjnego

Zadanie *Pobierz aktualizacje do repozytorium Serwera administracyjnego* umożliwia pobieranie aktualizacji baz danych i modułów oprogramowania dla aplikacji zabezpieczających Kaspersky z serwerów aktualizacji Kaspersky do repozytorium Serwera administracyjnego.

Kreator wstępnej konfiguracji Kaspersky Security Center automatycznie tworzy zadanie *Pobierz aktualizacje do repozytorium Serwera administracyjnego* Serwera administracyjnego. Na liście zadań może znajdować się tylko jedno zadanie *Pobierz aktualizacje do repozytorium Serwera administracyjnego*. Możesz ponownie utworzyć to zadanie, jeśli zostanie usunięte z listy zadań Serwera administracyjnego.

Po zakończeniu zadania *Pobierz aktualizacje do repozytorium Serwera administracyjnego* i pobraniu aktualizacji można je rozprzestrzenić na zarządzane urządzenia.

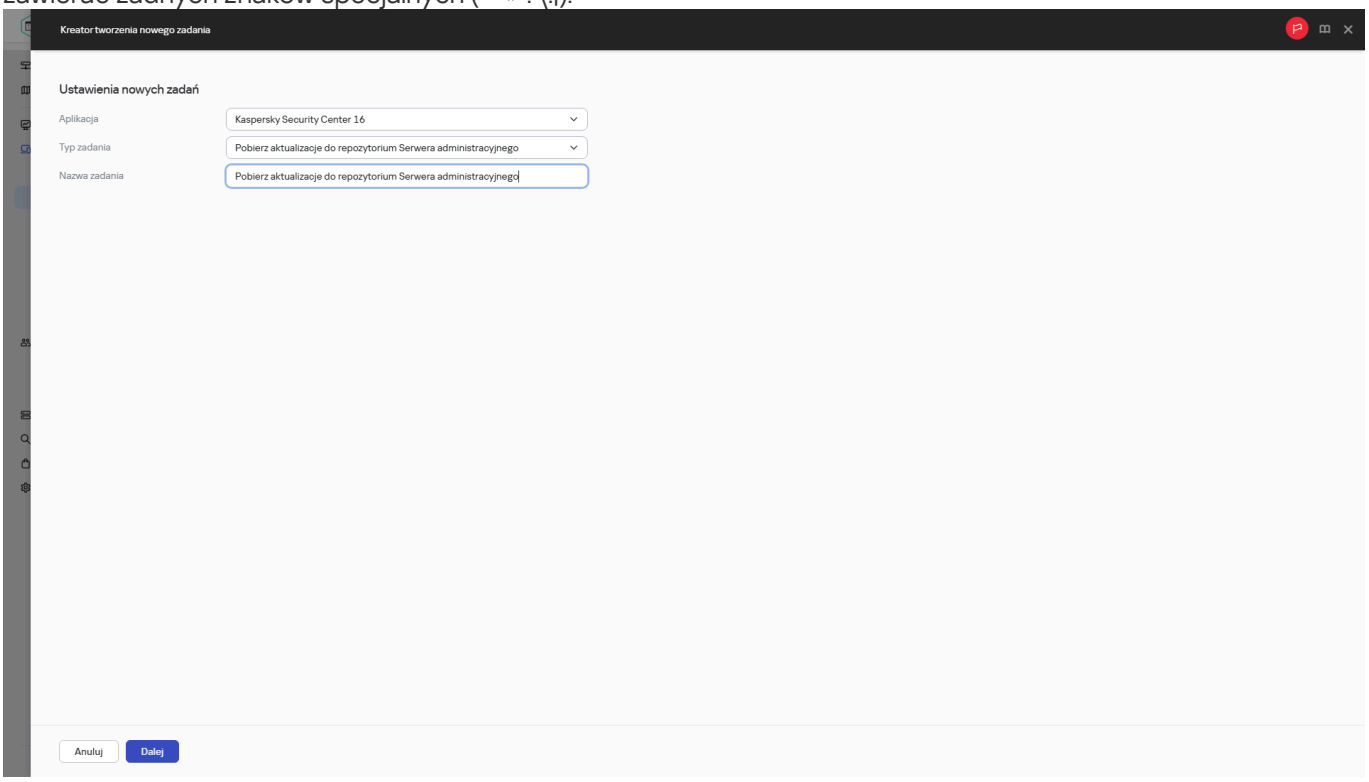
> Przed dystrybucją aktualizacji do urządzeń zarządzanych możesz uruchomić zadanie *Weryfikacja aktualizacji*. Pozwala to upewnić się, że Serwer administracyjny poprawnie zainstaluje pobrane aktualizacje, a poziom bezpieczeństwa nie zostanie obniżony z powodu aktualizacji. Aby zweryfikować je przed dystrybucją, skonfiguruj opcję **Uruchom weryfikację aktualizacji** w ustawieniach zadania *Pobierz aktualizacje do repozytorium Serwera administracyjnego*.

W celu utworzenia zadania Pobierz aktualizacje do repozytorium Serwera administracyjnego:

1. W menu głównym przejdź do **Zadania**.
2. Kliknij **Dodaj**.

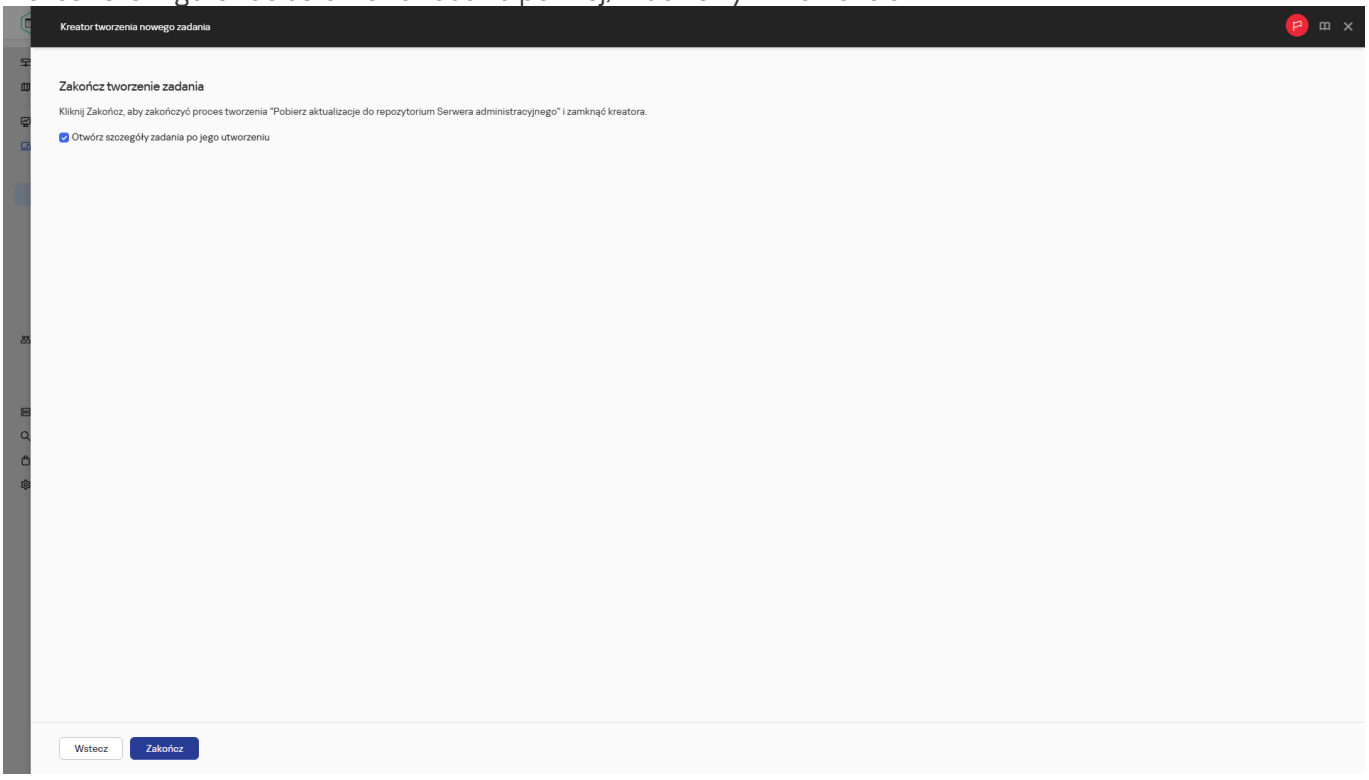
   Zostanie uruchomiony Kreator tworzenia nowego zadania. Postępuj zgodnie z krokami kreatora.
3. Dla aplikacji Kaspersky Security Center wybierz typ zadania **Pobierz aktualizacje do repozytorium Serwera administracyjnego**.

4. Określ nazwę tworzonego zadania. Nazwa zadania nie może zawierać więcej niż 100 znaków oraz nie może zawierać żadnych znaków specjalnych ("*<>?\:|).



Tworzenie zadania Pobierz aktualizacje do repozytorium serwera administracyjnego

5. Na stronie **Zakończ tworzenie zadania** możesz włączyć opcję **Otwórz szczegóły zadania po jego utworzeniu**, aby otworzyć okno właściwości zadania i zmodyfikować domyślne ustawienia zadania. W przeciwnym razie możesz skonfigurować ustawienia zadania później, w dowolnym momencie.



Zakończenie tworzenia zadania

6. Kliknij przycisk **Zakończ**.

   Zadanie zostanie utworzone i będzie wyświetlane na liście zadań.

7. Kliknij nazwę utworzonego zadania, aby otworzyć okno właściwości zadania.

8. W oknie właściwości zadania, na zakładce **Ustawienia aplikacji** określ następujące ustawienia:

- **Źródła aktualizacji**

  Jako źródło aktualizacji możesz użyć:

  - Serwery aktualizacji Kaspersky (wybrane domyślnie)
  - Główny Serwer administracyjny

    Ten zasób dotyczy zadań utworzonych dla podrzędnego lub wirtualnego Serwera administracyjnego.
  - Folder lokalny lub sieciowy

    Folder lokalny lub sieciowy, który zawiera najnowsze uaktualnienia. Folderem sieciowym może być serwer FTP lub HTTP lub udział SMB.

    Podczas wyboru folderu lokalnego powinieneś określić folder na urządzeniu z zainstalowanym Serwerem administracyjnym. Ścieżka do folderu zależy od systemu operacyjnego urządzenia. Ponieważ folder lokalny znajduje się na Serwerze administracyjnym opartym na systemie Linux, należy określić ścieżkę POSIX, na przykład: /path/to/dir.

    W przypadku wybrania folderu sieciowego SMB jako źródła uaktualnień przed jego wybraniem zamontuj go na urządzeniu, na którym jest zainstalowany Serwer administracyjny. Następnie określ ścieżkę do zamontowanego folderu, używając jego ścieżki w lokalnym systemie plików. Dostęp do folderu odbywa się za pośrednictwem protokołu SMB.

    > Folder lokalny lub sieciowy albo serwer FTP lub HTTP używany jako źródło uaktualnień musi zawierać strukturę folderów zgodną ze strukturą folderów na serwerach aktualizacji Kaspersky. Strukturę tę można uzyskać za pomocą narzędzia Kaspersky Update Utility.

  > W zadaniach Pobierz uaktualnienia do repozytorium *Serwera administracyjnego* i *Pobierz uaktualnienia do repozytoriów punktów dystrybucji* uwierzytelnianie użytkownika nie będzie działać, jeśli jako źródło aktualizacji wybierzesz chroniony hasłem folder lokalny lub sieciowy. Aby rozwiązać ten problem, najpierw zamontuj folder chroniony hasłem, a następnie określ wymagane poświadczenia, na przykład za pomocą systemu operacyjnego. Następnie możesz wybrać ten folder jako źródło aktualizacji w zadaniu pobierania aktualizacji. Kaspersky Security Center Linux nie będzie wymagał wprowadzania danych uwierzytelniających.

- **Folder do przechowywania aktualizacji**

  Ścieżka do określonego folderu na potrzeby przechowywania zapisanych aktualizacji. Możesz skopiować ścieżkę do określonego folderu do schowka. Nie możesz zmienić ścieżki do określonego folderu w przypadku zadania grupowego.

- **Wymuś aktualizację podrzędnych Serwerów administracyjnych**

  Jeżeli ta opcja jest włączona, Serwer administracyjny uruchomi zadania aktualizacji na podrzędnych Serwerach administracyjnych zaraz po pobraniu nowych aktualizacji. Zadania aktualizacji są uruchamiane przy użyciu źródła aktualizacji skonfigurowanego we właściwościach zadania na podrzędnych Serwerach administracyjnych.

  Jeśli ta opcja jest wyłączona, zadania aktualizacji na podrzędnych Serwerach administracyjnych będą uruchamiane zgodnie ze swoimi terminarzami.

  Domyślnie opcja ta jest wyłączona.

- **Kopiuj pobrane aktualizacje do dodatkowych folderów**

  Po otrzymaniu przez Serwer administracyjny uaktualnień skopiuje on je do określonych folderów. Użyj tej opcji, jeśli chcesz ręcznie zarządzać dystrybucją uaktualnień w sieci.

  Na przykład, chcesz użyć tej opcji w następującej sytuacji: sieć Twojej organizacji zawiera kilka niezależnych podsieci, a urządzenia z każdej podsieci nie mają dostępu do innych podsieci. Jednakże urządzenia we wszystkich podsieciach mają dostęp do wspólnego udziału sieciowego. W tym przypadku skonfiguruj Serwer administracyjny w jednej z podsieci tak, aby pobierał uaktualnienia z serwerów aktualizacji Kaspersky, włącz tę opcję, a następnie określ ten udział sieciowy. W zadaniach pobierania uaktualnień do repozytorium dla innych Serwerów administracyjnych określ ten sam udział sieciowy jako źródło uaktualnień.

  Jeżeli zdecydujesz się na skopiowanie pobranych aktualizacji do folderu lokalnego, musisz wskazać folder na urządzeniu, na którym jest zainstalowany Serwer administracyjny. Ścieżka do folderu zależy od systemu operacyjnego urządzenia. Ponieważ folder lokalny znajduje się na Serwerze administracyjnym opartym na systemie Linux, należy określić ścieżkę POSIX, na przykład: /path/to/dir.

  Wybierając folder sieciowy znajdujący się na Serwerze administracyjnym opartym na systemie Linux, należy wcześniej zapewnić dostęp do folderu sieciowego z urządzenia z zainstalowanym Serwerem administracyjnym, montując folder. Dostęp do folderu odbywa się za pomocą protokołu SMB.

  Domyślnie opcja ta jest wyłączona.

- **Pobierz pliki diff**

  Ta opcja włącza funkcję pobierania plików diff.

  Domyślnie opcja ta jest wyłączona.

- **Pobierz aktualizacje za pomocą starego schematu**

  Począwszy od wersji 14, Kaspersky Security Center pobiera aktualizacje baz danych i modułów oprogramowania przy użyciu nowego schematu. Aby aplikacja pobierała aktualizacje przy użyciu nowego schematu, źródło aktualizacji musi zawierać pliki aktualizacji z metadanymi zgodnymi z nowym schematem. Jeśli źródło aktualizacji zawiera pliki aktualizacji z metadanymi zgodnymi tylko ze starym schematem, włącz opcję **Pobierz aktualizacje za pomocą starego schematu**. W przeciwnym razie zadanie pobierania aktualizacji zakończy się niepowodzeniem.

  Na przykład musisz włączyć tę opcję, gdy folder lokalny lub sieciowy jest określony jako źródło aktualizacji, a pliki aktualizacji w tym folderze zostały pobrane przez jedną z następujących aplikacji:

  - Kaspersky Update Utility

    To narzędzie pobiera aktualizacje przy użyciu starego schematu.

  - Kaspersky Security Center 13 Linux

    Na przykład Twój serwer administracyjny 1 nie ma połączenia z Internetem. W takim przypadku możesz pobrać aktualizacje za pomocą serwera administracyjnego 2, który ma połączenie z Internetem, a następnie umieścić je w folderze lokalnym lub sieciowym, aby użyć go jako źródła uaktualnień dla serwera administracyjnego 1. Jeżeli serwer administracyjny 2 ma wersję 13, włącz opcję **Pobierz aktualizacje za pomocą starego schematu** w zadaniu dla serwera administracyjnego 1.

  Domyślnie opcja ta jest wyłączona.

- **Uruchom weryfikację aktualizacji**

  Serwer administracyjny pobiera uaktualnienia ze źródła, zapisuje je w tymczasowym repozytorium i uruchamia zadanie określone w polu **Zadanie weryfikacji uaktualnień**. Jeśli zadanie zakończy się pomyślnie, uaktualnienia są kopiowane z tymczasowego repozytorium do folderu współdzielonego na Serwerze administracyjnym, a następnie są rozsyłane do wszystkich urządzeń, dla których Serwer administracyjny pełni rolę źródła uaktualnień (zadania są uruchamiane zgodnie z opcją terminarza - **Po pobraniu nowych aktualizacji do repozytorium**). Zadanie pobierania uaktualnień do repozytorium zostaje zakończone dopiero po zakończeniu zadania *weryfikacji uaktualnień*.

  Domyślnie opcja ta jest wyłączona.

- **Pobierz automatycznie plik żądania aktualizacji**

  Jeśli chcesz, aby Kaspersky Update Utility pobierało tylko wymagane aktualizacje przy użyciu odpowiedniej konfiguracji, włącz tę opcję i określ ścieżkę, w której Kaspersky Security Center Linux utworzy plik żądania aktualizacji zawierający informacje o aktualizacjach, które mają zostać pobrane. Plik żądania aktualizacji zawiera znacznik czasu i skrót MD5 służący do kontroli wersji.

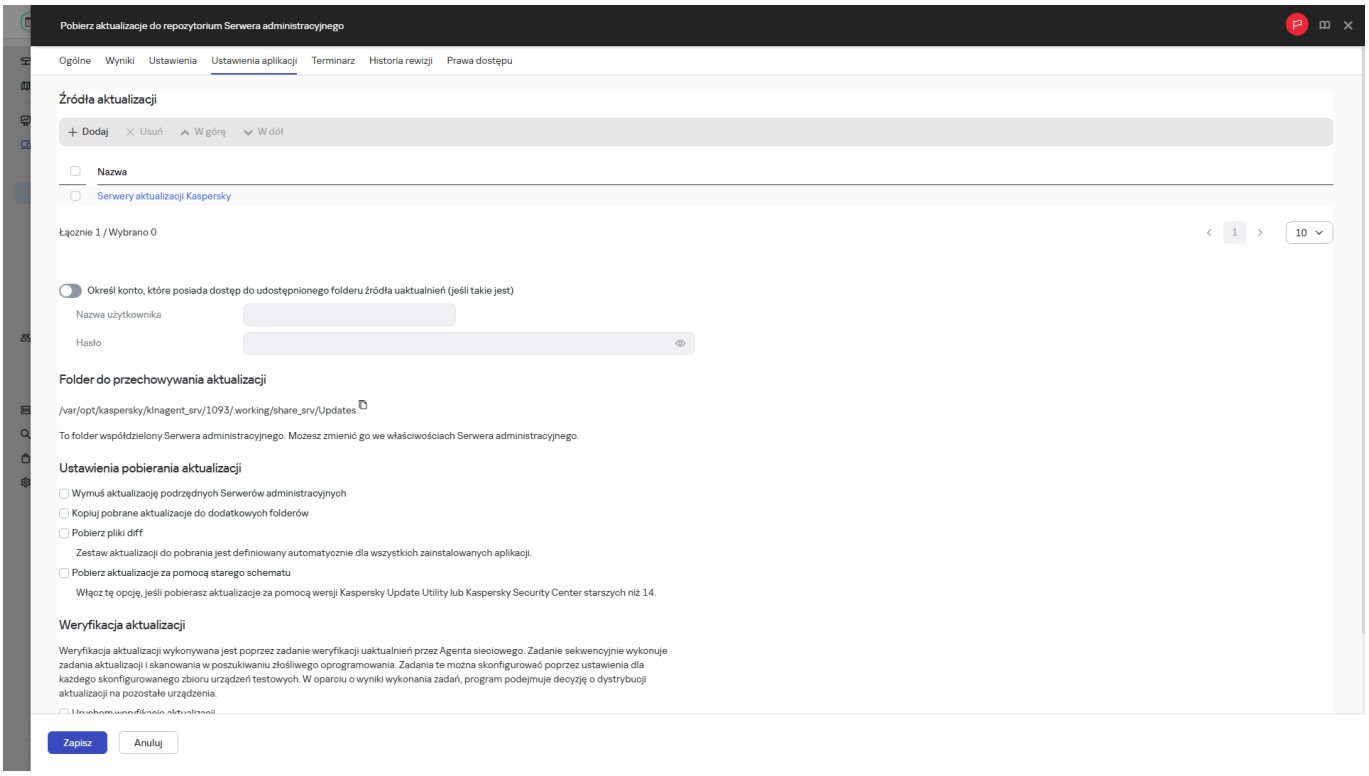
  Upewnij się, że opcja **Pobierz aktualizacje za pomocą starego schematu** jest wyłączona.

  Ponadto należy skonfigurować pobieranie aktualizacji w Kaspersky Update Utility.

  Domyślnie określona jest następująca ścieżka: /var/opt/kaspersky/klnagent_srv/1093/.working/share_srv/retranslation_request.xml. W razie potrzeby możesz zmienić domyślną nazwę (retranslation_request) i ścieżkę.

  > Plik żądania można umieścić w folderze lokalnym lub współdzielonym. W przypadku korzystania z folderu współdzielonego należy upewnić się, że dostęp do tego folderu jest możliwy z urządzenia, na którym zainstalowany jest Serwer administracyjny. Sposoby zapewnienia dostępu i stosowane narzędzia zależą od infrastruktury.

  Podczas wykonywania zadania *Pobierz aktualizacje do repozytorium Serwera administracyjnego*, Kaspersky Security Center Linux tworzy plik żądania aktualizacji w formacie .xml w ścieżce, którą określiłeś. Kaspersky Update Utility automatycznie pobiera informacje z pliku żądania i pobiera tylko wymagane aktualizacje. Jeśli Kaspersky Update Utility nie może uzyskać informacji automatycznie (na przykład Kaspersky Update Utility nie ma dostępu do folderu, w którym Kaspersky Security Center Linux utworzył plik żądania), należy przesłać plik, korzystając z narzędzi innych firm.



Określanie właściwości zadania Pobierz aktualizacje do repozytorium Serwera administracyjnego

9. W oknie właściwości zadania, na zakładce **Terminarz** utwórz terminarz uruchamiania zadania. Jeśli to konieczne, określ następujące ustawienia:

- **Uruchom zadanie**:

  - **Ręcznie** (zaznaczone domyślnie)

    Zadanie nie jest uruchamiane automatycznie. Możesz je uruchomić tylko ręcznie.

    Domyślnie opcja ta jest zaznaczona.

  - **Co N minut**

    Zadanie jest uruchamiane regularnie, w określonych przedziałach czasu, począwszy od określonej godziny w dniu utworzenia zadania.

    Domyślnie, zadanie jest uruchamiane co 30 minut, począwszy od bieżącego czasu systemowego.

  - **Co N godzin**

    Zadanie jest uruchamiane regularnie, w określonych przedziałach czasu, począwszy od określonego dnia i godziny.

    Domyślnie, zadanie jest uruchamiane co 6 godzin, począwszy od bieżącej daty i godziny systemowej.

  - **Co N dni**

    Zadanie jest uruchamiane regularnie, w określonych przedziałach czasu. Dodatkowo, możesz określić datę i godzinę pierwszego uruchomienia zadania. Te dodatkowe opcje staną się dostępne, jeśli są obsługiwane przez aplikację, dla której tworzysz zadanie.

    Domyślnie, zadanie jest uruchamiane codziennie, począwszy od bieżącej daty i godziny systemowej.

  - **Według dni tygodnia**

    Zadanie jest uruchamiane regularnie, w określone dni tygodnia i o określonej godzinie.

Domyślnie zadanie jest uruchamiane w każdy piątek o godzinie 18:00:00.

- **Co miesiąc**

  Zadanie jest uruchamiane regularnie, w określonym dniu miesiąca i o określonej godzinie.

  W miesiącach, w które nie ma określonego dnia, zadanie jest uruchamiane w ostatnim dniu.

  Domyślnie, zadanie jest uruchamiane w pierwszym dniu każdego miesiąca, o godzinie zgodnej z bieżącym czasem systemowym.

- **Miesięcznie wybranego dnia tygodnia**

  Zadanie jest uruchamiane regularnie, w określone dni każdego miesiąca i o określonej godzinie.

  Domyślnie godzina rozpoczęcia to 18:00, a żadne dni miesiąca nie są wybrane.

  > Należy pamiętać, że nie wybiera się konkretnej daty w miesiącu ani numeru tygodnia (pierwszy, drugi tydzień miesiąca), ale kolejny numer dnia tygodnia w miesiącu. Na przykład, jeśli ustawisz kursor w komórce **Wt** w **Pierwszy** wierszu, oznacza to, że zadanie będzie uruchamiane w każdy pierwszy wtorek każdego nowego miesiąca.

  Można wybrać kilka dni tygodnia.

- **Po zakończeniu wykonywania innego zadania**

  Bieżące zadanie jest uruchamiane po zakończeniu innego zadania. Opcja ta działa tylko wtedy, gdy oba zadania są przypisane do tych samych urządzeń. Na przykład możesz chcieć uruchomić zadanie *Zarządzaj urządzeniami* z opcją **Włącz urządzenie** i, po zakończeniu jego wykonywania, uruchomić zadanie *Skanowanie antywirusowe*, jako zadanie wyzwalające.

  Musisz wybrać z tabeli zadanie wyzwalające i status, z jakim to zadanie musi zostać ukończone (**Pomyślnie zakończone** lub **Niepowodzenie**).

  W razie potrzeby możesz wyszukiwać, sortować i filtrować zadania w tabeli w następujący sposób:

  - Wpisz nazwę zadania w polu wyszukiwania, aby wyszukać zadanie na podstawie jego nazwy.
  - Kliknij ikonę sortowania, aby posortować zadania według nazwy.

    Domyślnie zadania są sortowane alfabetycznie, w porządku rosnącym.
  - Kliknij ikonę filtra i w oknie, które zostanie otwarte, przefiltruj zadania według grupy, a następnie kliknij przycisk **Zastosuj**.

- Dodatkowe ustawienia zadań:

  - **Uruchom pominięte zadania**

    Ta opcja określa zachowanie zadania, jeśli urządzenie klienckie nie jest widoczne w sieci, gdy zadanie ma zostać uruchomione.

    Jeżeli ta opcja jest włączona, system podejmie próbę uruchomienia zadania podczas kolejnego uruchomienia aplikacji Kaspersky na urządzeniu klienckim. Jeśli terminarz uruchamiania zadania jest ustawiony na **Ręcznie**, **Raz** lub **Natychmiast**, zadanie jest uruchamiane, gdy urządzenie stanie się widoczne w sieci lub od razu po uwzględnieniu urządzenia w obszarze zadania.

Jeśli ta opcja jest wyłączona, na urządzeniach klienckich będą uruchamiane tylko zaplanowane zadania. W przypadku harmonogramu **Ręcznie**, **Raz** i **Natychmiast** zadania są uruchamiane tylko na tych urządzeniach klienckich, które są widoczne w sieci. Na przykład, możesz chcieć wyłączyć tę opcję dla zadań zużywających duże ilości zasobów, które chcesz uruchamiać tylko poza godzinami pracy.

Domyślnie opcja ta jest wyłączona.

- **Używaj automatycznie losowego opóźnienia dla uruchamiania zadań**

  Jeśli ta opcja jest włączona, zadanie jest uruchamiane na urządzeniach klienckich losowo, w określonym przedziale czasu, czyli z *rozproszonym uruchomieniem zadania*. Opcja ta pozwala uniknąć dużej liczby równoczesnych żądań wysyłanych przez urządzenia klienckie do Serwera administracyjnego, gdy uruchomione jest zaplanowane zadanie.

  Czas rozpoczęcia podjęcia próby uzyskania dostępu jest wyliczany automatycznie podczas tworzenia zadania, w zależności od liczby urządzeń klienckich, do których zadanie jest przypisane. Później zadanie będzie zawsze uruchamiane o wyliczonej godzinie uruchomienia. Jednakże, jeśli ustawienia zadania zostaną zmienione lub zadanie zostanie uruchomione ręcznie, zmieni się wyliczona wartość czasu uruchomienia zadania.

  Jeśli ta opcja jest wyłączona, zadanie jest uruchamiane na urządzeniach klienckich zgodnie z terminarzem.

- **Użyj automatycznego losowego opóźnienia dla zadań uruchamianych w przedziale**

  Jeśli ta opcja jest włączona, zadanie jest uruchamiane na urządzeniach klienckich losowo, w określonym przedziale czasu. Opcja ta pozwala uniknąć dużej liczby równoczesnych żądań wysyłanych przez urządzenia klienckie do Serwera administracyjnego, gdy uruchomione jest zaplanowane zadanie.

  Jeśli ta opcja jest wyłączona, zadanie jest uruchamiane na urządzeniach klienckich zgodnie z terminarzem.

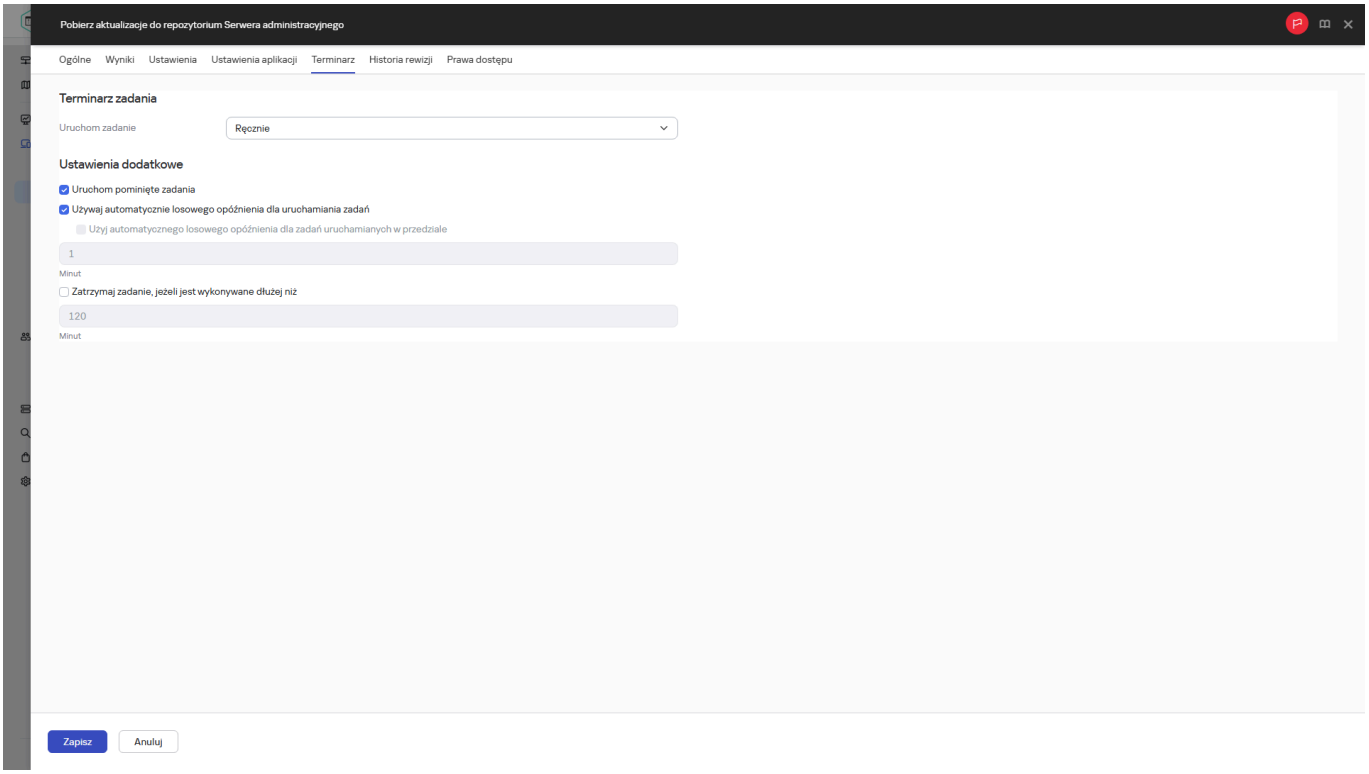
  Domyślnie opcja ta jest wyłączona. Domyślny przedział czasu wynosi 1 minutę.

- **Zatrzymaj zadanie, jeżeli jest wykonywane dłużej niż**

  Po minięciu określonego czasu, zadanie jest zatrzymywane automatycznie, niezależnie od tego, czy zostało zakończone.

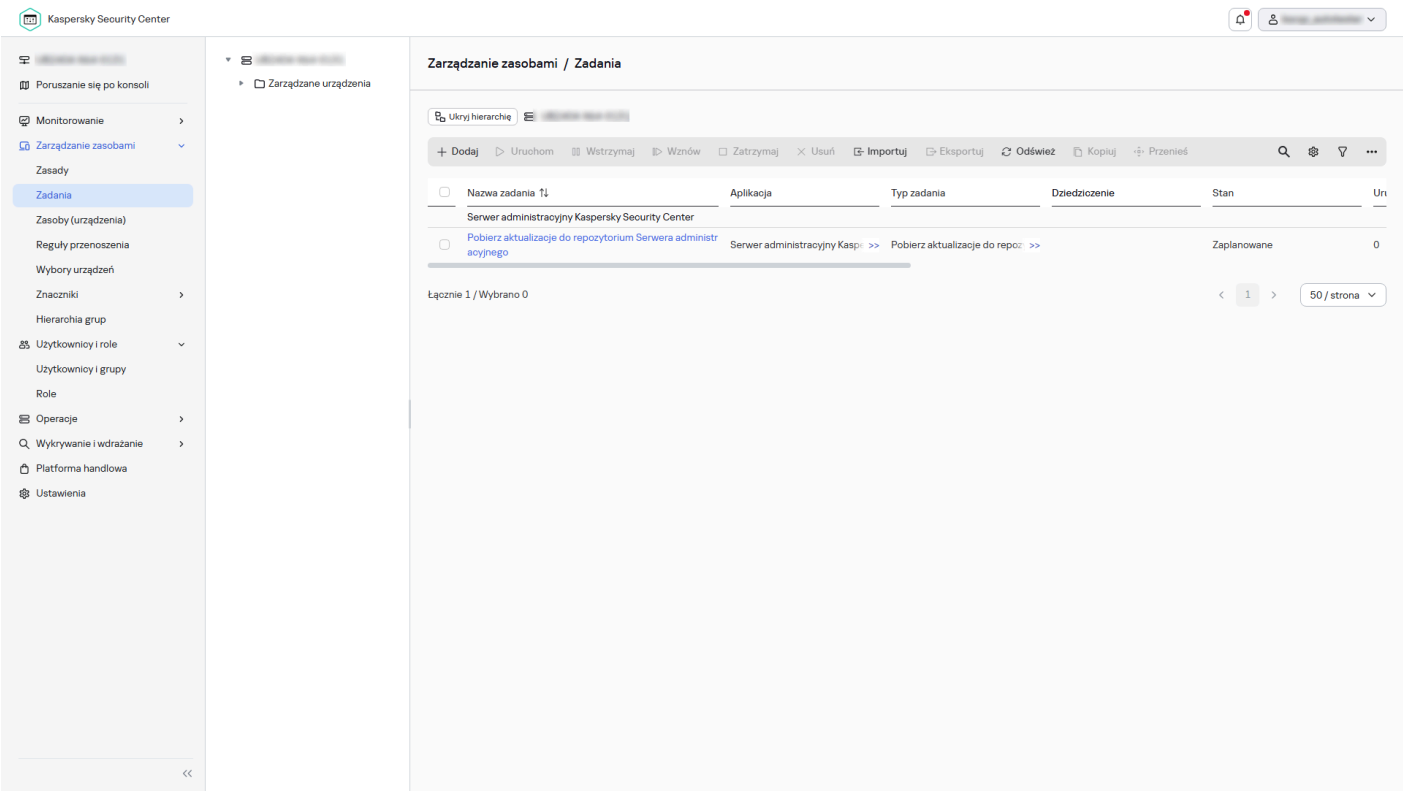
  Włącz tę opcję, jeśli chcesz przerwać (lub zatrzymać) zadania, których wykonanie zajmuje zbyt dużo czasu.

  Domyślnie opcja ta jest wyłączona. Domyślny czas wykonania zadania to 120 minut.



10. Kliknij przycisk **Zapisz**.

Zadanie zostało utworzone i skonfigurowane.



Lista zadań

Podczas wykonywania zadania *Pobierz aktualizacje do repozytorium Serwera administracyjnego* uaktualnienia baz danych i modułów programu są pobierane ze źródła uaktualnień i przechowywane w folderze współdzielonym Serwera administracyjnego. Jeśli tworzysz to zadanie dla grupy administracyjnej, zostanie ono zastosowane tylko do Agentów sieciowych umieszczonych w określonej grupie administracyjnej.

Uaktualnienia są rozsyłane do urządzeń klienckich i podrzędnych Serwerów administracyjnych z folderu współdzielonego Serwera administracyjnego.

Sprawdzanie pobranych uaktualnień

Przed zainstalowaniem aktualizacji na zarządzanych urządzeniach, w pierwszej kolejności możesz sprawdzić aktualizacje pod kątem łatwości obsługi i błędów poprzez zadanie *Weryfikacja aktualizacji*. Zadanie *Weryfikacja aktualizacji* jest wykonywane automatycznie jako część zadania *Pobierz aktualizacje do repozytorium Serwera administracyjnego*. Serwer administracyjny pobierze uaktualnienia ze źródła, zapisze je w repozytorium tymczasowym i uruchomi zadanie *weryfikacji uaktualnień*. Jeżeli zadanie zakończy się powodzeniem, uaktualnienia zostaną skopiowane z repozytorium tymczasowego do folderu współdzielonego na serwerze administracyjnym. Zostaną one rozesłane do wszystkich urządzeń klienckich, dla których Serwer administracyjny jest źródłem uaktualnień.

Jeżeli zadanie *weryfikacji uaktualnień* wykaże niepoprawność uaktualnień znajdujących się w repozytorium tymczasowym lub podczas wykonywania *tego zadania* wystąpi błąd, uaktualnienia nie zostaną skopiowane do folderu współdzielonego. Serwer administracyjny zachowa poprzedni zestaw uaktualnień. Zaplanowane zadania wykonywane zgodnie z opcją terminarza **Po pobraniu nowych aktualizacji do repozytorium** również nie zostaną uruchomione. Te działania są wykonywane podczas następnego uruchomienia zadania *Pobierz aktualizacje do repozytorium Serwera administracyjnego*, jeśli skanowanie nowych uaktualnień przebiegło bez problemów.

Zestaw uaktualnień jest uważany za nieprawidłowy, jeżeli przynajmniej na jednym urządzeniu testującym jest spełniony jeden z następujących warunków:

- Wystąpił błąd zadania aktualizacji.
- Stan ochrony w czasie rzeczywistym aplikacji zabezpieczającej zmienił się po zastosowaniu uaktualnień.
- W trakcie wykonywania zadania skanowania na żądanie wykryto zainfekowany obiekt.
- Wystąpił błąd w funkcjonowaniu aplikacji Kaspersky.

Jeśli żaden z powyższych warunków nie wystąpił na żadnym urządzeniu testującym, zestaw uaktualnień jest uważany za poprawny, a zadanie *weryfikacji uaktualnień* uważa się za zakończone pomyślnie.

Zanim zaczniesz tworzyć zadanie *Weryfikacja aktualizacji*, zrealizuj wymagania wstępne:

1. Utwórz grupę administracyjną z kilkoma urządzeniami testowymi. Ta grupa będzie potrzebna do weryfikacji uaktualnień.

   Zaleca się korzystanie z urządzeń z najbardziej niezawodną ochroną i najpowszechniejszą konfiguracją aplikacji w całej sieci. Takie podejście zwiększa jakość i prawdopodobieństwo wykrycia wirusa podczas skanowania oraz minimalizuje ryzyko fałszywych alarmów. Jeśli na urządzeniach testujących zostaną wykryte wirusy, zadanie *weryfikacji uaktualnień* zakończy się niepowodzeniem.

2. Utwórz zadania aktualizacji i skanowania pod kątem złośliwego oprogramowania dla aplikacji obsługiwanej przez Kaspersky Security Center Linux, na przykład Kaspersky Endpoint Security for Linux. Podczas tworzenia zadań aktualizacji i skanowania w poszukiwaniu szkodliwego oprogramowania określ grupę administracyjną z urządzeniami testowymi.

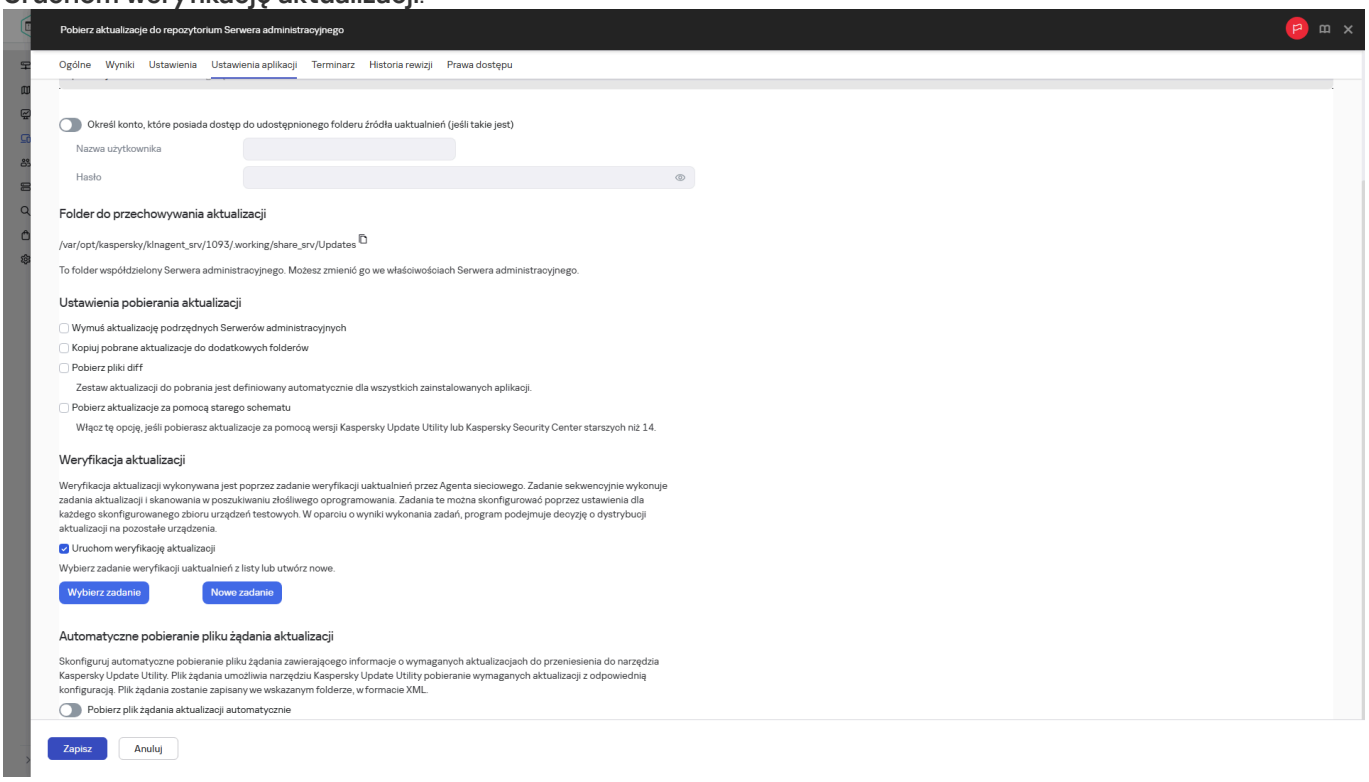
   Zadanie *Weryfikacja aktualizacji* uruchamia kolejno zadania Aktualizacja i Skanowanie w poszukiwaniu szkodliwego oprogramowania na urządzeniach testowych, aby sprawdzić, czy wszystkie aktualizacje są prawidłowe. Ponadto podczas tworzenia zadania *Weryfikacja aktualizacji* musisz określić zadania Aktualizacja i Skanowanie w poszukiwaniu złośliwego oprogramowania.

3. Utwórz zadanie *Pobierz aktualizacje do repozytorium Serwera administracyjnego*

W celu skonfigurowania Kaspersky Security Center Linux do sprawdzania pobranych uaktualnień przed rozesłaniem ich na urządzenia klienckie:

1. W menu głównym przejdź do **Zadania**.
2. Kliknij zadanie **Pobierz aktualizacje do repozytorium Serwera administracyjnego**.

3. W otwartym oknie właściwości zadania przejdź do zakładki **Ustawienia aplikacji**, a następnie włącz opcję **Uruchom weryfikację aktualizacji**.



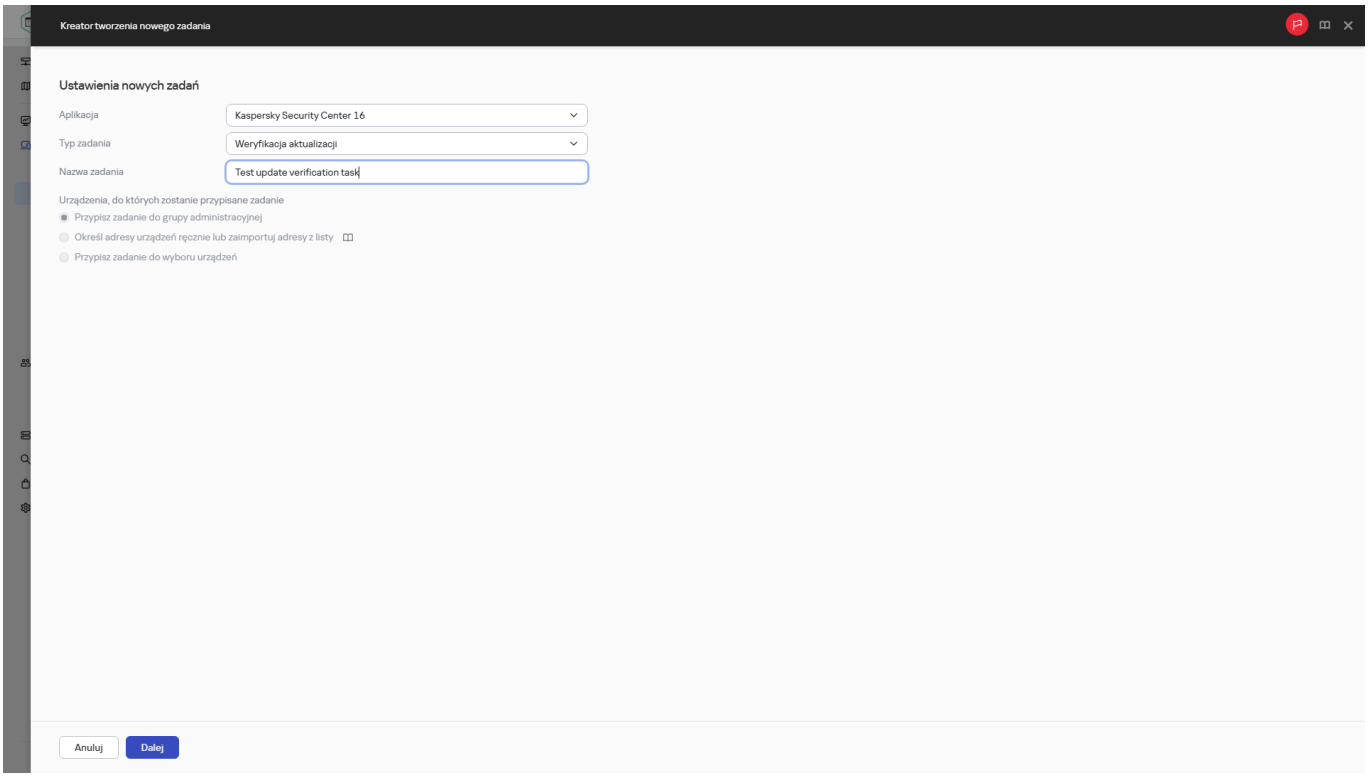
Właściwości zadania Pobierz aktualizacje do repozytorium Serwera administracyjnego

4. Jeśli zadanie *weryfikacji aktualizacji* istnieje, kliknij przycisk **Wybierz zadanie**. W oknie, które zostanie otwarte, wybierz zadanie *Weryfikacja aktualizacji* w grupie administracyjnej z urządzeniami testowymi.

5. Jeśli wcześniej nie utworzono zadania *Weryfikacja aktualizacji*, wykonaj następujące czynności:

a. Kliknij przycisk **Nowe zadanie**.

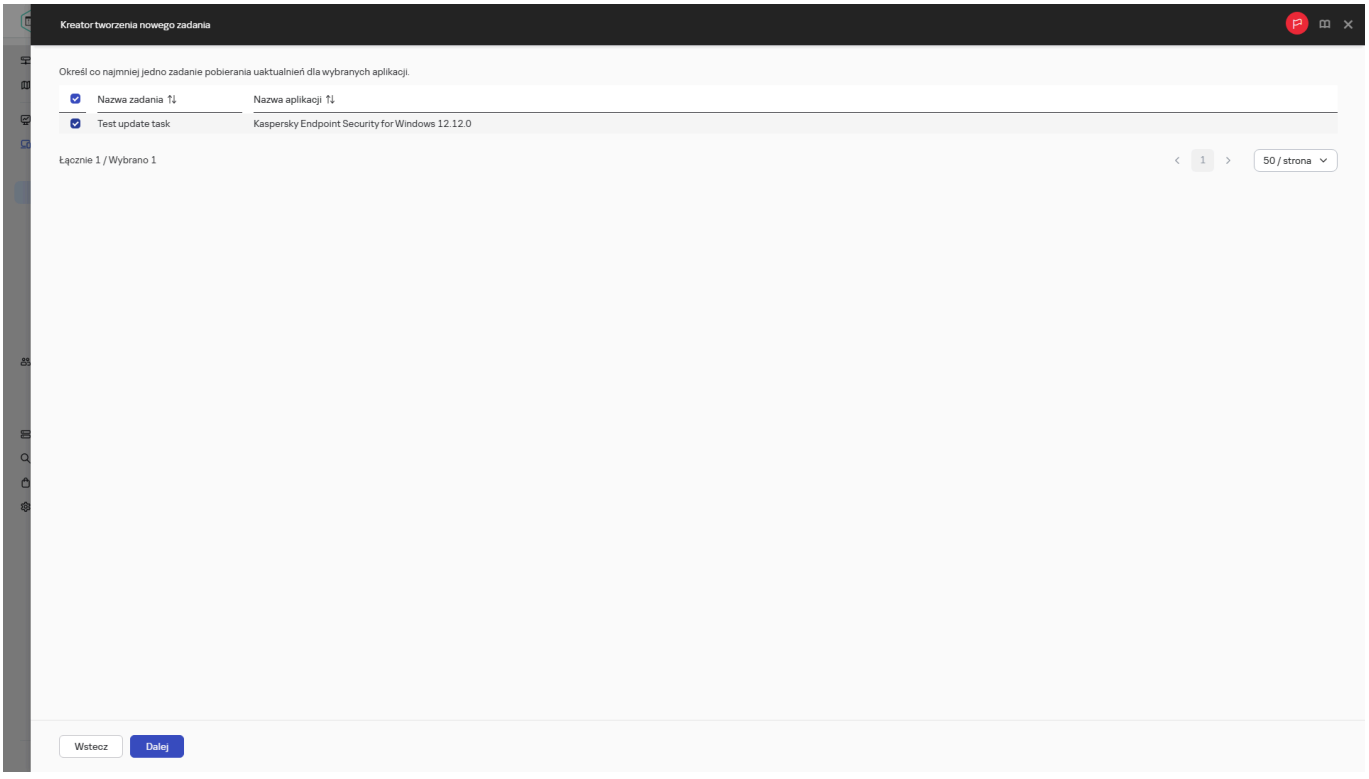
b. W otwartym kreatorze nowego zadania określ nazwę zadania, jeśli chcesz zmienić nazwę ustawienia wstępnego.



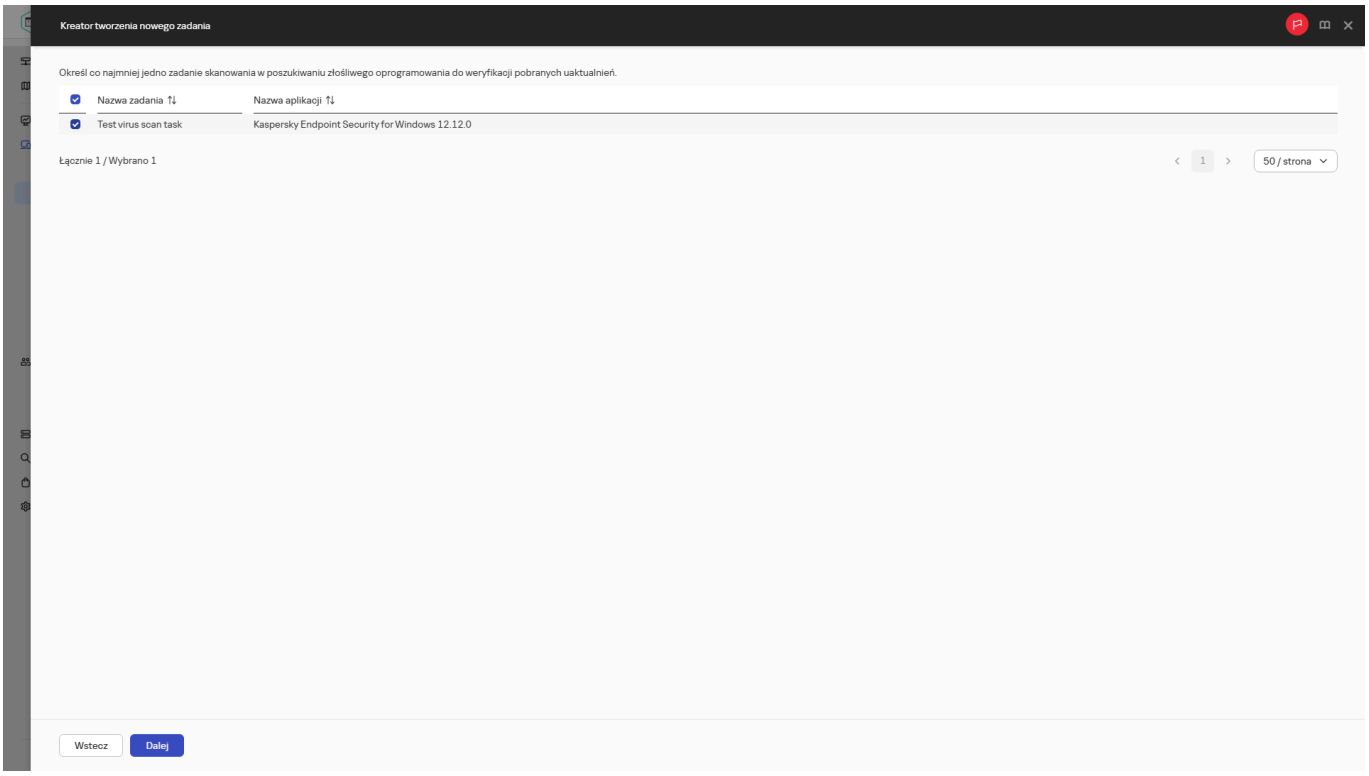
Tworzenie zadania Weryfikacji aktualizacji

a. Wybierz grupę administracyjną z urządzeniami testowymi, którą utworzono wcześniej.

b. Wybierz zadanie aktualizacji wymaganej aplikacji obsługiwanej przez Kaspersky Security Center Linux.



a. Wybierz zadanie skanowania w poszukiwaniu złośliwego oprogramowania dla wymaganej aplikacji obsługiwanej przez Kaspersky Security Center Linux.



Wybieranie skanowania w poszukiwaniu złośliwego oprogramowania

Następnie pojawiają się następujące opcje. Zalecamy pozostawienie ich włączonych:

- **Uruchom urządzenie ponownie po aktualizacji baz danych**

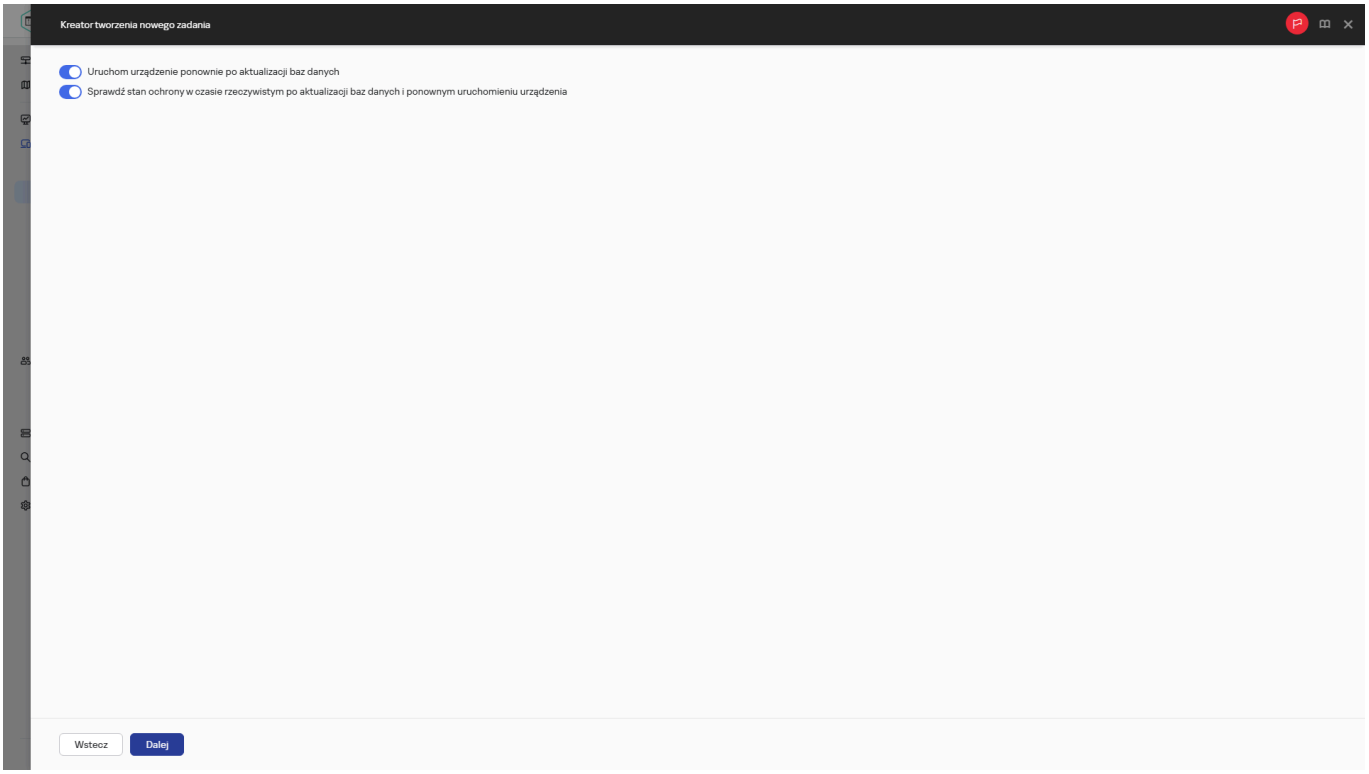
  Po zaktualizowaniu antywirusowych baz danych na urządzeniu zalecamy ponowne uruchomienie urządzenia.

  Domyślnie opcja ta jest włączona.

- **Sprawdź stan ochrony w czasie rzeczywistym po aktualizacji baz danych i ponownym uruchomieniu urządzenia**

  Jeżeli ta opcja jest włączona, zadanie *Weryfikacja aktualizacji* sprawdza, czy aktualizacje pobrane do repozytorium serwera administracyjnego są prawidłowe oraz czy poziom ochrony spadł po aktualizacji antywirusowej bazy danych i ponownym uruchomieniu urządzenia.

Domyślnie opcja ta jest włączona.



Określanie ustawień zadania

a. Określ konto, z którego zostanie uruchomione zadanie *Weryfikacja aktualizacji*. Możesz użyć swojego konta i pozostawić włączoną opcję **Konto domyślne**. Alternatywnie można określić, że zadanie powinno być uruchamiane na innym koncie, które ma niezbędne prawa dostępu. Aby to zrobić, wybierz opcję **Określ konto**, a następnie wprowadź poświadczenia tego konta.

6. Kliknij **Zapisz**, aby zamknąć okno właściwości zadania *Pobierz aktualizacje do repozytorium Serwera administracyjnego*.

Automatyczna weryfikacja aktualizacji zostanie włączona. Teraz możesz uruchomić zadanie *Pobierz aktualizacje do repozytorium Serwera administracyjnego*, które rozpocznie się od weryfikacji aktualizacji.

Tworzenie zadania pobierania aktualizacji do repozytoriów punktów dystrybucji

Możesz utworzyć zadanie *Pobierz uaktualnienia do repozytoriów punktów dystrybucji* dla grupy administracyjnej. To zadanie będzie uruchamiane dla punktów dystrybucji znajdujących się w określonej grupie administracyjnej.

Możesz użyć tego zadania, na przykład, jeśli ruch sieciowy pomiędzy Serwerem administracyjnym a punktem(ami) dystrybucji jest droższy niż ruch sieciowy pomiędzy punktem(ami) dystrybucji a serwerami aktualizacji Kaspersky lub jeśli Twój Serwer administracyjny nie ma dostępu do Internetu.

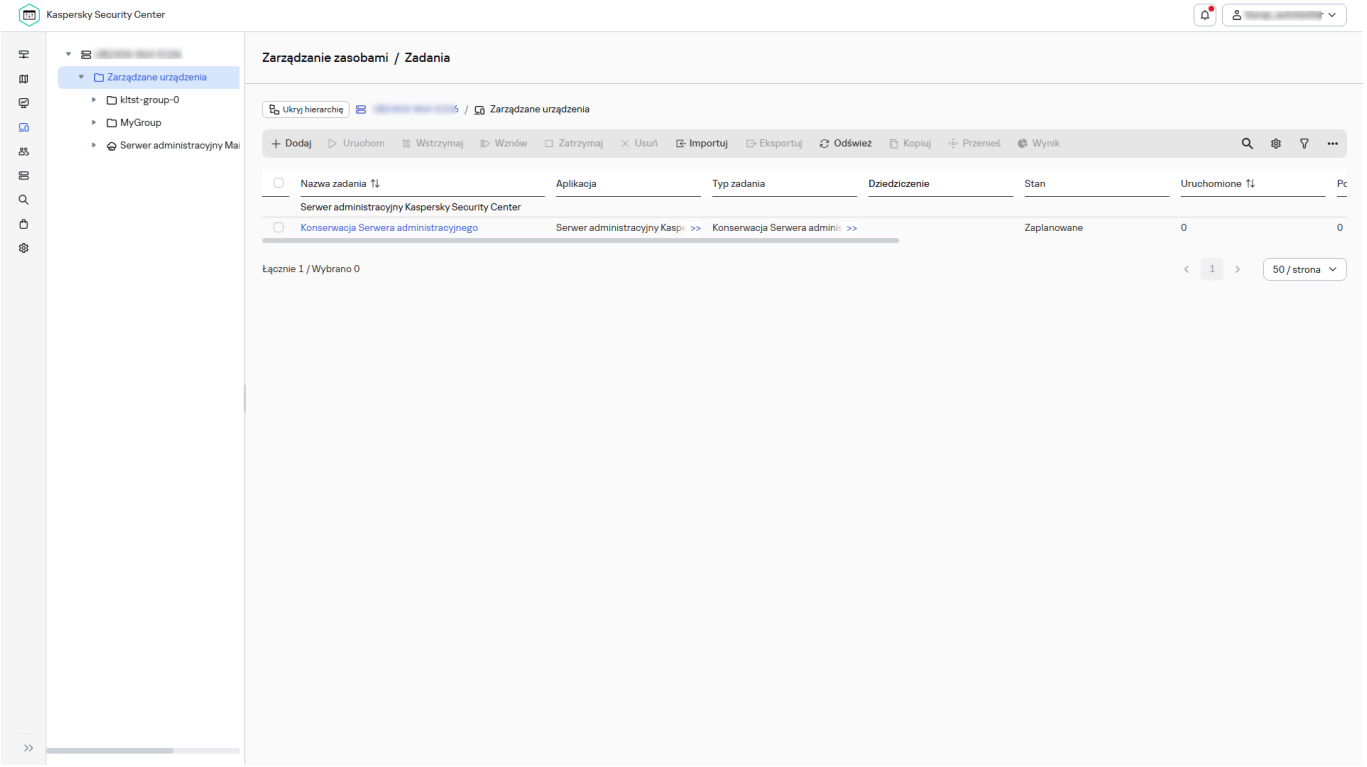
To zadanie jest wymagane do pobrania uaktualnień z serwerów aktualizacji Kaspersky do repozytoriów punktów dystrybucji. Lista aktualizacji obejmuje:

- Aktualizacje baz danych i modułów dla aplikacji zabezpieczających Kaspersky
- Aktualizacje komponentów Kaspersky Security Center
- Aktualizacje aplikacji zabezpieczających Kaspersky

Po pobraniu uaktualnień, mogą one zostać przesłane na zarządzane urządzenia.

*W celu utworzenia zadania **Pobierz aktualizacje do repozytoriów punktów dystrybucji** dla wybranej grupy administracyjnej:*

1. W menu głównym przejdź do **Zadania**.



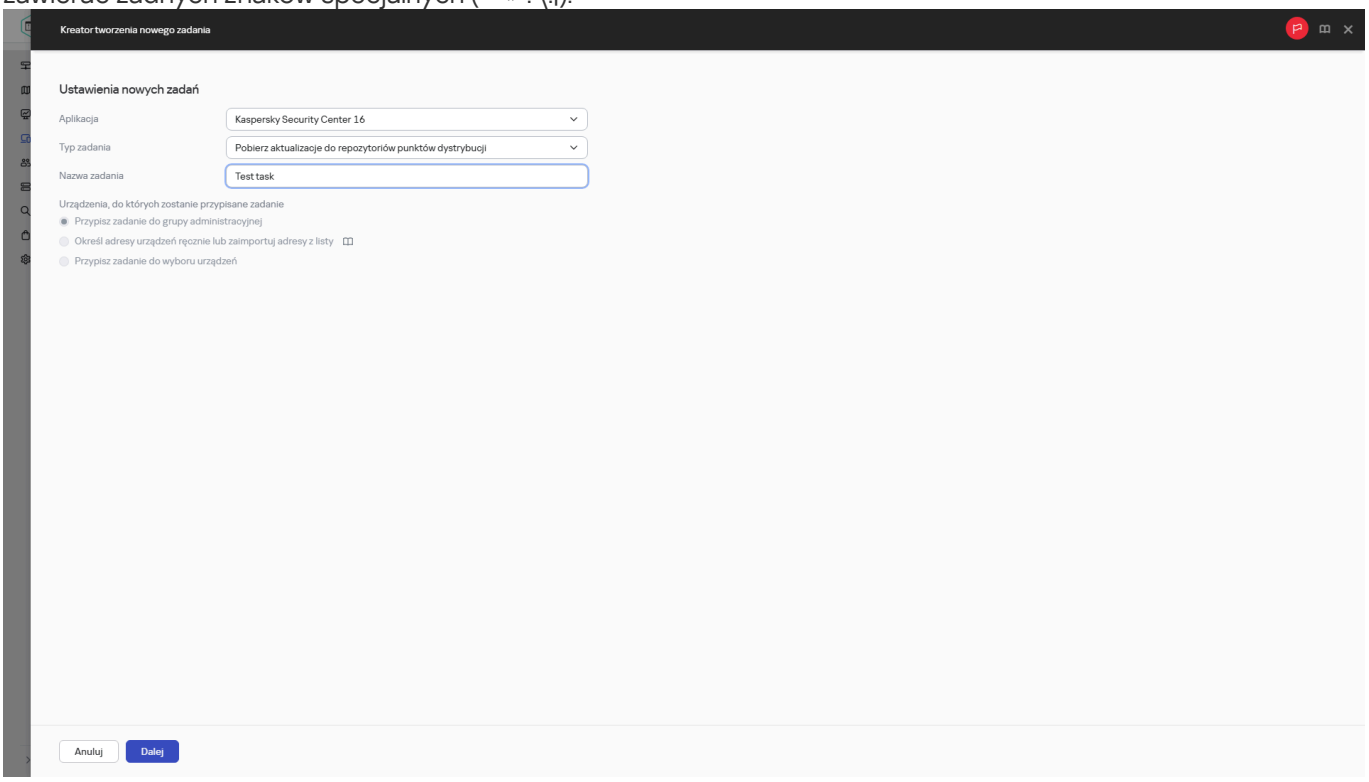
Sekcja Zadania

2. Kliknij przycisk **Dodaj**.

   Zostanie uruchomiony Kreator tworzenia nowego zadania. Postępuj zgodnie z krokami kreatora.

3. Dla aplikacji Kaspersky Security Center, w polu **Typ zadania** wybierz **Pobierz aktualizacje do repozytoriów punktów dystrybucji**.

4. Określ nazwę tworzonego zadania. Nazwa zadania nie może zawierać więcej niż 100 znaków oraz nie może zawierać żadnych znaków specjalnych ("*<>?\:|).



Tworzenie zadania Pobierz aktualizacje do repozytoriów punktów dystrybucji

5. Wybierz przycisk opcji do określenia grupy administracyjnej, wyboru urządzeń lub urządzeń, do których stosowane jest zadanie.

6. W kroku **Zakończ tworzenie zadania**, jeśli chcesz zmienić domyślne ustawienia zadania, włącz opcję **Otwórz szczegóły zadania po jego utworzeniu**. Jeśli nie włączysz tej opcji, zadanie zostanie utworzone z domyślnymi ustawieniami. Możesz zmodyfikować domyślne ustawienia później w dowolnym momencie.

7. Kliknij przycisk **Utwórz**.

   Zadanie zostanie utworzone i będzie wyświetlane na liście zadań.

8. Kliknij nazwę utworzonego zadania, aby otworzyć okno właściwości zadania.

9. Na zakładce **Ustawienia aplikacji** okna właściwości zadania określ następujące ustawienia:

   - **Źródła aktualizacji**

     Jako źródła uaktualnień dla punktu dystrybucji można użyć następujących zasobów:

     - Serwery aktualizacji Kaspersky

       Serwery HTTP(S) firmy Kaspersky, z których aplikacje Kaspersky pobierają uaktualnienia baz danych i modułów aplikacji.

       Opcja ta jest wybrana domyślnie.

     - Folder lokalny lub sieciowy

       Folder lokalny lub sieciowy, który zawiera najnowsze uaktualnienia. Jako folder sieciowy można używać wyłącznie zamontowanego udziału SMB. Podczas wyboru folderu lokalnego powinieneś określić folder na urządzeniu z zainstalowanym Serwerem administracyjnym.

W zadaniach Pobierz uaktualnienia do repozytorium *Serwera administracyjnego* i *Pobierz uaktualnienia do repozytoriów punktów dystrybucji* uwierzytelnianie użytkownika nie będzie działać, jeśli jako źródło aktualizacji wybierzesz chroniony hasłem folder lokalny lub sieciowy. Aby rozwiązać ten problem, najpierw zamontuj folder chroniony hasłem, a następnie określ wymagane poświadczenia, na przykład za pomocą systemu operacyjnego. Następnie możesz wybrać ten folder jako źródło aktualizacji w zadaniu pobierania aktualizacji. Kaspersky Security Center Linux nie będzie wymagał wprowadzania danych uwierzytelniających.

- **Folder do przechowywania aktualizacji**

  Ścieżka do określonego folderu na potrzeby przechowywania zapisanych aktualizacji. Możesz skopiować ścieżkę do określonego folderu do schowka. Nie możesz zmienić ścieżki do określonego folderu w przypadku zadania grupowego.

- **Pobierz pliki diff**

  Ta opcja włącza funkcję pobierania plików diff.

  Domyślnie opcja ta jest wyłączona.

- **Pobierz aktualizacje za pomocą starego schematu**

  Począwszy od wersji 14, Kaspersky Security Center pobiera aktualizacje baz danych i modułów oprogramowania przy użyciu nowego schematu. Aby aplikacja pobierała aktualizacje przy użyciu nowego schematu, źródło aktualizacji musi zawierać pliki aktualizacji z metadanymi zgodnymi z nowym schematem. Jeśli źródło aktualizacji zawiera pliki aktualizacji z metadanymi zgodnymi tylko ze starym schematem, włącz opcję **Pobierz aktualizacje za pomocą starego schematu**. W przeciwnym razie zadanie pobierania aktualizacji zakończy się niepowodzeniem.

  Na przykład musisz włączyć tę opcję, gdy folder lokalny lub sieciowy jest określony jako źródło aktualizacji, a pliki aktualizacji w tym folderze zostały pobrane przez jedną z następujących aplikacji:

  - Kaspersky Update Utility

    To narzędzie pobiera aktualizacje przy użyciu starego schematu.

  - Kaspersky Security Center 13 Linux

    Na przykład punkt dystrybucji jest skonfigurowany do pobierania aktualizacji z folderu lokalnego lub sieciowego. W takim przypadku aktualizacje można pobrać za pomocą serwera administracyjnego z połączeniem internetowym, a następnie umieścić je w folderze lokalnym w punkcie dystrybucji. Jeśli serwer administracyjny ma wersję 13, włącz opcję **Pobierz aktualizacje za pomocą starego schematu** w zadaniu *Pobierz aktualizacje do repozytoriów punktów dystrybucji*.

  Domyślnie opcja ta jest wyłączona.

10. Utwórz terminarz uruchamiania zadania. Jeśli to konieczne, określ następujące ustawienia:

- **Uruchom zadanie**:

  - **Ręcznie** (zaznaczone domyślnie)

    Zadanie nie jest uruchamiane automatycznie. Możesz je uruchomić tylko ręcznie.

    Domyślnie opcja ta jest zaznaczona.

  - **Co N minut**

    Zadanie jest uruchamiane regularnie, w określonych przedziałach czasu, począwszy od określonej godziny w dniu utworzenia zadania.

Domyślnie, zadanie jest uruchamiane co 30 minut, począwszy od bieżącego czasu systemowego.

- **Co N godzin**

  Zadanie jest uruchamiane regularnie, w określonych przedziałach czasu, począwszy od określonego dnia i godziny.

  Domyślnie, zadanie jest uruchamiane co 6 godzin, począwszy od bieżącej daty i godziny systemowej.

- **Co N dni**

  Zadanie jest uruchamiane regularnie, w określonych przedziałach czasu. Dodatkowo, możesz określić datę i godzinę pierwszego uruchomienia zadania. Te dodatkowe opcje staną się dostępne, jeśli są obsługiwane przez aplikację, dla której tworzysz zadanie.

  Domyślnie, zadanie jest uruchamiane codziennie, począwszy od bieżącej daty i godziny systemowej.

- **Według dni tygodnia**

  Zadanie jest uruchamiane regularnie, w określone dni tygodnia i o określonej godzinie.

  Domyślnie zadanie jest uruchamiane w każdy piątek o godzinie 18:00:00.

- **Co miesiąc**

  Zadanie jest uruchamiane regularnie, w określonym dniu miesiąca i o określonej godzinie.

  W miesiącach, w które nie ma określonego dnia, zadanie jest uruchamiane w ostatnim dniu.

  Domyślnie, zadanie jest uruchamiane w pierwszym dniu każdego miesiąca, o godzinie zgodnej z bieżącym czasem systemowym.

- **Miesięcznie wybranego dnia tygodnia**

  Zadanie jest uruchamiane regularnie, w określone dni każdego miesiąca i o określonej godzinie.

  Domyślnie godzina rozpoczęcia to 18:00, a żadne dni miesiąca nie są wybrane.

  > Należy pamiętać, że nie wybiera się konkretnej daty w miesiącu ani numeru tygodnia (pierwszy, drugi tydzień miesiąca), ale kolejny numer dnia tygodnia w miesiącu. Na przykład, jeśli ustawisz kursor w komórce **Wt** w **Pierwszy** wierszu, oznacza to, że zadanie będzie uruchamiane w każdy pierwszy wtorek każdego nowego miesiąca.

  Można wybrać kilka dni tygodnia.

- **Po ataku wirusa**

  Zadanie jest uruchamiane po wystąpieniu zdarzenia *Atak wirusa*. Wybierz typy aplikacji, które będą monitorować ataki wirusa. Dostępne są następujące typy aplikacji:

  - Ochrona antywirusowa stacji roboczych i serwerów plików
  - Ochrona antywirusowa bram internetowych
  - Ochrona antywirusowa serwerów pocztowych

  Domyślnie, zaznaczone są wszystkie typy aplikacji.

  Możesz chcieć uruchomić różne zadania w zależności od typu aplikacji zabezpieczającej, która zgłosiła atak wirusa. W tym przypadku, usuń wybór typów aplikacji, których nie potrzebujesz.

- **Po zakończeniu wykonywania innego zadania**

  Bieżące zadanie jest uruchamiane po zakończeniu innego zadania. Opcja ta działa tylko wtedy, gdy oba zadania są przypisane do tych samych urządzeń. Na przykład możesz chcieć uruchomić zadanie *Zarządzaj urządzeniami* z opcją **Włącz urządzenie** i, po zakończeniu jego wykonywania, uruchomić zadanie *Skanowanie antywirusowe*, jako zadanie wyzwalające.

  Musisz wybrać z tabeli zadanie wyzwalające i status, z jakim to zadanie musi zostać ukończone (**Pomyślnie zakończone** lub **Niepowodzenie**).

  W razie potrzeby możesz wyszukiwać, sortować i filtrować zadania w tabeli w następujący sposób:

  - Wpisz nazwę zadania w polu wyszukiwania, aby wyszukać zadanie na podstawie jego nazwy.
  - Kliknij ikonę sortowania, aby posortować zadania według nazwy.

    Domyślnie zadania są sortowane alfabetycznie, w porządku rosnącym.
  - Kliknij ikonę filtra i w oknie, które zostanie otwarte, przefiltruj zadania według grupy, a następnie kliknij przycisk **Zastosuj**.

- **Uruchom pominięte zadania**

  Ta opcja określa zachowanie zadania, jeśli urządzenie klienckie nie jest widoczne w sieci, gdy zadanie ma zostać uruchomione.

  Jeżeli ta opcja jest włączona, system podejmie próbę uruchomienia zadania podczas kolejnego uruchomienia aplikacji Kaspersky na urządzeniu klienckim. Jeśli terminarz uruchamiania zadania jest ustawiony na **Ręcznie**, **Raz** lub **Natychmiast**, zadanie jest uruchamiane, gdy urządzenie stanie się widoczne w sieci lub od razu po uwzględnieniu urządzenia w obszarze zadania.

  Jeśli ta opcja jest wyłączona, na urządzeniach klienckich będą uruchamiane tylko zaplanowane zadania. W przypadku harmonogramu **Ręcznie**, **Raz** i **Natychmiast** zadania są uruchamiane tylko na tych urządzeniach klienckich, które są widoczne w sieci. Na przykład, możesz chcieć wyłączyć tę opcję dla zadań zużywających duże ilości zasobów, które chcesz uruchamiać tylko poza godzinami pracy.

  Domyślnie opcja ta jest wyłączona.

- **Używaj automatycznie losowego opóźnienia dla uruchamiania zadań**

  Jeśli ta opcja jest włączona, zadanie jest uruchamiane na urządzeniach klienckich losowo, w określonym przedziale czasu, czyli z *rozproszonym uruchomieniem zadania*. Opcja ta pozwala uniknąć dużej liczby równoczesnych żądań wysyłanych przez urządzenia klienckie do Serwera administracyjnego, gdy uruchomione jest zaplanowane zadanie.

  Czas rozpoczęcia podjęcia próby uzyskania dostępu jest wyliczany automatycznie podczas tworzenia zadania, w zależności od liczby urządzeń klienckich, do których zadanie jest przypisane. Później zadanie będzie zawsze uruchamiane o wyliczonej godzinie uruchomienia. Jednakże, jeśli ustawienia zadania zostaną zmienione lub zadanie zostanie uruchomione ręcznie, zmieni się wyliczona wartość czasu uruchomienia zadania.

  Jeśli ta opcja jest wyłączona, zadanie jest uruchamiane na urządzeniach klienckich zgodnie z terminarzem.

- **Użyj automatycznego losowego opóźnienia dla zadań uruchamianych w przedziale**

  Jeśli ta opcja jest włączona, zadanie jest uruchamiane na urządzeniach klienckich losowo, w określonym przedziale czasu. Opcja ta pozwala uniknąć dużej liczby równoczesnych żądań wysyłanych przez urządzenia klienckie do Serwera administracyjnego, gdy uruchomione jest zaplanowane zadanie.

  Jeśli ta opcja jest wyłączona, zadanie jest uruchamiane na urządzeniach klienckich zgodnie z terminarzem.

  Domyślnie opcja ta jest wyłączona. Domyślny przedział czasu wynosi 1 minutę.

11. Kliknij przycisk **Zapisz**.

    Zadanie zostało utworzone i skonfigurowane.

    Oprócz ustawień, które określasz podczas tworzenia zadania, możesz zmienić inne właściwości utworzonego zadania.

Po wykonaniu zadania *Pobierz aktualizacje do repozytoriów punktów dystrybucji*, aktualizacje baz danych i modułów aplikacji zostaną pobrane ze źródła uaktualnień i będą przechowywane w folderze współdzielonym. Pobrane uaktualnienia zostaną użyte tylko przez punkty dystrybucji, które znajdują się w określonej grupie administracyjnej i dla których nie ustawiono zadania pobierania aktualizacji.

Dodawanie źródeł uaktualnień dla zadania Pobierz uaktualnienia do repozytorium Serwera administracyjnego

Podczas tworzenia lub używania zadania pobierania uaktualnień do repozytorium Serwera administracyjnego możesz wybrać następujące źródła uaktualnień:

- Serwery aktualizacji Kaspersky
- Główny Serwer administracyjny

  Ten zasób dotyczy zadań utworzonych dla podrzędnego lub wirtualnego Serwera administracyjnego.
- Folder lokalny lub sieciowy

> W zadaniach Pobierz uaktualnienia do repozytorium *Serwera administracyjnego* i *Pobierz uaktualnienia do repozytoriów punktów dystrybucji* uwierzytelnianie użytkownika nie będzie działać, jeśli jako źródło aktualizacji wybierzesz chroniony hasłem folder lokalny lub sieciowy. Aby rozwiązać ten problem, najpierw zamontuj folder chroniony hasłem, a następnie określ wymagane poświadczenia, na przykład za pomocą systemu operacyjnego. Następnie możesz wybrać ten folder jako źródło aktualizacji w zadaniu pobierania aktualizacji. Kaspersky Security Center Linux nie będzie wymagał wprowadzania danych uwierzytelniających.

Serwery aktualizacji Kaspersky są używane domyślnie, ale aktualizacje można również pobierać z folderu lokalnego lub sieciowego. Możesz chcieć użyć tego folderu, jeśli Twoja sieć nie ma dostępu do Internetu. W takim przypadku możesz ręcznie pobrać aktualizacje z serwerów aktualizacji Kaspersky i umieścić pobrane pliki w odpowiednim folderze. Możesz określić tylko jedną ścieżkę do folderu lokalnego lub sieciowego.

Podczas wyboru folderu lokalnego powinieneś określić folder na urządzeniu z zainstalowanym Serwerem administracyjnym. Ścieżka do folderu zależy od systemu operacyjnego urządzenia. Ponieważ folder lokalny znajduje się na Serwerze administracyjnym opartym na systemie Linux, należy określić ścieżkę POSIX, na przykład: /path/to/dir.

Jako folder sieciowy można używać wyłącznie zamontowanego udziału SMB. Jeśli udostępnienie SMB wymaga uwierzytelnienia, należy go wcześniej zamontować w systemie z wymaganymi poświadczeniami. Nie zalecamy używania protokołu SMB1, ponieważ nie jest on bezpieczny.

Aby dodać źródła aktualizacji:

1. W menu głównym przejdź do **Zadania**.
2. Kliknij **Pobierz aktualizacje do repozytorium Serwera administracyjnego**.
3. Przejdź do zakładki **Ustawienia aplikacji**.
4. W tabeli **Źródła aktualizacji** kliknij przycisk **Dodaj**.
5. W oknie, które zostanie otwarte, dodaj niezbędne źródła, a następnie kliknij przycisk **Zapisz**.

   Jeśli zaznaczysz pole wyboru **Folder lokalny lub sieciowy**, określ ścieżkę do folderu.
6. Kliknij przycisk **Zapisz** w oknie zadania.

Teraz aktualizacje są pobierane do repozytorium Serwera administracyjnego z określonych źródeł.

Jeśli dodasz zarówno serwery aktualizacji Kaspersky, jak i folder lokalny lub sieciowy, możesz ustawić priorytety aktualizacji. W tym celu w tabeli **Źródła aktualizacji** zaznacz pole wyboru obok aktualizacji, dla której chcesz zmienić priorytet, a następnie kliknij przycisk **W górę** lub **W dół**.

Zatwierdzanie i odrzucanie aktualizacji oprogramowania

Ustawienia zadania instalacji aktualizacji mogą wymagać zatwierdzenia aktualizacji, które mają zostać zainstalowane. Możesz zatwierdzić uaktualnienia, które muszą zostać zainstalowane, oraz odrzucić uaktualnienia, które nie muszą zostać zainstalowane.

Na przykład, możesz chcieć najpierw sprawdzić instalację aktualizacji w środowisku testowym i upewnić się, że nie wpływają negatywnie na działanie urządzeń, a następnie zezwolić na instalację tylko tych aktualizacji na urządzeniach klienckich.

Zatwierdzanie i odrzucanie aktualizacji jest dostępne tylko w przypadku Agenta sieciowego i aplikacji zarządzanych zainstalowanych na urządzeniach klienckich z systemem Windows. Bezproblemowa aktualizacja Serwera administracyjnego, Kaspersky Security Center Web Console i webowych wtyczek administracyjnych nie jest obsługiwana. Aby zaktualizować aplikacje, pobierz najnowsze wersje aplikacji z witryny internetowej Kaspersky, a następnie zainstaluj je ręcznie.

W celu zatwierdzenia lub odrzucenia jednej lub kilku aktualizacji:

1. W menu głównym przejdź do **Zarządzanie oprogramowaniem** → **Aplikacje Kaspersky** → **Aktualizacje SMU (Seamless update)**.

   Zostanie wyświetlona lista dostępnych aktualizacji.

   Aktualizacje zarządzanych aplikacji mogą wymagać zainstalowania określonej minimalnej wersji Kaspersky Security Center. Jeśli ta wersja jest nowsza niż aktualna wersja, te aktualizacje są wyświetlane, ale nie można ich zatwierdzić. Ponadto żadne pakiety instalacyjne nie mogą być tworzone z takich aktualizacji, dopóki nie zaktualizujesz Kaspersky Security Center. Zostaniesz poproszony o uaktualnienie instancji Kaspersky Security Center do wymaganej wersji minimalnej.

2. W razie potrzeby zaakceptuj Umowę licencyjną użytkownika końcowego, klikając przycisk **Wyświetl i zaakceptuj Umowy licencyjne**.

3. Wybierz uaktualnienia, które chcesz zatwierdzić lub odrzucić.

4. Kliknij **Zatwierdź**, aby zatwierdzić wybrane aktualizacje, lub **Odrzuć**, aby odrzucić wybrane aktualizacje.

   Domyślna wartość to *Niezdefiniowane*.

Aktualizacje, do których przypisałeś stan *Zatwierdzono*, są umieszczane w kolejce do instalacji.

Aktualizacje, do których przypisałeś stan *Odrzucono*, są odinstalowywane (jeśli to możliwe) ze wszystkich urządzeń, na których były wcześniej zainstalowane. Dodatkowo, nie zostaną one zainstalowane na innych urządzeniach w przyszłości.

Niektórych uaktualnień dla aplikacji firmy Kaspersky nie można odinstalować. Jeśli ustawiłeś dla nich stan *Odrzucono*, Kaspersky Security Center Linux nie odinstaluje tych uaktualnień z urządzeń, na których były wcześniej zainstalowane. Jednakże te uaktualnienia nigdy nie zostaną zainstalowane na innych urządzeniach w przyszłości.

Jeśli ustawisz stan *Odrzucono* dla aktualizacji oprogramowania firm trzecich, te aktualizacje nie zostaną zainstalowane na urządzeniach, dla których planowane było ich zainstalowanie, ale jeszcze nie zostały zainstalowane. Uaktualnienia pozostaną na urządzeniach, na których zostały już zainstalowane. Jeśli musisz usunąć aktualizacje, możesz je usunąć ręcznie lokalnie.

Pobieranie pakietu instalacyjnego dla Kaspersky Endpoint Security for Windows

Możesz skonfigurować automatyczne aktualizowanie baz danych i modułów aplikacji Kaspersky Endpoint Security for Windows na urządzeniach klienckich.

W celu skonfigurowania pobierania i automatycznej instalacji uaktualnień dla Kaspersky Endpoint Security for Windows na urządzeniach:

1. W menu głównym przejdź do **Zadania**.

2. Kliknij przycisk **Dodaj**.

   Zostanie uruchomiony Kreator tworzenia nowego zadania. Postępuj zgodnie z krokami kreatora.

3. Dla aplikacji Kaspersky Endpoint Security for Windows, jako podtyp zadania wybierz **Aktualizacja**.

4. Określ nazwę tworzonego zadania. Nazwa zadania nie może zawierać więcej niż 100 znaków oraz nie może zawierać żadnych znaków specjalnych ("*<>?\:|).

5. Wybierz obszar zadania.

6. Określ grupę administracyjną, wybór urządzeń lub urządzenia, do których stosowane jest zadanie.

7. W kroku **Zakończ tworzenie zadania**, jeśli chcesz zmienić domyślne ustawienia zadania, włącz opcję **Otwórz szczegóły zadania po jego utworzeniu**. Jeśli nie włączysz tej opcji, zadanie zostanie utworzone z domyślnymi ustawieniami. Możesz zmodyfikować domyślne ustawienia później w dowolnym momencie.

8. Kliknij przycisk **Utwórz**.

   Zadanie zostanie utworzone i będzie wyświetlane na liście zadań.

9. Kliknij nazwę utworzonego zadania, aby otworzyć okno właściwości zadania.

10. Na zakładce **Ustawienia aplikacji** okna właściwości zadania zdefiniuj ustawienia zadania aktualizacji w trybie lokalnym lub mobilnym:

    - **Tryb lokalny**: Połączenie jest nawiązywane między urządzeniem a Serwerem administracyjnym.

    - **Tryb mobilny**: Połączenie pomiędzy Kaspersky Security Center Linux a urządzeniem nie jest nawiązywane (na przykład, jeśli urządzenie nie jest podłączone do internetu).

11. Włącz źródło aktualizacji, którego chcesz użyć do zaktualizowania baz danych i modułów aplikacji dla Kaspersky Endpoint Security for Windows. Jeśli jest to wymagane, zmień pozycje źródeł na liście, korzystając z przycisków **W górę** i **W dół**. Jeśli włączonych jest kilka źródeł aktualizacji, Kaspersky Endpoint Security for Windows próbuje nawiązać z nimi połączenie po kolei, rozpoczynając od góry listy, i wykonać zadanie aktualizacji, pobierając pakiet aktualizacyjny z pierwszego dostępnego źródła.

12. Włącz opcję **Zainstaluj zatwierdzone aktualizacje modułów aplikacji**, aby pobrać i zainstalować uaktualnienia modułów aplikacji wraz z bazami danych aplikacji.

    Jeśli opcja jest włączona, Kaspersky Endpoint Security for Windows powiadamia użytkownika o dostępnych uaktualnieniach modułów aplikacji i włącza uaktualnienia modułów aplikacji do pakietu aktualizacyjnego podczas wykonywania zadania aktualizacji. Kaspersky Endpoint Security for Windows instaluje tylko te uaktualnienia, dla których ustawiłeś stan *Zatwierdzone*; zostaną zainstalowane lokalnie z poziomu interfejsu aplikacji lub poprzez Kaspersky Security Center Linux.

    Możesz także włączyć opcję **Automatycznie instaluj krytyczne aktualizacje modułów aplikacji**. Jeśli dla modułów aplikacji dostępne są jakiekolwiek aktualizacje, Kaspersky Endpoint Security for Windows automatycznie zainstaluje te ze stanem *Krytyczne*. Pozostałe aktualizacje zostaną zainstalowane, jak je zatwierdzisz.

    Jeśli do zainstalowania uaktualnień modułów aplikacji wymagane jest przejrzenie i zaakceptowanie warunków Umowy licencyjnej i Polityki prywatności, aplikacja zainstaluje uaktualnienia po zaakceptowaniu warunków Umowy licencyjnej i Polityki prywatności przez użytkownika.

13. Zaznacz pole **Kopiuj uaktualnienia do folderu**, aby aplikacja zapisywała pobrane uaktualnienia w folderze, a następnie określ ścieżkę folderu.

14. Skonfiguruj terminarz zadania. Aby zapewnić dostarczanie aktualizacji na czas, zalecane jest włączenie opcji **Po pobraniu nowych uaktualnień do repozytorium**.

15. Kliknij **Zapisz**.

Podczas wykonywania zadania **Aktualizacja** aplikacja wysyła żądanie do serwerów aktualizacji Kaspersky.

Niektóre aktualizacje wymagają zainstalowania najnowszych wersji wtyczek zarządzających.

Informacje o używaniu plików diff do aktualizowania baz danych i modułów aplikacji Kaspersky

Jeśli Kaspersky Security Center Linux pobiera uaktualnienia z serwerów aktualizacji Kaspersky, optymalizuje ruch sieciowy przy użyciu plików diff. Możesz także włączyć używanie plików diff przez urządzenia (Serwery administracyjne, punkty dystrybucji i urządzenia klienckie), które pobierają uaktualnienia z innych urządzeń w sieci.

Informacje o funkcji Pobierz pliki diff

Plik diff opisuje różnice między dwoma wersjami pliku bazy danych lub modułu programu. Użycie plików diff oszczędza ruch sieciowy w sieci firmowej, ponieważ pliki diff zajmują mniej miejsca niż całe pliki baz danych i modułów programu. Jeśli funkcja *Pobierz pliki diff* jest włączona na Serwerze administracyjnym lub w punkcie dystrybucji, pliki diff zostają zapisane na tym Serwerze administracyjnym lub w tym punkcie dystrybucji. W wyniku tego działania, urządzenia, które pobierają uaktualnienia z tego Serwera administracyjnego lub punktu dystrybucji, mogą używać zapisanych plików diff do aktualizacji swoich baz danych i modułów programu.

Aby zoptymalizować użycie plików diff, zalecana jest synchronizacja terminarza aktualizacji urządzeń z terminarzem aktualizacji Serwera administracyjnego lub punktu dystrybucji, z którego urządzenia pobierają uaktualnienia. Jednakże ruch sieciowy można oszczędzić nawet wtedy, gdy urządzenia są aktualizowane kilka razy rzadziej niż Serwer administracyjny lub punkt dystrybucji, z którego urządzenia pobierają uaktualnienia.

Punkty dystrybucji nie używają multiemisji IP do automatycznego rozsyłania plików diff.

Włączanie funkcji Pobierz pliki diff

Etapy

1. **Włączanie funkcji na Serwerze administracyjnym**

   Włącz funkcję w ustawieniach zadania *Pobierz uaktualnienia do repozytorium Serwera administracyjnego*.

2. **Włączanie funkcji dla punktu dystrybucji**

   Włącz funkcję dla punktu dystrybucji, który pobiera uaktualnienia przy użyciu zadania *Pobierz aktualizacje do repozytoriów punktów dystrybucji*.

   Następnie włącz tę funkcję w ustawieniach zasady Agenta sieciowego dla punktu dystrybucji, który otrzymuje aktualizacje z Serwera administracyjnego.

   Następnie włącz funkcję dla punktu dystrybucji, który pobiera uaktualnienia z Serwera administracyjnego.

   Funkcja jest włączona w ustawieniach zasady Agenta sieciowego i — jeśli punkty dystrybucji są przypisywane ręcznie i jeśli chcesz zastąpić ustawienia zasady — w sekcji **Punkty dystrybucji** właściwości Serwera administracyjnego.

Aby sprawdzić, czy funkcja Pobierz pliki diff została pomyślnie włączona, możesz zmierzyć wewnętrzny ruch sieciowy przed i po wykonaniu scenariusza.

Pobieranie uaktualnień przez punkty dystrybucji

Kaspersky Security Center Linux umożliwia punktom dystrybucji pobieranie uaktualnień z Serwera administracyjnego, serwerów Kaspersky bądź też folderu lokalnego lub sieciowego.

W celu skonfigurowania pobierania uaktualnień dla punktu dystrybucji:

1. W menu głównym kliknij nazwę Serwera administracyjnego.

   Zostanie otwarte okno właściwości Serwera administracyjnego.

2. Na zakładce **Ogólne** wybierz sekcję **Punkty dystrybucji**.

3. Kliknij nazwę punktu dystrybucji, przez który aktualizacje będą dostarczane na urządzenia klienckie w grupie.

4. W oknie właściwości punktu dystrybucji wybierz sekcję **Źródło aktualizacji**.

5. Wskaż źródło uaktualnień dla punktu dystrybucji:

   - **Źródło aktualizacji**

     Wybierz źródło aktualizacji dla punktu dystrybucji:

     - Aby zezwolić punktowi dystrybucji na pobieranie uaktualnień z Serwera administracyjnego, zaznacz opcję **Pobierz z Serwera administracyjnego**.

     - Aby umożliwić punktowi dystrybucji otrzymywanie aktualizacji za pomocą zadania, wybierz **Użyj zadania pobierania aktualizacji**, a następnie określ zadanie *Pobierz aktualizacje do repozytoriów punktów dystrybucji*.

       - Jeśli takie zadanie już istnieje na urządzeniu, wybierz zadanie z listy.

       - Jeśli takie zadanie jeszcze nie istnieje na urządzeniu, kliknij łącze **Utwórz zadanie**, aby utworzyć zadanie. Zostanie uruchomiony Kreator tworzenia nowego zadania. Postępuj zgodnie z instrukcjami kreatora.

   - **Pobierz pliki diff**

     Ta opcja włącza funkcję pobierania plików diff.

     Domyślnie opcja ta jest włączona.

Punkt dystrybucji będzie pobierał uaktualnienia z określonego źródła.

Aktualizowanie baz danych i modułów Kaspersky na urządzeniach offline

Aktualizowanie baz danych i modułów Kaspersky na zarządzanych urządzeniach jest ważnym zadaniem do utrzymania ochrony urządzeń przed wirusami i innymi zagrożeniami. Administratorzy zazwyczaj konfigurują regularne aktualizacje poprzez używanie repozytorium Serwera administracyjnego.

Jeśli musisz aktualizować bazy danych i moduły na urządzeniu (lub grupie urządzeń), które nie jest połączone z Serwerem administracyjnym (głównym lub podrzędnym), punktem dystrybucji lub internetem, musisz użyć alternatywnych źródeł aktualizacji, takich jak serwer FTP lub folder lokalny. W tym przypadku musisz dostarczyć pliki żądanych aktualizacji przy użyciu masowego urządzenia przechowywania, takiego jak dysk flash lub zewnętrzny dysk twardy.

Możesz skopiować wymagane aktualizacje z:

- Serwera administracyjnego.

  Aby mieć pewność, że repozytorium Serwera administracyjnego zawiera aktualizacje wymagane dla aplikacji zabezpieczającej zainstalowanej na urządzeniu offline, przynajmniej na jednym z zarządzanych urządzeń online musi być zainstalowana ta sama aplikacja zabezpieczająca. Ta aplikacja musi być skonfigurowana do odbierania aktualizacji z repozytorium Serwera administracyjnego poprzez zadanie *Pobierz aktualizacje do repozytorium Serwera administracyjnego*.

- Dowolne urządzenie, na którym ta sama aplikacja zabezpieczająca jest zainstalowana i skonfigurowana do pobierania aktualizacji z repozytorium Serwera administracyjnego, repozytorium punktu dystrybucji lub bezpośrednie z serwerów aktualizacji Kaspersky.

Poniżej znajduje się przykład konfigurowania aktualizacji baz danych i modułów poprzez kopiowanie ich z repozytorium Serwera administracyjnego.

W celu zaktualizowania baz danych i modułów Kaspersky na urządzeniach offline:

1. Podłącz dysk wymienny do urządzenia, na którym jest zainstalowany Serwer administracyjny.

2. Skopiuj pliki aktualizacji na dysk wymienny.

   Domyślnie, aktualizacje znajdują się w następującej lokalizacji: /var/opt/kaspersky/klnagent_srv/1093/.working/share_srv/Updates/.

   Alternatywnie możesz skonfigurować Kaspersky Security Center Linux do regularnego kopiowania uaktualnień do folderu, który wybierzesz. W tym celu użyj opcji **Kopiuj pobrane aktualizacje do dodatkowych folderów** we właściwościach zadania *Pobierz aktualizacje do repozytorium Serwera administracyjnego*. Jeśli dla tej opcji określisz folder znajdujący się na dysku flash lub wewnętrznym dysku twardym jako folder docelowy, to urządzenie masowego przechowywania będzie zawsze zawierało najnowszą wersję aktualizacji.

3. Na urządzeniach offline skonfiguruj aplikację Kaspersky Endpoint Security, aby odbierała aktualizacje z folderu lokalnego lub zasobu współdzielonego, takiego jak serwer FTP lub folder współdzielony.

   Dostępne instrukcje:

   - Pomoc Kaspersky Endpoint Security for Linux

   - Pomoc Kaspersky Endpoint Security for Windows

4. Skopiuj pliki aktualizacji z dysku wymiennego do folderu lokalnego lub zasobu współdzielonego, którego chcesz użyć jako źródła uaktualnień.

5. Na urządzeniu offline, które wymaga instalacji aktualizacji, uruchom zadanie *Aktualizacja* Kaspersky Endpoint Security for Linux lub Kaspersky Endpoint Security for Windows, w zależności od systemu operacyjnego urządzenia offline.

Po zakończeniu zadania aktualizacji, bazy danych i moduły Kaspersky są aktualne na urządzeniu.

Monitorowanie, raportowanie i audyt

W tej sekcji opisano możliwości monitorowania i raportowania Kaspersky Security Center Linux. Te możliwości dają ogląd infrastruktury, stanów ochrony i statystyk.

Po wdrożeniu Kaspersky Security Center Linux lub podczas jego działania możesz skonfigurować funkcje monitorowania i raportowania, aby najlepiej odpowiadały Twoim potrzebom.

Scenariusz: Monitorowanie i raportowanie

Ta sekcja zawiera scenariusz konfigurowania funkcji monitorowania i raportowania w Kaspersky Security Center Linux.

Wymagania wstępne

Po wdrożeniu Kaspersky Security Center Linux w sieci organizacji, możesz uruchomić jej monitorowanie i generować raporty dotyczące jej funkcjonowania.

Monitorowanie i raportowanie w sieci organizacji odbywa się w etapach:

1. **Konfigurowanie przełączania stanów urządzeń**

   Zapoznaj się z ustawieniami stanów urządzeń w zależności od określonych warunków. Zmieniając te ustawienia, możesz zmienić liczbę zdarzeń z poziomem istotności *Krytyczne* lub *Ostrzeżenie*. Podczas konfigurowania przełączania stanów urządzeń, upewnij się, że:

   - Nowe ustawienia nie są sprzeczne z polityką bezpieczeństwa informacji, obowiązującą w Twojej firmie.
   - Możesz reagować na ważne zdarzenia dotyczące bezpieczeństwa w sieci Twojej organizacji w odpowiednim momencie.

2. **Konfigurowanie powiadomień o zdarzeniach występujących na urządzeniach klienckich**

   Dostępne instrukcje:

   Skonfiguruj powiadamianie (poprzez e-mail, wiadomość SMS lub przez uruchomienie pliku wykonywalnego) o zdarzeniach na urządzeniach klienckich

3. **Wykonywanie zalecanych działań dla powiadomień krytycznych i ostrzegających**

   Dostępne instrukcje:

   Wykonaj zalecane działania dla sieci w swojej organizacji

4. **Sprawdzanie stanu ochrony sieci w swojej organizacji**

Dostępne instrukcje:

- Sprawdź widżeta Stan ochrony
- Wygeneruj i sprawdź Raport o stanie ochrony
- Wygeneruj i przeczytaj Raport o błędach

5. **Lokalizowanie urządzeń klienckich, które nie są chronione**

   Dostępne instrukcje:

   - Przejrzyj widżet Nowe urządzenia
   - Wygeneruj i przeczytaj Raport wdrażania ochrony

6. **Sprawdzanie ochrony urządzeń klienckich**

   Dostępne instrukcje:

   - Wygeneruj i sprawdź raporty z kategorii Stan ochrony i Statystyki zagrożeń
   - Uruchom i sprawdź wybór zdarzeń Krytyczny

7. **Oszacowanie i ograniczenie nagromadzenia zdarzeń w bazie danych**

   Informacje o zdarzeniach występujących podczas działania zarządzanych aplikacji są przesyłane z urządzenia klienckiego i zapisywane w bazie danych Serwera administracyjnego. Aby zmniejszyć obciążenie na Serwerze administracyjnym, oszacuj i ogranicz maksymalną liczbę zdarzeń przechowywanych w bazie danych.

   Dostępne instrukcje:

   - Ograniczanie maksymalnej liczby zdarzeń

8. **Przeglądanie informacji o licencji**

   Dostępne instrukcje:

   - Dodaj widżet Użycie kluczy licencyjnych do pulpitu nawigacyjnego i sprawdź go
   - Wygeneruj i przeczytaj Raport o użyciu kluczy licencyjnych

Wyniki

Po zakończeniu scenariusza zostaniesz poinformowany o ochronie sieci w swojej organizacji i tym samym będziesz mógł zaplanować działania związane z dalszą ochroną.

Informacje o typach monitorowania i raportowania

Informacje na temat zdarzeń dotyczących bezpieczeństwa w sieci organizacji są przechowywane w bazie danych Serwera administracyjnego. Na podstawie zdarzeń Kaspersky Security Center Web Console oferuje następujące typy monitorowania i raportowania w sieci Twojej organizacji:

- Pulpit nawigacyjny
- Raporty
- Wybory zdarzeń
- Powiadomienia

Pulpit nawigacyjny

Pulpit nawigacyjny umożliwia monitorowanie trendów bezpieczeństwa w sieci Twojej organizacji poprzez graficzne przedstawienie informacji.

Raporty

Raporty umożliwiają uzyskanie szczegółowych informacji liczbowych na temat ochrony sieci Twojej organizacji, zapisania tych informacji w pliku, wysłania ich w wiadomości e-mail oraz ich wydrukowania.

Wybory zdarzeń

Wybory zdarzeń oferują widok ekranowy nazwanych zestawów zdarzeń, które są wybrane z bazy danych Serwera administracyjnego. Te zestawy zdarzeń są grupowane zgodnie z następującymi kategoriami:

- Według istotności—**Zdarzenia krytyczne**, **Błędy funkcjonalne**, **Ostrzeżenia** i **Informacja o zdarzeniach**
- Według czasu—**Ostatnie zdarzenia**
- Według typu—**Żądania użytkownika** and **Zdarzenia audytu**

Możesz tworzyć i przeglądać wybory zdarzeń zdefiniowane przez użytkownika oparte na ustawieniach dostępnych do konfiguracji w interfejsie Kaspersky Security Center Web Console.

Powiadomienia

Powiadomienia informują o zdarzeniach oraz pomagają w przyspieszeniu odpowiedzi na te zdarzenia poprzez wykonanie zalecanych działań lub działań, które uznajesz za odpowiednie.

Wywoływanie reguł w trybie Inteligentne uczenie

Ta sekcja zawiera informacje o wykrywaniu obiektów, wykonywanym przez reguły Adaptacyjnej kontroli anomalii w Kaspersky Endpoint Security for Windows na urządzeniach klienckich.

Reguły wykrywają nietypowe zachowania na urządzeniach klienckich i mogą je zablokować. Jeśli reguły działają w trybie Inteligentne uczenie, wykrywają nietypowe zachowania i wysyłają raporty o każdym takim wystąpieniu do Serwera administracyjnego. Aby wyświetlić raporty dotyczące wykrytych nietypowych zachowań, przejdź do **Repozytoria** → **Wyzwalacze reguł w Trybie inteligentnego uczenia**. Możesz potwierdzić wykrycie obiektów jako poprawne lub dodać je jako wykluczenia, żeby ten typ zachowania nie był już uznawany za nietypowy.

Informacje o wykrytych obiektach są przechowywane w dzienniku zdarzeń na Serwerze administracyjnym (wraz z innymi zdarzeniami) i w raporcie Adaptacyjnej kontroli anomalii.

Więcej informacji o Adaptacyjnej kontroli anomalii, regułach, ich trybach i stanach można znaleźć w pomocy Kaspersky Endpoint Security for Windows.

Przeglądanie i potwierdzanie obiektów wykrytych przy użyciu reguł Adaptacyjnej kontroli anomalii

W celu przejrzenia listy obiektów wykrytych przez reguły Adaptacyjnej kontroli anomalii:

1. W menu głównym przejdź do **Repozytoria** → **Wyzwalacze reguł w Trybie inteligentnego uczenia**.

   Lista wyświetla następujące informacje o obiektach wykrytych przy użyciu reguł Adaptacyjnej kontroli anomalii:

   - **Grupa administracyjna**

     Nazwa grupy administracyjnej, do której należy urządzenie.

   - **Wirtualny Serwer administracyjny**

     Wirtualny Serwer administracyjny zarządzający urządzeniem.

   - **Nazwa urządzenia**

     Nazwa urządzenia klienckiego, do którego reguła została zastosowana.

   - **Nazwa**

     Nazwa zastosowanej reguły.

- **Stan**

  Wykluczanie—jeśli administrator przetworzył ten element i dodał go jako wykluczenie do reguł. Ten stan pozostanie do kolejnej synchronizacji urządzenia klienckiego z Serwerem administracyjnym; po synchronizacji element zniknie z listy.

  Potwierdzanie—jeśli administrator przetworzył ten element i zatwierdził go. Ten stan pozostanie do kolejnej synchronizacji urządzenia klienckiego z Serwerem administracyjnym; po synchronizacji element zniknie z listy.

  Pusty—jeśli administrator nie przetworzył tego elementu.

- **Liczba wykryć**

  Liczba wykryć w obrębie jednej reguły heurystycznej, jeden proces i jedno urządzenie klienckie. Ta liczba jest zliczana przez Kaspersky Endpoint Security.

- **Nazwa użytkownika**

  Nazwa użytkownika urządzenia klienckiego, który uruchomił proces, który wygenerował wykrycie.

- **Ścieżka procesu źródłowego**

  Ścieżka do procesu źródłowego, czyli do procesu, który wykonuje akcję (więcej informacji znajdziesz w pomocy do Kaspersky Endpoint Security).

- **Suma kontrolna procesu źródłowego**

  Suma kontrolna SHA256 pliku procesu źródłowego (więcej informacji znajdziesz w pomocy do Kaspersky Endpoint Security).

- **Ścieżka obiektu źródłowego**

  Ścieżka do obiektu, który uruchomił proces (więcej informacji znajdziesz w pomocy do Kaspersky Endpoint Security).

- **Suma kontrolna obiektu źródłowego**

  Suma kontrolna SHA256 pliku źródłowego (więcej informacji znajdziesz w pomocy do Kaspersky Endpoint Security).

- **Ścieżka procesu docelowego**

  Ścieżka do procesu docelowego (więcej informacji znajdziesz w pomocy do Kaspersky Endpoint Security).

- **Suma kontrolna procesu docelowego**

  Suma kontrolna SHA256 pliku docelowego (więcej informacji znajdziesz w pomocy do Kaspersky Endpoint Security).

- **Ścieżka obiektu docelowego**

  Ścieżka do obiektu docelowego (więcej informacji znajdziesz w pomocy do Kaspersky Endpoint Security).

- **Suma kontrolna obiektu docelowego**

  Suma kontrolna SHA256 pliku docelowego (więcej informacji znajdziesz w pomocy do Kaspersky Endpoint Security).

- **Przetworzono**

  Data wykrycia anomalii.

W celu przejrzenia właściwości wykrycia:

1. W menu głównym przejdź do **Repozytoria** → **Wyzwalacze reguł w Trybie inteligentnego uczenia**.

2. Wykonaj jedną z poniższych czynności:

   - W kolumnie **Nazwa** kliknij odnośnik z nazwą wykrycia, które chcesz wyświetlić.

   - Na liście wykryć zaznacz pole wyboru obok wykrycia, które chcesz wyświetlić, a następnie kliknij przycisk **Właściwości**.

   Otworzy się okno właściwości wybranego wykrycia, wyświetlające informacje na jego temat.

Możesz potwierdzić każde wykrycie z listy obiektów wykrytych przez reguły Adaptacyjnej kontroli anomalii lub z okna właściwości wybranego wykrycia.

Aby potwierdzić wykrycie:

- Wybierz jedno lub kilka wykryć na liście wykrytych obiektów i kliknij przycisk **Potwierdź**.

- Otwórz okno właściwości wybranego wykrycia, jak opisano powyżej, a następnie kliknij przycisk **Potwierdź**.

  Stan wykrycia zostanie zmieniony na **Potwierdzanie**. Wykrycie zniknie z listy wykryć po następnej synchronizacji urządzenia klienta z Serwerem administracyjnym.

  Twoje potwierdzenie zostanie uwzględnione w statystykach wykorzystywanych w ramach zasad. Aby uzyskać więcej informacji, zapoznaj się z Pomocą programu Kaspersky Endpoint Security for Windows.

Dodawanie wykluczeń z reguł Adaptacyjnej kontroli anomalii

Kreator Dodaj do wykluczeń Adaptacyjnej kontroli anomalii umożliwia dodawanie wykluczeń z reguł Adaptacyjnej kontroli anomalii dla Kaspersky Endpoint Security.

Aby dodać wykluczenia z reguł Adaptacyjnej kontroli anomalii za pomocą kreatora:

1. Uruchom kreatora w jeden z następujących sposobów:

   - W menu głównym przejdź do **Repozytoria** → **Wyzwalacze reguł w Trybie inteligentnego uczenia**, wybierz jedno lub kilka wykryć, a następnie kliknij przycisk **Wyklucz**.

     Za jednym razem możesz dodać do 1000 wykluczeń.

     Przed dodaniem wykrycia do wykluczeń możesz wyświetlić właściwości wykrycia, klikając nazwę wykrycia lub przycisk **Właściwości**. W otwartym oknie właściwości wykrycia możesz także kliknąć przycisk **Wyklucz**.

   - W menu głównym przejdź do **Monitorowanie** → **Wybory zdarzeń**, kliknij odnośnik z wybranym zdarzeniem, zaznacz pole wyboru obok wykrycia, które chcesz wykluczyć, a następnie kliknij przycisk **Wyklucz z Adaptacyjnej kontroli anomalii**.

   Zostanie uruchomiony kreator Dodaj do wykluczeń Adaptacyjnej kontroli anomalii. Przejdź przez kroki kreatora, korzystając z przycisku **Dalej**.

2. Wybierz zasady i profile, do których chcesz dodać wykluczenia.

   Zasad dziedziczonych nie można aktualizować. Jeśli nie masz uprawnień do modyfikowania zasady, ta zasada nie zostanie zaktualizowana.

3. Kliknij **Gotowe**, aby zamknąć kreator.

Stan wykrycia zostanie zmieniony na **Wykluczanie**. Wykrycie zniknie z listy wykryć po następnej synchronizacji urządzenia klienckiego z Serwerem administracyjnym. Wykluczenie z reguł Adaptacyjnej kontroli anomalii zostało skonfigurowane i zastosowane.

Pulpit nawigacyjny i widżety

Ta sekcja zawiera informacje o panelu kontrolnym i widżetach udostępnianych przez panel kontrolny. Sekcja zawiera instrukcje dotyczące zarządzania widżetami i konfigurowania ich ustawień.

Korzystanie z pulpitu nawigacyjnego

Pulpit nawigacyjny umożliwia monitorowanie trendów bezpieczeństwa w sieci Twojej organizacji poprzez graficzne przedstawienie informacji.

Pulpit nawigacyjny jest dostępny w Kaspersky Security Center Web Console w sekcji **Monitorowanie** po kliknięciu **Pulpit nawigacyjny**.

Pulpit nawigacyjny zawiera widżety, które można dostosować. Możesz wybrać dużą liczbę różnych widżetów, przedstawionych w postaci wykresu kołowego lub diagramu pierścieniowego, tabeli, wykresów, wykresów słupkowych oraz list. Informacje wyświetlane w widżetach są automatycznie aktualizowane, okres aktualizacji wynosi od jednej do dwóch minut. Przedział czasu między aktualizacjami jest inny dla każdego widżeta. Możesz ręcznie odświeżyć dane dotyczące widżeta w dowolnym momencie, korzystając z menu ustawień.

Domyślnie widżety zawierają informacje o wszystkich zdarzeniach przechowywanych w bazie danych Serwera administracyjnego.

Kaspersky Security Center Web Console zawiera domyślny zestaw widżetów należących do następujących kategorii:

- **Stan ochrony**
- **Wdrażanie**
- **Aktualizowanie**
- **Statystyki zagrożeń**
- **Inne**

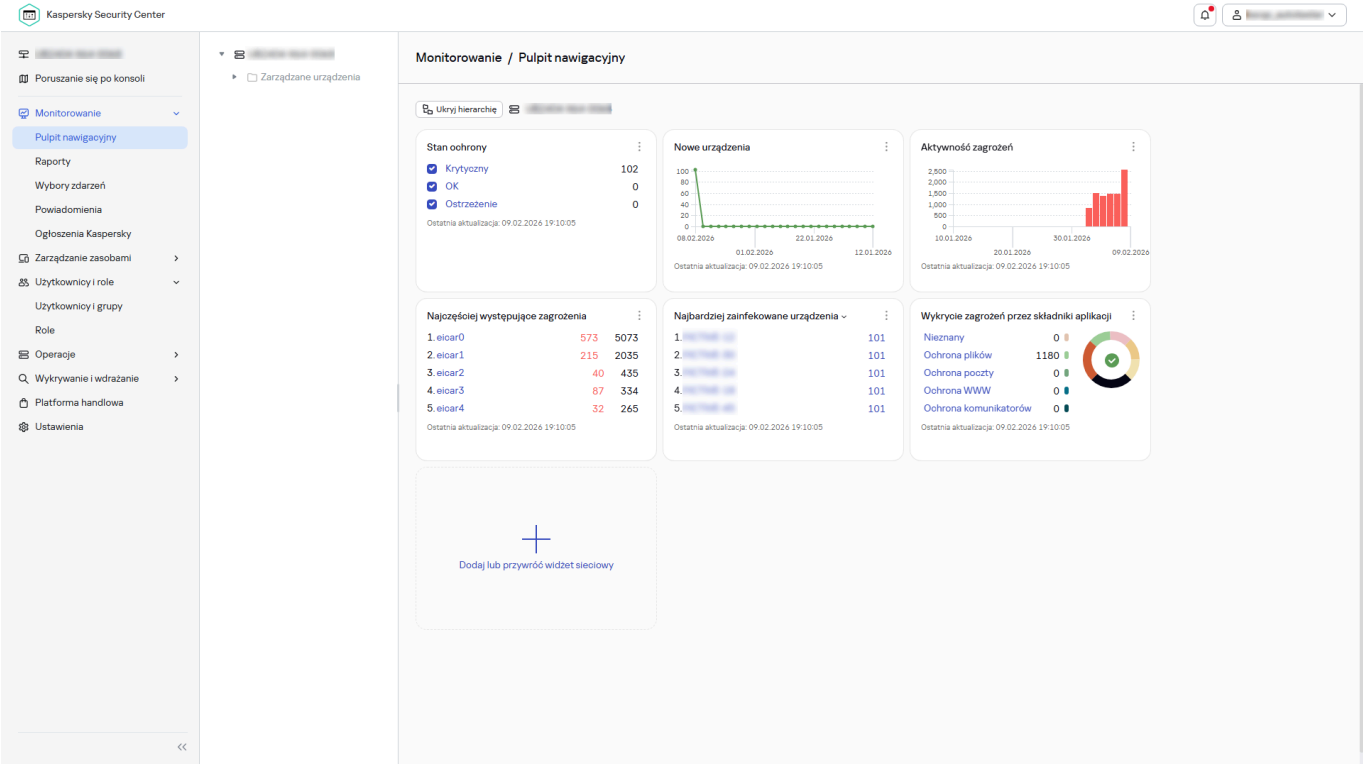
Niektóre widżety posiadają informacje tekstowe z odnośnikami. Po kliknięciu odnośnika zostaną wyświetlone informacje szczegółowe.

Podczas konfigurowania pulpitu nawigacyjnego możesz dodać widżety, których potrzebujesz, ukryć widżety, których nie potrzebujesz, zmienić rozmiar lub wygląd widżetów, przenieść widżety, a także zmienić ich ustawienia.

Dodawanie widżetów do pulpitu nawigacyjnego

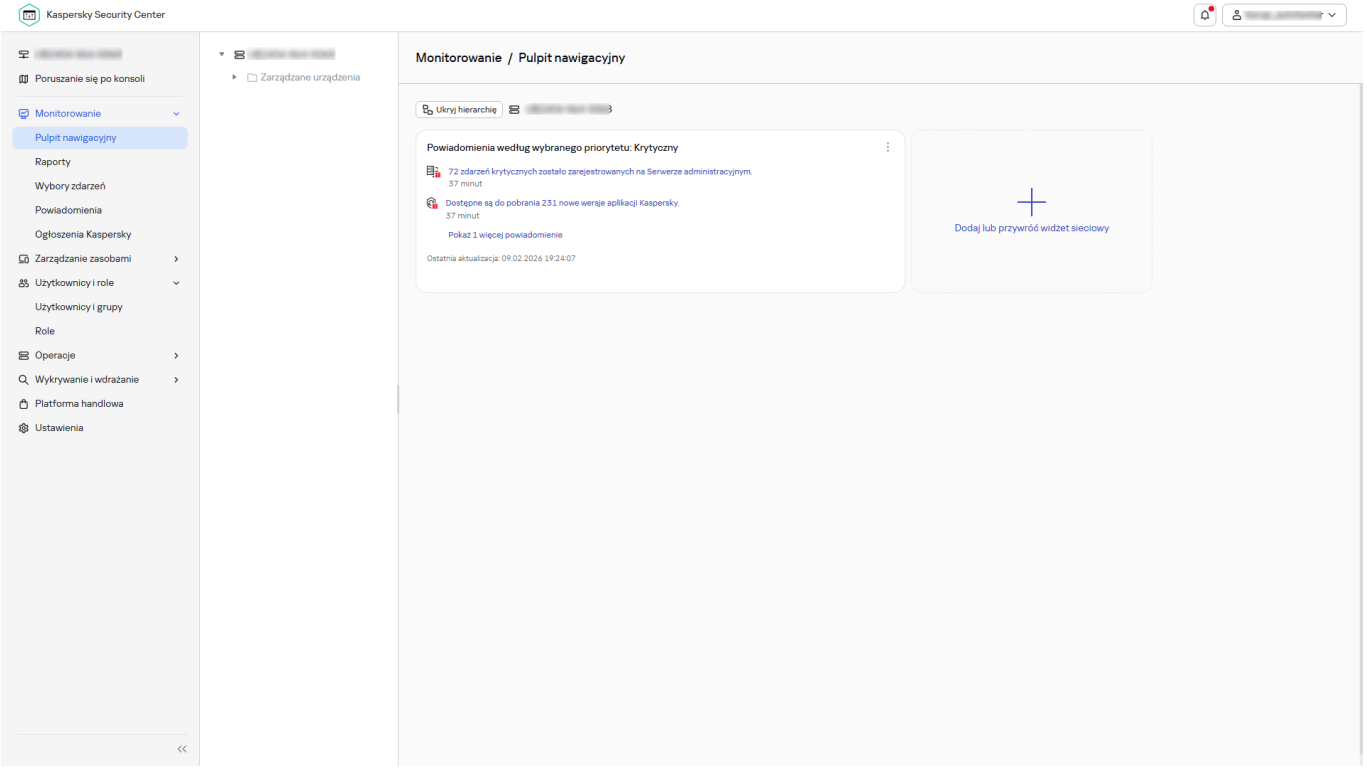
W celu dodania widżetów do pulpitu nawigacyjnego:

1. W menu głównym przejdź do **Monitorowanie** → **Pulpit nawigacyjny**.



Pulpit nawigacyjny z widżetami

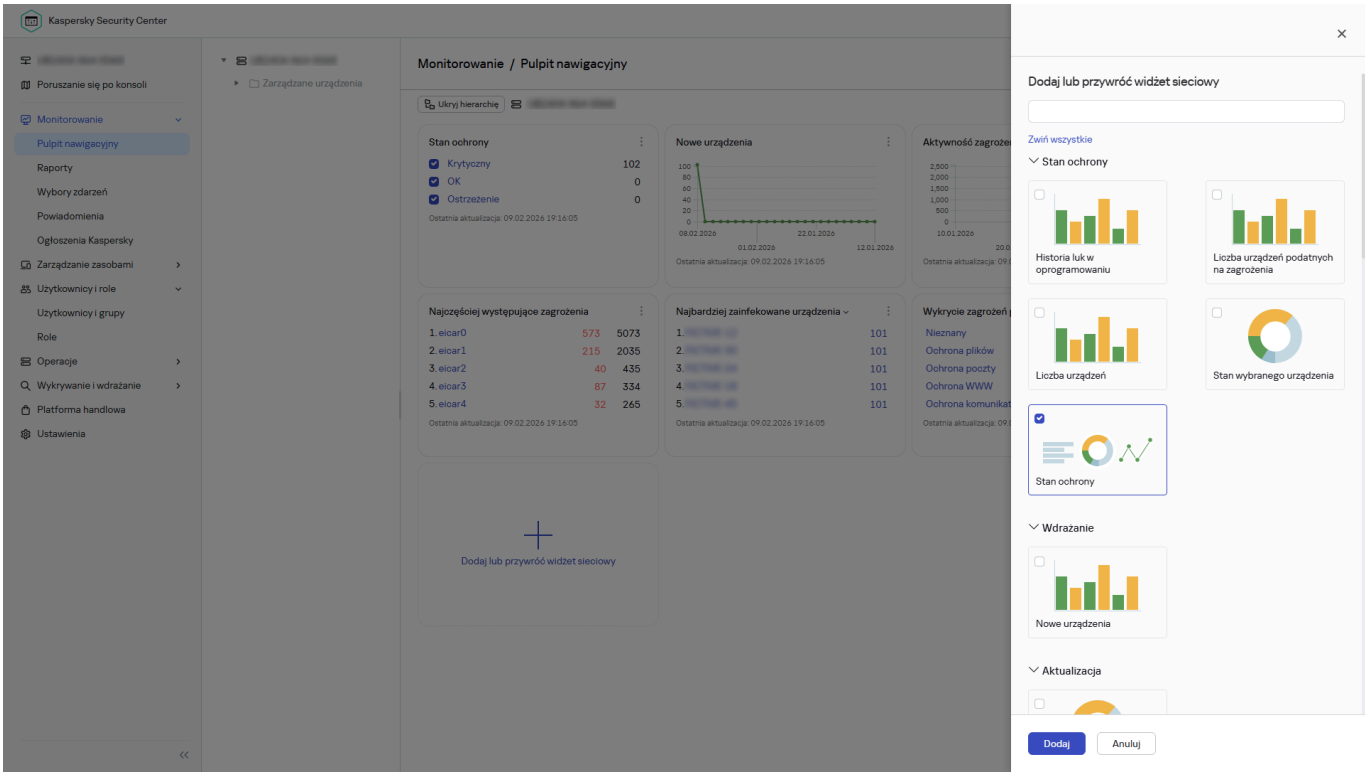
2. Kliknij przycisk **Dodaj lub przywróć widżet sieciowy**.



Dodawanie widżetu

3. Na liście dostępnych widżetów wybierz widżety, które chcesz dodać do pulpitu nawigacyjnego.

Widżety są pogrupowane według kategorii. Aby wyświetlić listę widżetów należących do kategorii, kliknij ikonę strzałki skierowanej w prawo (>), znajdującą się obok nazwy kategorii.



Wybieranie typu widżetu

4. Kliknij przycisk **Dodaj**.

Wybrane widżety zostaną dodane na końcu pulpitu nawigacyjnego.

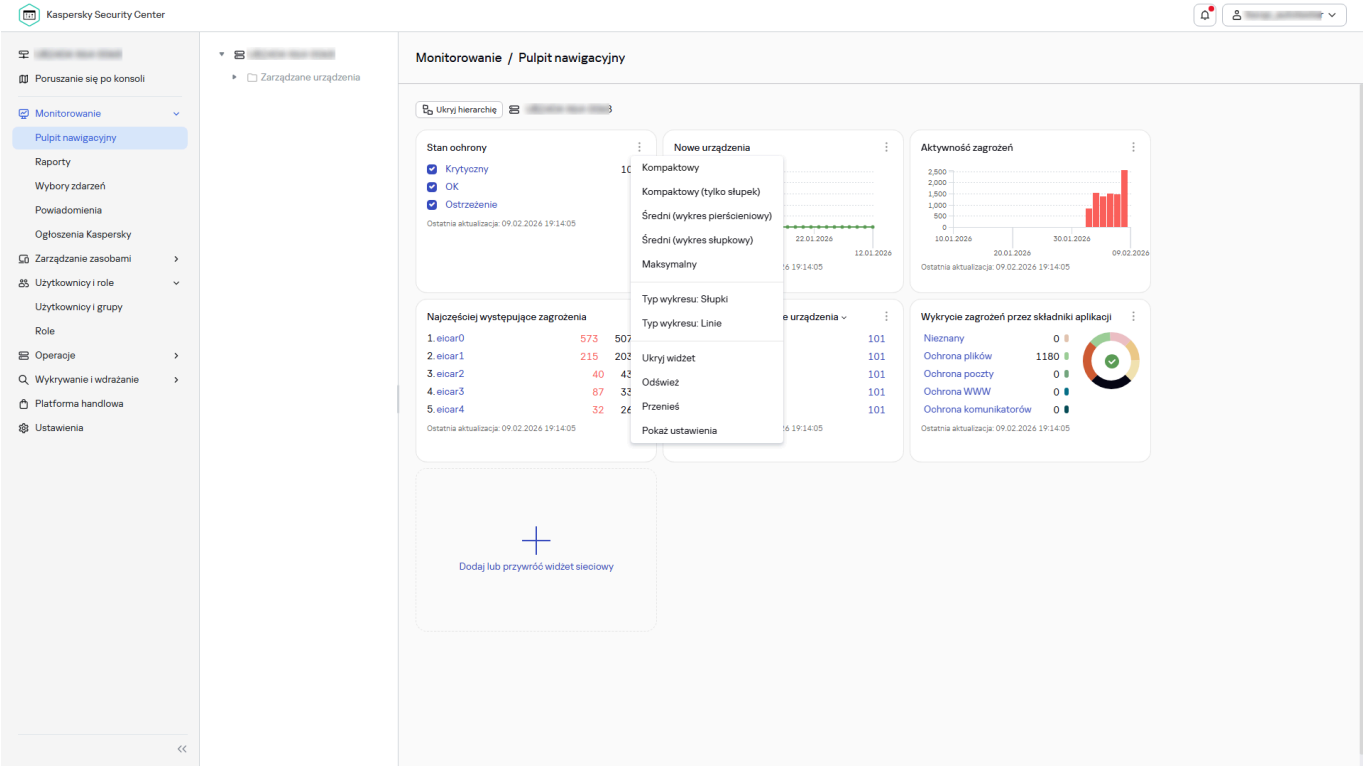
Teraz możesz edytować reprezentację i parametry dodanych widżetów.

Ukrywanie widżetu na pulpicie nawigacyjnym

W celu ukrycia widżetu na pulpicie nawigacyjnym:

1. W menu głównym przejdź do **Monitorowanie** → **Pulpit nawigacyjny**.

2. Kliknij ikonę ustawienia(⚙), znajdującą się obok widżetu, który chcesz ukryć.



Menu widżetu

3. Wybierz **Ukryj widżet**.

4. W otwartym oknie **Ostrzeżenie** kliknij **OK**.

Wybrany widżet zostanie ukryty. Następnie możesz ponownie dodać ten widżet do pulpitu nawigacyjnego.

Przenoszenie widżetu na pulpicie nawigacyjnym

W celu przeniesienia widżetu na pulpicie nawigacyjnym:

1. W menu głównym przejdź do **Monitorowanie** → **Pulpit nawigacyjny**.

2. Kliknij ikonę ustawienia (⚙), znajdującą się obok widżetu, który chcesz przenieść.

3. Wybierz **Przenieś**.

4. Kliknij miejsce, do którego chcesz przenieść widżet. Możesz wybrać tylko inny widżet.

Miejsca wybranych widżetów zostaną zamienione.

Zmiana wyglądu i rozmiaru widżetu

Dla widżetów, które wyświetlają wykres, możesz zmienić jego reprezentację-wykres słupkowy lub wykres liniowy. Dla niektórych widżetów możesz zmienić ich rozmiar: kompaktowy, średni lub maksymalny.

W celu zmiany reprezentacji widżetu:

1. W menu głównym przejdź do **Monitorowanie** → **Pulpit nawigacyjny**.
2. Kliknij ikonę ustawienia (⚙), znajdującą się obok widżetu, który chcesz edytować.
3. Wykonaj jedną z poniższych czynności:
   - Aby wyświetlić widżet jako wykres słupkowy, wybierz **Typ wykresu: Słupki**.
   - Aby wyświetlić widżet jako wykres liniowy, wybierz **Typ wykresu: Linie**.
   - W celu zmiany obszaru zajętego przez widżet, wybierz jedną z wartości:
     - **Kompaktowy**
     - **Kompaktowy (tylko słupek)**
     - **Średni (wykres pierścieniowy)**
     - **Średni (wykres słupkowy)**
     - **Maksymalny**

Reprezentacja wybranego widżetu zostanie zmieniona.

Zmiana ustawień widżetu

W celu zmiany ustawień widżetu:

1. W menu głównym przejdź do **Monitorowanie** → **Pulpit nawigacyjny**.
2. Kliknij ikonę ustawienia (⚙), znajdującą się obok widżetu, który chcesz zmienić.
3. Wybierz **Pokaż ustawienia**.
4. Jeśli zostanie otwarte okno ustawień widżetu, zmień ustawienia widżetu zgodnie z wymaganiami.
5. Kliknij **Zapisz**, aby zachować zmiany.

Ustawienia wybranego widżetu zostaną zmienione.

Zestaw ustawień zależy od określonego widżetu. Poniżej znajdują się podstawowe ustawienia:

- **Zakres widżeta** (zestaw obiektów, dla których widżet wyświetla informacje)—na przykład, grupa administracyjna lub wybór urządzeń.
- **Wybierz zadanie** (zadanie, dla którego widżet wyświetla informacje).
- **Przedział czasu** (przedział czasu, w trakcie którego informacje są wyświetlane w widżecie)—między dwoma określonymi datami; od określonej daty do bieżącego dnia; lub od bieżącego dnia minus określoną liczbę dni do bieżącego dnia.
- **Ustaw na Krytyczne, jeśli określono następujące ustawienia** i **Ustaw na Ostrzeżenie, jeśli określono następujące ustawienia** (reguły, które określają kolor wskaźnika).

Po zmianie ustawień widżetu możesz ręcznie odświeżyć dane w widżecie.

Aby odświeżyć dane w widżecie:

1. W menu głównym przejdź do **Monitorowanie** → **Pulpit nawigacyjny**.
2. Kliknij ikonę ustawienia (⚙), znajdującą się obok widżetu, który chcesz przenieść.
3. Wybierz opcję **Odśwież**.

   Dane w widżecie zostaną odświeżone.

Informacje o trybie korzystania tylko z pulpitu

Możesz skonfigurować tryb korzystania tylko z pulpitu dla pracowników, którzy nie zarządzają siecią, ale chcą przeglądać statystyki ochrony sieci w Kaspersky Security Center Linux (na przykład dla menedżera najwyższego poziomu). Gdy użytkownik ma włączony ten tryb, wyświetlany jest tylko pulpit nawigacyjny z predefiniowanym zestawem widżetów. Dzięki temu może monitorować statystyki określone w widżetach, na przykład stan ochrony wszystkich zarządzanych urządzeń, liczbę ostatnio wykrytych zagrożeń lub listę najczęstszych zagrożeń w sieci.

Gdy użytkownik pracuje w trybie korzystania tylko z pulpitu, stosowane są następujące ograniczenia:

- Menu główne nie jest wyświetlane użytkownikowi, więc nie może on zmienić ustawień ochrony sieci.
- Użytkownik nie może wykonywać żadnych akcji z widżetami, na przykład dodawać widżetów lub ich ukrywać. Dlatego należy umieścić w pulpicie nawigacyjnym wszystkie potrzebne użytkownikowi widżety i skonfigurować je, np. ustawić zasadę liczenia obiektów lub określić przedział czasowy.

Nie można przypisać sobie trybu korzystania tylko z pulpitu. Jeśli chcesz pracować w tym trybie, skontaktuj się z administratorem systemu, dostawcą usług zarządzanych (MSP) lub użytkownikiem z uprawnieniami **Modyfikacja listy ACL obiektów** w obszarze **Funkcje ogólne: uprawnienia użytkownika**.

Konfigurowanie trybu korzystania tylko z pulpitu

Zanim zaczniesz konfigurować Tryb korzystania tylko z pulpitu, upewnij się, że spełnione są następujące wymagania wstępne:

- Masz uprawnienia **Modyfikacja list ACL obiektów** w obszarze funkcjonalnym **Funkcje ogólne: uprawnienia użytkownika**. Jeśli nie masz tych uprawnień, nie będzie zakładki do konfiguracji trybu.
- Użytkownik ma uprawnienia **Odczyt** w obszarze funkcjonalnym **Funkcje ogólne: funkcjonalność podstawowa**.

Jeśli w Twojej sieci istnieje hierarchia Serwerów administracyjnych, aby skonfigurować tryb korzystania tylko z pulpitu, przejdź do serwera, na którym dostępne jest konto użytkownika na zakładce **Użytkownicy** sekcji **Użytkownicy i role** → **Użytkownicy i grupy**. Może to być serwer główny lub fizyczny serwer pomocniczy. Nie ma możliwości dostosowania trybu na serwerze wirtualnym.

W celu skonfigurowania trybu korzystania tylko z pulpitu:

1. W menu głównym przejdź do opcji **Użytkownicy i role** → **Użytkownicy i grupy**, a następnie wybierz zakładkę **Użytkownicy**.
2. Kliknij nazwę konta użytkownika, dla którego chcesz dostosować pulpit nawigacyjny za pomocą widżetów.
3. W otwartym oknie ustawień konta wybierz zakładkę **Pulpit nawigacyjny**.

   Na karcie, która się otworzy, zostanie wyświetlony ten sam pulpit nawigacyjny, co pulpit dla użytkownika.
4. Jeśli opcja **Wyświetlaj konsolę w trybie korzystania tylko z pulpitu** jest włączona, przełącz przełącznik, aby ją wyłączyć.

   Gdy ta opcja jest włączona, nie można również zmienić pulpitu nawigacyjnego. Po wyłączeniu opcji możesz zarządzać widżetami.
5. Skonfiguruj wygląd pulpitu nawigacyjnego. Zestaw widżetów przygotowany w zakładce **Pulpit nawigacyjny** jest dostępny dla użytkownika z konfigurowalnym kontem. Użytkownik nie może zmieniać żadnych ustawień ani rozmiaru widżetów, dodawać ani usuwać żadnych widżetów z pulpitu nawigacyjnego. Dlatego dostosuj je dla użytkownika, aby mógł przeglądać statystyki ochrony sieci. W tym celu w zakładce **Pulpit nawigacyjny** możesz wykonać te same akcje z widżetami, co w sekcji **Monitorowanie** → **Pulpit nawigacyjny**:
   - Dodaj nowe widżety do pulpitu nawigacyjnego.
   - Ukryj widżety, których użytkownik nie potrzebuje.
   - Przenieś widżety w określonej kolejności.
   - Zmień rozmiar lub wygląd widżetów.
   - Zmień ustawienia widżetu.
6. Przełącz przycisk przełącznika, aby włączyć opcję **Wyświetlaj konsolę w trybie korzystania tylko z pulpitu**.

   Następnie dla użytkownika dostępny będzie tylko pulpit nawigacyjny. Użytkownik może monitorować statystyki, ale nie może zmieniać ustawień ochrony sieci i wyglądu pulpitu nawigacyjnego. Ponieważ wyświetlany jest ten sam pulpit nawigacyjny, co dla użytkownika, nie można również zmienić pulpitu nawigacyjnego.

Jeśli pozostawisz tę opcję wyłączoną, dla użytkownika zostanie wyświetlone menu główne, dzięki czemu będzie on mógł wykonywać różne akcje w Kaspersky Security Center Linux, w tym zmieniać ustawienia bezpieczeństwa i widżety.

7. Po zakończeniu konfigurowania trybu korzystania tylko z pulpitu kliknij przycisk **Zapisz**. Dopiero po tym przygotowany pulpit nawigacyjny zostanie wyświetlony użytkownikowi.

8. Jeśli użytkownik chce przeglądać statystyki obsługiwanych aplikacji Kaspersky i potrzebuje do tego uprawnień dostępu, skonfiguruj uprawnienia dla użytkownika. Następnie dane aplikacji Kaspersky będą wyświetlane dla użytkownika w widżetach tych aplikacji.

Teraz użytkownik może zalogować się do Kaspersky Security Center Linux na swoim koncie i monitorować statystyki ochrony sieci w trybie korzystania tylko z pulpitu.

Raporty administracyjne i ochrony

W tej sekcji opisano, jak używać raportów, zarządzać niestandardowymi szablonami raportów, używać szablonów raportów do generowania nowych raportów i tworzyć zadania dostarczania raportów.

Korzystanie z raportów

Raporty umożliwiają uzyskanie szczegółowych informacji liczbowych na temat ochrony sieci Twojej organizacji, zapisania tych informacji w pliku, wysłania ich w wiadomości e-mail oraz ich wydrukowania.

Raporty są dostępne w Kaspersky Security Center Web Console w sekcji **Monitorowanie** po kliknięciu **Raporty**.

Domyślnie, raporty zawierają informacje dla ostatnich 30 dni.

Kaspersky Security Center Linux zawiera domyślny zestaw raportów należących do następujących kategorii:

- **Stan ochrony**
- **Wdrażanie**
- **Aktualizowanie**
- **Statystyki zagrożeń**
- **Inne**

Możesz tworzyć niestandardowe szablony raportu, edytować szablony raportu oraz usuwać je.

Możesz tworzyć raporty, które są oparte na istniejących szablonach, eksportować raporty do plików, a także tworzyć zadania dostarczania raportów.

Tworzenie szablonu raportu

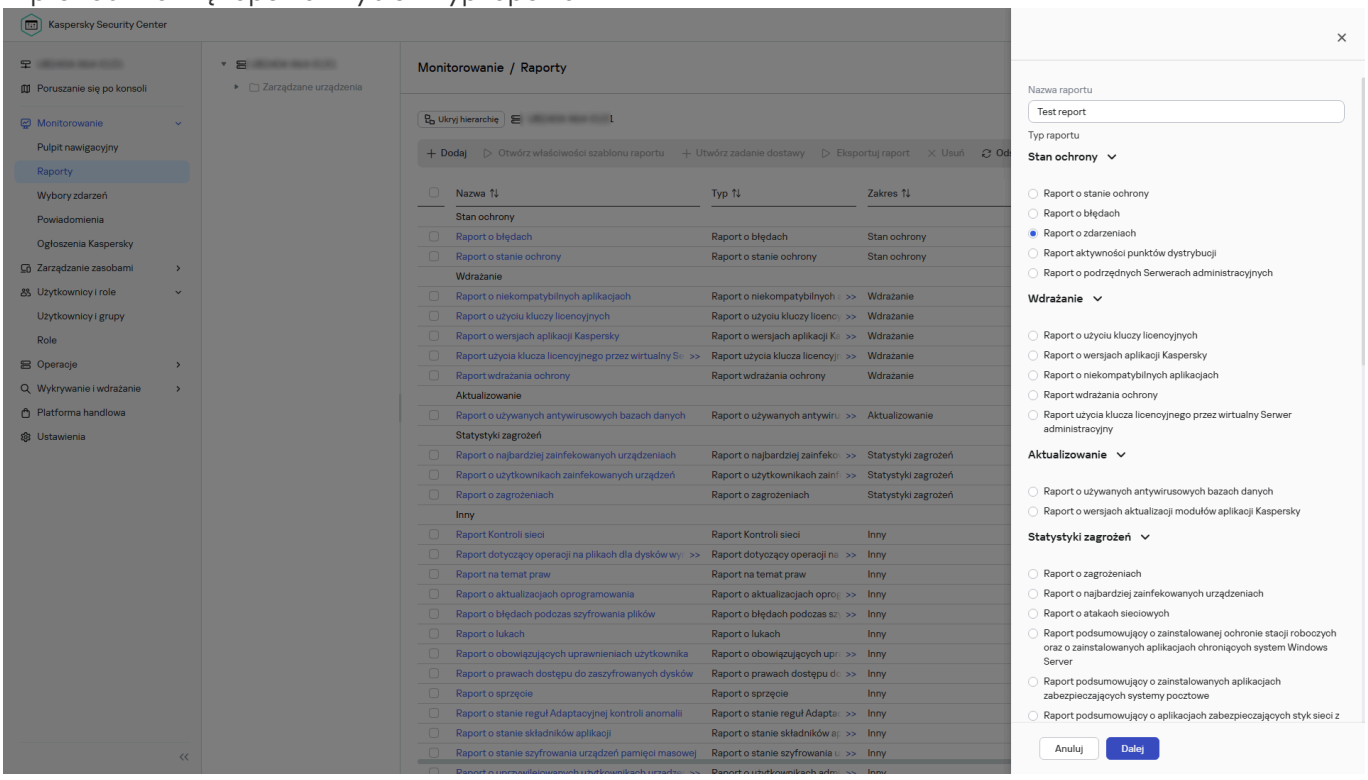
W celu utworzenia szablonu raportu:

1. W menu głównym przejdź do **Monitorowanie** → **Raporty**.

2. Kliknij **Dodaj**.

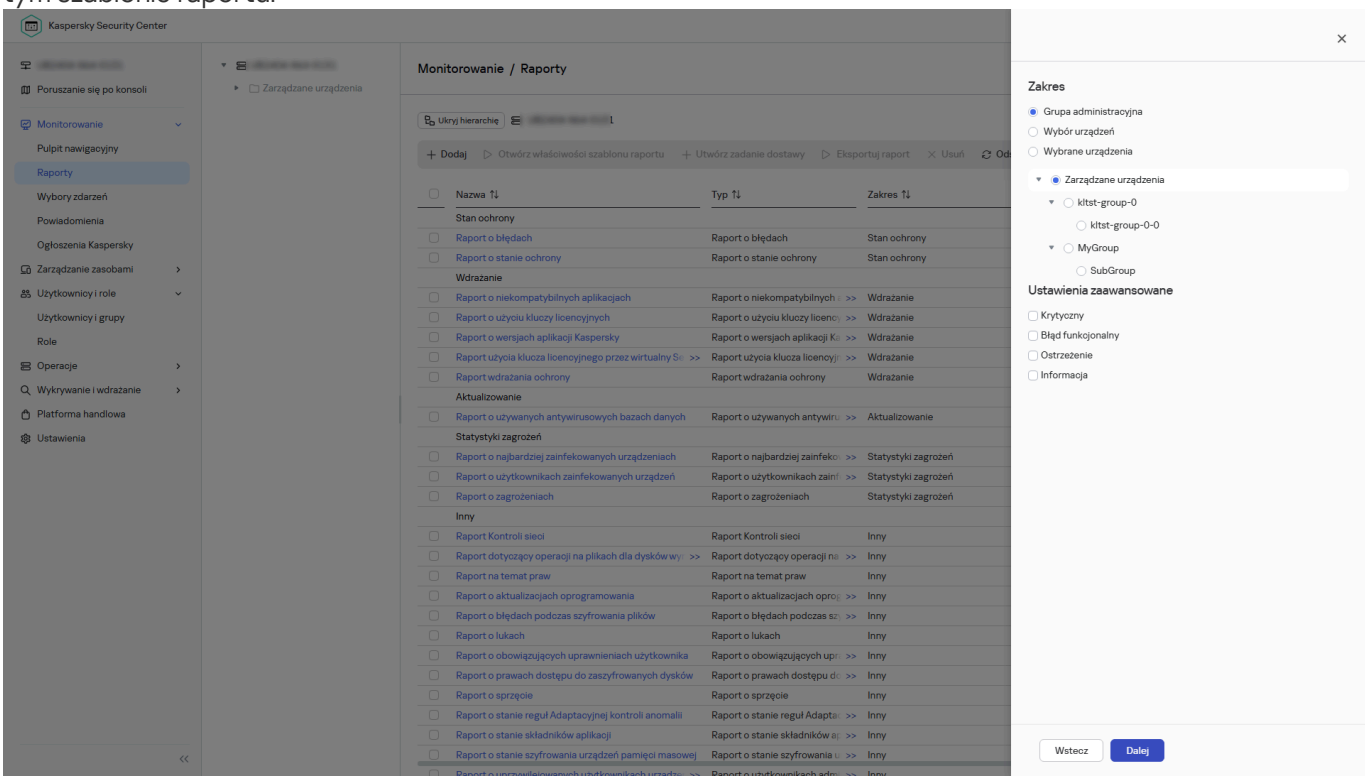
   Zostanie uruchomiony Kreator tworzenia nowego szablonu raportu. Przejdź przez kroki kreatora, korzystając z przycisku **Dalej**.

3. Wprowadź nazwę raportu i wybierz typ raportu.



Określanie nazwy raportu i wybieranie typu raportu

4. W kroku **Zakres** wybierz zestaw urządzeń klienckich (grupę administracyjną, wybór urządzeń, wybrane urządzenia lub wszystkie urządzenia w sieci), których dane zostaną wyświetlone w raportach, które są oparte na tym szablonie raportu.

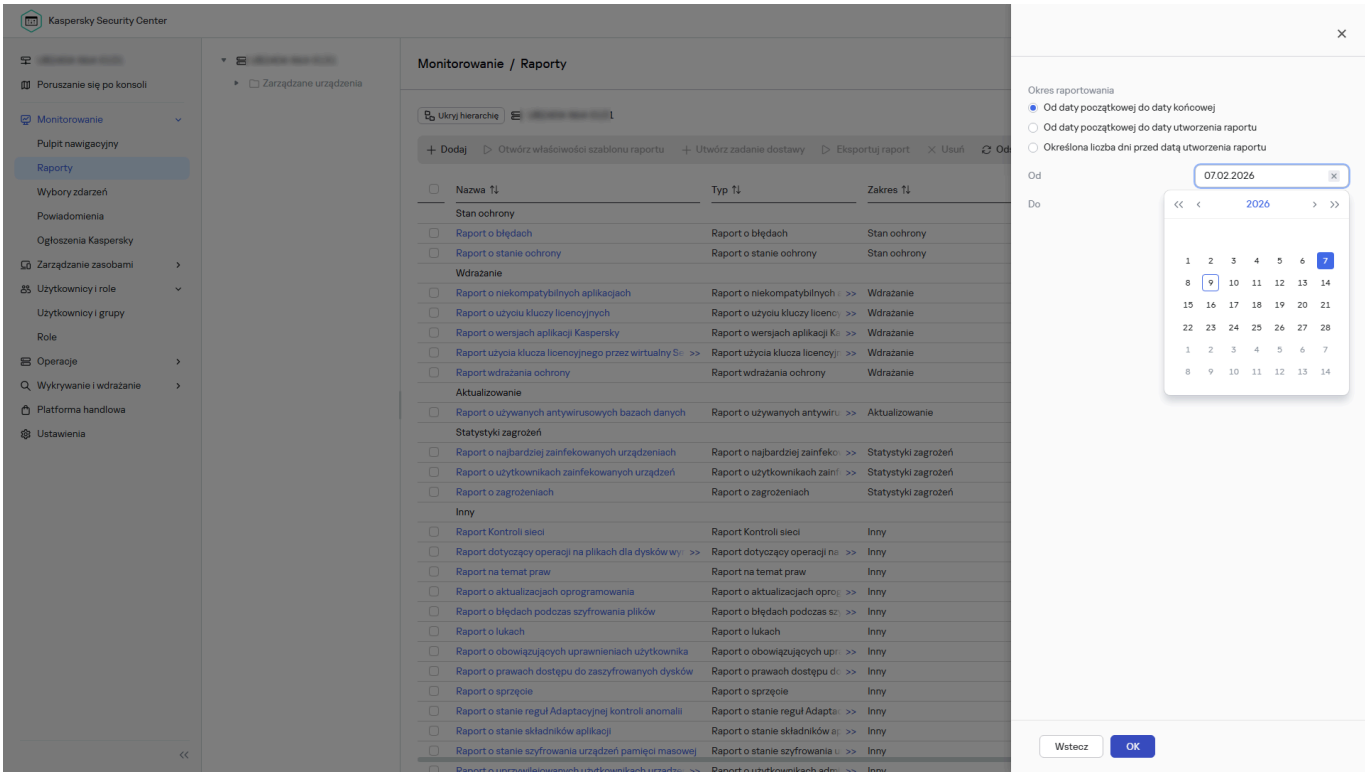


Określanie zakresu raportu

5. W kroku **Okres raportowania** kreatora określ okres raportowania. Dostępne wartości wyglądają następująco:

- Między dwoma określonymi datami
- Od określonej daty do daty utworzenia raportu
- Od daty utworzenia raportu minus określona liczba dni do daty utworzenia raportu

Dla niektórych raportów ta strona może nie być wyświetlana.



Określanie okresu raportowania

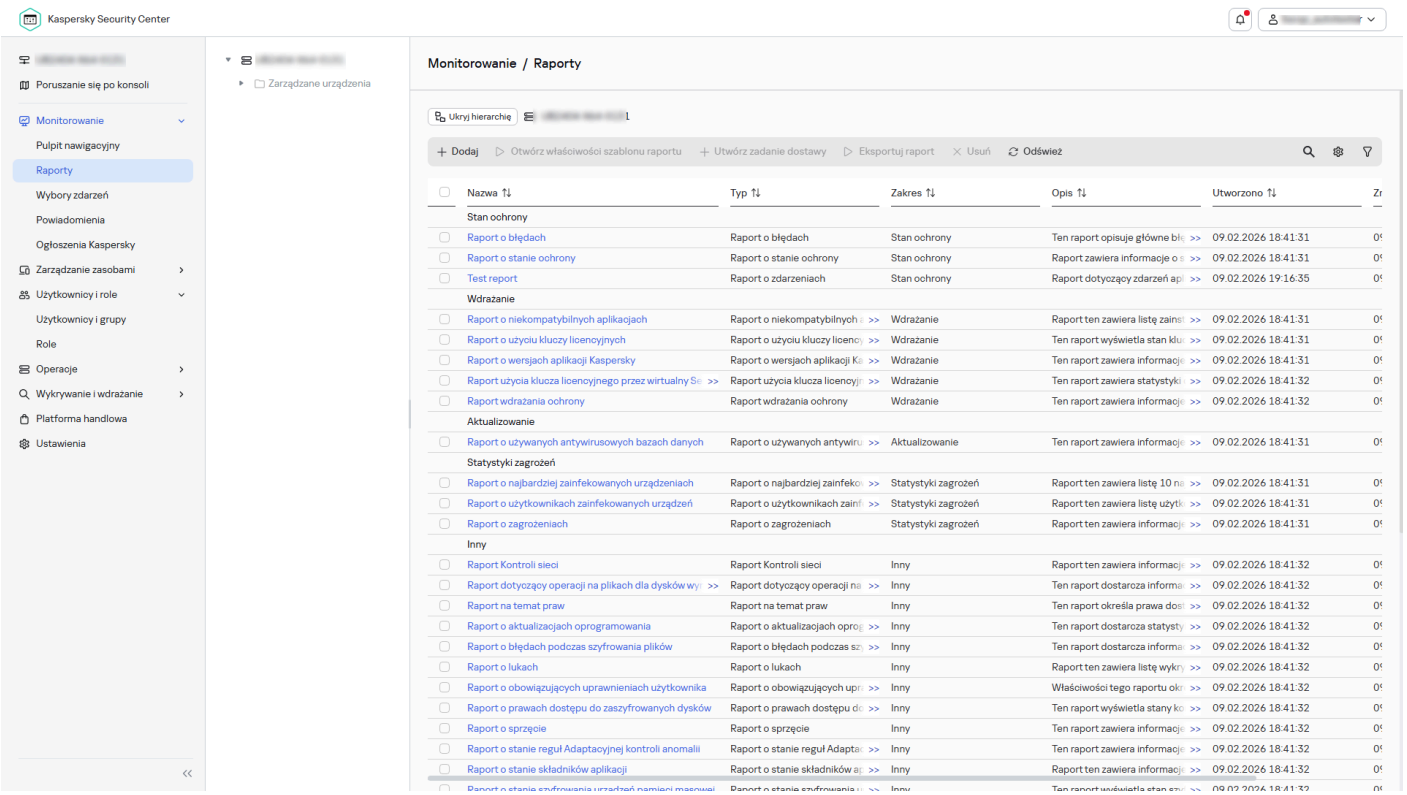
6. Kliknij **OK**, aby zamknąć kreator.

7. Wykonaj jedną z poniższych czynności:

- Kliknij przycisk **Zapisz i uruchom**, aby zapisać nowy szablon raportu i uruchomić raport w oparciu o niego.
  Szablon raportu zostanie zapisany. Raport zostanie wygenerowany.

- Kliknij przycisk **Zapisz**, aby zapisać nowy szablon raportu.
  Szablon raportu zostanie zapisany.

Możesz użyć nowego szablonu do generowania i wyświetlania raportów.



Lista raportów

Przeglądanie i edytowanie właściwości szablonu raportu

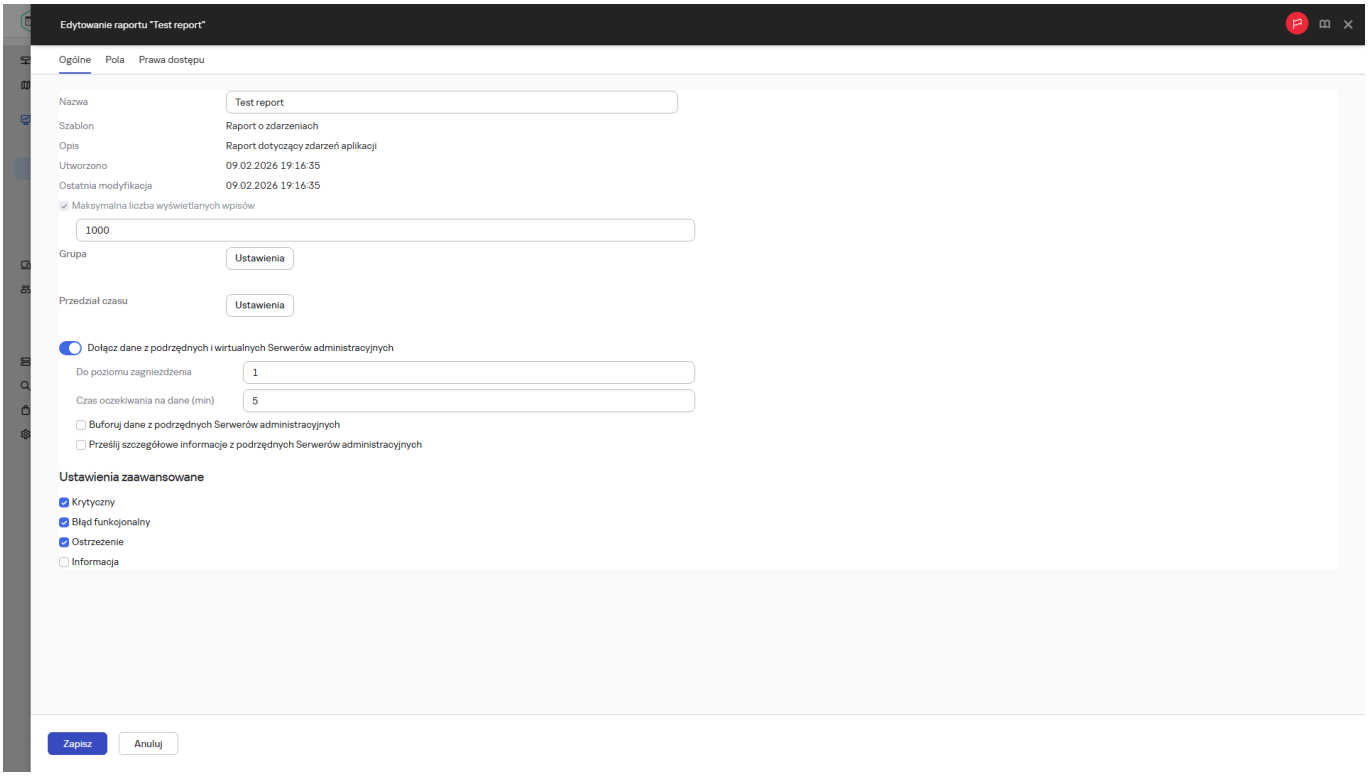
Możesz przeglądać i edytować podstawowe właściwości szablonu raportu, na przykład, nazwę szablonu raportu lub pola wyświetlane w raporcie.

W celu przejrzenia i edytowania właściwości szablonu raportu:

1. W menu głównym przejdź do **Monitorowanie** → **Raporty**.
2. Zaznacz pole obok szablonu raportu, którego właściwości chcesz przejrzeć i edytować.

   Alternatywnie możesz w pierwszej kolejności wygenerować raport, a następnie kliknąć przycisk **Edytuj**.
3. Kliknij przycisk **Otwórz właściwości szablonu raportu**.

Zostanie otwarte okno **Edytowanie raportu <Nazwa raportu>** na zakładce **Ogólne**.



Właściwości szablonu raportu

4. Edytuj właściwości szablonu raportu:

- Zakładka **Ogólne**:

  - Nazwa szablonu raportu

  - **Maksymalna liczba wyświetlanych wpisów**

    Jeśli ta opcja jest włączona, liczba wpisów wyświetlanych w tabeli ze szczegółowymi danymi raportu nie wynosi więcej niż określona wartość. Należy pamiętać, że ta opcja nie wpływa na maksymalną liczbę zdarzeń, które można uwzględnić w raporcie podczas eksportowania raportu do pliku.

    Wpisy w raporcie są najpierw przechowywane zgodnie z regułami określonymi w sekcji **Pola** → **Pola szczegółów** właściwości szablonu raportu, a następnie przechowywane są tylko pierwsze wpisy wynikowe. Nagłówek tabeli ze szczegółowymi danymi raportu pokazuje wyświetloną liczbę wpisów oraz całkowitą dostępną liczbę wpisów, które odpowiadają ustawieniom innego szablonu raportu.

    Jeśli ta opcja jest wyłączona, tabela ze szczegółowymi danymi raportu wyświetla wszystkie dostępne wpisy. Nie jest zalecane wyłączenie tej opcji. Ograniczenie liczby wyświetlanych wpisów raportu zmniejsza obciążenie systemu zarządzania bazą danych (DBMS) i skraca czas wymagany do wygenerowania i eksportowania raportu. Niektóre z raportów zawierają zbyt wiele wpisów. W takiej sytuacji może być trudno przeczytać i przeanalizować je wszystkie. Dodatkowo, podczas tworzenia takiego raportu, na Twoim urządzeniu może zabraknąć pamięci, co w konsekwencji uniemożliwi przejrzenie raportu.

    Domyślnie opcja ta jest włączona. Domyślna wartość to 1000.

  - **Grupa**

    Kliknij przycisk **Ustawienia**, aby zmienić zestaw urządzeń klienckich, dla których tworzony jest raport. Dla niektórych typów raportów przycisk może być niedostępny. Rzeczywiste ustawienia zależą od ustawień określonych podczas tworzenia szablonu raportu.

  - **Przedział czasu**

Kliknij przycisk **Ustawienia**, aby zmodyfikować okres raportowania. Dla niektórych typów raportów przycisk może być niedostępny. Dostępne wartości wyglądają następująco:

- Między dwoma określonymi datami
- Od określonej daty do daty utworzenia raportu
- Od daty utworzenia raportu minus określona liczba dni do daty utworzenia raportu

- **Dołącz dane z podrzędnych i wirtualnych Serwerów administracyjnych**

  Jeśli ta opcja jest włączona, raport zawiera informacje z podrzędnych i wirtualnych Serwerów administracyjnych, które podlegają Serwerowi administracyjnemu, dla którego utworzono szablon raportu.

  Wyłącz tę opcję, jeśli chcesz przejrzeć dane tylko z bieżącego Serwera administracyjnego.

  Domyślnie opcja ta jest włączona.

- **Do poziomu zagnieżdżenia**

  Raport zawiera dane z podrzędnych i wirtualnych Serwerów administracyjnych, które znajdują się pod bieżącym Serwerem administracyjnym na poziomie zagnieżdżenia, który jest mniejszy niż lub równy określonej wartości.

  Domyślna wartość to 1. Możesz chcieć zmienić tę wartość, jeśli musisz zbierać informacje z podrzędnych Serwerów administracyjnych znajdujących się na niższych poziomach drzewa.

- **Czas oczekiwania na dane (min)**

  Przed wygenerowaniem raportu, Serwer administracyjny, dla którego tworzony jest szablon raportu, oczekuje na dane z podrzędnych Serwerów administracyjnych przez określoną liczbę minut. Jeśli żadne dane nie są pobierane z podrzędnego Serwera administracyjnego pod koniec tego okresu, raport i tak zostanie uruchomiony. Zamiast rzeczywistych danych, raport wyświetla dane pobrane z pamięci podręcznej (jeśli opcja **Buforuj dane z podrzędnych Serwerów administracyjnych** jest włączona) lub **N/A** (nie jest dostępne) w innym przypadku.

  Domyślna wartość to 5 (minuty).

- **Buforuj dane z podrzędnych Serwerów administracyjnych**

  Podrzędne Serwery administracyjne regularnie przesyłają dane do Serwera administracyjnego, dla którego został utworzony szablon raportu. Przesłane dane są przechowywane w pamięci podręcznej.

  Jeśli podczas generowania raportu bieżący Serwer administracyjny nie może odbierać danych z podrzędnego Serwera administracyjnego, raport wyświetla dane pobrane z pamięci podręcznej. Wyświetlana jest także data przesłania danych do pamięci podręcznej.

  Włączenie tej opcji umożliwia przeglądanie informacji z podrzędnych Serwerów administracyjnych nawet wtedy, gdy aktualne dane nie mogą zostać pobrane. Jednakże wyświetlane dane mogą być przestarzałe.

  Domyślnie opcja ta jest wyłączona.

- **Częstotliwość aktualizacji pamięci podręcznej (godz.)**

  Podrzędne Serwery administracyjne regularnie przesyłają dane do Serwera administracyjnego, dla którego został utworzony szablon raportu. Możesz określić ten okres w godzinach. Jeśli określisz 0 godzin, dane są przesyłane tylko wtedy, gdy raport zostaje wygenerowany.

  Domyślna wartość to 0.

- **Prześlij szczegółowe informacje z podrzędnych Serwerów administracyjnych**

  W wygenerowanym raporcie tabela ze szczegółowymi danymi raportu zawiera dane z podrzędnych Serwerów administracyjnych Serwera administracyjnego, dla którego został utworzony szablon raportu.

  Włączenie tej opcji spowalnia tworzenie raportu i zwiększa ruch sieciowy między Serwerami administracyjnymi. Jednakże możesz przejrzeć wszystkie dane w jednym raporcie.

  Zamiast włączyć tę opcję, możesz chcieć przeanalizować szczegółowe dane raportu, aby wykryć wadliwy podrzędny Serwer administracyjny, a następnie wygenerować ten sam raport tylko dla tego wadliwego Serwera administracyjnego.

  Domyślnie opcja ta jest wyłączona.

- Zakładka **Pola**

  Wybierz pola, które będą wyświetlane w raporcie i użyj przycisku **W górę** oraz przycisku **W dół**, aby zmienić kolejność tych pól. Użyj przycisku **Dodaj** lub przycisku **Edytuj**, aby określić, czy informacje w raporcie muszą być sortowane i filtrowane według każdego z pól.

  W sekcji **Pola filtrów szczegółów** możesz również kliknąć przycisk **Konwertuj filtry**, aby rozpocząć korzystanie z rozszerzonego formatu filtrowania. Ten format umożliwia łączenie warunków filtrowania określonych w różnych polach za pomocą operacji logicznej LUB. Po kliknięciu przycisku po prawej stronie zostanie otwarty panel **Konwertuj filtry**. Kliknij przycisk **Konwertuj filtry**, aby potwierdzić konwersję. Możesz teraz zdefiniować przekonwertowany filtr z warunkami z sekcji **Pola szczegółów**, które są stosowane przy użyciu operacji logicznej LUB.

  > Konwersja raportu do formatu obsługującego złożone warunki filtrowania spowoduje, że raport będzie niezgodny z poprzednimi wersjami Kaspersky Security Center (11 i starszymi). Przekonwertowany raport nie będzie zawierał żadnych danych z podrzędnych Serwerów administracyjnych, na których działają takie niekompatybilne wersje.

5. Kliknij **Zapisz**, aby zachować zmiany.

6. Zamknij okno **Edycja raportu <Nazwa raportu>**.

Zaktualizowany szablon raportu pojawi się na liście szablonów raportu.

Eksportowanie raportu do pliku

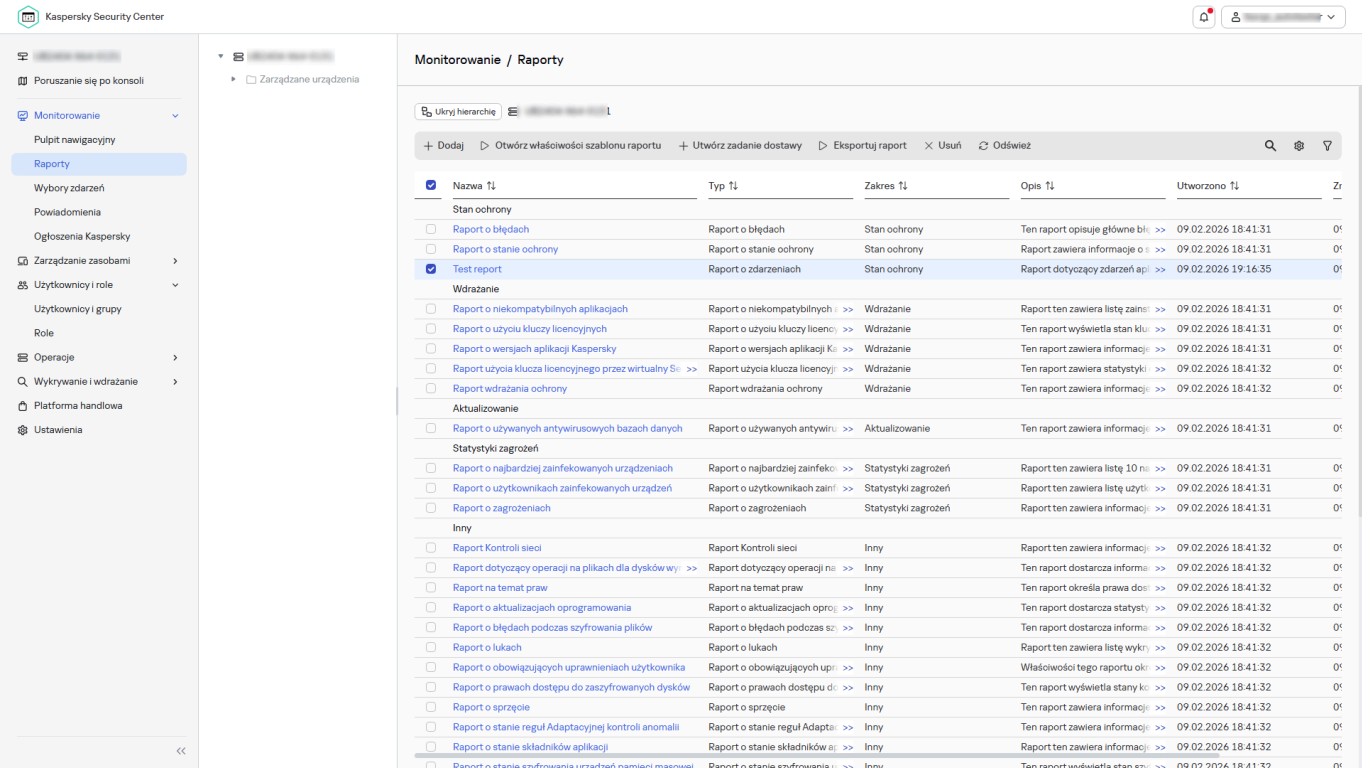
Możesz zapisać jeden lub kilka raportów w formacie XML, HTML lub PDF. Kaspersky Security Center Linux umożliwia jednoczesne wyeksportowanie maksymalnie 10 raportów do plików w określonym formacie.

W celu wyeksportowania raportu do pliku:

1. W menu głównym przejdź do **Monitorowanie** → **Raporty**.

2. Wybierz raporty, które chcesz wyeksportować.

Jeśli wybierzesz więcej niż 10 raportów, przycisk **Eksportuj raport** będzie nieaktywny.



Lista raportów

3. Kliknij przycisk **Eksportuj raport**.

4. W otwartym oknie określ następujące parametru eksportu:

- **Nazwa pliku**.

  Jeśli wybierzesz jeden raport do wyeksportowania, podaj nazwę pliku raportu.

  Jeśli wybierzesz więcej niż jeden raport, nazwy plików raportów będą zgodne z nazwami wybranych szablonów raportów.

- **Maksymalna liczba wpisów**.

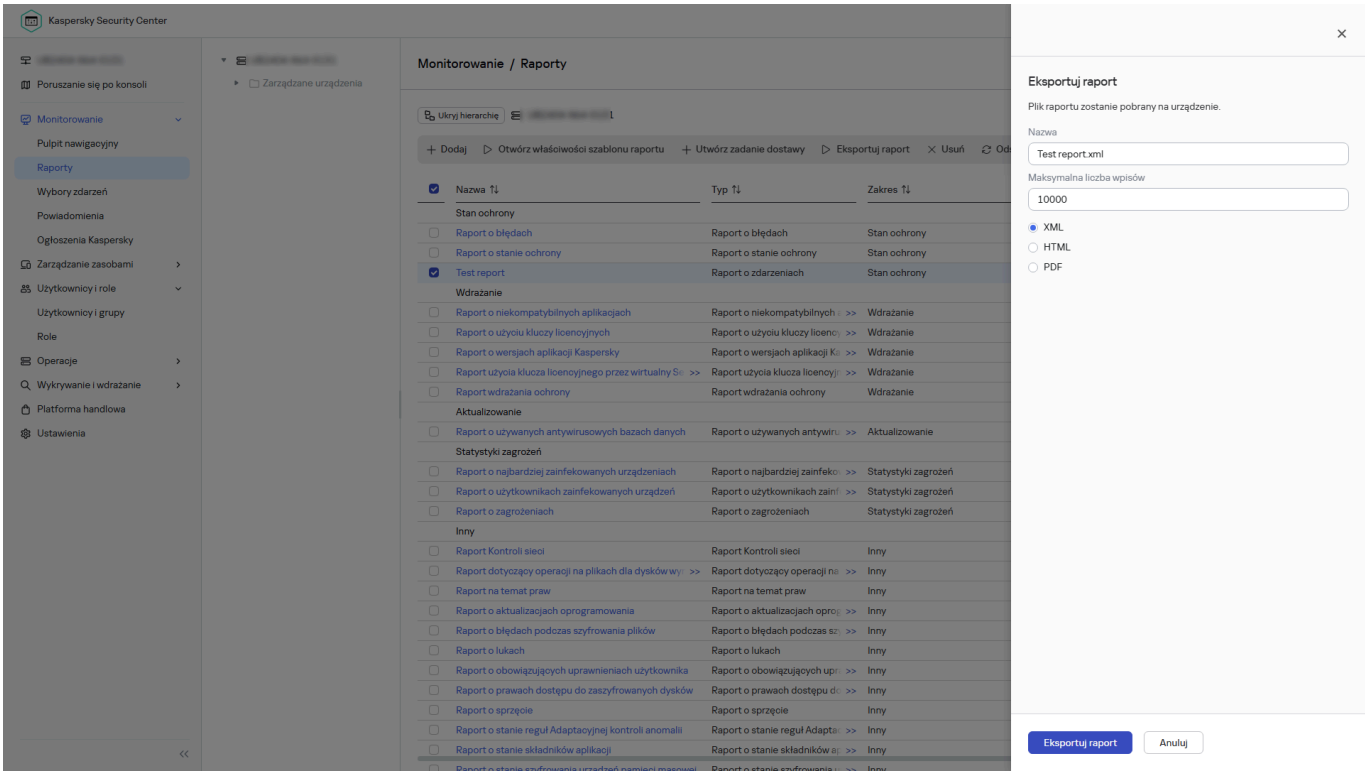
  Określ maksymalną liczbę wpisów zawartych w pliku raportu. Domyślna wartość to 10000.

  Możesz wyeksportować raport z nieograniczoną liczbą wpisów. Należy pamiętać, że jeśli raport zawiera dużą liczbę wpisów, wydłuża się czas potrzebny na wygenerowanie i wyeksportowanie raportu.

- **Format pliku**.

  Wybierz format pliku raportu: XML, HTML lub PDF. W przypadku eksportowania wielu raportów wszystkie wybrane raporty są zapisywane w określonym formacie jako osobne pliki.

Do konwersji raportu do formatu PDF wymagane jest narzędzie wkhtmltopdf. Po wybraniu opcji PDF Serwer administracyjny sprawdza, czy na urządzeniu jest zainstalowane narzędzie wkhtmltopdf. Jeżeli narzędzie nie jest zainstalowane, aplikacja wyświetla komunikat o konieczności zainstalowania narzędzia na urządzeniu Serwera administracyjnego. Zainstaluj narzędzie ręcznie, a następnie przejdź do następnego kroku.



Określanie ustawień eksportu raportu

5. Kliknij przycisk **Eksportuj raport**.

Raport jest zapisywany do pliku w określonym formacie.

Generowanie i przeglądanie raportu

W celu utworzenia i przejrzenia raportu:

1. W menu głównym przejdź do **Monitorowanie** → **Raporty**.

2. Kliknij nazwę szablonu raportu, którego chcesz użyć do utworzenia raportu.

Raport zostanie wygenerowany przy użyciu wybranego szablonu i wyświetlony.

Dane raportu są wyświetlane zgodnie z lokalizacją ustawioną dla Serwera administracyjnego.

W generowanych raportach niektóre czcionki mogą być nieprawidłowo wyświetlane na diagramach. Aby rozwiązać ten problem, zainstaluj bibliotekę fontconfig. Sprawdź również, czy w systemie operacyjnym są zainstalowane czcionki odpowiadające ustawieniom regionalnym Twojego systemu operacyjnego.

Raport wyświetla następujące dane:

- Na zakładce **Podsumowanie**:
  - Nazwę i typ raportu, krótki opis i okres raportowania, a także informacje o grupie urządzeń, dla których generowany jest raport.
  - Wykres graficzny przedstawiający najbardziej reprezentatywne dane raportu.
  - Tabelę zbiorczą z wyliczonymi wskaźnikami raportu.
- Na zakładce **Szczegóły** wyświetlona zostanie tabela ze szczegółowymi danymi raportu.

Tworzenie zadania dostarczania raportu

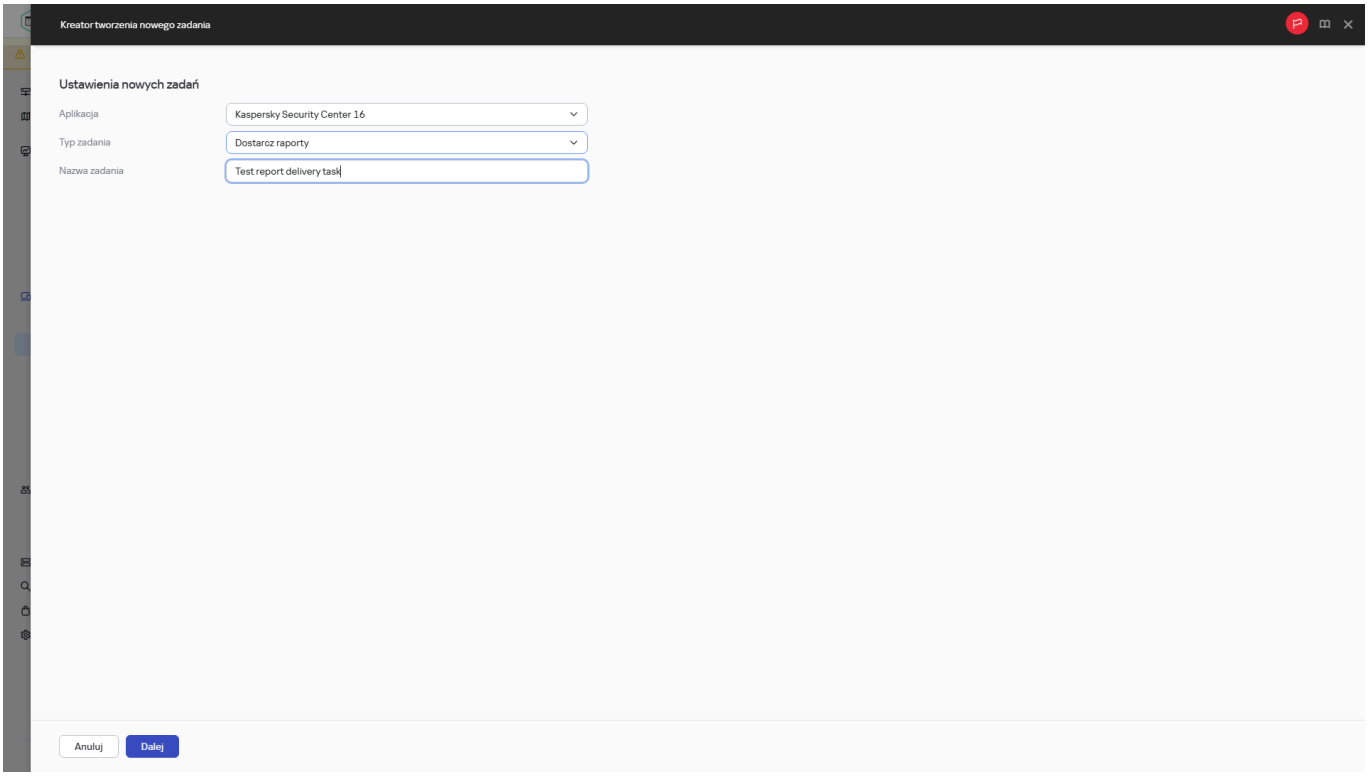
Możesz utworzyć zadanie, które będzie dostarczać wybrane raporty.

W celu utworzenia zadania dostarczania raportu:

1. W menu głównym przejdź do **Monitorowanie** → **Raporty**.
2. Zaznacz pole obok szablonów raportu, dla którego chcesz utworzyć zadanie dostarczania raportu.
3. Kliknij przycisk **Utwórz zadanie dostawy**.

   Zostanie uruchomiony Kreator tworzenia nowego zadania. Przejdź przez kroki kreatora, korzystając z przycisku **Dalej**.
4. W kroku kreatora **Ustawienia nowych zadań** wprowadź nazwę zadania.

   Domyślna nazwa to **Dostarcz raporty.** Jeżeli zadanie o tej nazwie już istnieje, do nazwy zadania dodawany jest numer porządkowy (<N>).



Tworzenie zadania dostarczania raportu

5. W kroku **Konfiguracja raportu** kreatora określ następujące ustawienia:

   a. Szablony raportu, które zostaną dostarczone przez zadanie.

   b. Format raportu: HTML, XLS lub PDF.

      Do konwersji raportu do formatu PDF wymagane jest narzędzie wkhtmltopdf. Po wybraniu opcji PDF Serwer administracyjny sprawdza, czy na urządzeniu jest zainstalowane narzędzie wkhtmltopdf. Jeżeli narzędzie nie jest zainstalowane, aplikacja wyświetla komunikat o konieczności zainstalowania narzędzia na urządzeniu Serwera administracyjnego. Zainstaluj narzędzie ręcznie, a następnie przejdź do następnego kroku.

   c. Czy raporty są wysyłane za pośrednictwem poczty elektronicznej wraz z ustawieniami powiadomień e-mail.

      Możesz określić maksymalnie 20 adresów e-mail. Aby oddzielić adresy e-mail, naciśnij klawisz **Enter**. Możesz także wkleić listę adresów e-mail rozdzielonych przecinkami, a następnie nacisnąć klawisz **Enter**.

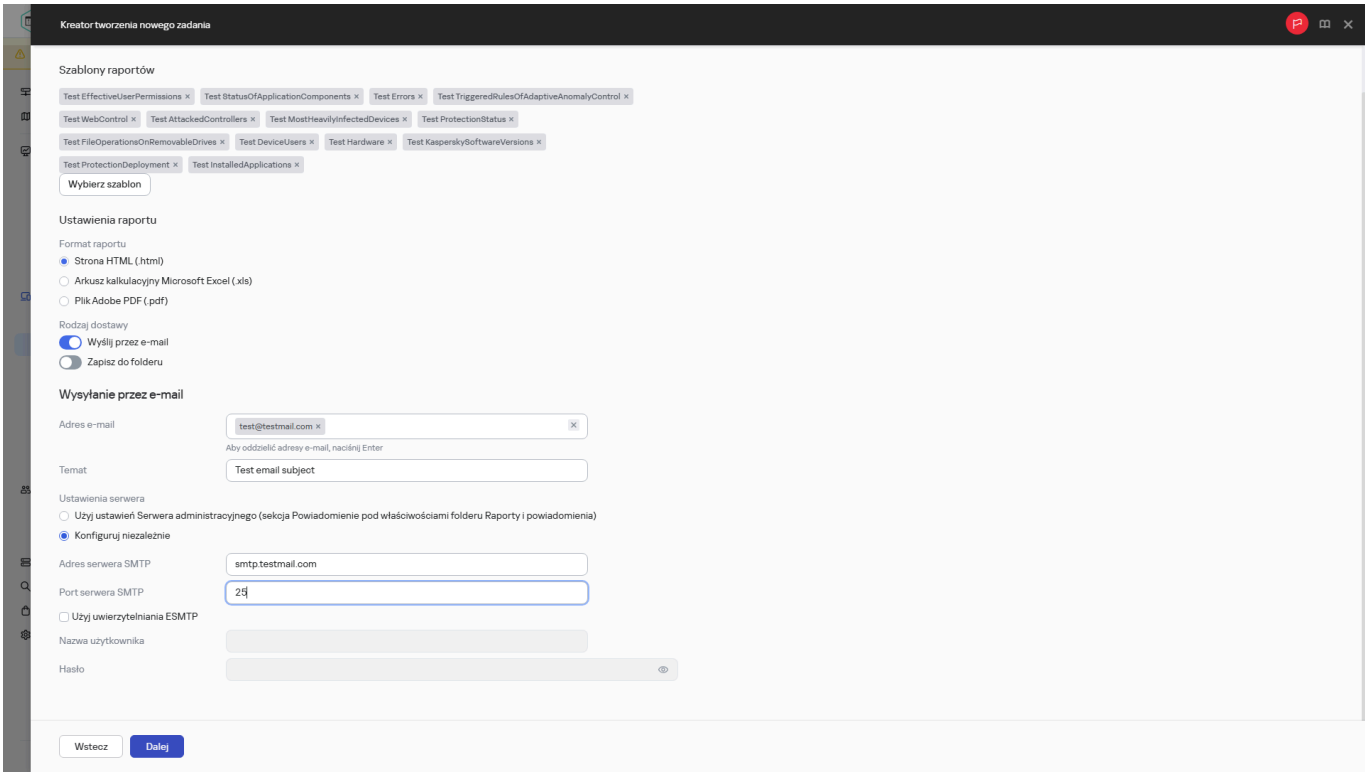
   d. Czy raporty mają być zapisywane do folderu wraz z odpowiadającymi im ustawieniami.

      Po włączeniu opcji **Zapisz do folderu**, musisz określić ścieżkę POSIX do folderu. Jeżeli chcesz zapisać raporty w folderze współdzielonym, musisz również zaznaczyć pole wyboru **Określ konto, które ma mieć dostęp do folderu współdzielonego**, a następnie określić konto użytkownika i hasło dostępu do tego folderu.

      > Jeżeli wybierzesz opcję zapisywania raportów w folderze współdzielonym, musisz zapewnić dostęp do tego folderu z urządzenia z zainstalowanym Serwerem administracyjnym. Sposoby zapewnienia dostępu i stosowane narzędzia zależą od infrastruktury.

      Podczas zapisywania raportów w folderze lokalnym zazwyczaj nie są potrzebne dane uwierzytelniające, ponieważ konto, na którym uruchomiony jest Serwer administracyjny, ma dostęp do tego folderu. W razie potrzeby możesz określić dane uwierzytelniające użytkownika w kroku **Wybieranie konta do uruchomienia zadania** kreatora.

Niezależnie od wybranego folderu możesz także zaznaczyć pole wyboru **Nadpisz starsze raporty tego samego typu**, jeśli chcesz, aby nowy plik raportu nadpisał plik zapisany w folderze raportów podczas poprzedniego uruchomienia zadania.



Określanie ustawień zadania

6. W kroku **Konfiguruj terminarz zadania** kreatora wybierz harmonogram rozpoczęcia zadania.

   Dostępne są następujące opcje harmonogramu zadań:

   - **Ręcznie**

     Zadanie nie jest uruchamiane automatycznie. Możesz je uruchomić tylko ręcznie.

     Domyślnie opcja ta jest zaznaczona.

   - **Co N minut**

     Zadanie jest uruchamiane regularnie, w określonych przedziałach czasu, począwszy od określonej godziny w dniu utworzenia zadania.

     Domyślnie, zadanie jest uruchamiane co 30 minut, począwszy od bieżącego czasu systemowego.

   - **Co N godzin**

     Zadanie jest uruchamiane regularnie, w określonych przedziałach czasu, począwszy od określonego dnia i godziny.

     Domyślnie, zadanie jest uruchamiane co 6 godzin, począwszy od bieżącej daty i godziny systemowej.

   - **Co N dni**

     Zadanie jest uruchamiane regularnie, w określonych przedziałach czasu. Dodatkowo, możesz określić datę i godzinę pierwszego uruchomienia zadania. Te dodatkowe opcje staną się dostępne, jeśli są obsługiwane przez aplikację, dla której tworzysz zadanie.

     Domyślnie, zadanie jest uruchamiane codziennie, począwszy od bieżącej daty i godziny systemowej.

- **Co N tygodni**

  Zadanie jest uruchamiane regularnie, w określonych przedziałach czasu, w określonym dniu tygodnia i o określonej godzinie.

  Domyślnie, zadanie jest uruchamiane w każdy piątek o godzinie zgodnej z bieżącym czasem systemowym.

- **Co miesiąc**

  Zadanie jest uruchamiane regularnie, w określonym dniu miesiąca i o określonej godzinie.

  W miesiącach, w które nie ma określonego dnia, zadanie jest uruchamiane w ostatnim dniu.

  Domyślnie, zadanie jest uruchamiane w pierwszym dniu każdego miesiąca, o godzinie zgodnej z bieżącym czasem systemowym.

- **W określone dni**

  Zadanie jest uruchamiane regularnie, w określone dni każdego miesiąca i o określonej godzinie.

  Domyślnie godzina rozpoczęcia to 18:00, a żadne dni miesiąca nie są wybrane.

  > Należy pamiętać, że nie wybiera się konkretnej daty w miesiącu ani numeru tygodnia (pierwszy, drugi tydzień miesiąca), ale kolejny numer dnia tygodnia w miesiącu. Na przykład, jeśli ustawisz kursor w komórce **Wt** w **Pierwszy** wierszu, oznacza to, że zadanie będzie uruchamiane w każdy pierwszy wtorek każdego nowego miesiąca.

  Można wybrać kilka dni tygodnia.

- **Po ataku wirusa**

  Zadanie jest uruchamiane po wystąpieniu zdarzenia *Atak wirusa*. Wybierz typy aplikacji, które będą monitorować ataki wirusa. Dostępne są następujące typy aplikacji:

  - Ochrona antywirusowa stacji roboczych i serwerów plików
  - Ochrona antywirusowa bram internetowych
  - Ochrona antywirusowa serwerów pocztowych

  Domyślnie, zaznaczone są wszystkie typy aplikacji.

  Możesz chcieć uruchomić różne zadania w zależności od typu aplikacji zabezpieczającej, która zgłosiła atak wirusa. W tym przypadku, usuń wybór typów aplikacji, których nie potrzebujesz.

- **Po zakończeniu wykonywania innego zadania**

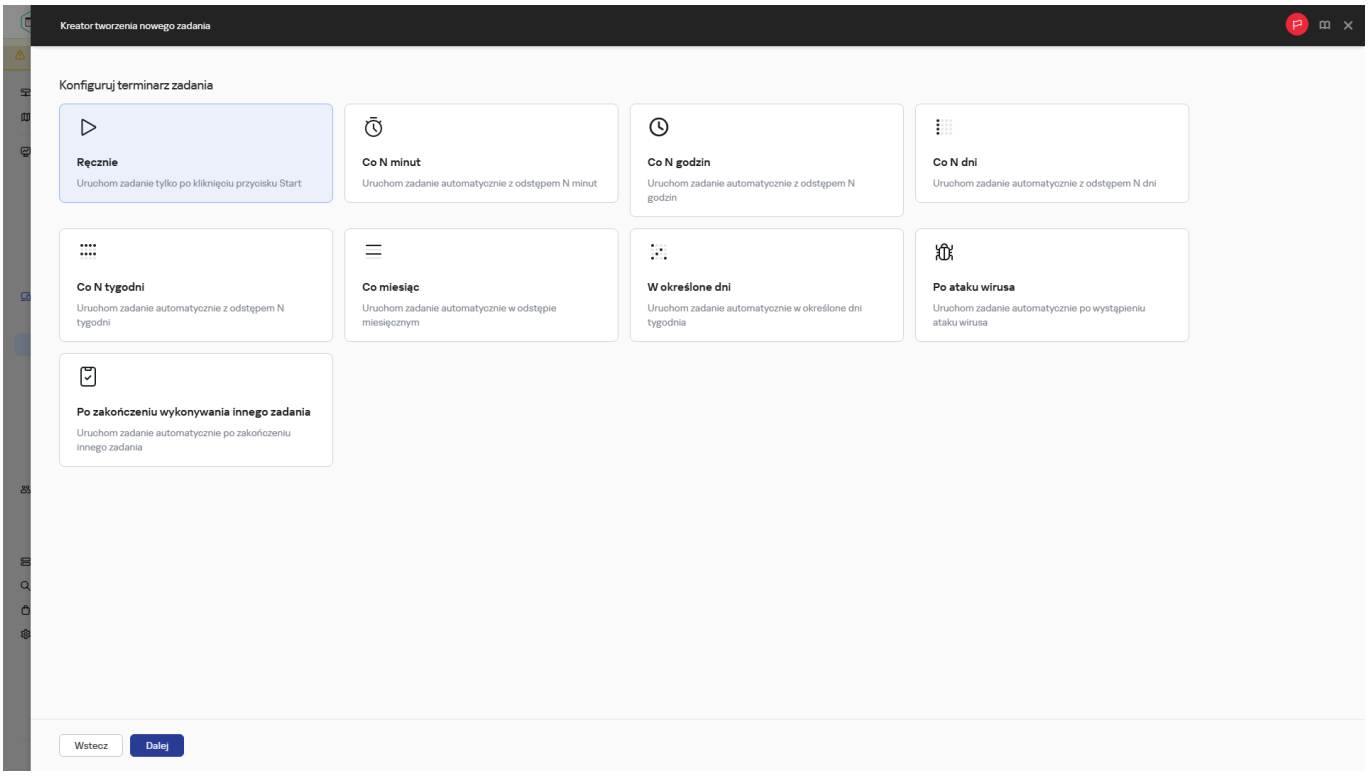
  Bieżące zadanie jest uruchamiane po zakończeniu innego zadania. Opcja ta działa tylko wtedy, gdy oba zadania są przypisane do tych samych urządzeń. Na przykład możesz chcieć uruchomić zadanie *Zarządzaj urządzeniami* z opcją **Włącz urządzenie** i, po zakończeniu jego wykonywania, uruchomić zadanie *Skanowanie antywirusowe*, jako zadanie wyzwalające.

  Musisz wybrać z tabeli zadanie wyzwalające i status, z jakim to zadanie musi zostać ukończone (**Pomyślnie zakończone** lub **Niepowodzenie**).

W razie potrzeby możesz wyszukiwać, sortować i filtrować zadania w tabeli w następujący sposób:

- Wpisz nazwę zadania w polu wyszukiwania, aby wyszukać zadanie na podstawie jego nazwy.
- Kliknij ikonę sortowania, aby posortować zadania według nazwy.

  Domyślnie zadania są sortowane alfabetycznie, w porządku rosnącym.
- Kliknij ikonę filtra i w oknie, które zostanie otwarte, przefiltruj zadania według grupy, a następnie kliknij przycisk **Zastosuj**.



Wybieranie harmonogramu uruchamiania zadania

7. W tym kroku kreatora skonfiguruj pozostałe ustawienia harmonogramu zadań:

- W sekcji **Terminarz zadania** sprawdź lub skonfiguruj wcześniej wybrany harmonogram i ustaw przedział czasowy, dni miesiąca lub tygodnia, ustaw stan ataku wirusa lub wykonanie innego zadania jako wyzwalacz uruchomienia zadania. W tej sekcji można również określić godzinę rozpoczęcia, jeśli wybrany zostanie odpowiedni harmonogram.
- W sekcji **Ustawienia dodatkowe** określ następujące ustawienia:
  - **Uruchom pominięte zadania**

    Ta opcja określa zachowanie zadania, jeśli urządzenie klienckie nie jest widoczne w sieci, gdy zadanie ma zostać uruchomione.

    Jeżeli ta opcja jest włączona, system podejmie próbę uruchomienia zadania podczas kolejnego uruchomienia aplikacji Kaspersky na urządzeniu klienckim. Jeśli terminarz uruchamiania zadania jest ustawiony na **Ręcznie**, **Raz** lub **Natychmiast**, zadanie jest uruchamiane, gdy urządzenie stanie się widoczne w sieci lub od razu po uwzględnieniu urządzenia w obszarze zadania.

    Jeśli ta opcja jest wyłączona, na urządzeniach klienckich będą uruchamiane tylko zaplanowane zadania. W przypadku harmonogramu **Ręcznie**, **Raz** i **Natychmiast** zadania są uruchamiane tylko na tych urządzeniach klienckich, które są widoczne w sieci. Na przykład, możesz chcieć wyłączyć tę opcję dla zadań zużywających duże ilości zasobów, które chcesz uruchamiać tylko poza godzinami pracy.

    Domyślnie opcja ta jest wyłączona.

- **Używaj automatycznie losowego opóźnienia dla uruchamiania zadań**

  Jeśli ta opcja jest włączona, zadanie jest uruchamiane na urządzeniach klienckich losowo, w określonym przedziale czasu, czyli z *rozproszonym uruchomieniem zadania*. Opcja ta pozwala uniknąć dużej liczby równoczesnych żądań wysyłanych przez urządzenia klienckie do Serwera administracyjnego, gdy uruchomione jest zaplanowane zadanie.

  Czas rozpoczęcia podjęcia próby uzyskania dostępu jest wyliczany automatycznie podczas tworzenia zadania, w zależności od liczby urządzeń klienckich, do których zadanie jest przypisane. Później zadanie będzie zawsze uruchamiane o wyliczonej godzinie uruchomienia. Jednakże, jeśli ustawienia zadania zostaną zmienione lub zadanie zostanie uruchomione ręcznie, zmieni się wyliczona wartość czasu uruchomienia zadania.

  Jeśli ta opcja jest wyłączona, zadanie jest uruchamiane na urządzeniach klienckich zgodnie z terminarzem.

- **Użyj automatycznego losowego opóźnienia dla zadań uruchamianych w przedziale**

  Jeśli ta opcja jest włączona, zadanie jest uruchamiane na urządzeniach klienckich losowo, w określonym przedziale czasu. Opcja ta pozwala uniknąć dużej liczby równoczesnych żądań wysyłanych przez urządzenia klienckie do Serwera administracyjnego, gdy uruchomione jest zaplanowane zadanie.

  Jeśli ta opcja jest wyłączona, zadanie jest uruchamiane na urządzeniach klienckich zgodnie z terminarzem.

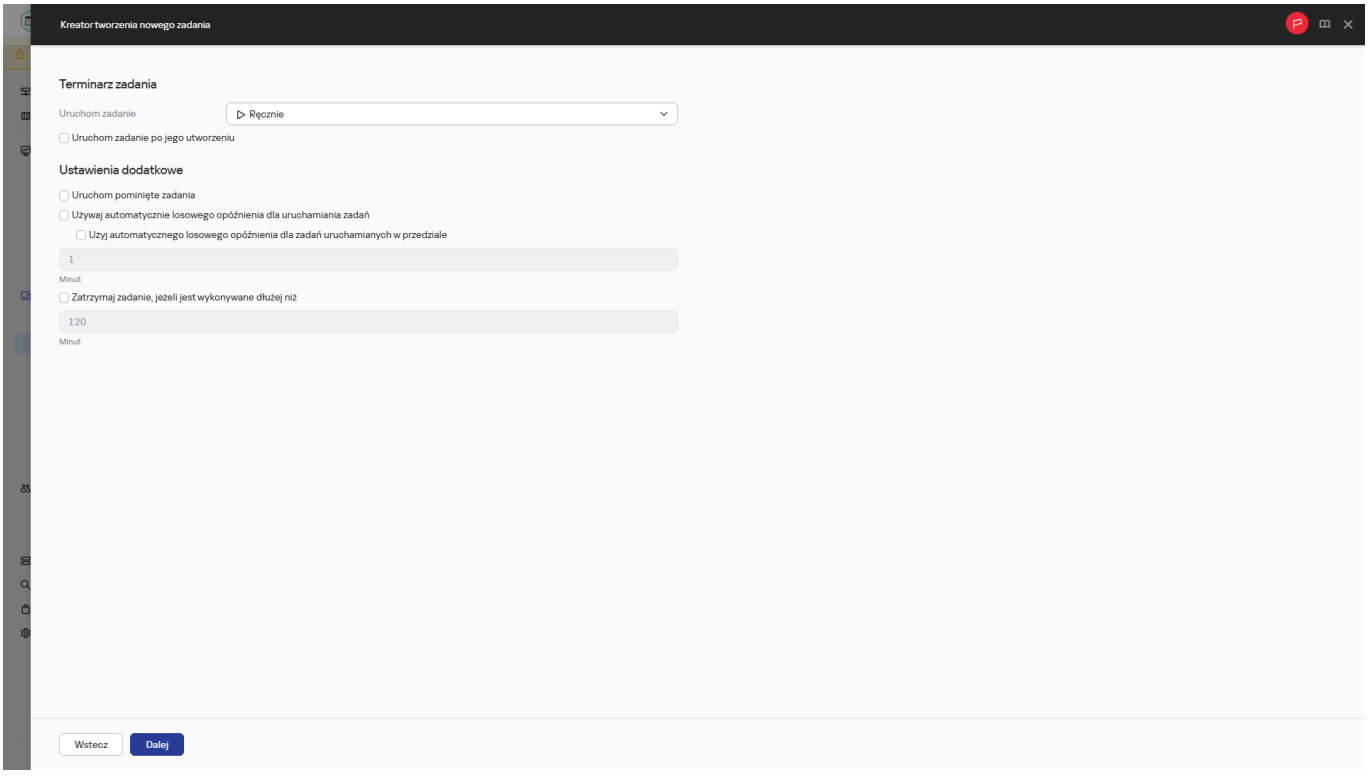
  Domyślnie opcja ta jest wyłączona. Domyślny przedział czasu wynosi 1 minutę.

- **Zatrzymaj zadanie, jeżeli jest wykonywane dłużej niż**

  Po minięciu określonego czasu, zadanie jest zatrzymywane automatycznie, niezależnie od tego, czy zostało zakończone.

  Włącz tę opcję, jeśli chcesz przerwać (lub zatrzymać) zadania, których wykonanie zajmuje zbyt dużo czasu.

  Domyślnie opcja ta jest wyłączona. Domyślny czas wykonania zadania to 120 minut.

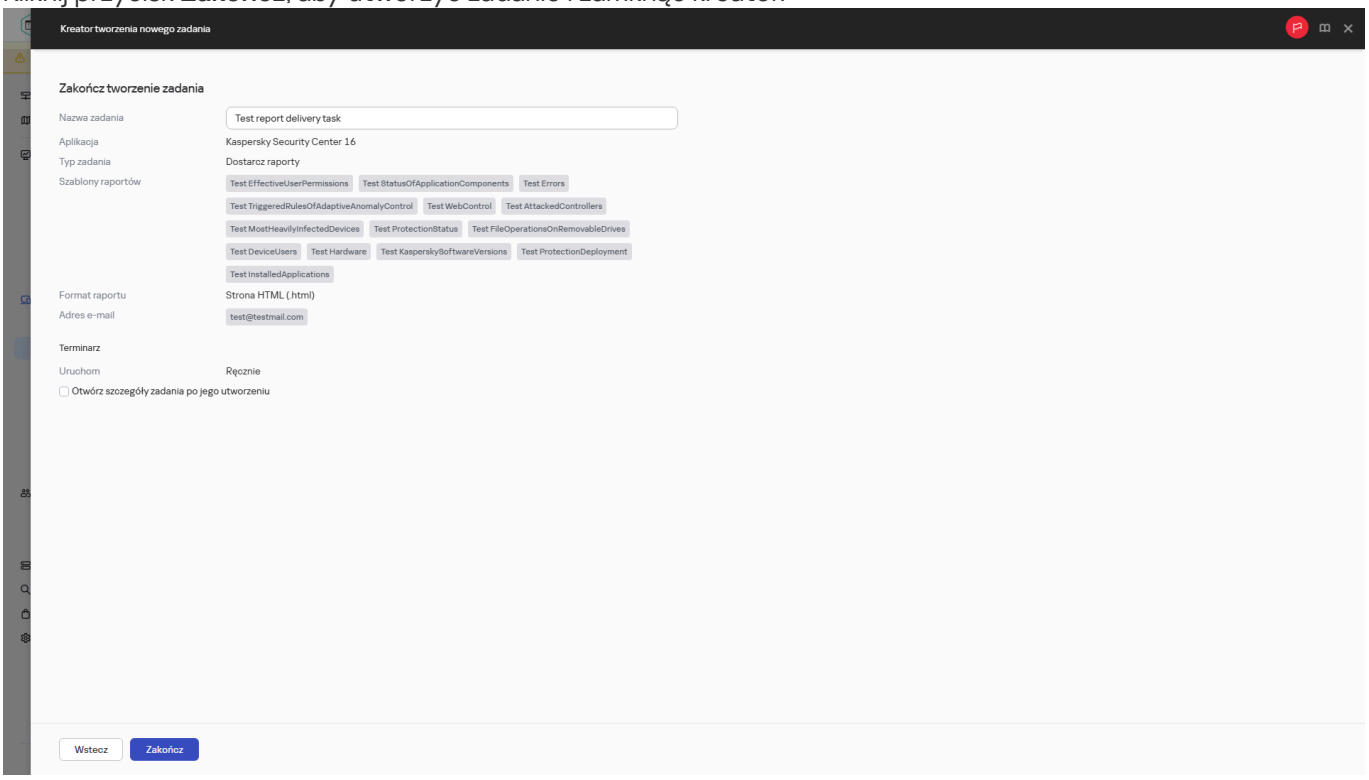


Określanie ustawień harmonogramu zadań

8. Na etapie **Wybieranie konta do uruchomienia zadania** kreatora określ poświadczenia konta użytkownika używanego do uruchomienia zadania.

9. Jeśli chcesz zmodyfikować inne ustawienia zadania po utworzeniu zadania, w kroku **Zakończ tworzenie zadania** włącz opcję **Otwórz szczegóły zadania po jego utworzeniu** (ta opcja jest domyślnie włączona).

10. Kliknij przycisk **Zakończ**, aby utworzyć zadanie i zamknąć kreator.



Zakończenie tworzenia zadania

Zostanie utworzone zadanie dostarczania raportów. Jeśli włączyłeś opcję **Otwórz szczegóły zadania po jego utworzeniu**, zostanie otwarte okno ustawień zadania.

Usuwanie szablonów raportu

W celu usunięcia jednego lub kilku szablonów raportu:

1. W menu głównym przejdź do **Monitorowanie** → **Raporty**.

2. Zaznacz pola obok szablonów raportu, które chcesz usunąć.

3. Kliknij przycisk **Usuń**.

4. W otwartym oknie kliknij **OK**, aby potwierdzić swój wybór.

Wybrane szablony raportu zostaną usunięte. Jeśli te szablony raportu znajdowały się w zadaniach dostarczania raportów, zostaną usunięte z zadań.

Wskaźnik poziomu ochrony

Wskaźnik poziomu ochrony wyświetla aktualne informacje o ochronie Serwera administracyjnego i punktów dystrybucji. Umożliwia to śledzenie wdrażania zaleceń opisanych w dokumencie Przewodnik po zwiększaniu odporności. Wskaźnik jest wyświetlany w sekcji **Monitorowanie** → **Pulpit nawigacyjny** i nie można go ukryć ani przenieść do innej sekcji menu Web Console. Kliknięcie wskaźnika umożliwia przejście do Centrum zwiększania odporności i wyświetlenie stanów parametrów ochrony Serwera administracyjnego oraz punktów dystrybucji. Aby zwiększyć bezpieczeństwo infrastruktury, należy rozwiązać wskazane problemy, jeśli takie występują.

Wskaźnik może mieć jeden z następujących stanów:

- Ochrona skonfigurowana.
- Ochrona częściowo skonfigurowana.
- Ochrona nie została skonfigurowana.

Jak wyświetlić szczegółowe informacje o poziomie ochrony?

Ogólny stan wskaźnika jest tworzony na podstawie stanów parametrów ochrony.

Aby wyświetlić parametry, kliknij wskaźnik.

W otwartym oknie **Centrum zwiększania odporności** parametry są pogrupowane według chronionych obiektów: Serwera administracyjnego i punktów dystrybucji.

Każdy parametr ochrony jest wyświetlany w jednym ze stanów w zależności od posiadanych uprawnień dostępu:

- ✅ jeśli nie ma żadnych problemów do rozwiązania lub użytkownik nie ma wymaganych uprawnień dostępu.
- ⚠️ lub ❌ jeśli występują problemy do rozwiązania.

Następujące parametry są wyświetlane tylko dla Serwera administracyjnego:

- Kopia zapasowa skonfigurowana
- Konserwacja Serwera administracyjnego skonfigurowana
- Szyfrowanie TLS włączone

Następujące parametry są wyświetlane zarówno dla Serwera administracyjnego, jak i punktów dystrybucji:

- Aplikacja zabezpieczająca jest zainstalowana
- Zasada zastosowana
- Aktualizacja antywirusowych baz danych skonfigurowana

Funkcje Serwera administracyjnego:

- Wszystkie parametry ochrony są obliczane wyłącznie dla fizycznego Serwera administracyjnego i nie są stosowane do serwerów wirtualnych.

  Jeśli używasz struktury hierarchicznej obejmującej kilka Serwerów administracyjnych, wskaźnik poziomu ochrony jest obliczany osobno dla każdego serwera fizycznego.

- Parametry **Aplikacja zabezpieczająca zainstalowana**, **Zasada zastosowana**, **Aktualizacja antywirusowych baz danych skonfigurowana** są obliczane dla urządzenia z zainstalowanym Serwerem administracyjnym.

- Podczas wdrażania klastra pracy awaryjnej Kaspersky Security Center Linux parametry **Aplikacja zabezpieczająca zainstalowana**, **Zasada zastosowana**, **Aktualizacja antywirusowych baz danych skonfigurowana** są obliczane dla każdego węzła. Węzeł jest uwzględniany podczas obliczania stanu wskaźnika dopiero wtedy, gdy stanie się aktywny.

Jak obliczany jest stan wskaźnika?

Stan wskaźnika jest obliczany w sposób opisany w tabeli.

Stan wskaźnika	Warunek
Ochrona skonfigurowana.	Wszystkie parametry ochrony mają stan ✅.
Ochrona częściowo skonfigurowana.	Parametr **Aktualizacja antywirusowych baz danych skonfigurowana** ma stan ⚠️, podczas gdy wszystkie pozostałe parametry mają stan ✅.
Ochrona nie została skonfigurowana.	Jeśli co najmniej jeden z następujących parametrów ochrony ma stan ❌.

Aplikacja zabezpieczająca jest zainstalowana

Aplikacje zabezpieczające umożliwiają ochronę urządzeń przed różnymi typami zagrożeń, w tym atakami sieciowymi, phishingowymi i oszustwami.

Parametr jest wyświetlany w stanie ✅, jeśli spełniony jest jeden z warunków:

- Nie masz praw dostępu do urządzeń.

- Masz uprawnienia do **Odczyt** w obszarze funkcjonalnym **Funkcje ogólne** → **Podstawowa funkcjonalność**, a na urządzeniach zainstalowano Agenta sieciowego i aplikację zabezpieczającą.

  > Warunek musi być spełniony na wszystkich urządzeniach dostępnych dla Ciebie na podstawie Twoich praw dostępu, z wyłączeniem urządzeń z zainstalowaną aplikacją, która nie wymaga ochrony antywirusowej (na przykład zabezpieczonym systemem operacyjnym), urządzeń bez zainstalowanego Agenta sieciowego, w przypadku których informacje o urządzeniu pojawiły się na Serwerze administracyjnym mniej niż 24 godziny temu, oraz urządzeń offline, które ostatnio połączyły się z Serwerem administracyjnym 7 lub więcej dni temu.

Parametr jest wyświetlany w stanie ❌, jeśli spełniony jest co najmniej jeden z poniższych warunków.

Musisz kliknąć przycisk **Wyświetl urządzenia** i wykonać czynności opisane w tabeli dla wyświetlonych urządzeń.

Warunek	Rozwiązanie
Agent sieciowy nie jest zainstalowany na urządzeniu	Zainstaluj Agenta sieciowego. W przypadku urządzenia z Serwerem administracyjnym najprostszym sposobem instalacji Agenta sieciowego jest użycie autonomicznego pakietu instalacyjnego.
Urządzenie znajduje się w grupie **Urządzenia nieprzypisane**	Przenieś urządzenie do grupy Zarządzane urządzenia lub jej podgrupy
Nie znaleziono żadnych aplikacji zabezpieczających albo ochrona w czasie rzeczywistym nie jest uruchomiona dla zainstalowanej aplikacji zabezpieczającej	Zainstaluj aplikację zabezpieczającą. Aplikacja będzie przesyłać dane o stanie ochrony do Serwera administracyjnego. Możesz wyświetlić stan ochrony urządzenia w ustawieniach urządzenia: sekcja **Ogólne** → **Stan urządzenia**. Na urządzeniu z Serwerem administracyjnym należy zainstalować Kaspersky Endpoint Security for Linux.

Zasada zastosowana

Zasada to zbiór ustawień aplikacji zabezpieczającej, które są stosowane do grupy administracyjne i jej podgrup.

Parametr jest wyświetlany w stanie ✅, jeśli spełniony jest jeden z warunków:

- Nie masz praw dostępu do urządzeń.
- Masz uprawnienia do **Odczyt** w obszarze funkcjonalnym **Funkcje ogólne** → **Podstawowa funkcjonalność**, a na urządzeniach jest zainstalowana aplikacja zabezpieczająca i do urządzeń jest stosowana zasada aktywna tej aplikacji zabezpieczającej.

  Warunek musi być spełniony na wszystkich urządzeniach dostępnych dla Ciebie na podstawie Twoich praw dostępu, z wyłączeniem urządzeń z zainstalowaną aplikacją, która nie wymaga ochrony antywirusowej (na przykład zabezpieczonym systemem operacyjnym), urządzeń bez zainstalowanego Agenta sieciowego, w przypadku których informacje o urządzeniu pojawiły się na Serwerze administracyjnym mniej niż 24 godziny temu, oraz urządzeń offline, które ostatnio połączyły się z Serwerem administracyjnym 7 lub więcej dni temu.

Parametr jest wyświetlany w stanie ❌, jeśli spełniony jest co najmniej jeden z poniższych warunków.

Musisz kliknąć przycisk **Wyświetl urządzenia** i wykonać czynności opisane w tabeli dla wyświetlonych urządzeń.

Warunek	Rozwiązanie
Aplikacja zabezpieczająca nie jest zainstalowana na urządzeniu.	Upewnij się, że urządzenie nie znajduje się w wyborze dla parametru ochrony **Zainstalowano aplikację zabezpieczającą**.

Zasada nie jest stosowana do urządzenia.	Upewnij się, że zasada została utworzona dla grupy administracyjnej, do której należy urządzenie. Jeśli nie, utwórz i aktywuj zasadę. Jeśli tak, upewnij się, że: • Utworzona zasada jest aktywna. Jeśli nie, aktywuj zasadę. • Stan dystrybucji zasady to **Zastosowano pomyślnie**. Jeśli stan to **Zastosowano z błędem**, problem należy rozwiązać po stronie aplikacji zabezpieczającej.

Aktualizacja antywirusowych baz danych skonfigurowana

Ponieważ antywirusowe bazy danych chronią urządzenia przed zagrożeniami, należy regularnie i terminowo aktualizować bazy danych na urządzeniach.

Parametr jest wyświetlany w stanie ✅, jeśli spełniony jest jeden z warunków:

- Nie masz praw dostępu do urządzeń.
- Masz uprawnienia do Odczyt w obszarze funkcjonalnym Funkcje ogólne → Podstawowa funkcjonalność, a antywirusowe bazy danych na urządzeniach są aktualizowane.

> Warunek musi być spełniony na wszystkich urządzeniach dostępnych dla Ciebie na podstawie Twoich praw dostępu, z wyłączeniem urządzeń z zainstalowaną aplikacją, która nie wymaga ochrony antywirusowej (na przykład zabezpieczonym systemem operacyjnym), urządzeń bez zainstalowanego Agenta sieciowego, w przypadku których informacje o urządzeniu pojawiły się na Serwerze administracyjnym mniej niż 24 godziny temu, oraz urządzeń offline, które ostatnio połączyły się z Serwerem administracyjnym 7 lub więcej dni temu.

Parametr jest wyświetlany w stanie ⚠️, jeśli ostatnia aktualizacja antywirusowych baz danych na urządzeniu miała miejsce ponad 3 dni temu.

Parametr jest wyświetlany w stanie ❌, jeśli ostatnia aktualizacja antywirusowych baz danych na urządzeniu miała miejsce ponad 7 dni temu.

Aby rozwiązać problemy:

1. Kliknij przycisk Wyświetl urządzenia obok parametru.
2. Dla wyświetlonych urządzeń wykonaj następujące czynności:
   a. Upewnij się, że zostało nawiązane połączenie między Agentem sieciowym a Serwerem administracyjnym.
   Jeśli nie, zapoznaj się z następującymi artykułami:
   Rozwiązywanie problemów z aktualizacją antywirusowych baz danych programu Kaspersky Endpoint Security for Linux
   Problemy podczas aktualizacji antywirusowych baz danych z repozytorium Kaspersky Security Center
   b. Upewnij się, że aplikacja Kaspersky, której antywirusowe bazy danych sprawdzasz, nie jest zatrzymana.
   Jeśli aplikacja jest zatrzymana, uruchom ją.
   c. Na urządzeniu wyświetl błędy, które wystąpiły po aktualizacji.

Kopia zapasowa skonfigurowana

Zalecenia dotyczące tworzenia kopii zapasowej danych Serwera administracyjnego można znaleźć w sekcji Tworzenie kopii zapasowej i przywracanie danych Serwera administracyjnego.

Parametr jest wyświetlany w stanie ✅, jeśli spełniony jest jeden z warunków:

- Nie masz praw dostępu wymaganych do pracy z zadaniem tworzenia kopii zapasowej danych Serwera administracyjnego.
- Masz uprawnienia do **Odczyt, Zapis** i **Wykonywanie** w obszarze funkcjonalnym **Funkcje ogólne** → **Operacje na Serwerze administracyjnym**, a kopia zapasowa jest skonfigurowana i wykonywana regularnie.

Parametr jest wyświetlany w stanie ❌, jeśli spełniony jest co najmniej jeden z poniższych warunków.

Warunek	Rozwiązanie
Zadanie tworzenia kopii zapasowej danych Serwera administracyjnego nie zostało utworzone.	Utwórz zadanie.
Nie skonfigurowano niezbędnych ustawień harmonogramu dla zadania tworzenia kopii zapasowej danych Serwera administracyjnego.	W zadaniu konserwacji Serwera administracyjnego określ **Uruchom zadanie** Zadania uruchomienia inne niż **Po ataku wirusa** i **Ręcznie**.

Konserwacja Serwera administracyjnego skonfigurowana

Zadanie Konserwacja Serwera administracyjnego pozwala zwolnić miejsce w folderze Serwera administracyjnego oraz zminimalizować rozmiar bazy danych. Pomaga to przyspieszyć przetwarzanie żądań i zwiększa ogólną stabilność systemu.

Parametr jest wyświetlany w stanie ✅, jeśli spełniony jest jeden z warunków:

- Nie masz praw dostępu do pracy z zadaniem konserwacji Serwera administracyjnego.
- Masz uprawnienia do **Odczyt, Zapis** oraz **Wykonywanie** w obszarze funkcjonalnym **Funkcje ogólne** → **Operacje na Serwerze administracyjnym**, a Konserwacja Serwera administracyjnego jest skonfigurowana i wykonywana regularnie.

> Uprawnienia muszą być ustawione na poziomie Serwera administracyjnego.

Parametr jest wyświetlany w stanie ❌, jeśli spełniony jest co najmniej jeden z poniższych warunków.

Warunek	Rozwiązanie
Zadanie konserwacji Serwera administracyjnego nie zostało utworzone.	Utwórz zadanie.
Niezbędne ustawienia harmonogramu nie zostały skonfigurowane dla zadania konserwacji Serwera administracyjnego.	W zadaniu konserwacji Serwera administracyjnego określ **Uruchom zadanie** Zadania uruchomienia inne niż **Po ataku wirusa** i **Ręcznie**.

Szyfrowanie TLS włączone

Należy upewnić się, że dozwolone są wyłącznie wersje 1.2 i 1.3 protokołu TLS. Zezwalanie na wcześniejsze wersje stwarza poważne zagrożenia dla bezpieczeństwa danych i sprawia, że systemy stają się podatne na ataki.

Parametr jest wyświetlany w stanie ✓, jeśli dozwolone są wyłącznie wersje 1.2 i 1.3 protokołu TLS.

Parametr jest wyświetlany w stanie ✗, jeśli dozwolone są nieaktualne wersje protokołu TLS starsze niż 1.2.

Aby rozwiązać ten problem, należy ustawić flagę `SrvUseStrictSslSettings` na wartość `4` lub `5`.

Zdarzenia i wybory zdarzeń

Ta sekcja zawiera informacje o zdarzeniach i wyborach zdarzeń, o typach zdarzeń występujących w komponentach Kaspersky Security Center Linux oraz o zarządzaniu blokowaniem częstych zdarzeń.

Informacje o zdarzeniach w Kaspersky Security Center Linux

Kaspersky Security Center Linux umożliwia otrzymywanie informacji o zdarzeniach występujących podczas działania Serwera administracyjnego i aplikacji firmy Kaspersky zainstalowanych na zarządzanych urządzeniach. Informacje o zdarzeniach są zapisywane w bazie danych Serwera administracyjnego.

Wydarzenia według typu

W Kaspersky Security Center Linux dostępne są następujące typy zdarzeń:

- Zdarzenia ogólne. Te zdarzenia występują we wszystkich zarządzanych aplikacjach firmy Kaspersky. Przykładem zdarzenia ogólnego jest Atak wirusa. Zdarzenia ogólne mają dokładnie zdefiniowaną składnię i semantykę. Zdarzenia ogólne są używane, na przykład, w raportach i pulpitach nawigacyjnych.
- Zarządzane zdarzenia charakterystyczne dla aplikacji firmy Kaspersky. Każda zarządzana aplikacja firmy Kaspersky posiada swój zestaw zdarzeń.

Wydarzenia według źródła

Możesz wyświetlić pełną listę zdarzeń, które mogą być generowane przez aplikację na karcie **Konfiguracja zdarzenia** w zasadzie aplikacji. W przypadku Serwera administracyjnego możesz dodatkowo wyświetlić listę zdarzeń we właściwościach Serwera administracyjnego.

Zdarzenia mogą być generowane przez następujące aplikacje:

- Składniki Kaspersky Security Center Linux:
  - Serwer administracyjny
  - Agent sieciowy
- Zarządzane aplikacje Kaspersky

  Szczegółowe informacje na temat zdarzeń generowanych przez aplikacje zarządzane przez Kaspersky można znaleźć w dokumentacji odpowiedniej aplikacji.

Zdarzenia według istotności

Każde zdarzenie posiada określony poziom istotności. W zależności od warunków wystąpienia zdarzenia, może ono posiadać różne poziomy istotności. Istnieją cztery poziomy istotności zdarzeń:

- *Zdarzenie krytyczne* to zdarzenie, które wskazuje wystąpienie krytycznego problemu mogącego prowadzić do utraty danych, problemów z działaniem lub błędu krytycznego.
- *Błąd funkcjonalny* to zdarzenie, które wskazuje poważny problem, błąd lub problem z działaniem, który wystąpił podczas działania aplikacji lub podczas przeprowadzania procedury.
- *Ostrzeżenie* to zdarzenie, które niekoniecznie jest poważne, ale wskazuje możliwość wystąpienia potencjalnego problemu w przyszłości. Większość zdarzeń otrzymuje priorytet „Ostrzeżenie", jeśli aplikacja może zostać przywrócona bez utraty danych lub możliwości funkcyjnych aplikacji.
- *Informacja* to zdarzenie, którego celem jest informowanie o pomyślnym zakończeniu działania, właściwym funkcjonowaniu aplikacji lub zakończeniu procedury.

Każde zdarzenie posiada zdefiniowany okres przechowywania, w trakcie którego możesz przejrzeć lub zmodyfikować to zdarzenie w Kaspersky Security Center Linux. Niektóre zdarzenia nie są domyślnie zapisywane w bazie danych Serwera administracyjnego, ponieważ ich zdefiniowany okres przechowywania wynosi zero. Tylko te zdarzenia, które będą przechowywane w bazie danych Serwera administracyjnego przynajmniej jeden dzień, mogą zostać wyeksportowane do systemów zewnętrznych.

Zdarzenia składników Kaspersky Security Center Linux

Każdy komponent Kaspersky Security Center Linux posiada swój zestaw typów zdarzeń. W tej sekcji wymieniono typy zdarzeń występujących na Serwerze administracyjnym i Agencie sieciowym. Typy zdarzeń, które występują w aplikacjach Kaspersky, nie zostały wymienione w tej sekcji.

Dla każdego zdarzenia, które może być generowane przez aplikację, określić można ustawienia powiadomień i ustawienia dot. przechowywania w zasadzie aplikacji, w karcie **Konfiguracja zdarzenia**. W przypadku Serwera administracyjnego możesz dodatkowo wyświetlić i skonfigurować listę zdarzeń we właściwościach Serwera administracyjnego. Jeśli chcesz skonfigurować ustawienia powiadomień dla wszystkich zdarzeń jednocześnie, skonfiguruj ogólne ustawienia powiadomień we właściwościach Serwera administracyjnego.

Struktura danych opisu typu zdarzeń

Dla każdego typu zdarzenia dostarczone są następujące elementy: wyświetlana nazwa, identyfikator (ID), kod alfabetyczny, opis oraz domyślny czas przechowywania.

- **Nazwa wyświetlanego typu zdarzenia**. Ten tekst jest wyświetlany w Kaspersky Security Center Linux, gdy konfigurujesz zdarzenia oraz podczas występowania zdarzeń.
- **ID typu zdarzenia**. Ten kod numeryczny jest używany, gdy przetwarzasz zdarzenia przy użyciu narzędzi firm trzecich do analizy zdarzeń.
- **Typ zdarzenia** (kod alfabetyczny). Ten kod jest używany, gdy przeglądasz i przetwarzasz zdarzenia, korzystając z widoków publicznych, dostępnych w bazie danych Kaspersky Security Center Linux, a także podczas eksportowania zdarzeń do systemu SIEM.
- **Opis**. Ten tekst zawiera sytuacje, gdy zdarzenie wystąpi i co należy zrobić w takiej sytuacji.
- **Domyślny czas przechowywania**. To jest liczba dni, przez jaką zdarzenie jest przechowywane w bazie danych Serwera administracyjnego i jest wyświetlane na liście zdarzeń na Serwerze administracyjnym. Po upłynięciu tego czasu, zdarzenie jest usuwane. Jeśli wartość czasu przechowywania zdarzenia to 0, takie zdarzenia są wykrywane, ale nie są wyświetlane na liście zdarzeń na Serwerze administracyjnym. Jeśli skonfigurowałeś zapisywanie takich zdarzeń w dzienniku zdarzeń systemu operacyjnego, znajdziesz je tam.

  Możesz zmienić okres przechowywania zdarzeń: Ustawianie okresu przechowywania zdarzenia

Zdarzenia Serwera administracyjnego

Ta sekcja zawiera informacje o zdarzeniach dotyczących Serwera administracyjnego.

Zdarzenia krytyczne Serwera administracyjnego

Poniższa tabela przedstawia zdarzenia Serwera administracyjnego, których istotność to **Krytyczny**.

Dla każdego zdarzenia, które może być generowane przez aplikację, określić można ustawienia powiadomień i ustawienia dot. przechowywania w zasadzie aplikacji, w karcie **Konfiguracja zdarzenia**. W przypadku Serwera administracyjnego możesz dodatkowo wyświetlić i skonfigurować listę zdarzeń we właściwościach Serwera administracyjnego. Jeśli chcesz skonfigurować ustawienia powiadomień dla wszystkich zdarzeń jednocześnie, skonfiguruj ogólne ustawienia powiadomień we właściwościach Serwera administracyjnego.

Zdarzenia krytyczne Serwera administracyjnego

Nazwa wyświetlanego typu zdarzenia	ID typu zdarzenia	Typ zdarzenia	Opis	Domyślny czas przechowywania
Certyfikat Serwera administracyjnego dla urządzeń mobilnych utracił ważność	6129	KLSRV_EV_SRV_CERT_EXPIRED_DN	Zdarzenia tego typu występują, gdy certyfikat Serwera administracyjnego dla urządzeń mobilnych i urządzeń UEFI utraci ważność. Należy zaktualizować certyfikat, który utracił ważność.	180 dni
Audyt: Eksport do SIEM nie powiódł się	5130	KLAUD_EV_SIEM_EXPORT_ERROR	Zdarzenia tego typu mają miejsce, gdy eksport zdarzeń do systemu SIEM nie powiódł się z powodu błędu połączenia z systemem SIEM.	180 dni

Nazwa wyświetlanego typu zdarzenia	ID typu zdarzenia	Typ zdarzenia	Opis	Domyślny czas przechowywania
Zarządzanie urządzeniem nie jest możliwe	4111	KLSRV_HOST_OUT_CONTROL	Zdarzenia tego typu występują, jeśli zarządzane urządzenie jest widoczne w sieci, ale nie ma podłączonego Serwera administracyjnego przez pewien czas. Dowiedz się, co uniemożliwia poprawne działanie Agenta sieciowego na urządzeniu. Możliwe przyczyny obejmują problemy z siecią i usuwanie Agenta sieciowego z urządzenia.	180 dni
Stan urządzenia: Krytyczny	4113	KLSRV_HOST_STATUS_CRITICAL	Zdarzenia tego typu występują, gdy do zarządzanego urządzenia zostanie przypisany stan *Krytyczny*. Możesz skonfigurować warunki, zgodnie z którymi stan urządzenia zostanie zmieniony na *Krytyczny*.	180 dni
Licencja wkrótce utraci ważność	4129	KLSRV_EV_LICENSE_SRV_EXPIRE_SOON	Tego typu zdarzenia mają miejsce, gdy zbliża się data wygaśnięcia licencji komercyjnej. Raz dziennie Kaspersky Security Center Linux sprawdza, czy nie zbliża się data wygaśnięcia licencji. Wydarzenia tego typu publikowane są 30 dni, 15 dni, 5 dni i 1 dzień przed datą wygaśnięcia licencji. Tej liczby dni nie można zmienić. Jeśli Serwer administracyjny zostanie wyłączony określonego dnia przed datą wygaśnięcia licencji, zdarzenie nie zostanie opublikowane, aż do następnego dnia. Po wygaśnięciu licencji komercyjnej Kaspersky Security Center Linux zapewnia tylko podstawową funkcjonalność. Możesz zareagować na zdarzenie w następujące sposoby: • Upewnij się, że zapasowy klucz licencyjny został dodany do Serwera administracyjnego. • Jeśli korzystasz z subskrypcji, pamiętaj o jej odnowieniu. Nieograniczona subskrypcja jest odnawiana automatycznie, jeśli została opłacona w odpowiednim terminie.	180 dni

Nazwa wyświetlanego typu zdarzenia	ID typu zdarzenia	Typ zdarzenia	Opis	Domyślny czas przechowywania
Limit licencji został przekroczony	4099	KLSRV_EV_LICENSE_CHECK_MORE_110	Raz dziennie Kaspersky Security Center Linux sprawdza, czy limity licencyjne nie są przekroczone. Zdarzenia tego typu występują, gdy Serwer administracyjny wykryje, że niektóre ograniczenia licencyjne są przekroczone przez aplikacje firmy Kaspersky zainstalowane na urządzeniach klienckich i czy liczba aktualnie używanych jednostek licencyjnych objętych jedną licencją przekracza 110% całkowitej liczby jednostek objętych licencją. Nawet jeśli to zdarzenie wystąpi, urządzenia klienckie są chronione. Możesz zareagować na zdarzenie w następujące sposoby: • Zapoznaj się z listą zarządzanych urządzeń. Usuń urządzenia, które nie są w użyciu. • Dostarcz licencję dla większej liczby urządzeń (dodaj ważny kod aktywacyjny lub plik klucza do Serwera administracyjnego). Kaspersky Security Center Linux określa reguły generowania zdarzeń, gdy limity licencjonowania zostaną przekroczone.	180 dni
Tryb ograniczonej funkcjonalności	4130	KLSRV_EV_LICENSE_SRV_LIMITED_MODE	Zdarzenia tego typu występują, gdy Kaspersky Security Center Linux zaczyna działać z podstawową funkcjonalnością, bez funkcji Zarządzanie lukami i poprawkami oraz bez funkcji Zarządzanie urządzeniami mobilnymi. Poniższe elementy są przyczynami i odpowiednimi odpowiedziami na zdarzenie: • Okres licencji wygasł. Zapewnij licencję do korzystania z trybu pełnej funkcjonalności Kaspersky Security Center Linux (dodaj ważny kod aktywacyjny lub plik klucza do Serwera administracyjnego). • Serwer administracyjny zarządza większą liczbą urządzeń niż określona przez ograniczenie licencji. Przenieś urządzenia z grup administracyjnych Serwera administracyjnego do tych należących do innego Serwera administracyjnego (jeśli ograniczenie licencji innego Serwera administracyjnego zezwala na to).	180 dni
Certyfikat MDM wygasł	4132	KLSRV_CERTIFICATE_EXPIRED	Wydarzenia tego typu występują, gdy certyfikat mobilny klienta na urządzeniu mobilnym wygaśnie.	180 dni
Plik klucza został dodany do listy zablokowanych	4124	KLSRV_LICENSE_BLACKLISTED	Zdarzenia tego typu występują, gdy firma Kaspersky dodała kod aktywacyjny lub plik klucza, którego używasz, do listy zablokowanych. Aby uzyskać więcej informacji, skontaktuj się z działem pomocy technicznej.	180 dni

Nazwa wyświetlanego typu zdarzenia	ID typu zdarzenia	Typ zdarzenia	Opis	Domyślny czas przechowywania
Aktualizacje dla modułów aplikacji Kaspersky zostały wycofane	4142	KLSRV_SEAMLESS_UPDATE_REVOKED	Zdarzenia tego typu występują, jeśli aktualizacje typu seamless zostały wycofane (dla tych aktualizacji wyświetlany jest stan *Wycofano*) przez specjalistów z pomocy technicznej Kaspersky; na przykład, muszą zostać zaktualizowane do nowszej wersji. Zdarzenie dotyczy poprawek Kaspersky Security Center Linux i nie dotyczy modułów zarządzanych aplikacji firmy Kaspersky. Zdarzenie zawiera przyczynę niezainstalowania aktualizacji typu seamless.	180 dni
Atak wirusa	• 26 (dla Ochrony plików) • 27 (dla Ochrony poczty) • 28 (dla Zapory sieciowej)	GNRL_EV_VIRUS_OUTBREAK	Zdarzenia tego typu występują, gdy liczba szkodliwych obiektów, wykrytych na kilku zarządzanych urządzeniach przekracza wartość progową w krótkim przedziale czasu. Możesz zareagować na zdarzenie w następujące sposoby: • Skonfiguruj wartość progową we właściwościach Serwera administracyjnego. • Utwórz rygorystyczną zasadę, która zostanie aktywowana, lub utwórz zadanie, które zostanie uruchomione przy wystąpieniu tego zdarzenia.	

Zdarzenia błędu funkcjonalnego Serwera administracyjnego

Poniższa tabela przedstawia zdarzenia Serwera administracyjnego o istotności **Błąd funkcjonalny**.

Dla każdego zdarzenia, które może być generowane przez aplikację, określić można ustawienia powiadomień i ustawienia dot. przechowywania w zasadzie aplikacji, w karcie **Konfiguracja zdarzenia**. W przypadku Serwera administracyjnego możesz dodatkowo wyświetlić i skonfigurować listę zdarzeń we właściwościach Serwera administracyjnego. Jeśli chcesz skonfigurować ustawienia powiadomień dla wszystkich zdarzeń jednocześnie, skonfiguruj ogólne ustawienia powiadomień we właściwościach Serwera administracyjnego.

Nazwa wyświetlanego typu zdarzenia	ID typu zdarzenia	Typ zdarzenia	Opis	Domyślny czas przechowywania
Kopiowanie aktualizacji do określonego folderu nie powiodło się	4123	KLSRV_UPD_REPL_FAIL	Zdarzenia tego typu występują, gdy aktualizacje oprogramowania są kopiowane do dodatkowych folderów współdzielonych. Możesz zareagować na zdarzenie w następujące sposoby: • Sprawdź, czy konto użytkownika, który ma uzyskać dostęp do folderu(ów) posiada prawo do zapisu. • Sprawdź, czy nazwa użytkownika i/lub hasło do folderu/-ów nie uległy zmianie. • Sprawdź połączenie z internetem, gdyż to może być przyczyną zdarzenia. Aby zaktualizować bazy danych i moduły oprogramowania, postępuj zgodnie z instrukcjami.	180 dni
Przeszukanie segmentu chmury nie powiodło się	4143	KLSRV_KLCLOUD_SCAN_ERROR	Zdarzenia tego typu występują, gdy Serwer administracyjny nie może przeszukać segmentu sieci w środowisku chmury. Przeczytaj szczegóły w opisie zdarzenia i zareaguj odpowiednio.	Nie jest przechowywany
Przekroczono limit instalacji dla jednej z grup licencjonowanych aplikacji	4126	KLSRV_INVLICPROD_EXCEDED	Serwer administracyjny generuje zdarzenia tego typu okresowo (co godzinę). Zdarzenia tego typu występują, jeśli w Kaspersky Security Center Linux zarządzasz kluczami licencyjnymi aplikacji innych firm i jeśli liczba instalacji przekroczyła ograniczenie ustawione przez klucz licencyjny aplikacji innej firmy. Możesz zareagować na zdarzenie w następujące sposoby: • Zapoznaj się z listą zarządzanych urządzeń. Usuń aplikację innej firmy z urządzeń, na których aplikacja nie jest używana. • Użyj licencji innej firmy dla większej liczby urządzeń. Możesz zarządzać kluczami licencyjnymi aplikacji firm trzecich, korzystając z funkcjonalności grup licencjonowanych aplikacji. Grupa licencjonowanych aplikacji zawiera aplikacje firm trzecich spełniające kryteria ustalone przez Ciebie.	180 dni
Brak wolnego miejsca na dysku	4107	KLSRV_DISK_FULL	Tego typu zdarzenia występują, gdy dysk twardy urządzenia, na którym jest zainstalowany Serwer administracyjny, zabraknie wolnego miejsca. Zwolnij miejsce na dysku na urządzeniu.	180 dni

Nazwa wyświetlanego typu zdarzenia	ID typu zdarzenia	Typ zdarzenia	Opis	Domyślny czas przechowywania
Brak wolnego miejsca w bazie danych Serwera administracyjnego	4110	KLSRV_DATABASE_FULL	Zdarzenia tego typu występują, gdy nie ma wolnego miejsca w bazie danych Serwera administracyjnego. Serwer administracyjny nie działa, gdy jego baza danych osiągnęła swoją pojemność i gdy dalsze zapisywanie w bazie danych nie jest możliwe. Poniżej wymienione są przyczyny tego zdarzenia, w zależności od systemu DBMS, którego używasz, oraz odpowiednie reakcje na to zdarzenie: • Ograniczanie liczby zdarzeń przechowywanych w bazie danych Serwera administracyjnego. • W bazie danych Serwera administracyjnego istnieje zbyt dużo zdarzeń wysłanych przez komponent Kontrola aplikacji. Możesz zmienić ustawienia zasady Kaspersky Endpoint Security dotyczące przechowywania zdarzeń Kontroli aplikacji w bazie danych Serwera administracyjnego. Przeglądanie informacji dotyczących wyboru systemu DBMS.	180 dni
Błąd w czasie wykonywania	4125	KLSRV_RUNTIME_ERROR	Zdarzenia tego typu występują w wyniku nieznanych problemów. Najczęściej są to problemy z systemem DBMS, problemy z siecią oraz inne problemy z oprogramowaniem i sprzętem. Szczegóły zdarzenia można znaleźć w opisie zdarzenia.	180 dni
Folder współdzielony nie jest dostępny	4108	KLSRV_SHARED_FOLDER_UNAVAILABLE	Zdarzenia tego typu występują, jeśli folder współdzielony Serwera administracyjnego jest niedostępny. Możesz zareagować na zdarzenie w następujące sposoby: • Sprawdź, czy Serwer administracyjny (na którym znajduje się folder współdzielony) jest włączony i dostępny. • Sprawdź, czy nazwa użytkownika i/lub hasło do folderu uległy zmianie. • Sprawdź połączenie sieciowe.	180 dni
Baza danych Serwera administracyjnego jest niedostępna	4109	KLSRV_DATABASE_UNAVAILABLE	Zdarzenia tego typu występują, jeśli baza danych Serwera administracyjnego stała się niedostępna. Możesz zareagować na zdarzenie w następujące sposoby: • Sprawdź, czy zdalny serwer, na którym jest zainstalowany serwer DBMS, jest dostępny. • Przejrzyj raporty systemu DBMS, aby odkryć przyczynę braku dostępności bazy danych Serwera administracyjnego.	180 dni

Zdarzenia ostrzegające Serwera administracyjnego

Poniższa tabela przedstawia zdarzenia Serwera administracyjnego o istotności **Ostrzeżenie**.

Dla każdego zdarzenia, które może być generowane przez aplikację, określić można ustawienia powiadomień i ustawienia dot. przechowywania w zasadzie aplikacji, w karcie **Konfiguracja zdarzenia**. W przypadku Serwera administracyjnego możesz dodatkowo wyświetlić i skonfigurować listę zdarzeń we właściwościach Serwera administracyjnego. Jeśli chcesz skonfigurować ustawienia powiadomień dla wszystkich zdarzeń jednocześnie, skonfiguruj ogólne ustawienia powiadomień we właściwościach Serwera administracyjnego.

Zdarzenia ostrzegające Serwera administracyjnego

Nazwa wyświetlanego typu zdarzenia	ID typu zdarzenia	Typ zdarzenia	Opis	Domyślny czas przechowywania
Certyfikat Serwera administracyjnego dla urządzeń mobilnych wkrótce utraci ważność	6128	KLSRV_EV_SRV_CERT_EXPIRES_SOON	Zdarzenia tego typu występują, gdy certyfikat Serwera administracyjnego dla urządzeń mobilnych i urządzeń UEFI utraci ważność. Należy zaktualizować certyfikat, który utracił ważność.	90 dni
Certyfikat APNs wkrótce utraci ważność	4136	KLSRV_APN_CERTIFICATE_EXPIRES_SOON	Zdarzenia tego typu występują, gdy do wygaśnięcia certyfikatu APNs pozostało mniej niż 14 dni. Jeśli certyfikat APNs utraci ważność, należy ręcznie odnowić certyfikat APNs i zainstalować go na serwerze iOS MDM. Zalecane jest wcześniejsze utworzenie terminarza odnawiania certyfikatu APNs.	Nie jest przechowywany
Certyfikat APNs wygasł	4135	KLSRV_APN_CERTIFICATE_EXPIRED	Zdarzenia tego typu występują, gdy certyfikat APNs utraci ważność. Należy ręcznie odnowić certyfikat APNs i zainstalować go na serwerze iOS MDM.	Nie jest przechowywany
Audyt: połączenie testowe z serwerem SIEM nie powiodło się	5120	KLAUD_EV_SIEM_TEST_FAILED	Zdarzenia tego typu mają miejsce w przypadku niepowodzenia automatycznego testu połączenia z serwerem SIEM.	90 dni
Certyfikat został usunięty	4134	KLSRV_CERTIFICATE_REMOVED	Zdarzenia tego typu występują, gdy administrator usunie dowolny typ certyfikatu (Ogólny, Poczta, VPN) dla Zarządzania urządzeniami mobilnymi. Po usunięciu certyfikatu urządzenia mobilne, podłączone za pośrednictwem tego certyfikatu, nie nawiążą połączenia z Serwerem administracyjnym. To zdarzenie może być pomocne podczas sprawdzania problemów z działaniem, skojarzonych z zarządzaniem urządzeń mobilnych.	90 dni

Nazwa wyświetlanego typu zdarzenia	ID typu zdarzenia	Typ zdarzenia	Opis	Domyślny czas przechowywania
Certyfikat został zażądany	4133	KLSRV_CERTIFICATE_REQUESTED	Zdarzenia tego typu występują, gdy certyfikat dla Zarządzania urządzeniami mobilnymi nie zostanie automatycznie wystawiony ponownie. Poniżej znajdują się możliwe przyczyny wystąpienia tego zdarzenia oraz odpowiednie reakcje na nie: • Automatyczne ponowne wydawanie zostało zainicjowane dla certyfikatu, dla którego wyłączona jest opcja **Odnów certyfikat automatycznie, jeśli jest to możliwe**. Może to być spowodowane błędem, który wystąpił podczas tworzenia certyfikatu. Konieczne może być ręczne ponowne wystawienie certyfikatu. • Jeśli korzystasz z integracji z infrastrukturą klucza publicznego, przyczyną może być brak atrybutu SAM-Account-Name konta użytego do integracji z PKI oraz do wydania certyfikatu. Przejrzyj właściwości konta.	90 dni
Konflikt nazw urządzeń	4102	KLSRV_EVENT_HOSTS_CONFLICT	Zdarzenia tego typu występują, gdy Serwer administracyjny traktuje dwa lub więcej zarządzanych urządzeń jako jedno urządzenie. Ma to miejsce najczęściej wtedy, gdy sklonowany dysk twardy został użyty do wdrożenia oprogramowania na zarządzanych urządzeniach i bez przełączania Agenta sieciowego do trybu klonowania dedykowanego dysku na odpowiednim urządzeniu. Aby uniknąć tego problemu, przełącz Agenta sieciowego do trybu klonowania dysku na odpowiednim urządzeniu przed sklonowaniem dysku twardego tego urządzenia.	90 dni
Połączenie z głównym Serwerem administracyjnym zostało zerwane	4118	KLSRV_EV_MASTER_SRV_DISCONNECTED	Zdarzenia tego typu występują, gdy połączenie z głównym Serwerem administracyjnym zostanie przerwane. Przeczytaj dziennik systemu operacyjnego na urządzeniu, na którym jest zainstalowany główny Serwer administracyjny i zareaguj odpowiednio.	90 dni
Połączenie z podrzędnym Serwerem administracyjnym zostało zerwane	4116	KLSRV_EV_SLAVE_SRV_DISCONNECTED	Zdarzenia tego typu występują, gdy połączenie z podrzędnym Serwerem administracyjnym zostanie przerwane. Przeczytaj dziennik systemu operacyjnego na urządzeniu, na którym jest zainstalowany podrzędny Serwer administracyjny i zareaguj odpowiednio.	90 dni

Nazwa wyświetlanego typu zdarzenia	ID typu zdarzenia	Typ zdarzenia	Opis	Domyślny czas przechowywania
Urządzenie było nieaktywne w sieci od dłuższego czasu	4103	KLSRV_EVENT_HOSTS_NOT_VISIBLE	Zdarzenia tego typu występują, gdy zarządzane urządzenie nie wykazuje brak aktywności przez pewien czas. Najczęściej dzieje się tak, gdy zarządzane urządzenie zostaje wycofane z eksploatacji. Możesz zareagować na zdarzenie w następujące sposoby: • W celu usunięcia urządzenia z listy zarządzanych urządzeń. Określ przedział czasu, po którym tworzone jest zdarzenie **Urządzenie było nieaktywne w sieci od dłuższego czasu**, przy użyciu Kaspersky Security Center Web Console. • Określ przedział czasu, po którym urządzenie zostanie automatycznie usunięte z grupy, przy użyciu Kaspersky Security Center Web Console.	90 dni
Stan urządzenia: Ostrzeżenie	4114	KLSRV_HOST_STATUS_WARNING	Zdarzenia tego typu występują, gdy do zarządzanego urządzenia zostanie przypisany stan *Ostrzeżenie*. Możesz skonfigurować warunki, zgodnie z którymi stan urządzenia zostanie zmieniony na *Ostrzeżenie*.	90 dni
Nie udało się pobrać pliku do urządzenia	4165	KLSRV_FILE_DOWNLOAD_FAILED	Zdarzenia tego typu występują w następujących przypadkach: • Próbujesz pobrać plik do kontenera korporacyjnego, ale kontener korporacyjny nie został utworzony. • Brak wystarczającej ilości miejsca na urządzeniu. • Nie udało się pobrać informacji o pliku z serwera. • Nie udało się pobrać zawartości pliku z serwera. • Nie można utworzyć folderu na urządzeniu. • Brak uprawnień dostępu do pliku na urządzeniu osobistym. • Brak uprawnień dostępu do pliku w kontenerze firmowym.	90 dni
Błąd podczas przesyłania wiadomości FCM do serwera FCM	4140	KLSRV_GCM_GENERAL_ERROR	Zdarzenia tego typu występują w wyniku niespodziewanych błędów po stronie Serwera administracyjnego podczas pracy z protokołem Google Firebase Cloud Messaging HTTP. Przeczytaj szczegóły w opisie zdarzenia i zareaguj odpowiednio. Jeżeli nie znajdziesz rozwiązania swojego problemu, skontaktuj się z działem pomocy technicznej firmy Kaspersky.	90 dni

Nazwa wyświetlanego typu zdarzenia	ID typu zdarzenia	Typ zdarzenia	Opis	Domyślny czas przechowywania
Błąd podczas przesyłania wiadomości FCM do urządzenia mobilnego	4138	KLSRV_GCM_DEVICE_ERROR	Zdarzenia tego typu występują, gdy Zarządzanie urządzeniami mobilnymi jest skonfigurowane do użycia Google Firebase Cloud Messaging (FCM) w celu połączenia z zarządzanymi urządzeniami mobilnymi z systemem operacyjnym Android, a serwer FCM nie może obsłużyć niektórych żądań otrzymanych z Serwera administracyjnego. To oznacza, że niektóre zarządzane urządzenia mobilne nie otrzymają powiadomienia push. Przeczytaj kod Http w szczegółach opisu zdarzenia i zareaguj odpowiednio. Więcej informacji na temat kodów HTTP otrzymanych z FCM Server i powiązanych błędów można znaleźć w dokumentacji do usługi Google Firebase (zajrzyj do rozdziału „Podrzędne kody odpowiedzi na komunikaty o błędzie").	90 dni
Wykryto często występujące zdarzenia		KLSRV_EVENT_SPAM_EVENTS_DETECTED	Zdarzenia tego typu występują, gdy Serwer administracyjny wykryje często występujące zdarzenie na zarządzanym urządzeniu. Aby uzyskać szczegółowe informacje, zapoznaj się z następującą sekcją: Blokowanie często występujących zdarzeń.	90 dni
Dysk twardy jest prawie pełny	4105	KLSRV_NO_SPACE_ON_VOLUMES	Tego typu zdarzenia występują, gdy dysk twardy urządzenia, na którym jest zainstalowany Serwer administracyjny, prawie zabraknie wolnego miejsca. Zwolnij miejsce na dysku na urządzeniu.	90 dni
Błąd HTTP podczas wysyłania wiadomości FCM do serwera FCM	4139	KLSRV_GCM_HTTP_ERROR	Zdarzenia tego typu występują, gdy Zarządzanie urządzeniami mobilnymi jest skonfigurowane do użycia Google Firebase Cloud Messaging (FCM) w celu połączenia z zarządzanymi urządzeniami mobilnymi z systemem operacyjnym Android, a FCM Server przywróci żądanie Serwera administracyjnego z kodem HTTP innym niż 200 (OK). Poniżej znajdują się możliwe przyczyny wystąpienia tego zdarzenia oraz odpowiednie reakcje na nie: • Problemy po stronie serwera FCM. Przeczytaj kod Http w szczegółach opisu zdarzenia i zareaguj odpowiednio. Więcej informacji na temat kodów HTTP otrzymanych z FCM Server i powiązanych błędów można znaleźć w dokumentacji do usługi Google Firebase (zajrzyj do rozdziału „Podrzędne kody odpowiedzi na komunikaty o błędzie"). • Problemy po stronie serwera proxy (jeśli korzystasz z serwera proxy). Przeczytaj kod HTTP w szczegółach zdarzenia i zareaguj odpowiednio.	90 dni

Nazwa wyświetlanego typu zdarzenia	ID typu zdarzenia	Typ zdarzenia	Opis	Domyślny czas przechowywania
Limit licencji został przekroczony	4098	KLSRV_EV_LICENSE_CHECK_100_110	Raz dziennie Kaspersky Security Center Linux sprawdza, czy limity licencyjne nie są przekroczone. Zdarzenia tego typu występują, gdy Serwer administracyjny wykryje, że niektóre ograniczenia licencyjne są przekroczone przez aplikacje firmy Kaspersky zainstalowane na urządzeniach klienckich i czy liczba aktualnie używanych jednostek licencyjnych objętych jedną licencją stanowi od 100% do 110% całkowitej liczby jednostek objętych licencją. Nawet jeśli to zdarzenie wystąpi, urządzenia klienckie są chronione. Możesz zareagować na zdarzenie w następujące sposoby: • Zapoznaj się z listą zarządzanych urządzeń. Usuń urządzenia, które nie są w użyciu. • Dostarcz licencję dla większej liczby urządzeń (dodaj ważny kod aktywacyjny lub plik klucza do Serwera administracyjnego). Kaspersky Security Center Linux określa reguły generowania zdarzeń, gdy limity licencjonowania zostaną przekroczone.	90 dni
Limit instalacji w jednej z grup licencjonowanych aplikacji zostanie wkrótce osiągnięty	4128	KLSRV_INVLICPROD_EXPIRED_SOON	Zdarzenia tego typu występują, gdy jeden z kluczy licencyjnych aplikacji innych firm, znajdujących się w grupie licencjonowanych aplikacji, ma wkrótce wygasnąć. W rezultacie limit instalacji dla jednej z grup zostanie zmniejszony. Możesz zareagować na zdarzenie w następujące sposoby: • Jeśli aplikacja innej firmy nie jest używana na niektórych zarządzanych urządzeniach, usuń aplikację z tych urządzeń. • Jeśli spodziewasz się, że w najbliższej przyszłości liczba instalacji dla aplikacji innej firmy przekroczy dozwoloną maksymalną wartość, uwzględnij uzyskanie licencji innej firmy dla większej liczby urządzeń w przyszłości. Możesz zarządzać kluczami licencyjnymi aplikacji firm trzecich, korzystając z funkcjonalności grup licencjonowanych aplikacji.	90 dni
Zarejestrowano nowe aktualizacje dla modułów aplikacji Kaspersky	4141	KLSRV_SEAMLESS_UPDATE_REGISTERED	Zdarzenia tego typu występują, gdy Serwer administracyjny zarejestruje nowe aktualizacje dla oprogramowania firmy Kaspersky, zainstalowanego na zarządzanych urządzeniach, których instalacja wymaga zatwierdzenia. Zatwierdź lub odrzuć aktualizacje, korzystając z Kaspersky Security Center Web Console.	90 dni

Nazwa wyświetlanego typu zdarzenia	ID typu zdarzenia	Typ zdarzenia	Opis	Domyślny czas przechowywania
Brak wolnego miejsca w bazie danych Serwera administracyjnego	4106	KLSRV_NO_SPACE_IN_DATABASE	Zdarzenia tego typu występują, jeśli miejsce w bazie danych Serwera administracyjnego jest zbyt ograniczone. Jeśli nie rozwiążesz tego problemu, wkrótce baza danych Serwera administracyjnego osiągnie swoją pojemność, a Serwer administracyjny nie będzie działał. Poniżej wymienione są przyczyny tego zdarzenia, w zależności od systemu DBMS, którego używasz, oraz odpowiednie reakcje na to zdarzenie. • Nieograniczanie liczby zdarzeń przechowywanych w bazie danych Serwera administracyjnego. • Zmniejszenie listy zdarzeń przechowywanych w bazie danych Serwera administracyjnego. Przeglądanie informacji dotyczących wyboru systemu DBMS.	90 dni
Przekroczono limit zdarzeń w bazie danych. Rozpoczęto usuwanie zdarzeń	4145	KLSRV_EVP_DB_TRUNCATING	Zdarzenia tego typu występują, jeśli usuwanie starszych zdarzeń z bazy danych Serwera administracyjnego rozpoczęło się, gdy pojemność bazy danych Serwera administracyjnego została osiągnięta. Możesz zareagować na zdarzenie w następujące sposoby: • Zmiana maksymalnej liczby zdarzeń przechowywanych w bazie danych Serwera administracyjnego. • Zmniejszenie listy zdarzeń przechowywanych w bazie danych Serwera administracyjnego.	Nie jest przechowywany
Przekroczono limit zdarzeń w bazie danych, zdarzenia zostały usunięte	4146	KLSRV_EVP_DB_TRUNCATED	Zdarzenia tego typu występują, jeśli starsze zdarzenia zostały usunięte z bazy danych Serwera administracyjnego po osiągnięciu pojemności bazy danych Serwera administracyjnego. Możesz zareagować na zdarzenie w następujące sposoby: • Zmiana maksymalnej dozwolonej liczby zdarzeń przechowywanych w bazie danych Serwera administracyjnego. • Zmniejszenie listy zdarzeń przechowywanych w bazie danych Serwera administracyjnego.	Nie jest przechowywany

Zdarzenia informacyjne Serwera administracyjnego

W poniższej tabeli przedstawiono zdarzenia Serwera administracyjnego o istotności **Informacja**.

Dla każdego zdarzenia, które może być generowane przez aplikację, określić można ustawienia powiadomień i ustawienia dot. przechowywania w zasadzie aplikacji, w karcie **Konfiguracja zdarzenia**. W przypadku Serwera administracyjnego możesz dodatkowo wyświetlić i skonfigurować listę zdarzeń we właściwościach Serwera administracyjnego. Jeśli chcesz skonfigurować ustawienia powiadomień dla wszystkich zdarzeń jednocześnie, skonfiguruj ogólne ustawienia powiadomień we właściwościach Serwera administracyjnego.

Nazwa wyświetlanego typu zdarzenia	ID typu zdarzenia	Typ zdarzenia	Opis	Domyślny czas przechowywania
Odnowienie certyfikatu Serwera administracyjnego dla urządzeń mobilnych	6127	KLSRV_EV_SRV_CERT_RENEWED	To zdarzenie występuje, gdy zostanie odnowiony certyfikat Serwera administracyjnego.	30 dni
Audyt: polecenie zostało wysłane na urządzenie	4170	KLAUD_EV_COMMAND_SENT	Zdarzenia tego typu występują, gdy użytkownik wysyła polecenie do urządzenia mobilnego.	30 dni
Audyt: Połączenie z Serwerem administracyjnym zostało zakończone	4151	KLAUD_EV_SERVERDISCONNECT		30 dni
Audyt: Połączenie z Serwerem administracyjnym zostało nawiązane	4147	KLAUD_EV_SERVERCONNECT	Zdarzenia tego typu występują, gdy użytkownik łączy się z Serwerem administracyjnym za pomocą Kaspersky Security Center Web Console. Do zdarzeń tych należy adres IP urządzenia, na którym zainstalowano Kaspersky Security Center Web Console Server.	30 dni
Audyt: Klucze szyfrujące zostały zaimportowane/wyeksportowane	5100	KLAUD_EV_DPEKEYSEXPORT	Na przykład to zdarzenie występuje podczas migracji.	30 dni
Audyt: Ustawienia grupy zostały zmodyfikowane	4149	KLAUD_EV_ADMGROUP_CHANGED	Zdarzenia tego typu mają miejsce w przypadku edycji grupy bezpieczeństwa.	30 dni
Audyt: Obiekt został zmodyfikowany	4148	KLAUD_EV_OBJECTMODIFY	To zdarzenie śledzi zmiany w następujących obiektach: • Grupa administracyjna • Grupa bezpieczeństwa • Użytkownik • Pakiet • Zadanie • Zasada • Serwer • Wirtualny Serwer	30 dni
Audyt: Właściwości obiektu zostały zmodyfikowane	4152	KLAUD_EV_OBJECTPROPMODIFIED	To zdarzenie śledzi zmiany w następujących właściwościach: • Użytkownik • Licencja • Serwer • Wirtualny serwer	30 dni

Nazwa wyświetlanego typu zdarzenia	ID typu zdarzenia	Typ zdarzenia	Opis	Domyślny czas przechowywania
Audyt: Stan obiektu zmienił się	4150	KLAUD_EV_TASK_STATE_CHANGED	Na przykład to zdarzenie występuje, gdy zadanie nie powiodło się z powodu błędu.	30 dni
Audyt: połączenie testowe z serwerem SIEM powiodło się	5110	KLAUD_EV_SIEM_TEST_SUCCESS	Zdarzenia tego typu mają miejsce w przypadku udanego połączenia testowego z serwerem SIEM.	30 dni
Audyt: uprawnienia użytkownika zostały zmodyfikowane	4153	KLAUD_EV_OBJECTACLMODIFIED	To zdarzenie występuje, gdy uprawnienia użytkownika zostały zmodyfikowane	30 dni
Nawiązano połączenie z głównym Serwerem administracyjnym	4117	KLSRV_EV_MASTER_SRV_CONNECTED		30 dni
Nawiązano połączenie z podrzędnym Serwerem administracyjnym	4115	KLSRV_EV_SLAVE_SRV_CONNECTED	Aby uzyskać szczegółowe informacje, zobacz następujący artykuł: Tworzenie hierarchii Serwerów administracyjnych: dodawanie podrzędnego Serwera administracyjnego.	30 dni
Bazy danych zostały zaktualizowane	4144	KLSRV_UPD_BASES_UPDATED	Zdarzenia tego typu mają miejsce, gdy zadanie **Pobierz aktualizacje do repozytorium Serwera administracyjnego** zakończy aktualizację baz danych.	30 dni
Urządzenie zostało automatycznie dodane do grupy	4101	KLSRV_EVENT_HOSTS_NEW_REDIRECTED	Zdarzenia tego typu mają miejsce, gdy urządzenia zostały przypisane do grupy zgodnie z regułami przenoszenia urządzeń.	30 dni
Urządzenie zostało automatycznie przeniesione zgodnie z regułą	1074	KLSRV_HOST_MOVED_WITH_RULE_EX	Zdarzenia tego typu występują, gdy urządzenia zostały przeniesione do grup administracyjnych za pomocą reguł przenoszenia urządzeń.	30 dni
Urządzenie zostało usunięte z grupy: nieaktywność w sieci od dłuższego czasu	4104	KLSRV_INVISIBLE_HOSTS_REMOVED	Zdarzenia tego typu mają miejsce, gdy urządzenia zostały automatycznie usunięte z grupy z powodu braku aktywności.	30 dni
ID instancji FCM na tym urządzeniu mobilnym zmieniło się	4137	KLSRV_GCM_DEVICE_REGID_CHANGED	Zdarzenia tego typu mają miejsce w przypadku zmiany tokena Firebase Cloud Messaging na urządzeniu. Informacje na temat rotacji tokenów FCM znajdziesz w dokumentacji usługi Firebase.	30 dni
Plik usunięty z Serwera administracyjnego	4163	KLSRV_FILE_REMOVED	To zdarzenie występuje, gdy plik zostanie usunięty z Serwera administracyjnego.	30 dni

Nazwa wyświetlanego typu zdarzenia	ID typu zdarzenia	Typ zdarzenia	Opis	Domyślny czas przechowywania
Plik pobrany na urządzenie	4164	KLSRV_FILE_DOWNLOADED	To zdarzenie ma miejsce w następujących przypadkach: • Plik został pobrany na urządzenie podczas sesji. • Plik został pobrany z Serwera administracyjnego.	30 dni
Wykryto pliki do przesłania do firmy Kaspersky w celu analizy	4131	KLSRV_APS_FILE_APPEARED		30 dni
Plik przesłany na Serwer administracyjny	4162	KLSRV_FILE_UPLOADED	To zdarzenie występuje, gdy plik zostanie przesłany na Serwer administracyjny.	30 dni
Limit instalacji w jednej z grup licencjonowanych aplikacji zostanie wkrótce przekroczony (wykorzystywanych jest więcej niż 90%)	4127	KLSRV_INVLICPROD_FILLED	Zdarzenia tego typu występują, gdy liczba instalacji aplikacji innych firm, zawartych w grupie licencjonowanych aplikacji osiągnie 90% maksymalnej dozwolonej wartości określonej we właściwościach klucza licencyjnego. Możesz zareagować na zdarzenie w następujące sposoby: • Jeśli aplikacja innej firmy nie jest używana na niektórych zarządzanych urządzeniach, usuń aplikację z tych urządzeń. • Jeśli spodziewasz się, że w najbliższej przyszłości liczba instalacji dla aplikacji innej firmy przekroczy dozwoloną maksymalną wartość, uwzględnij uzyskanie licencji innej firmy dla większej liczby urządzeń w przyszłości. Możesz zarządzać kluczami licencyjnymi aplikacji firm trzecich, korzystając z funkcjonalności grup licencjonowanych aplikacji.	30 dni
Wykryto nowe urządzenie	4100	KLSRV_EVENT_HOSTS_NEW_DETECTED	Zdarzenia tego typu mają miejsce, gdy zostaną wykryte nowe urządzenia sieciowe.	30 dni

Nazwa wyświetlanego typu zdarzenia	ID typu zdarzenia	Typ zdarzenia	Opis	Domyślny czas przechowywania
Ponad 90% tego klucza licencyjnego jest wykorzystane	4097	KLSRV_EV_LICENSE_CHECK_90	Zdarzenia tego typu występują, gdy Serwer administracyjny wykryje, że niektóre limity licencyjne zbliżają się do przekroczenia przez aplikacje firmy Kaspersky zainstalowane na urządzeniach klienckich i czy liczba aktualnie używanych jednostek licencyjnych objętych jedną licencją obejmuje co najmniej 90% całkowitej liczby jednostek objętych licencją. Nawet w przypadku przekroczenia limitu licencji urządzenia klienckie są chronione. Możesz zareagować na zdarzenie w następujące sposoby: • Zapoznaj się z listą zarządzanych urządzeń. Usuń urządzenia, które nie są w użyciu. • Dostarcz licencję dla większej liczby urządzeń (dodaj ważny kod aktywacyjny lub plik klucza do Serwera administracyjnego). Kaspersky Security Center Linux określa reguły generowania zdarzeń, gdy limity licencjonowania zostaną przekroczone.	30 dni
Certyfikat Serwera administracyjnego dla urządzeń mobilnych został utworzony	6126	KLSRV_EV_SRV_CERT_RESERVE_CREATED	To zdarzenie występuje, gdy zostanie utworzony certyfikat Serwera administracyjnego.	30 dni
Aktualizacje zostały pomyślnie skopiowane do wskazanego folderu	4122	KLSRV_UPD_REPL_OK	Zdarzenia tego typu mają miejsce, gdy zadanie **Pobierz aktualizacje do repozytorium Serwera administracyjnego** zakończy kopiowanie plików do określonego folderu.	30 dni

Zdarzenia **Utworzono certyfikat zapasowy** oraz **Odnowienie certyfikatu** są automatycznie publikowane przez Serwer administracyjny i wyświetlane w Konsoli administracyjnej tylko wtedy, gdy operacje odpowiadające tym zdarzeniom zostaną wykonane dla certyfikatów Serwera administracyjnego dla urządzeń mobilnych i urządzeń UEFI.

Zdarzenia Agenta sieciowego

Ta sekcja zawiera informacje o zdarzeniach dotyczących Agenta sieciowego.

Zdarzenia błędu funkcjonalnego Agenta sieciowego

Poniższa tabela wyświetla zdarzenia Agenta sieciowego Kaspersky Security Center Linux, które posiadają priorytet **Błąd funkcjonalny**.

Dla każdego zdarzenia, które może być generowane przez aplikację, określić można ustawienia powiadomień i ustawienia dot. przechowywania w zasadzie aplikacji, w karcie **Konfiguracja zdarzenia**. Jeśli chcesz skonfigurować ustawienia powiadomień dla wszystkich zdarzeń jednocześnie, skonfiguruj ogólne ustawienia powiadomień we właściwościach Serwera administracyjnego.

Zdarzenia błędu funkcjonalnego Agenta sieciowego

Nazwa wyświetlanego typu zdarzenia	ID typu zdarzenia	Typ zdarzenia	Opis	Domyślny czas przechowywania
Instalacja certyfikatów głównych nie powiodła się	7728	KLNAG_EV_ROOT_CERT_INSTALL_ERR	Zdarzenie zawiera opis błędu instalacji certyfikatów.	30 dni
Instalacja aktualizacji oprogramowania firmy trzeciej nie powiodła się	7697	KLNAG_EV_3P_PATCH_INSTALL_ERROR	Zdarzenia tego typu występują, jeśli używane są funkcje Zarządzanie lukami i poprawkami oraz jeśli aktualizacja oprogramowania innych firm nie zakończyła się pomyślnie. Sprawdź, czy odnośnik do oprogramowania innej firmy jest ważny. Przeczytaj opis zdarzenia.	30 dni
Zainstalowanie aktualizacji Windows Update nie powiodło się	7717	KLNAG_EV_WUA_INSTALL_ERROR	Zdarzenia tego typu występują, jeśli aktualizacje systemu Windows nie zakończyły się pomyślnie. Przeczytaj opis zdarzenia. Poszukaj błędu w Bazie wiedzy Microsoft. Skontaktuj się z pomocą techniczną Microsoft, jeśli sam nie możesz rozwiązać problemu.	30 dni
Usunięcie certyfikatów głównych nie powiodło się	7730	KLNAG_EV_ROOT_CERT_REMOVE_ERR	Zdarzenie zawiera opis błędu usunięcia certyfikatów.	30 dni
Nie udało się przywrócić pliku sudoers do wartości referencyjnej	7726	KLNAG_EV_SUDOER_RESTORED_ERR	Zdarzenie zawiera opis błędu zamiany pliku sudoers.	30 dni
Błąd podczas instalacji aktualizacji	7702	KLNAG_EV_PATCH_INSTALL_ERROR	Zdarzenia tego typu występują, jeśli automatyczne aktualizowanie i instalowanie poprawek dla składników Kaspersky Security Center Linux nie zakończyło się pomyślnie. Zdarzenie nie dotyczy aktualizacji zarządzanych aplikacji firmy Kaspersky. Przeczytaj opis zdarzenia. Przyczyną tego zdarzenia może być problem z systemem Windows na Serwerze administracyjnym. Jeśli w opisie wspomniany jest jakikolwiek problem z konfiguracją systemu Windows, rozwiąż ten problem.	30 dni
Zarządzanie użytkownikami: błędy	7723	KLNAG_EV_USR_MNG_ERR	Ogólne zdarzenie ostrzegające.	30 dni

Zdarzenia ostrzegające Agenta sieciowego

Poniższa tabela wyświetla zdarzenia Agenta sieciowego, które posiadają priorytet **Ostrzeżenie**.

Dla każdego zdarzenia, które może być generowane przez aplikację, określić można ustawienia powiadomień i ustawienia dot. przechowywania w zasadzie aplikacji, w karcie **Konfiguracja zdarzenia**. Jeśli chcesz skonfigurować ustawienia powiadomień dla wszystkich zdarzeń jednocześnie, skonfiguruj ogólne ustawienia powiadomień we właściwościach Serwera administracyjnego.

Zdarzenia ostrzegające Agenta sieciowego

Nazwa wyświetlanego typu zdarzenia	ID typu zdarzenia	Typ zdarzenia	Opis	Domyślny czas przechowywania
Serwer KSN proxy został uruchomiony. Sprawdzenie dostępności KSN nie powiodło się	7718	KSNPROXY_STARTED_CON_CHK_FAILED	Zdarzenia tego typu mają miejsce w przypadku niepowodzenia połączenia testowego dla skonfigurowanego połączenia proxy KSN.	30 dni
Wystąpił incydent związany z bezpieczeństwem	549	GNRL_EV_APP_INCIDENT_OCCURED	Zdarzenia tego typu mają miejsce w przypadku wykrycia incydentu na urządzeniu. Na przykład to zdarzenie występuje, gdy na urządzeniu jest mało miejsca na dysku.	30 dni
Plik Sudoers nie pasuje do wartości referencyjnej	7724	KLNAG_EV_SUDOER_DIFFERENT	Zdarzenia tego typu występują, gdy plik sudoers nie jest zgodny z plikiem referencyjnym.	30 dni
Instalacja aktualizacji oprogramowania firmy trzeciej została odroczona	7698	KLNAG_EV_3P_PATCH_INSTALL_SLIPPED	Na przykład zdarzenia tego typu mają miejsce, gdy umowa licencyjna użytkownika końcowego dotycząca instalacji aktualizacji innej firmy zostanie odrzucona.	30 dni
Instalacja aktualizacji oprogramowania firmy trzeciej została zakończona ostrzeżeniem	7696	KLNAG_EV_3P_PATCH_INSTALL_WARNING	Pobierz pliki śledzenia i sprawdź wartość pola KLRI_PATCH_RES_DESC, aby uzyskać szczegółowe informacje.	30 dni
Zarządzanie użytkownikami: ostrzeżenia	7722	KLNAG_EV_USR_MNG_WRN	Ogólne zdarzenie ostrzegające.	30 dni
Proces instalacji aktualizacji modułów oprogramowania zwrócił ostrzeżenie	7701	KLNAG_EV_PATCH_INSTALL_WARNING	Pobierz pliki śledzenia i sprawdź wartość pola KLRI_PATCH_RES_DESC, aby uzyskać szczegółowe informacje.	30 dni

Zdarzenia informacyjne Agenta sieciowego

Poniższa tabela wyświetla zdarzenia Agenta sieciowego, które posiadają priorytet **Informacja**.

Dla każdego zdarzenia, które może być generowane przez aplikację, określić można ustawienia powiadomień i ustawienia dot. przechowywania w zasadzie aplikacji, w karcie **Konfiguracja zdarzenia**. Jeśli chcesz skonfigurować ustawienia powiadomień dla wszystkich zdarzeń jednocześnie, skonfiguruj ogólne ustawienia powiadomień we właściwościach Serwera administracyjnego.

Zdarzenia informacyjne Agenta sieciowego

Nazwa wyświetlanego typu zdarzenia	ID typu zdarzenia	Typ zdarzenia	Domyślny czas przechowywania
Aplikacja została zainstalowana	7703	KLNAG_EV_INV_APP_INSTALLED	30 dni
Aplikacja została odinstalowana	7704	KLNAG_EV_INV_APP_UNINSTALLED	30 dni

Nazwa wyświetlanego typu zdarzenia	ID typu zdarzenia	Typ zdarzenia	Domyślny czas przechowywania
Certyfikat otrzymany dla portu HTTPS serwera WWW	—	WEB_SERVER_CERTIFICATE_RENEWED	30 dni
Urządzenie zostało zautoryzowane	7711	KLNAG_EV_NAC_HOST_AUTHORIZED	30 dni
Wykryto nowe urządzenie	7710	KLNAG_EV_NAC_DEVICE_DISCOVERED	30 dni
Urządzenie zostało usunięte	7709	KLNAG_EV_DEVICE_REMOVE	30 dni
Instalacja aktualizacji modułów oprogramowania została uruchomiona	7700	KLNAG_EV_PATCH_INSTALL_STARTING	30 dni
Serwer KSN proxy został uruchomiony. Sprawdzenie dostępności KSN zostało pomyślnie zakończone	7719	KSNPROXY_STARTED_CON_CHK_OK	30 dni
KSN Proxy został zatrzymany	7720	KSNPROXY_STOPPED	30 dni
Monitorowana aplikacja została zainstalowana	7705	KLNAG_EV_INV_OBS_APP_INSTALLED	30 dni
Monitorowana aplikacja została odinstalowana	7706	KLNAG_EV_INV_OBS_APP_UNINSTALLED	30 dni
Dodano nowe urządzenie	7708	KLNAG_EV_DEVICE_ARRIVAL	30 dni
Zainstalowano certyfikaty główne	7727	KLNAG_EV_ROOT_CERT_INSTALLED	30 dni
Usunięto certyfikaty główne	7729	KLNAG_EV_ROOT_CERT_REMOVED	30 dni
Plik sudoers został pomyślnie przywrócony do wartości referencyjnej	7725	KLNAG_EV_SUDOER_RESTORED	30 dni
Aplikacja innego producenta została zainstalowana	7707	KLNAG_EV_INV_CMPTR_APP_INSTALLED	30 dni
Aktualizacja oprogramowania firmy trzeciej została pomyślnie zainstalowana	7694	KLNAG_EV_3P_PATCH_INSTALLED_SUCCESSFULLY	30 dni
Instalacja aktualizacji oprogramowania firmy trzeciej została uruchomiona	7695	KLNAG_EV_3P_PATCH_INSTALL_STARTING	30 dni
Aktualizacja modułów aplikacji została pomyślnie zainstalowana	7699	KLNAG_EV_PATCH_INSTALLED_SUCCESSFULLY	30 dni
Zarządzanie użytkownikami: info	7721	KLNAG_EV_USR_MNG_INF	30 dni
Serwer sieciowy został uruchomiony na hoście	—	WEB_SERVER_STARTED	30 dni
Serwer sieciowy zatrzymany na hoście	—	WEB_SERVER_STOPPED	30 dni
Windows Desktop Sharing: Aplikacja została uruchomiona	7714	KLUSRLOG_EV_PROCESS_LAUNCHED	30 dni
Windows Desktop Sharing: Plik został zmodyfikowany	7713	KLUSRLOG_EV_FILE_MODIFIED	30 dni
Windows Desktop Sharing: Plik został odczytany	7712	KLUSRLOG_EV_FILE_READ	30 dni
Windows Desktop Sharing: Uruchomiono	7715	KLUSRLOG_EV_WDS_BEGIN	30 dni
Windows Desktop Sharing: Zatrzymano	7716	KLUSRLOG_EV_WDS_END	30 dni

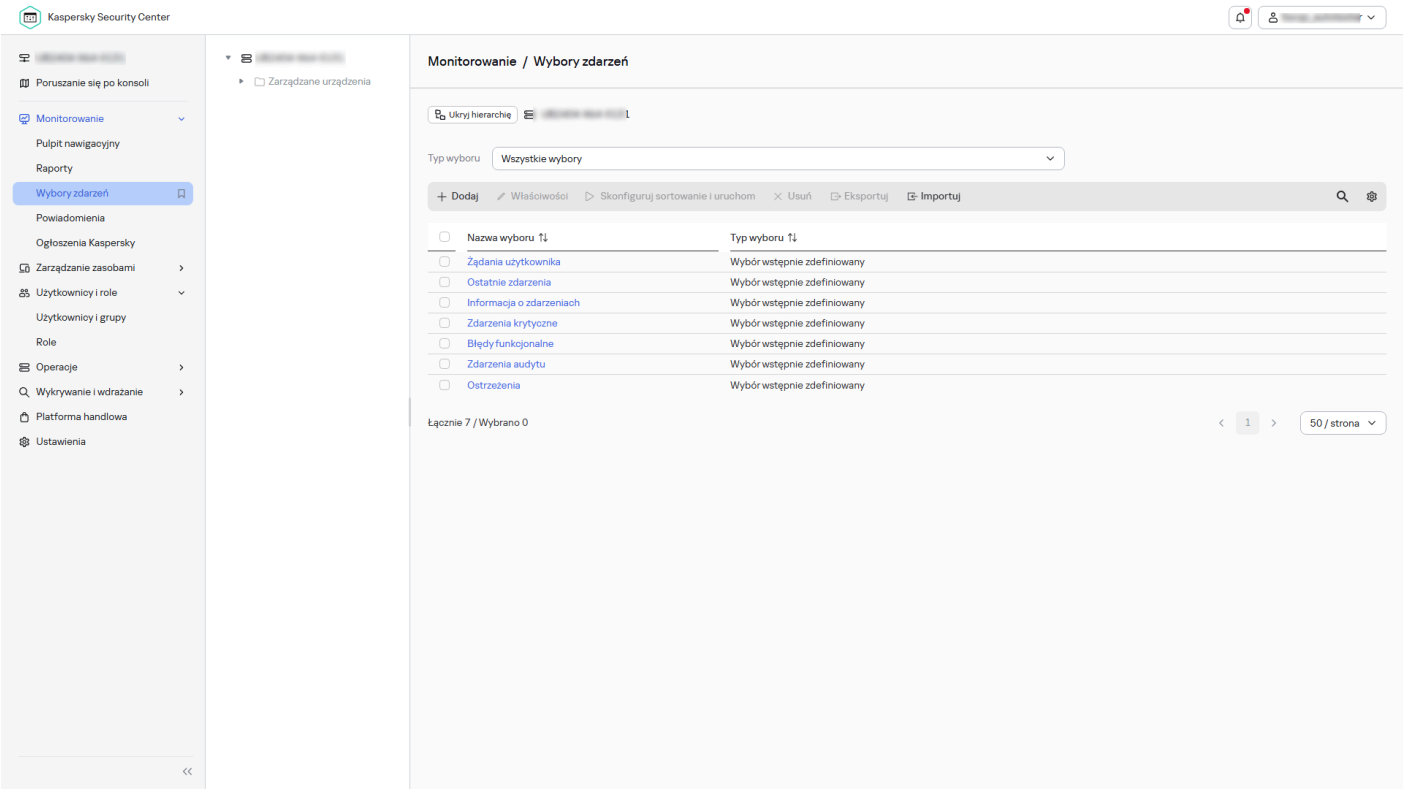
Używanie wyborów zdarzeń

Wybory zdarzeń oferują widok ekranowy nazwanych zestawów zdarzeń, które są wybrane z bazy danych Serwera administracyjnego. Te zestawy zdarzeń są grupowane zgodnie z następującymi kategoriami:

- Według istotności—**Zdarzenia krytyczne**, **Błędy funkcjonalne**, **Ostrzeżenia** i **Informacja o zdarzeniach**
- Według czasu—**Ostatnie zdarzenia**
- Według typu—**Żądania użytkownika** and **Zdarzenia audytu**

Możesz tworzyć i przeglądać wybory zdarzeń zdefiniowane przez użytkownika oparte na ustawieniach dostępnych do konfiguracji w interfejsie Kaspersky Security Center Web Console.

Wybory zdarzeń są dostępne w Kaspersky Security Center Web Console w sekcji **Monitorowanie** po kliknięciu **Wybory zdarzeń**.



Lista wyborów zdarzeń

Domyślnie, wybory zdarzeń zawierają informacje dla ostatnich siedmiu dni.

Kaspersky Security Center Linux zawiera domyślny (predefiniowany) zestaw wyborów zdarzeń:

- Zdarzenia z różnymi priorytetami:
  - **Zdarzenia krytyczne**
  - **Błędy funkcjonalne**

    - **Ostrzeżenia**
    - **Zdarzenia informacyjne**
- **Żądania użytkownika** (zdarzenia zarządzanych aplikacji)
- **Ostatnie zdarzenia** (w ostatnim tygodniu)
- **Zdarzenia audytu**.

Możesz także utworzyć i skonfigurować dodatkowe wybory zdefiniowane przez użytkownika. W wyborach zdefiniowanych przez użytkownika możesz filtrować zdarzenia według właściwości urządzeń, z których pochodzą (nazwy urządzeń, zakresy IP i grupy administracyjne), według typów zdarzeń i priorytetów, według aplikacji i nazwy komponentu oraz według przedziału czasu. Możliwe jest także uwzględnienie wyników zadania w obszarze wyszukiwania. Możesz także użyć pola prostego wyszukiwania, gdzie można wpisać słowo lub kilka słów. Zostaną wyświetlone wszystkie zdarzenia, które zawierają dowolne z wpisanych słów w swoich atrybutach (takie jak: nazwa zdarzenia, opis, nazwa komponentu).

Dla predefiniowanych wyborów oraz wyborów zdefiniowanych przez użytkownika możesz ograniczyć liczbę wyświetlanych zdarzeń lub liczbę wyszukiwanych wpisów. Obie opcje wpływają na czas, jakie zajmuje programowi Kaspersky Security Center Linux wyświetlanie zdarzeń. Im większa baza danych, tym więcej czasu może zająć proces.

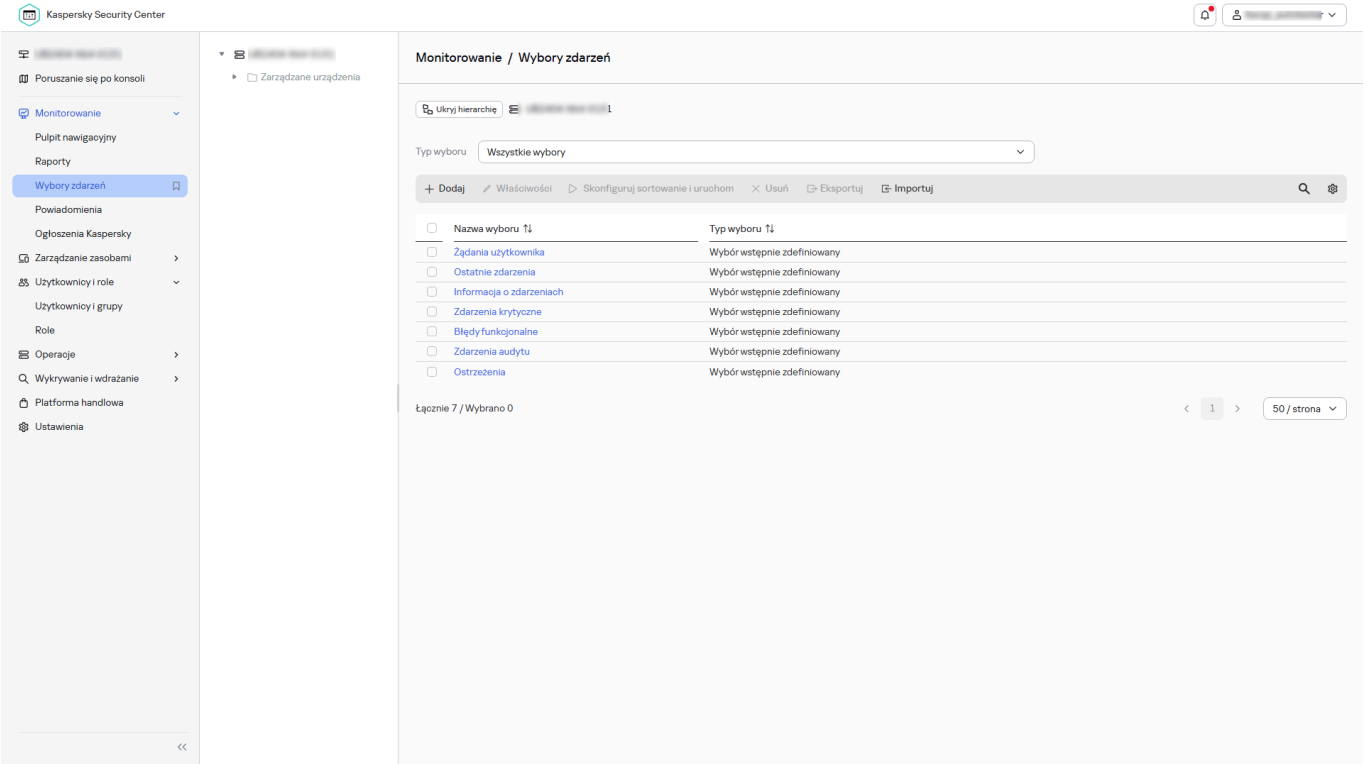
Możesz wykonać następujące czynności:

- Edytuj właściwości wyborów zdarzeń
- Wygeneruj wybory zdarzeń
- Zobacz szczegóły wyborów zdarzeń
- Usuń wybory zdarzeń
- Usuń zdarzenia z bazy danych Serwera administracyjnego

Tworzenie kryterium wyboru zdarzenia

W celu utworzenia wyboru zdarzeń:

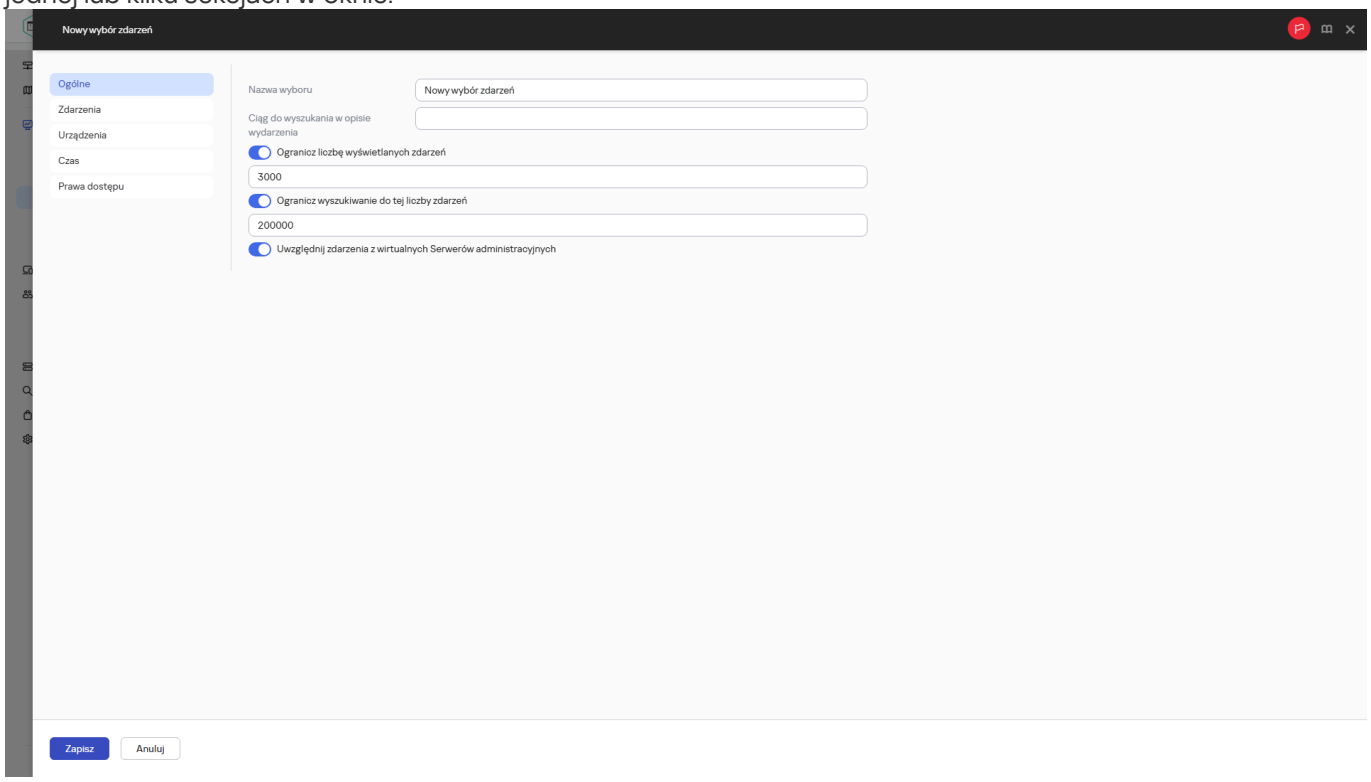
1. W menu głównym przejdź do **Monitorowanie** → **Wybory zdarzeń**.



Lista wyborów zdarzeń

2. Kliknij **Dodaj**.

3. W otwartym oknie **Nowy wybór zdarzeń** określ ustawienia nowego wyboru zdarzeń. Wykonaj te czynności w jednej lub kilku sekcjach w oknie.



Tworzenie nowego wyboru zdarzenia

4. Kliknij **Zapisz**, aby zachować zmiany.

   Zostanie otwarte okno potwierdzenia.

5. Aby sprawdzić wynik wyboru zdarzenia, pozostaw pole **Przejdź do wyniku wyboru** zaznaczone.

6. Kliknij **Zapisz**, aby potwierdzić tworzenie wyboru zdarzenia.

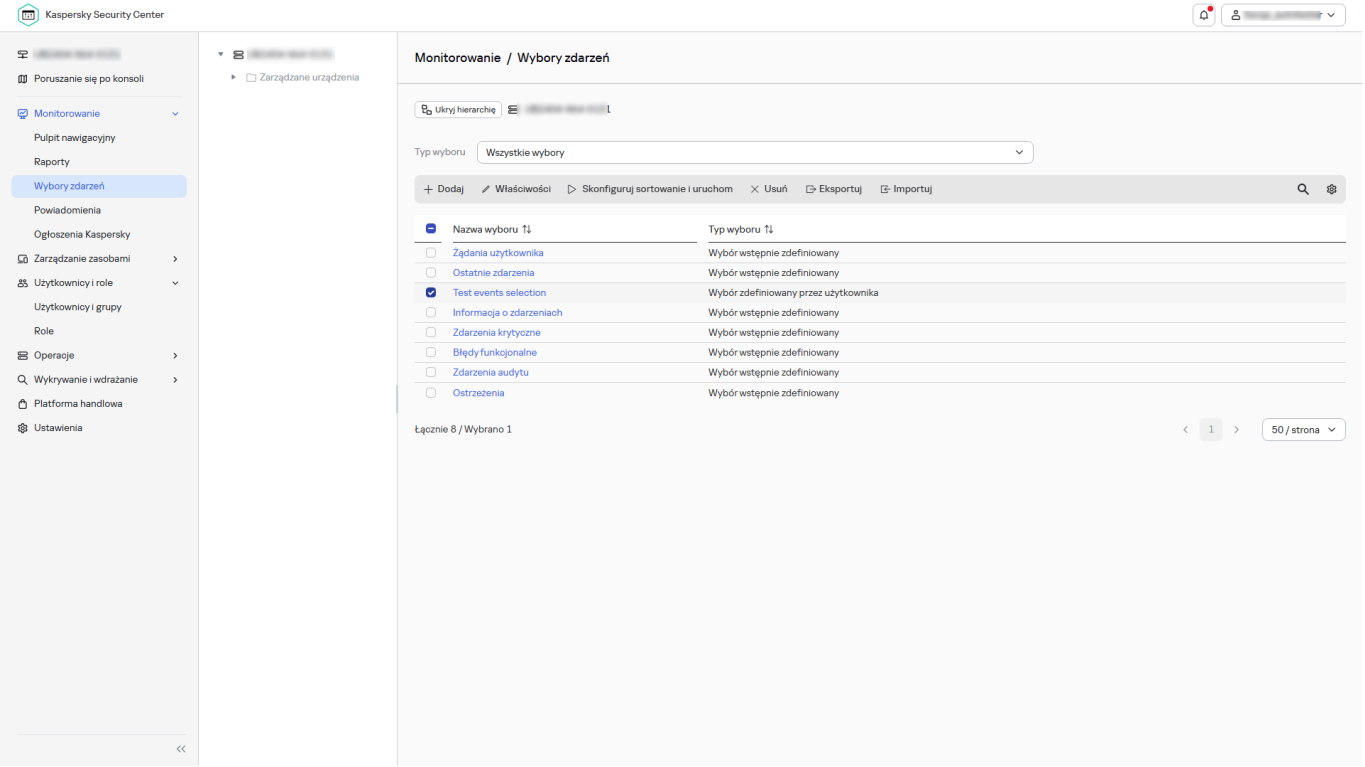
Jeśli pozostawiłeś pole **Przejdź do wyniku wyboru** zaznaczone, zostanie wyświetlony wynik wyboru zdarzenia. Jeśli tak się nie stanie, nowy wybór zdarzenia pojawi się na liście wyborów zdarzeń.

Edytowanie kryterium wyboru zdarzenia

W celu edytowania kryterium wyboru zdarzenia:

1. W menu głównym przejdź do **Monitorowanie** → **Wybory zdarzeń**.

2. Zaznacz pole obok wyboru zdarzeń, który chcesz edytować.



Lista wyborów zdarzeń

3. Kliknij przycisk **Właściwości**.

   Zostanie otwarte okno ustawień wyboru zdarzenia.

4. Edytuj właściwości wyboru zdarzenia.

   > Dla predefiniowanych wyborów zdarzeń możesz edytować tylko właściwości na następujących zakładkach: **Ogólne** (za wyjątkiem nazwy wyboru), **Czas** i **Prawa dostępu**.

   Dla wyborów zdefiniowanych przez użytkownika możesz edytować wszystkie właściwości.

5. Kliknij **Zapisz**, aby zachować zmiany.

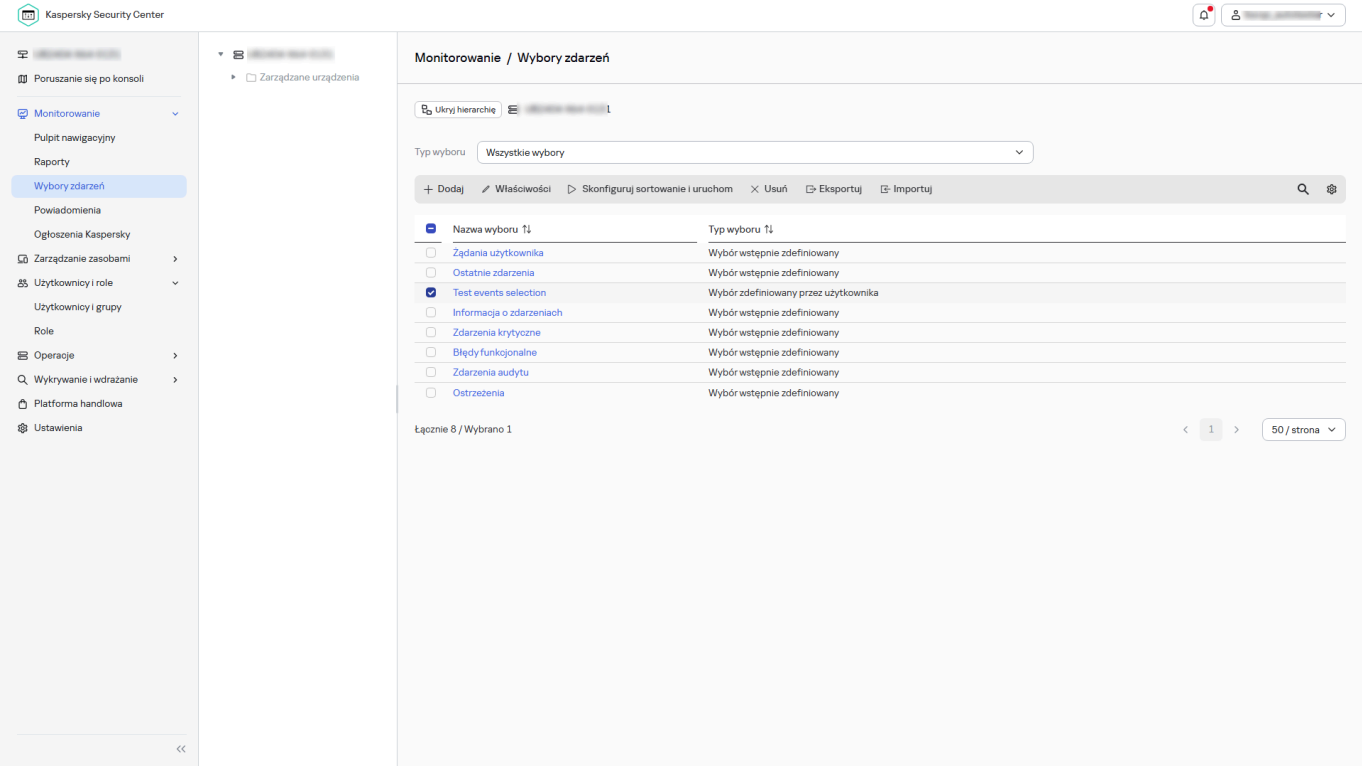
Edytowany wybór zdarzenia zostanie wyświetlony na liście.

Przeglądanie listy wyboru zdarzeń

W celu przejrzenia wyboru zdarzeń:

1. W menu głównym przejdź do **Monitorowanie** → **Wybory zdarzeń**.

2. Zaznacz pole obok wyboru zdarzeń, który chcesz uruchomić.



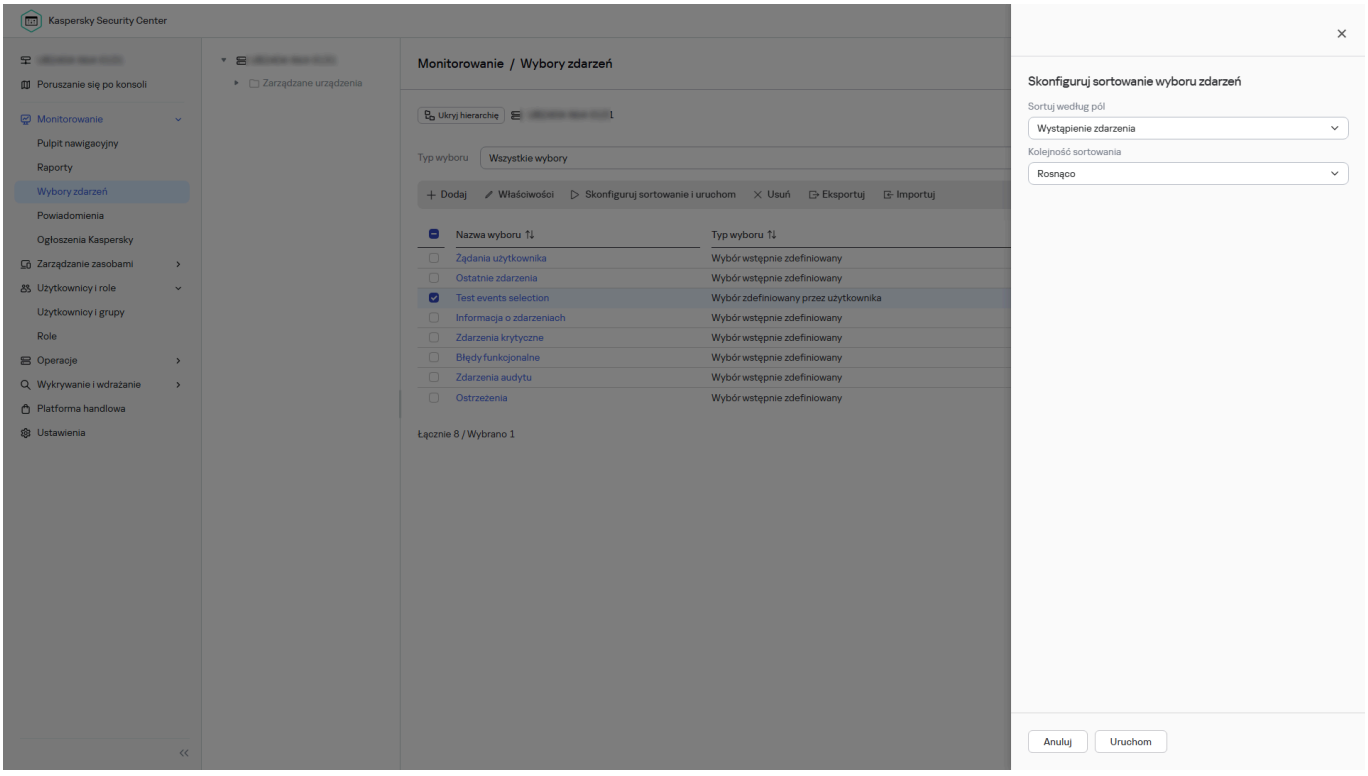
Lista wyborów zdarzeń

3. Wykonaj jedną z poniższych czynności:

- Jeśli chcesz skonfigurować sortowanie w wyniku wyboru zdarzeń, wykonaj następujące czynności:

  a. Kliknij przycisk **Skonfiguruj sortowanie i uruchom**.

  b. W wyświetlonym oknie **Skonfiguruj sortowanie wyboru zdarzeń** określ ustawienia sortowania.

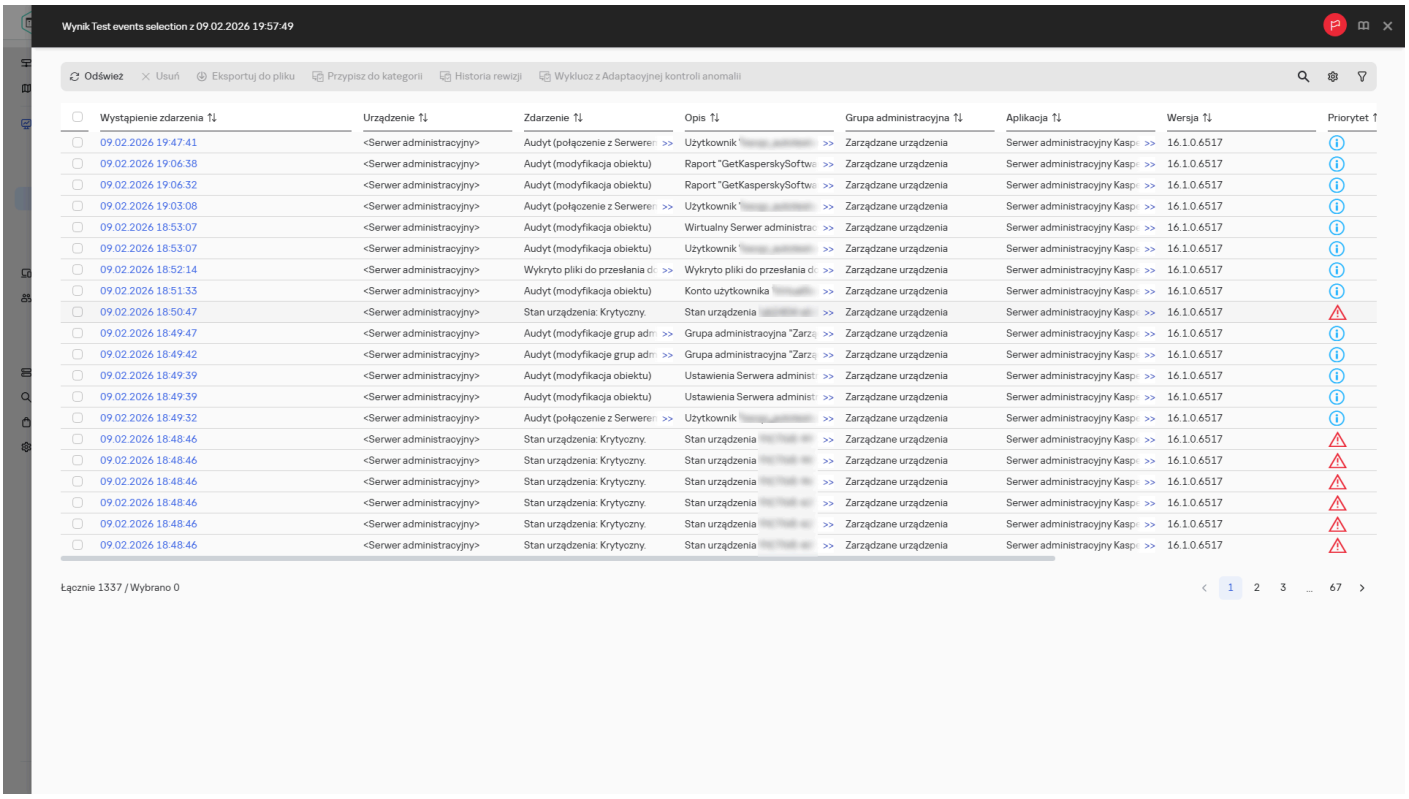


Określanie ustawień sortowania wyboru zdarzenia

  a. Kliknij nazwę wyboru.

- W innej sytuacji, jeśli chcesz przejrzeć listę zdarzeń posortowanych na Serwerze administracyjnym, kliknij nazwę wyboru.

Zostanie wyświetlony wynik wyboru zdarzeń.



Wynik wyboru zdarzeń

Eksportowanie wyboru zdarzeń

Kaspersky Security Center Linux umożliwia zapisanie wyboru zdarzeń i jego ustawień w pliku KLO. Możesz użyć tego pliku KLO do zaimportowania zapisanego wyboru zdarzeń zarówno do Kaspersky Security Center Windows, jak i Kaspersky Security Center Linux.

Należy pamiętać, że możesz eksportować tylko wybory zdarzeń zdefiniowane przez użytkownika. Wybory zdarzeń z domyślnego zestawu Kaspersky Security Center Linux (wybory predefiniowane) nie mogą zostać zapisane do pliku.

W celu wyeksportowania wyboru zdarzeń:

1. W menu głównym przejdź do **Monitorowanie** → **Wybory zdarzeń**.
2. Zaznacz pole obok wyboru zdarzeń, który chcesz wyeksportować.

   Nie można jednocześnie eksportować kilku wyborów zdarzeń. Jeśli wybierzesz więcej niż jeden zestaw, przycisk **Eksportuj** będzie nieaktywny.
3. Kliknij przycisk **Eksportuj**.
4. W otwartym oknie **Zapisz jako** określ nazwę i ścieżkę pliku wyboru zdarzeń, a następnie kliknij przycisk **Zapisz**.

   Okno **Zapisz jako** jest wyświetlane tylko wtedy, gdy korzystasz z przeglądarki Google Chrome, Microsoft Edge lub Opera. Jeśli używasz innej przeglądarki, plik wyboru zdarzeń jest automatycznie zapisywany w folderze **Pobrane**.

Importowanie wyboru zdarzeń

Kaspersky Security Center Linux umożliwia import zestawu wybranych zdarzeń z pliku KLO. Plik KLO zawiera wyeksportowany zestaw wybranych zdarzeń i jego ustawienia.

W celu importowania wyboru zdarzeń:

1. W menu głównym przejdź do **Monitorowanie** → **Wybory zdarzeń**.
2. Kliknij przycisk **Importuj**, a następnie wybierz plik wyboru zdarzeń, który chcesz zaimportować.
3. W otwartym oknie określ ścieżkę do pliku KLO, a następnie kliknij przycisk **Otwórz**. Należy pamiętać, że można wybrać tylko jeden wybór zdarzeń.

   Rozpoczyna się przetwarzanie wyboru zdarzeń.

Pojawi się powiadomienie z wynikami importu. Jeśli wybór zdarzeń zostanie pomyślnie zaimportowany, możesz kliknąć odnośnik **Wyświetl szczegóły importu**, aby wyświetlić właściwości wyboru zdarzeń.

Po pomyślnym imporcie wybór zdarzeń zostanie wyświetlony na liście wyborów. Importowane są również ustawienia wyboru zdarzeń.

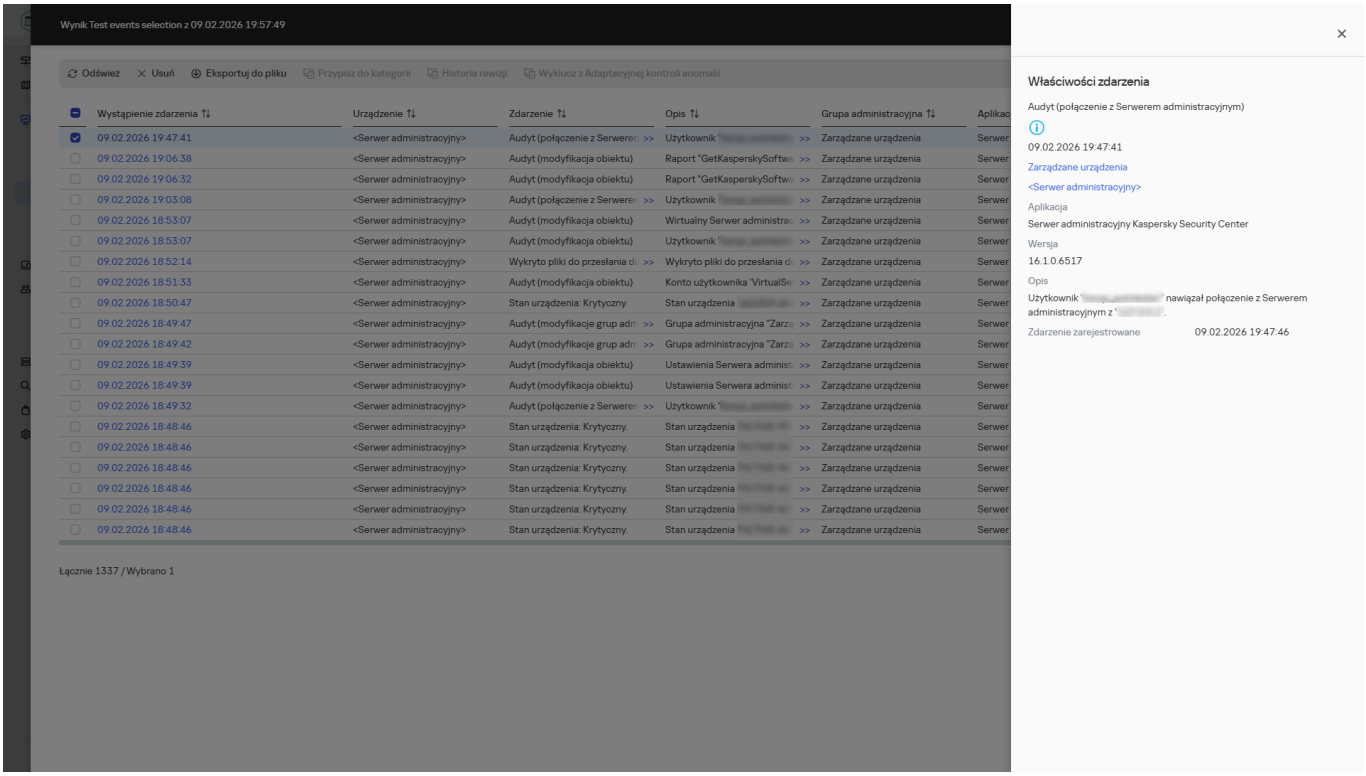
> Jeżeli nowo importowany zdarzeń ma nazwę identyczną z nazwą istniejącego wyboru zdarzeń, nazwa importowanego wyboru zdarzeń jest rozszerzana o indeks **(<następny numer sekwencji>)**, na przykład: **(1)**, **(2)**.

Przeglądanie szczegółów zdarzenia

W celu przejrzenia szczegółów zdarzenia:

1. Uruchom wybór zdarzeń.
2. Kliknij czas żądanego zdarzenia.

Zostanie otwarte okno **Właściwości zdarzenia**.



Okno właściwości zdarzenia

3. W wyświetlonym oknie możesz wykonać następujące czynności:
   - Przejrzeć informacje o wybranym zdarzeniu
   - Przejść do urządzenia, na którym wystąpiło zdarzenie
   - Przejść do grupy administracyjnej, która zawiera urządzenie, na którym wystąpiło zdarzenie
   - W przypadku zdarzenia związanego z zadaniem przejdź do właściwości zadania

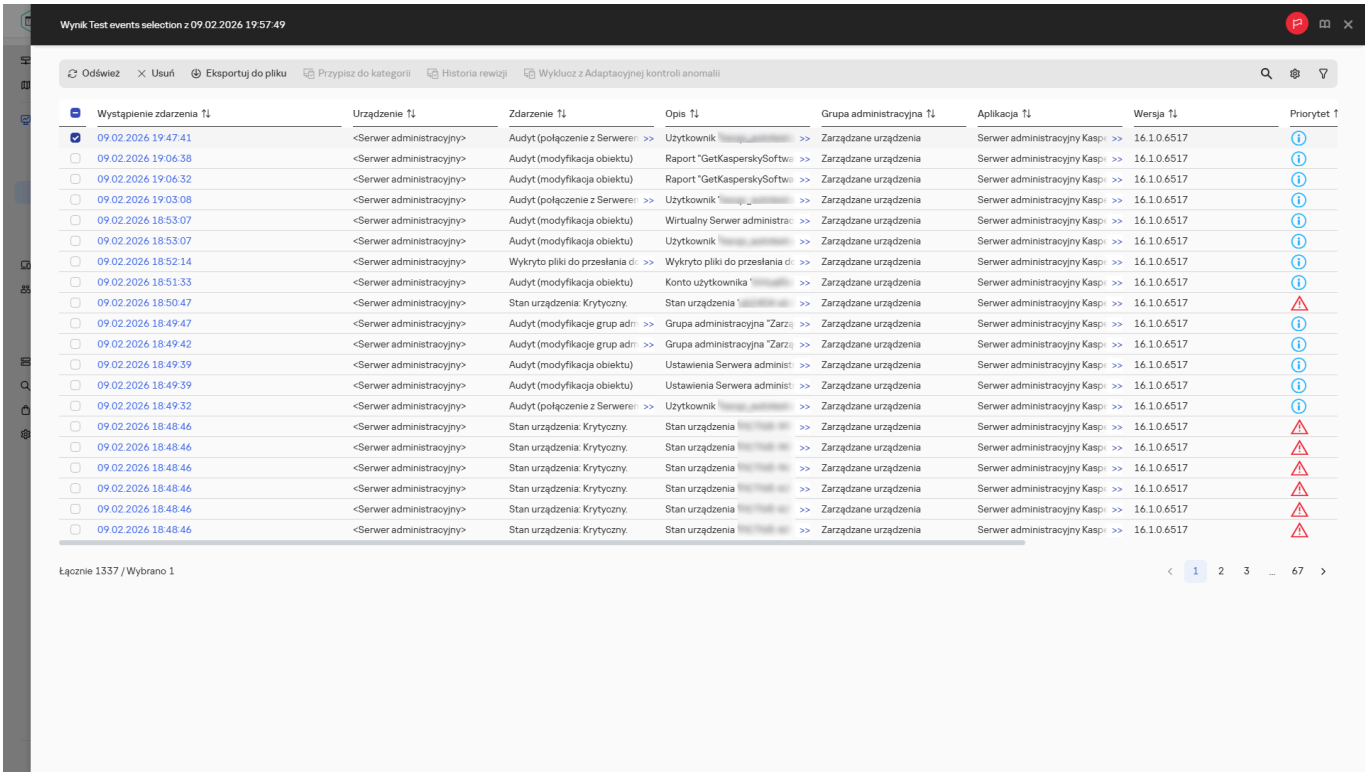
Eksportowanie zdarzeń do pliku

Kaspersky Security Center Linux umożliwia zapisywanie zdarzeń z wybranego wyboru zdarzeń do pliku TXT.

W celu wyeksportowania zdarzeń do pliku:

1. Uruchom wybór zdarzeń.
2. Zaznacz pole obok żądanego zdarzenia.

Można również zaznaczyć kilka wydarzeń lub cały wybór wydarzeń.



Wynik wyboru zdarzeń

3. Kliknij przycisk **Eksportuj do pliku**.

   Wybrane zdarzenie zostanie wyeksportowane do pliku TXT.

Przeglądanie historii obiektu ze zdarzenia

Ze zdarzenia utworzenia lub modyfikacji obiektu, które obsługuje zarządzanie rewizją, możesz przełączyć się na historię rewizji obiektu.

W celu przejrzenia historii obiektu ze zdarzenia:

1. Uruchom wybór zdarzeń.

2. Zaznacz pole obok żądanego zdarzenia.

3. Kliknij przycisk **Historia rewizji**.

   Historia rewizji obiektu zostanie otwarta.

Usuwanie zdarzeń

W celu usunięcia zdarzeń z wyboru zdarzeń:

1. Uruchom wybór zdarzeń.
2. Wybierz zdarzenia:
   - Jeśli chcesz usunąć jedno lub kilka zdarzeń, zaznacz pola wyboru obok nich.
   - Jeśli chcesz usunąć wszystkie zdarzenia na bieżącej stronie, zaznacz pole wyboru nad listą zdarzeń i kliknij opcję **Wybierz wszystko na bieżącej stronie**.
   - Jeśli chcesz usunąć wszystkie zdarzenia z wyboru zdarzeń, zaznacz pole wyboru nad listą zdarzeń i kliknij opcję **Wybierz wszystkie**.
3. Kliknij przycisk **Usuń**.
4. W otwartym oknie kliknij **Usuń**.

Aby usunąć zdarzenia z listy zdarzeń urządzenia:

1. Otwórz listę urządzeń.
   - W przypadku zarządzanych urządzeń: **Zarządzanie zasobami** → **Zasoby (urządzenia)**.
   - W przypadku urządzeń nieprzypisanych: **Zarządzanie zasobami** → **Urządzenia nieprzypisane**.
2. Na liście urządzeń kliknij odnośnik z nazwą odpowiedniego urządzenia, a następnie przejdź do zakładki **Zdarzenia**.
3. Wybierz zdarzenia:
   - Jeśli chcesz usunąć jedno lub kilka zdarzeń, zaznacz pola wyboru obok nich.
   - Jeśli chcesz usunąć wszystkie zdarzenia na bieżącej stronie, zaznacz pole wyboru nad listą zdarzeń i kliknij opcję **Wybierz wszystko na bieżącej stronie**.
   - Jeśli chcesz usunąć wszystkie zdarzenia z wyboru zdarzeń, zaznacz pole wyboru nad listą zdarzeń i kliknij opcję **Wybierz wszystkie**.
4. Kliknij **Usuń**, a następnie potwierdź akcję.
5. W otwartym oknie kliknij **Usuń**.

Wybrane zdarzenia zostaną usunięte i nie można ich przywrócić.

Usuwanie wyborów zdarzeń

Możesz usuwać tylko wybory zdarzeń zdefiniowane przez użytkownika. Predefiniowanych wyborów zdarzeń nie można usunąć.

W celu usunięcia jednego lub kilku wyborów zdarzeń:

1. W menu głównym przejdź do **Monitorowanie** → **Wybory zdarzeń**.
2. Zaznacz pola obok wyborów zdarzeń, które chcesz usunąć.
3. Kliknij **Usuń**.
4. W otwartym oknie potwierdzenia kliknij **OK**.

   Wybór zdarzenia zostanie usunięty.

Ustawianie czasu przechowywania dla zdarzenia

Kaspersky Security Center Linux umożliwia otrzymywanie informacji o zdarzeniach występujących podczas działania Serwera administracyjnego i aplikacji firmy Kaspersky zainstalowanych na zarządzanych urządzeniach. Informacje o zdarzeniach są zapisywane w bazie danych Serwera administracyjnego. Konieczne może być przechowywanie niektórych zdarzeń przez dłuższy lub krótszy okres niż określony przez wartości domyślne. Możesz zmienić domyślne ustawienia czasu przechowywania zdarzenia.

Jeśli nie masz zamiaru przechowywać niektórych zdarzeń w bazie danych Serwera administracyjnego, możesz wyłączyć odpowiednie ustawienie w zasadzie Serwera administracyjnego oraz w zasadzie aplikacji Kaspersky lub we właściwościach Serwera administracyjnego (tylko dla zdarzeń Serwera administracyjnego). Zmniejszy to liczbę typów zdarzeń w bazie danych.

Im dłuższy okres przechowywania zdarzenia, tym szybciej baza danych osiągnie maksymalną pojemność. Jednakże dłuższy okres przechowywania zdarzenia umożliwia monitorowanie i raportowanie zadań dla dłuższego przedziału czasu.

W celu skonfigurowania czasu przechowywania zdarzenia w bazie danych Serwera administracyjnego:

1. W menu głównym przejdź do **Zarządzanie zasobami** → **Zasady**.
2. Kliknij nazwę żądanej zasady.

   Możesz wybrać zasady zarządzanej aplikacji Kaspersky, Agenta sieciowego lub Serwera administracyjnego. W przypadku Serwera administracyjnego można również skonfigurować okres przechowywania zdarzeń, klikając nazwę Serwera administracyjnego.
3. Wybierz zakładkę **Konfiguracja zdarzenia**.

   Zostanie wyświetlona lista typów zdarzeń dotyczących sekcji **Krytyczny**. W razie potrzeby możesz przejść do sekcji **Błąd funkcjonalny**, **Ostrzeżenie** lub **Informacja**.

4. Na liście typów zdarzeń w prawej części okna kliknij odnośnik dla zdarzenia, którego okres przechowywania chcesz zmienić.

   W sekcji **Rejestracja zdarzenia** otwartego okna dostępny jest przycisk **Przechowuj w bazie danych Serwera administracyjnego przez (dni)**.

5. W polu edycji znajdującym się pod tym przyciskiem przełącznika wprowadź liczbę dni, przez jaką zdarzenie ma być przechowywane.

6. Jeśli nie chcesz przechowywać zdarzenia w bazie danych Serwera administracyjnego, wyłącz opcję **Przechowuj w bazie danych Serwera administracyjnego przez (dni)**.

   Jeśli skonfigurujesz zdarzenia Serwera administracyjnego w oknie właściwości Serwera administracyjnego, a ustawienia zdarzeń są zablokowane w zasadzie Serwera administracyjnego, nie możesz zmienić wartości okresu przechowywania zdarzenia.

7. Kliknij przycisk **OK**, a następnie po zamknięciu prawego panelu kliknij przycisk **Zapisz**.

   Okno właściwości zasady zostanie zamknięte.

Od tej chwili, gdy serwer administracyjny odbiera i przechowuje zdarzenia wybranego typu, będą one miały zmieniony okres przechowywania. Serwer administracyjny nie zmienia okresu przechowywania wcześniej odebranych zdarzeń.

Blokowanie często występujących zdarzeń

Ta sekcja zawiera informacje dotyczące zarządzania blokowaniem często występujących zdarzeń oraz usuwania blokowania często występujących zdarzeń.

Informacje o blokowaniu często występujących zdarzeń

Zarządzana aplikacja, na przykład Kaspersky Endpoint Security for Linux, zainstalowana na jednym lub kilku zarządzanych urządzeniach, może wysyłać wiele zdarzeń tego samego typu do Serwera administracyjnego. Otrzymywanie częstych zdarzeń może przeciążyć bazę danych Serwera administracyjnego i nadpisać inne zdarzenia. Serwer administracyjny zaczyna blokować najczęstsze zdarzenia, gdy liczba wszystkich odebranych zdarzeń przekracza określony limit dla bazy danych.

Serwer administracyjny blokuje automatyczne odbieranie często występujących zdarzeń. Nie możesz samodzielnie blokować często występujących zdarzeń ani wybierać, które zdarzenia mają być blokowane.

Jeśli chcesz dowiedzieć się, czy zdarzenie jest zablokowane, możesz sprawdzić listę powiadomień lub możesz sprawdzić, czy to zdarzenie jest obecne w sekcji **Blokowanie często występujących zdarzeń** właściwości Serwera administracyjnego. Jeśli zdarzenie jest zablokowane, możesz wykonać następujące czynności:

- Jeśli chcesz zapobiec nadpisywaniu bazy danych, możesz kontynuować blokowanie odbieranie tego typu zdarzeń.
- Jeśli chcesz, na przykład, znaleźć przyczynę wysyłania często występujących zdarzeń na Serwer administracyjny, możesz odblokować często występujące zdarzenia i mimo wszystko nadal otrzymywać tego typu zdarzenia.
- Jeśli chcesz nadal otrzymywać często występujące zdarzenia, dopóki nie zostaną ponownie zablokowane, możesz usunąć z blokowania często występujące zdarzenia.

Zarządzanie blokowaniem często występujących zdarzeń

Serwer administracyjny blokuje automatyczne odbieranie często występujących zdarzeń, ale możesz odblokować tę opcję i nadal odbierać często występujące zdarzenia. Możesz także zablokować odbieranie często występujących zdarzeń, które wcześniej odblokowałeś.

W celu zarządzania blokowaniem często występujących zdarzeń:

1. W menu głównym kliknij nazwę Serwera administracyjnego.

   Zostanie otwarte okno właściwości Serwera administracyjnego.

2. Na zakładce **Ogólne** wybierz sekcję **Blokowanie często występujących zdarzeń**.

3. W sekcji **Blokowanie często występujących zdarzeń**:

   - Jeśli chcesz odblokować odbieranie często występujących zdarzeń:

     a. Wybierz często występujące zdarzenia, które chcesz odblokować, a następnie kliknij przycisk **Wyklucz**.

     b. Kliknij przycisk **Zapisz**.

   - Jeśli chcesz zablokować często występujące zdarzenia:

     a. Wybierz często występujące zdarzenia, które chcesz zablokować, a następnie kliknij przycisk **Zablokuj**.

     b. Kliknij przycisk **Zapisz**.

Serwer administracyjny odbiera odblokowane często występujące zdarzenia i nie odbiera zablokowanych często występujących zdarzeń.

Usuwanie blokowania często występujących zdarzeń

Możesz usunąć blokowanie często występujących zdarzeń i rozpocząć ich odbieranie, dopóki Serwer administracyjny nie zablokuje ponownie tych często występujących zdarzeń.

W celu usunięcia blokowania często występujących zdarzeń:

1. W menu głównym kliknij nazwę Serwera administracyjnego.

   Zostanie otwarte okno właściwości Serwera administracyjnego.

2. Na zakładce **Ogólne** wybierz sekcję **Blokowanie często występujących zdarzeń**.

3. W sekcji **Blokowanie często występujących zdarzeń** wybierz typy często występujących zdarzeń, dla których chcesz usunąć blokowanie.

4. Kliknij przycisk **Usuń z blokowania**.

Często występujące zdarzenie zostanie usunięte z listy często występujących zdarzeń. Serwer administracyjny będzie odbierał zdarzenia tego typu.

Przetwarzanie i przechowywanie zdarzeń na Serwerze administracyjnym

Informacje o zdarzeniach, występujących podczas działania aplikacji, oraz o zarządzanych urządzeniach są zapisywane w bazie danych Serwera administracyjnego. Każdemu zdarzeniu przypisywany jest określony typ i priorytet (*Zdarzenie krytyczne*, *Błąd funkcjonalny*, *Ostrzeżenie* lub *Informacja*). W zależności od warunków, przez które pojawiło się zdarzenie, do zdarzeń tego samego typu aplikacja może przypisywać różne priorytety.

Typy i priorytety przypisane do zdarzeń można sprawdzić w sekcji **Konfiguracja zdarzenia** okna właściwości Serwera administracyjnego. W sekcji **Konfiguracja zdarzenia** możesz także skonfigurować przetwarzanie każdego zdarzenia przez Serwer administracyjny:

- Rejestrację zdarzeń na Serwerze administracyjnym i w raporcie zdarzeń systemu operacyjnego na urządzeniu i na Serwerze administracyjnym.

- Metodę używaną do informowania administratora o zdarzeniu (na przykład, wiadomość SMS lub e-mail).

W sekcji **Repozytorium zdarzeń** okna właściwości Serwera administracyjnego możesz zmodyfikować ustawienia przechowywania zdarzeń w bazie danych Serwera administracyjnego, ograniczając liczbę wpisów zdarzeń i czas przechowywania wpisów. Jeśli określisz maksymalną liczbę zdarzeń, aplikacja oblicza przybliżoną ilość miejsca przechowywania, wymaganą dla określonej liczby. Możesz użyć tego przybliżonego obliczenia do oszacowania wystarczającej ilości wolnego miejsca na dysku, aby uniknąć przepełnienia bazy danych. Domyślna pojemność bazy danych Serwera administracyjnego wynosi 400 000 zdarzeń. Maksymalną dozwoloną pojemnością bazy danych jest 45 milionów zdarzeń.

Aplikacja sprawdza bazę danych co 10 minut. Jeśli liczba zdarzeń osiągnie określoną maksymalną wartość plus 10 000, aplikacja usunie najstarsze zdarzenia, tak aby pozostała tylko określona maksymalna liczba zdarzeń.

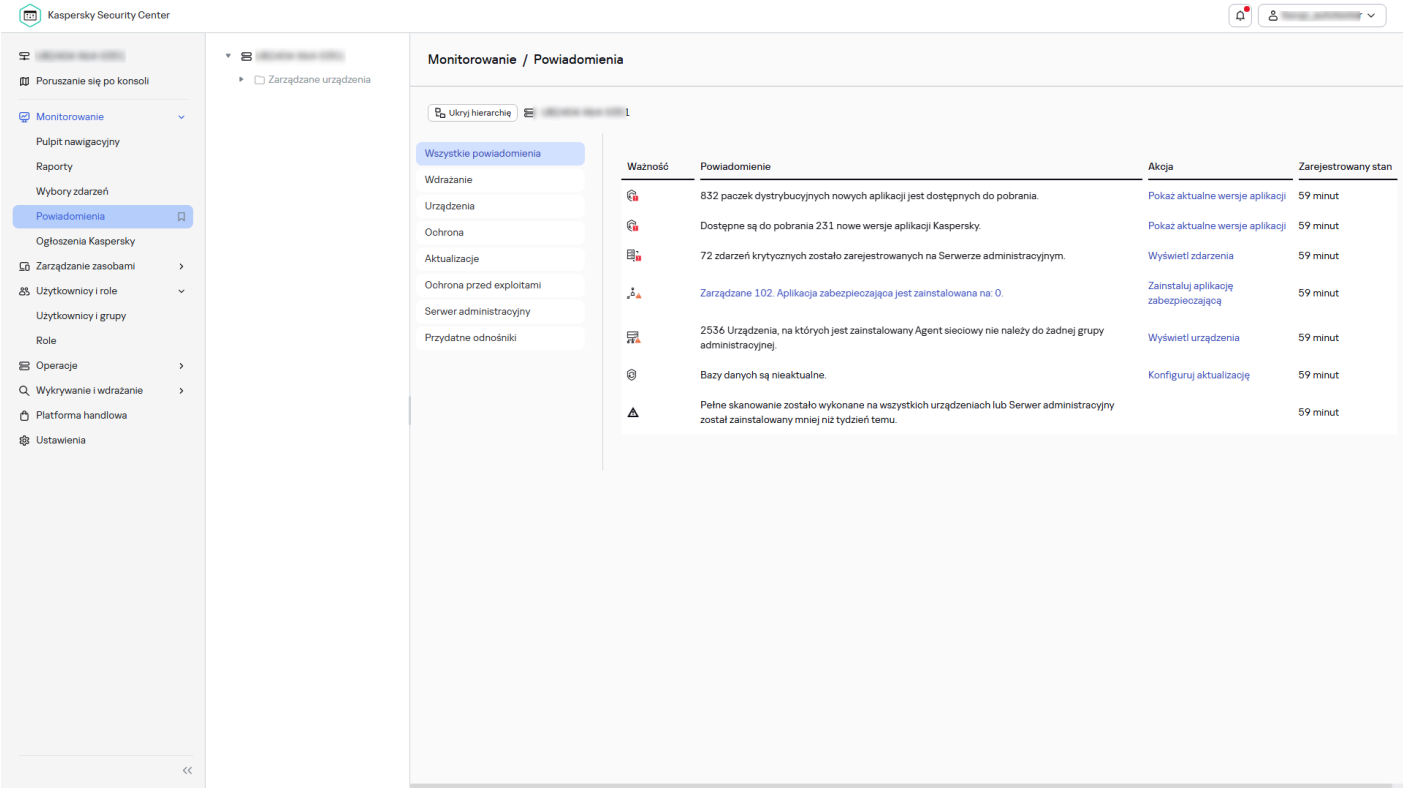
Jeśli Serwer administracyjny usuwa starsze zdarzenia, nie może zapisywać nowych zdarzeń do bazy danych. W tym czasie informacje o odrzuconych zdarzeniach są zapisywane w dzienniku systemu operacyjnego. Nowe zdarzenia zostają zakolejkowane, a następnie zapisane do bazy danych po zakończeniu operacji usuwania. Domyślnie kolejka zdarzeń jest ograniczona do 20 000 zdarzeń. Możesz dostosować limit kolejki, edytując wartość flagi KLEVP_MAX_POSTPONED_CNT.

Powiadomienia i stany urządzeń

Ta sekcja zawiera informacje o tym, jak przeglądać powiadomienia, konfigurować dostarczanie powiadomień, używać stanów urządzeń i włączać zmianę stanów urządzeń.

Korzystanie z powiadomień

Powiadomienia informują o zdarzeniach oraz pomagają w przyspieszeniu odpowiedzi na te zdarzenia poprzez wykonanie zalecanych działań lub działań, które uznajesz za odpowiednie.



Lista powiadomień

W zależności od wybranej metody powiadamiania, dostępne są następujące typy powiadomień:

- Powiadomienia na ekranie
- Powiadomienia przez SMS
- Powiadomienia przez e-mail
- Powiadomienia przez uruchomienie pliku wykonywalnego lub skryptu

Powiadomienia na ekranie

Powiadomienia ekranowe informują o zdarzenia pogrupowanych według istotności (*Krytyczne*, *Ostrzeżenie* i *Komunikaty informacyjne*).

Powiadomienie ekranowe może przyjąć jeden z dwóch stanów:

- *Przejrzane*. Oznacza to, że wykonałeś zalecane działanie dla powiadomienia lub ręcznie przypisałeś ten stan do powiadomienia.
- *Nieprzejrzane*. Oznacza to, że nie wykonałeś zalecanego działania dla powiadomienia lub nie przypisałeś tego stanu do powiadomienia ręcznie.

Domyślnie, lista powiadomień zawiera powiadomienia ze stanem *Nieprzejrzane*.

Możesz monitorować sieć organizacji, przeglądając powiadomienia ekranowe i odpowiadając na nie w czasie rzeczywistym.

Powiadomienia przez e-mail, przez SMS i przez plik wykonywalny lub skrypt

Kaspersky Security Center Linux oferuje możliwość monitorowania sieci organizacji, wysyłając powiadomienia o zdarzeniu, które uważasz za ważne. Dla każdego zdarzenia możesz skonfigurować powiadomienia przez e-mail, przez SMS lub przez uruchomienie pliku wykonywalnego lub skryptu.

Po otrzymaniu powiadomień przez e-mail lub przez SMS, możesz zdecydować, jaka będzie odpowiedź na zdarzenie. Ta odpowiedź powinna być najbardziej odpowiednia dla sieci Twojej organizacji. Uruchamiając plik wykonywalny lub skrypt, wcześniej definiujesz odpowiedź na zdarzenie. Możesz także rozważyć uruchomienie pliku wykonywalnego lub skryptu jako głównej odpowiedzi na zdarzenie. Po uruchomieniu pliku wykonywalnego, możesz podjąć inne kroki w celu odpowiedzi na zdarzenie.

Przeglądanie powiadomień na ekranie

Powiadomienia na ekranie można wyświetlać na trzy sposoby:

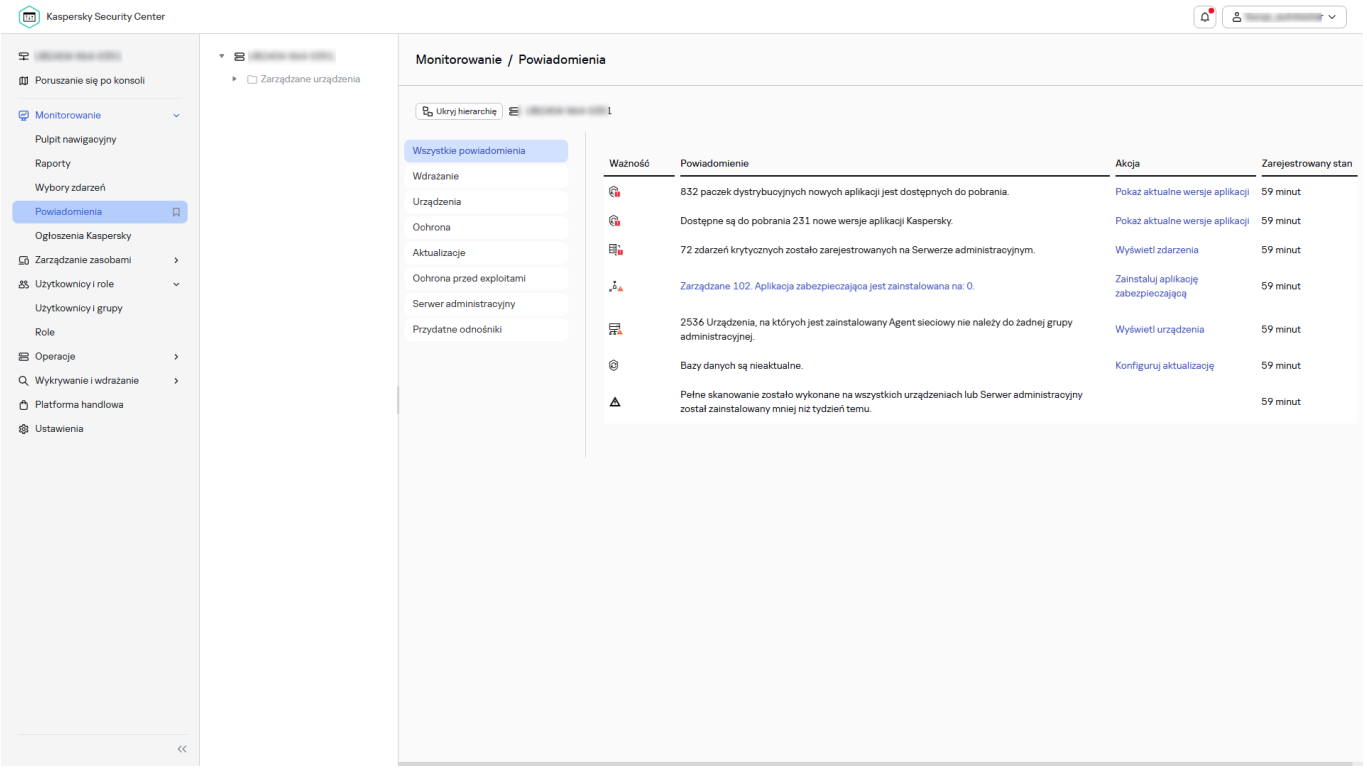
- W sekcji **Monitorowanie** → **Powiadomienia**. W tym miejscu możesz przejrzeć powiadomienia dotyczące predefiniowanych kategorii.
- W oddzielnym oknie, które może zostać otwarte niezależnie od sekcji, której używasz w danym momencie. W tym przypadku możesz oznaczyć powiadomienia jako przejrzane.
- W widżecie **Powiadomienia według wybranego priorytetu**, w sekcji **Monitorowanie** → **Pulpit nawigacyjny**. W widżecie możesz przeglądać tylko powiadomienia o zdarzeniach na poziomach istotności *Krytyczny* i *Ostrzeżenie*.

Możesz wykonywać akcje, na przykład, odpowiadać na zdarzenie.

W celu przejrzenia powiadomień z predefiniowanych kategorii:

1. W menu głównym przejdź do **Monitorowanie** → **Powiadomienia**.

Kategoria **Wszystkie powiadomienia** została wybrana w lewej części okna, a w prawej części okna są wyświetlane wszystkie powiadomienia.



Lista powiadomień

2. W lewej części okna wybierz jedną z kategorii:

   - **Wdrażanie**
   - **Urządzenia**
   - **Ochrona**
   - **Aktualizacje** (obejmuje powiadomienia o aplikacjach Kaspersky dostępnych do pobrania, powiadomienia o pobranych aktualizacjach antywirusowych baz danych, a także powiadomienia o urządzeniach (jeśli takie istnieją), które wymagają ponownego uruchomienia po aktualizacji Agenta sieciowego)
   - **Ochrona przed exploitami**
   - **Serwer administracyjny** (ta kategoria obejmuje zdarzenia dotyczące tylko Serwera administracyjnego)
   - **Przydatne odnośniki** (ta kategoria obejmuje odnośniki do zasobów Kaspersky, na przykład pomocy technicznej Kaspersky, forum Kaspersky, strony odnowienia licencji lub Encyklopedii IT Kaspersky)

Zostanie wyświetlona lista powiadomień wybranej kategorii. Lista zawiera następujące elementy:

- Ikona związana z tematem powiadomienia: wdrożenie (), ochrona (), aktualizacje (), zarządzanie urządzeniami (), Ochrona przed exploitami (), Serwer administracyjny ().
- Poziom istotności powiadomienia. Wyświetlane są powiadomienia następujących poziomów istotności: **Powiadomienia krytyczne** (), **Powiadomienia ostrzegawcze** (), **Powiadomienia informacyjne**. Powiadomienia na liście są pogrupowane według poziomów istotności.
- **Powiadomienie**. Ta kategoria zawiera opis powiadomienia.

- **Akcja**. Ta kategoria zawiera odnośnik do akcji, której wykonanie zalecamy. Na przykład, klikając ten odnośnik, możesz przejść do repozytorium i zainstalować aplikacje zabezpieczające na urządzeniach lub przejrzeć listę urządzeń lub listę zdarzeń. Po wykonaniu zalecanego działania dla powiadomienia, do tego powiadomienia przypisano stan *Przejrzane*.

- **Zarejestrowany stan**. Ta kategoria zawiera liczbę dni lub godzin, które minęły od momentu, gdy powiadomienie zostało zarejestrowane na Serwerze administracyjnym.

W celu przejrzenia powiadomień ekranowych w oddzielnym oknie według poziomu istotności:

1. W prawym górnym rogu Kaspersky Security Center Web Console kliknij ikonę flagi ( ).

   Jeśli ikona flagi posiada czerwoną kropkę, oznacza to, że istnieją powiadomienia, które nie zostały przejrzane.

   Zostanie otwarte okno wyświetlające powiadomienia. Domyślnie wybrana jest zakładka **Wszystkie powiadomienia**, a powiadomienia są pogrupowane według poziomów istotności: *Krytyczne*, *Ostrzeżenie* i *Informacja*.

2. Wybierz zakładkę **System**.

   Zostanie wyświetlona lista z powiadomieniami posiadającymi poziom istotności powiadomienia *Krytyczne* ( ) i *Ostrzeżenie* ( ). Lista powiadomień obejmuje następujące obiekty:

   - Znacznik koloru. Powiadomienia krytyczne są oznaczone na czerwono. Powiadomienia ostrzegające są oznaczone na żółto.
   - Ikona wskazująca temat powiadomienia: wdrożenie ( ), ochrona ( ), aktualizacje ( ), zarządzanie urządzeniami ( ), Ochrona przed exploitami ( ), Serwer administracyjny ( ).
   - Opis powiadomienia.
   - Ikona flagi. Ikona flagi jest szara, jeśli do powiadomień jest przypisany stan *Nieprzejrzane*. Jeśli wybierzesz szarą ikonę flagi i przypiszesz stan *Przejrzane* do powiadomienia, ikona zmieni kolor na biały.
   - Odnośnik do zalecanej akcji. Jeśli po kliknięciu odnośnika wykonasz zalecaną akcję, do powiadomienia zostanie przypisany stan *Przejrzane*.
   - Liczba dni, jaka minęła od daty zarejestrowania powiadomienia na Serwerze administracyjnym.

3. Wybierz zakładkę **Więcej**.

   Zostanie wyświetlona lista powiadomień posiadających poziom istotności *Informacja*.

   Organizacja listy jest taka sama, jak listy na zakładce **System** (zapoznaj się z powyższym opisem). Jedyna różnica to brak znacznika koloru.

Możesz filtrować powiadomienia według dat, gdy zostały zarejestrowane na Serwerze administracyjnym. Użyj pola **Pokaż filtr**, aby zarządzać filtrem.

W celu wyświetlenia powiadomień ekranowych na widżecie:

1. W sekcji **Pulpit nawigacyjny** wybierz **Dodaj lub przywróć widżet sieciowy**.

2. W otwartym oknie kliknij kategorię **Inne**, wybierz widżet **Powiadomienia według wybranego priorytetu** i kliknij Dodaj.

Teraz widżet pojawi się na zakładce **Pulpit nawigacyjny**. Domyślnie, powiadomienia z poziomem istotności *Krytyczne* są wyświetlane na widżecie.

Możesz kliknąć przycisk **Ustawienia** na widżecie i zmienić ustawienia widżetu, aby przejrzeć powiadomienia z poziomem istotności *Ostrzeżenie*. Lub możesz dodać inny widżet: **Powiadomienia według wybranego poziomu istotności** z priorytetem *Ostrzeżenie*.

Lista powiadomień na widżecie jest ograniczona według rozmiaru i zawiera dwa powiadomienia. Te dwa powiadomienia odnoszą się do najnowszych zdarzeń.

Lista powiadomień na widżecie obejmuje następujące obiekty:

- Ikona związana z tematem powiadomienia: wdrożenie ( ), ochrona ( ), aktualizacje ( ), zarządzanie urządzeniami ( ), Ochrona przed exploitami ( ), Serwer administracyjny ( ).
- Opis powiadomienia z odnośnikiem do zalecanej akcji. Jeśli po kliknięciu odnośnika wykonasz zalecaną akcję, do powiadomienia zostanie przypisany stan *Przejrzane*.
- Liczbę dni lub liczbę godzin, które minęły od daty zarejestrowania powiadomienia na Serwerze administracyjnym.
- Odnośnik do innych powiadomień. Po kliknięciu tego odnośnika, zostajesz przeniesiony do widoku powiadomień w sekcji **Powiadomienia** sekcji **Monitorowanie**.

Informacje o stanach urządzeń

Kaspersky Security Center Linux przypisze stan do każdego zarządzanego urządzenia. Określony stan zależy od tego, czy spełnione są warunki zdefiniowane przez użytkownika. W niektórych przypadkach, podczas przypisywania stanu do urządzenia, Kaspersky Security Center Linux bierze pod uwagę flagę widoczności urządzenia w sieci (patrz tabela poniżej). Na przykład, jeśli do zarządzanego urządzenia został przypisany stan *Krytyczny*, ponieważ spełniony był warunek *Bazy danych są nieaktualne*, a później flaga widoczności została ustawiona dla urządzenia, wówczas do urządzenia zostanie przypisany stan *OK*. Jeśli Kaspersky Security Center Linux nie znajdzie urządzenia w sieci w ciągu dwóch godzin, flaga widoczności urządzenia zostanie ustawiona na *Nie jest widoczne.*

Stany są następujące:

- *Krytyczny* lub *Krytyczny / Widoczny*
- *Ostrzeżenie* lub *Ostrzeżenie / Widoczne*
- *OK* lub *OK/Widoczne*

Poniższa tabela wyświetla domyślne warunki, które muszą być spełnione, aby przypisać stan *Krytyczny* lub *Ostrzeżenie* do urządzenia, wraz ze wszystkimi możliwymi wartościami.

Warunki przypisania stanu do urządzenia

Warunek	Opis warunku	Dostępne wartości
Aplikacja zabezpieczająca nie jest zainstalowana	Agent sieciowy jest zainstalowany na urządzeniu, ale aplikacja zabezpieczająca nie jest zainstalowana.	• Przycisk przełącznika jest ustawiony w pozycji włączenia. • Przycisk przełącznika jest ustawiony w pozycji wyłączenia.

Warunek	Opis warunku	Dostępne wartości
Wykryto zbyt wiele wirusów	Niektóre wirusy zostały wykryte na urządzeniu przez zadanie wykrywania wirusów, na przykład, zadanie Skanowanie w poszukiwaniu szkodliwego oprogramowania oraz liczba wykrytych wirusów przekraczają określoną wartość.	Większe niż 0.
Poziom ochrony w czasie rzeczywistym jest inny niż poziom zdefiniowany przez administratora	Urządzenie jest widoczne w sieci, ale poziom ochrony w czasie rzeczywistym różni się od poziomu ustawionego (w warunku) przez administratora dla stanu urządzenia.	• Zatrzymane. • Wstrzymane. • Uruchomione.
Skanowanie w poszukiwaniu złośliwego oprogramowania nie było wykonywane od dłuższego czasu	Urządzenie jest widoczne w sieci, a aplikacja zabezpieczająca jest zainstalowana na urządzeniu, ale zadanie *Skanowanie w poszukiwaniu szkodliwego oprogramowania* ani zadanie lokalnego skanowania nie było uruchamiane w określonym przedziale czasu. Warunek jest stosowany tylko do urządzeń, które zostały dodane do bazy danych Serwera administracyjnego 7 dni temu lub wcześniej.	Więcej niż 1 dzień.
Bazy danych są nieaktualne	Urządzenie jest widoczne w sieci, a aplikacja zabezpieczająca jest zainstalowana na urządzeniu, ale antywirusowe bazy danych nie były aktualizowane na tym urządzeniu w określonym przedziale czasu. Warunek jest stosowany tylko do urządzeń, które zostały dodane do bazy danych Serwera administracyjnego dzień wcześniej lub jeszcze wcześniej.	Więcej niż 1 dzień.
Niepołączony od dłuższego czasu	Agent sieciowy jest zainstalowany na urządzeniu, ale urządzenie nie było połączone z Serwerem administracyjnym w określonym przedziale czasu, ponieważ urządzenie było wyłączone.	Więcej niż 1 dzień.
Wykryto aktywne zagrożenia	Liczba nieprzetworzonych obiektów w folderze **Aktywne zagrożenia** przekracza określoną wartość.	Więcej niż 0 elementów.
Czas od momentu zażądania restartu	Urządzenie jest widoczne w sieci, ale aplikacja wymaga ponownego uruchomienia urządzenia dłużej niż określony przedział czasu.	Więcej niż 0 minut.
Przyczyna restartu	Urządzenie jest widoczne w sieci, ale aplikacja wymaga ponownego uruchomienia urządzenia z jednego z wybranych powodów.	• Nieznana przyczyna • Aplikacja nie będzie działała do czasu ponownego uruchomienia • W celu zakończenia aktualizacji wymagane jest ponowne uruchomienie; aplikacja jest uruchomiona • W celu zainicjowania aktualizacji wymagane jest ponowne uruchomienie • W celu zakończenia procesu skanowania lub leczenia wymagane jest ponowne uruchomienie komputera • W celu zakończenia zdalnej instalacji/dezinstalacji wymagane jest ponowne uruchomienie • Kończenie szyfrowania danych na dysku
Zainstalowane są niekompatybilne aplikacje	Urządzenie jest widoczne w sieci, ale inwentaryzacja oprogramowania wykonywana poprzez Agenta sieciowego wykryła niekompatybilne aplikacje zainstalowane na urządzeniu.	• Przycisk przełącznika jest ustawiony w pozycji wyłączenia. • Przycisk przełącznika jest ustawiony w pozycji włączenia.
Wykryto luki w oprogramowaniu	Urządzenie jest widoczne w sieci, a Agent sieciowy jest zainstalowany na urządzeniu, ale zadanie *Wyszukiwania luk i wymaganych aktualizacji* wykryło luki z określonym priorytetem w aplikacjach zainstalowanych na urządzeniu.	• Krytyczny. • Wysoki. • Średni. • Ignoruj, jeśli luka nie może być naprawiona. • Ignoruj, jeśli aktualizacja jest przypisana do instalacji.
Licencja utraciła ważność	Urządzenie jest widoczne w sieci, ale licencja utraciła ważność.	• Przycisk przełącznika jest ustawiony w pozycji wyłączenia. • Przycisk przełącznika jest ustawiony w pozycji włączenia.

Warunek	Opis warunku	Dostępne wartości
Licencja wkrótce utraci ważność	Urządzenie jest widoczne w sieci, ale licencja utraci ważność na urządzeniu za mniej niż określona liczba dni.	Więcej niż 0 dni.
Wyszukiwanie aktualizacji Windows Update nie było przeprowadzane od dłuższego czasu	Urządzenie jest widoczne w sieci, ale zadanie *Wyszukiwania luk i wymaganych aktualizacji* nie było uruchamiane w zdefiniowanym przedziale czasu.	Więcej niż 1 dzień.
Nieprawidłowy stan szyfrowania	Agent sieciowy jest zainstalowany na urządzeniu, ale wynik szyfrowania urządzenia jest równy określonej wartości.	• Nie zgadza się z zasadą w wyniku odmowy użytkownika (tylko dla urządzeń zewnętrznych). • Nie zgadza się z zasadą w wyniku błędu. • Po zastosowaniu zasady wymagane jest ponowne uruchomienie. • Nie określono zasady szyfrowania. • Nieobsługiwany. • Po zastosowaniu zasady.
Ustawienia urządzenia mobilnego nie są zgodne z zasadą	Ustawienia urządzenia mobilnego są inne niż ustawienia, które zostały określone w zasadzie Kaspersky Endpoint Security for Android podczas sprawdzania reguł zgodności.	• Przycisk przełącznika jest ustawiony w pozycji wyłączenia. • Przycisk przełącznika jest ustawiony w pozycji włączenia.
Wykryto nieprzetworzone incydenty związane z bezpieczeństwem	Na urządzeniu zostały wykryte pewne nieprzetworzone problemy bezpieczeństwa. Problemy bezpieczeństwa mogą być tworzone automatycznie poprzez zarządzane aplikacje firmy Kaspersky zainstalowane na urządzeniu klienckim, a także ręcznie przez administratora.	• Przycisk przełącznika jest ustawiony w pozycji wyłączenia. • Przycisk przełącznika jest ustawiony w pozycji włączenia.
Stan urządzenia zdefiniowany przez aplikację	Stan urządzenia jest definiowany przez zarządzaną aplikację. Zarządzane urządzenia mogą mieć stan zdefiniowany przez zarządzane aplikacje, niezależnie od ustawień Kaspersky Security Center Linux. Po zwróceniu przez ten stan jednego ze stanów zdefiniowanych przez Kaspersky Security Center Linux, Serwer administracyjny przypisuje zarządzanemu urządzeniu najbardziej krytyczny stan spośród stanów zwróconych przez zarządzaną aplikację i przypisanych przez Serwer administracyjny. Stany zdefiniowane przez zarządzane aplikacje mają opisy przekazane przez zarządzane aplikacje. Możesz wyświetlić opisy na liście zarządzanych urządzeń, w kolumnie **Opis stanu**.	• Przycisk przełącznika jest ustawiony w pozycji wyłączenia. • Przycisk przełącznika jest ustawiony w pozycji włączenia.
Brakuje miejsca na dysku urządzenia	Wolnego miejsca na dysku jest mniej niż określona wartość lub urządzenie nie mogło zostać zsynchronizowane z Serwerem administracyjnym. Stan *Krytyczny* lub *Ostrzeżenie* zmieniło się na stan *OK*, gdy urządzenie zostało pomyślnie zsynchronizowane z Serwerem administracyjnym, a wolna przestrzeń na urządzeniu jest większa niż lub równa określonej wartości.	Więcej niż 0 MB.
Zarządzanie urządzeniem nie jest możliwe	Podczas wykrywania urządzeń, urządzenie zostało rozpoznane jako widoczne w sieci, ale więcej niż trzy próby synchronizacji z Serwerem administracyjnym nie powiodły się.	• Przycisk przełącznika jest ustawiony w pozycji wyłączenia. • Przycisk przełącznika jest ustawiony w pozycji włączenia.
Ochrona jest wyłączona	Urządzenie jest widoczne w sieci, ale aplikacja zabezpieczająca na urządzeniu została wyłączona na dłużej niż określony przedział czasu. W tym przypadku stan aplikacji zabezpieczającej to *zatrzymany* lub *błąd* i różni się od następujących: *uruchamianie*, *uruchomiony* lub *zawieszony*.	Więcej niż 0 minut.
Aplikacja zabezpieczająca nie jest uruchomiona	Urządzenie jest widoczne w sieci, a aplikacja zabezpieczająca jest zainstalowana na urządzeniu, ale nie jest uruchomiona.	• Przycisk przełącznika jest ustawiony w pozycji wyłączenia. • Przycisk przełącznika jest ustawiony w pozycji włączenia.

Kaspersky Security Center Linux umożliwia skonfigurowanie automatycznego przełączania stanu urządzenia w grupie administracyjnej, gdy spełnione są określone warunki. Jeśli określone warunki są spełnione, do urządzenia klienckiego zostanie przypisany jeden z następujących stanów: *Krytyczny* lub *Ostrzeżenie*. Jeśli określone warunki zostaną spełnione, urządzeniu klienckiemu zostanie przypisany stan *OK*.

Różne stany mogą odpowiadać różnym wartościom jednego warunku. Na przykład, domyślnie, jeśli warunek **Bazy danych są nieaktualne** posiada wartość **Ponad 3 dni**, do urządzenia klienckiego zostaje przypisany stan *Ostrzeżenie*; jeśli wartość to **Ponad 7 dni**, wówczas zostanie przypisany stan *Krytyczny*.

Jeśli aktualizujesz Kaspersky Security Center Linux z poprzedniej wersji, wartości warunku **Bazy danych są nieaktualne** dla przypisania stanu do *Krytyczne* lub *Ostrzeżenie* nie zmienią się.

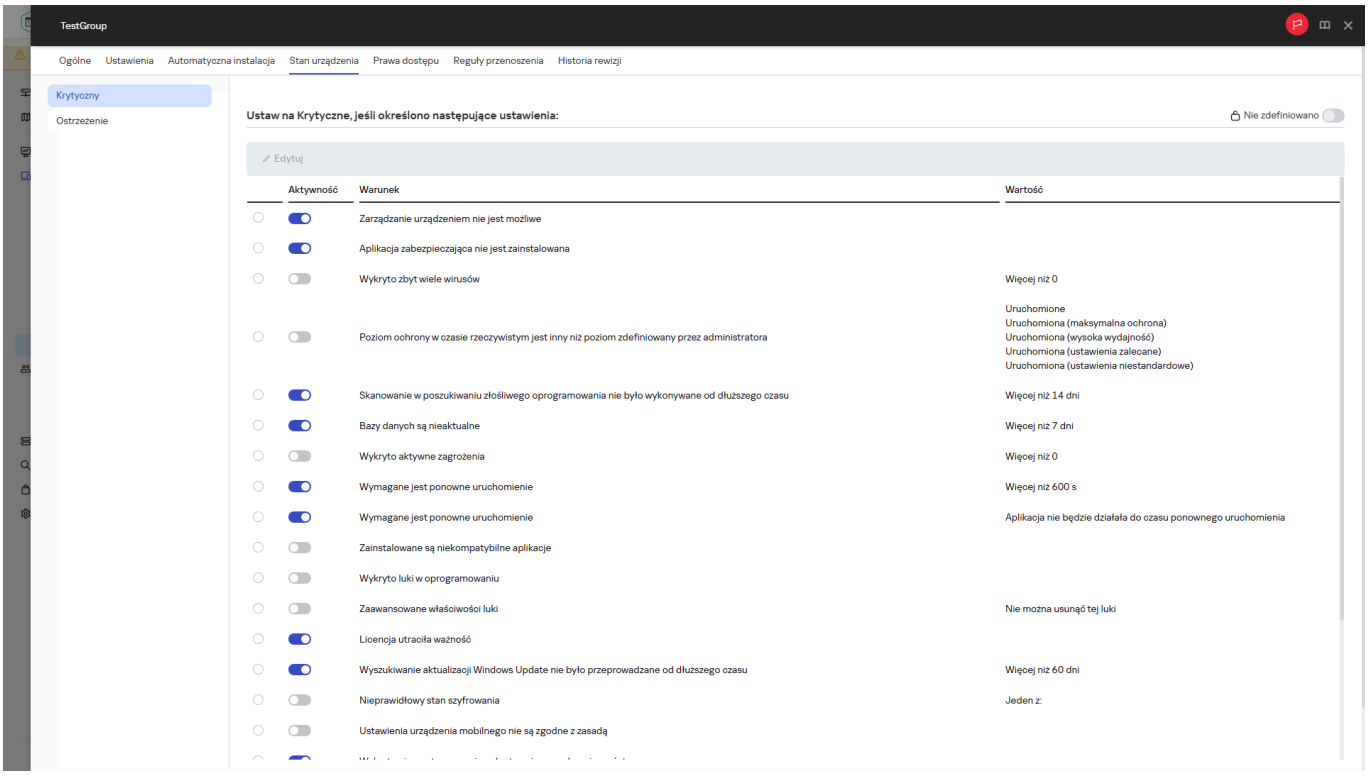
Konfigurowanie przełączania stanów urządzeń

Możesz zmienić warunki, aby przypisać stan *Krytyczny* lub *Ostrzeżenie* do urządzenia.

W celu włączenia zmiany stanu urządzenia na Krytyczny:

1. W menu głównym przejdź do **Zarządzanie zasobami** → **Hierarchia grup**.
2. Przejdź do właściwości grupy administracyjnej, dla której chcesz zmienić przełączanie statusów urządzeń, w jeden z następujących sposobów:
   - Kliknij nazwę żądanej grupy administracyjnej.
   - Kliknij przycisk **Pokaż hierarchię** znajdujący się na górze strony. W otwartym panelu nawigacyjnym najedź kursorem myszy na nazwę wymaganej grupy, a następnie kliknij ikonę ustawień (⚙).

   Zostanie otwarte okno właściwości grupy administracyjnej.
3. W otwartym oknie właściwości wybierz zakładkę **Stan urządzenia**.
4. W lewej części okna wybierz **Krytyczny**.
5. W prawej części okna, w sekcji **Ustaw na Krytyczne, jeśli określono następujące ustawienia** włącz warunek, aby przełączyć urządzenie do stanu *Krytyczny*.



> Możesz zmienić tylko ustawienia, które nie są zablokowane w zasadzie nadrzędnej.

6. Wybierz przycisk radiowy obok warunku na liście.
7. W lewym górnym rogu listy kliknij przycisk **Edytuj**.
8. Dla wybranego warunku ustaw żądaną wartość.

   Nie dla każdego warunku można ustawić wartości.
9. Kliknij **OK**.
10. Kliknij **Zapisz**, aby zachować zmiany.

Jeśli określone warunki zostaną spełnione, zarządzanemu urządzeniu zostanie przypisany stan *Krytyczne*.

W celu włączenia zmiany stanu urządzenia na Ostrzeżenie:

1. W menu głównym przejdź do **Zarządzanie zasobami** → **Hierarchia grup**.
2. Na otwartej liście grup kliknij odnośnik z nazwą grupy, dla której chcesz zmienić przełączanie stanów urządzeń.
3. W otwartym oknie właściwości wybierz zakładkę **Stan urządzenia**.
4. W lewej części okna wybierz **Ostrzeżenie**.
5. W prawej części okna, w sekcji **Ustaw na Ostrzeżenie, jeśli określono następujące ustawienia** włącz warunek, aby przełączyć urządzenie do stanu *Ostrzeżenie*.

> Możesz zmienić tylko ustawienia, które nie są zablokowane w zasadzie nadrzędnej.

6. Wybierz przycisk radiowy obok warunku na liście.

7. W lewym górnym rogu listy kliknij przycisk **Edytuj**.

8. Dla wybranego warunku ustaw żądaną wartość.

   Nie dla każdego warunku można ustawić wartości.

9. Kliknij **OK**.

10. Kliknij **Zapisz**, aby zachować zmiany.

Jeśli określone warunki zostaną spełnione, zarządzanemu urządzeniu zostanie przypisany stan *Ostrzeżenie*.

Konfigurowanie dostarczania powiadomień

Możesz skonfigurować powiadomienie o zdarzeniach występujących w Kaspersky Security Center Linux. W zależności od wybranej metody powiadamiania, dostępne są następujące typy powiadomień:

- E-mail — Po wystąpieniu zdarzenia, Kaspersky Security Center Linux wyśle powiadomienie na określone adresy e-mail.

- SMS — Po wystąpieniu zdarzenia, Kaspersky Security Center Linux wyśle powiadomienie na określone numery telefonu.

- Plik wykonywalny—Po wystąpieniu zdarzenia, plik wykonywalny jest uruchamiany na Serwerze administracyjnym.

W celu skonfigurowania dostarczania powiadomień o zdarzeniach występujących w Kaspersky Security Center Linux:

1. W menu głównym kliknij nazwę Serwera administracyjnego.

   Okno właściwości Serwera administracyjnego zostanie otwarte na zakładce **Ogólne**.

2. Kliknij sekcję **Powiadomienie** i w prawej części okna wybierz zakładkę dla metody powiadamiania, którą chcesz:

   - **E-mail**

     Na zakładce **E-mail** można skonfigurować wysyłanie powiadomień o zdarzeniach za pośrednictwem poczty elektronicznej.

     W polu **Serwer SMTP** określ adresy serwera poczty e-mail, oddzielając je średnikami. Możesz użyć następujących wartości:

     - Adres IPv4 lub IPv6

     - Nazwa DNS serwera SMTP

     W polu **Port serwera SMTP** określ numer portu komunikacji serwera SMTP. Domyślny numer portu to 25.

Jeśli włączysz opcję **Użyj przeszukiwania DNS MX**, możesz użyć kilku wpisów MX adresów IP dla tej samej nazwy DNS serwera SMTP. Ta sama nazwa DNS może posiadać kilka wpisów MX z różnymi wartościami priorytetu odbierania wiadomości e-mail. Serwer administracyjny spróbuje wysłać powiadomienia e-mail do serwera SMTP w kolejności rosnącej priorytetów wpisów MX.

Jeśli włączysz opcję **Użyj przeszukiwania DNS MX** i nie włączysz korzystania z ustawień TLS, zalecane jest użycie ustawień DNSSEC na urządzeniu serwerowym jako dodatkowego środka ochrony wysyłania powiadomień e-mail.

Jeśli włączysz opcję **Użyj uwierzytelniania ESMTP**, możesz określić ustawienia uwierzytelniania ESMTP w polach **Nazwa użytkownika** i **Hasło**. Domyślnie, opcja ta jest wyłączona, a ustawienia uwierzytelniania ESMTP są niedostępne.

Możesz określić ustawienia TLS połączenia z serwerem SMTP:

- **Nie używaj TLS**

Możesz wybrać tę opcję, jeśli chcesz wyłączyć szyfrowanie wiadomości e-mail.

- **Użyj TLS, jeśli jest obsługiwany przez serwer SMTP**

Możesz wybrać tę opcję, jeśli chcesz korzystać z połączenia TLS z serwerem SMTP. Jeśli serwer SMTP nie obsługuje TLS, Serwer administracyjny nawiąże połączenie z serwerem SMTP bez korzystania z TLS.

- **Zawsze używaj TLS, sprawdź ważność certyfikatu serwera**

Możesz wybrać tę opcję, jeśli chcesz korzystać z ustawień uwierzytelniania TLS. Jeśli serwer SMTP nie obsługuje TLS, Serwer administracyjny nie może nawiązać połączenia z serwerem SMTP.

Zalecane jest użycie tej opcji dla lepszej ochrony połączenia z serwerem SMTP. Jeśli wybierzesz tę opcję, możesz skonfigurować ustawienia uwierzytelniania dla połączenia TLS.

Jeśli wybierzesz wartość **Zawsze używaj TLS, sprawdź ważność certyfikatu serwera**, możesz określić certyfikat do uwierzytelniania serwera SMTP i wybrać, czy chcesz włączyć komunikację za pośrednictwem dowolnej wersji TLS, czy tylko za pośrednictwem TLS 1.2 lub nowszych wersji. Możesz także określić certyfikat do uwierzytelniania klienta na serwerze SMTP.

Możesz określić certyfikat dla połączenia TLS, klikając odnośnik **Określ certyfikaty**:

- Odszukaj plik certyfikatu serwera SMTP:

Możesz otrzymać plik z listą certyfikatów od zaufanych urzędów certyfikacji i przesłać go do Serwera administracyjnego. Kaspersky Security Center Linux sprawdza, czy certyfikat serwera SMTP jest również podpisany przez zaufane urzędy certyfikacji. Kaspersky Security Center Linux nie może nawiązać połączenia z serwerem SMTP, jeśli certyfikat serwera SMTP nie zostanie odebrany z zaufanych urzędów certyfikacji.

- Odszukaj plik certyfikatu klienta:

Możesz użyć certyfikatu otrzymanego z dowolnego źródła, na przykład, z dowolnego zaufanego urzędu certyfikacji. Musisz określić certyfikat i jego klucz prywatny, używając jednego z następujących typów certyfikatów:

- Certyfikat X-509:

Musisz określić plik z certyfikatem oraz plik z kluczem prywatnym. Oba pliki nie są od siebie zależne, a kolejność wczytywania plików nie ma znaczenia. Po załadowaniu obu plików należy określić hasło do dekodowania klucza prywatnego. Hasło może mieć pustą wartość, jeśli klucz prywatny nie jest zakodowany.

- Kontener pkcs12:

Musisz przesłać pojedynczy plik zawierający certyfikat i jego klucz prywatny. Po załadowaniu pliku należy podać hasło do dekodowania klucza prywatnego. Hasło może mieć pustą wartość, jeśli klucz prywatny nie jest zakodowany.

Przycisk **Wyślij wiadomość testową** umożliwia sprawdzenie, czy ustawienia powiadamiania zostały skonfigurowane poprawnie: aplikacja wyśle testowe powiadomienie na wskazany adres e-mail.

W polu **Adresaci (adresy e-mail)** określ adresy e-mail, na jaki aplikacja będzie wysyłać powiadomienia. W tym polu możesz określić kilka adresów, oddzielając je średnikami.

W polu **Temat** wprowadź temat wiadomości e-mail. Możesz zostawić to pole puste.

Z listy rozwijalnej **Szablon tematu** wybierz szablon tematu. Zmienna określona przez wybrany szablon zostanie automatycznie umieszczona w polu **Temat**. Możesz utworzyć temat wiadomości, wybierając kilka szablonów tematu.

W oknie **Adres e-mail nadawcy: Jeśli to ustawienie nie jest określone, użyty zostanie adres odbiorcy. Uwaga: Nie zalecamy używania adresu e-mail, który nie istnieje** określ adres e-mail nadawcy. Jeśli pozostawisz to pole puste, domyślnie użyty zostanie adres odbiorcy. Nie jest zalecane użycie adresu e-mail, który nie istnieje.

Pole **Treść powiadomienia** zawiera standardowy tekst z informacjami dotyczącymi zdarzenia, który aplikacja wysyła po wystąpieniu zdarzenia. Ten tekst zawiera dodatkowe parametry, takie jak: nazwa zdarzenia, nazwa urządzenia oraz nazwa domeny. Istnieje możliwość zmodyfikowania treści wiadomości poprzez dodanie innych parametrów zastępczych z bardziej szczegółowymi danymi dotyczącymi zdarzenia.

> Jeżeli tekst powiadomienia zawiera znak procentu (%), należy wpisać go dwa razy z rzędu, aby umożliwić wysyłanie wiadomości. Na przykład, „obciążenie procesora wynosi 100%%".

Kliknięcie odnośnika **Ustaw limit liczby powiadomień** umożliwia zdefiniowanie maksymalnej liczby powiadomień, które aplikacja może wysłać w określonym przedziale czasu.

- **SMS**

Na zakładce **SMS** możesz skonfigurować wysyłanie powiadomień SMS o różnych zdarzeniach na telefon komórkowy. Wiadomości SMS są wysyłane poprzez bramkę pocztową.

W polu **Serwer SMTP** określ adresy serwera poczty e-mail, oddzielając je średnikami. Możesz użyć następujących wartości:

- Adres IPv4 lub IPv6
- Nazwa DNS serwera SMTP

W polu **Port serwera SMTP** określ numer portu komunikacji serwera SMTP. Domyślny numer portu to 25.

Jeśli opcja **Użyj uwierzytelniania ESMTP** jest włączona, możesz określić ustawienia uwierzytelniania ESMTP w polach **Nazwa użytkownika** i **Hasło**. Domyślnie, opcja ta jest wyłączona, a ustawienia uwierzytelniania ESMTP są niedostępne.

Możesz określić ustawienia TLS połączenia z serwerem SMTP:

- **Nie używaj TLS**

Możesz wybrać tę opcję, jeśli chcesz wyłączyć szyfrowanie wiadomości e-mail.

- **Użyj TLS, jeśli jest obsługiwany przez serwer SMTP**

Możesz wybrać tę opcję, jeśli chcesz korzystać z połączenia TLS z serwerem SMTP. Jeśli serwer SMTP nie obsługuje TLS, Serwer administracyjny nawiąże połączenie z serwerem SMTP bez korzystania z TLS.

- **Zawsze używaj TLS, sprawdź ważność certyfikatu serwera**

Możesz wybrać tę opcję, jeśli chcesz korzystać z ustawień uwierzytelniania TLS. Jeśli serwer SMTP nie obsługuje TLS, Serwer administracyjny nie może nawiązać połączenia z serwerem SMTP.

Zalecane jest użycie tej opcji dla lepszej ochrony połączenia z serwerem SMTP. Jeśli wybierzesz tę opcję, możesz skonfigurować ustawienia uwierzytelniania dla połączenia TLS.

Jeśli wybierzesz wartość **Zawsze używaj TLS, sprawdź ważność certyfikatu serwera**, możesz określić certyfikat do uwierzytelniania serwera SMTP i wybrać, czy chcesz włączyć komunikację za pośrednictwem dowolnej wersji TLS, czy tylko za pośrednictwem TLS 1.2 lub nowszych wersji. Możesz także określić certyfikat do uwierzytelniania klienta na serwerze SMTP.

Możesz określić plik certyfikatu serwera SMTP, klikając odnośnik **Określ certyfikaty**. Możesz otrzymać plik z listą certyfikatów od zaufanych urzędów certyfikacji i przesłać go do Serwera administracyjnego. Kaspersky Security Center Linux sprawdza, czy certyfikat serwera SMTP jest również podpisany przez zaufane urzędy certyfikacji. Kaspersky Security Center Linux nie może nawiązać połączenia z serwerem SMTP, jeśli certyfikat serwera SMTP nie zostanie odebrany z zaufanych urzędów certyfikacji.

W polu **Adresaci (adresy e-mail)** określ adresy e-mail, na jaki aplikacja będzie wysyłać powiadomienia. W tym polu możesz określić kilka adresów, oddzielając je średnikami. Powiadomienia będą dostarczane na numery telefonów skojarzone z określonymi adresami e-mail.

W polu **Temat** wprowadź temat wiadomości e-mail.

Z listy rozwijalnej **Szablon tematu** wybierz szablon tematu. Zgodnie z wybranym szablonem zmienna zostanie umieszczona w polu **Temat**. Możesz utworzyć temat wiadomości, wybierając kilka szablonów tematu.

W oknie **Adres e-mail nadawcy: Jeśli to ustawienie nie jest określone, użyty zostanie adres odbiorcy. Uwaga: Nie zalecamy używania adresu e-mail, który nie istnieje** określ adres e-mail nadawcy. Jeśli pozostawisz to pole puste, domyślnie użyty zostanie adres odbiorcy. Nie jest zalecane użycie adresu e-mail, który nie istnieje.

W polu **Numery telefonów odbiorców wiadomości SMS** określ numery telefonów komórkowych odbiorców powiadomień SMS.

W polu **Treść powiadomienia** określ tekst z informacjami dotyczącymi zdarzenia, który aplikacja wysyła po wystąpieniu zdarzenia. Ten tekst zawiera parametry zastępcze, takie jak: nazwa zdarzenia, nazwa urządzenia oraz nazwa domeny.

Jeżeli tekst powiadomienia zawiera znak procentu (%), należy wpisać go dwa razy z rzędu, aby umożliwić wysyłanie wiadomości. Na przykład, „obciążenie procesora wynosi 100%%”.

Kliknięcie **Wyślij wiadomość testową** umożliwia sprawdzenie, czy ustawienia powiadamiania zostały skonfigurowane poprawnie: aplikacja wyśle testowe powiadomienie do określonego odbiorcy.

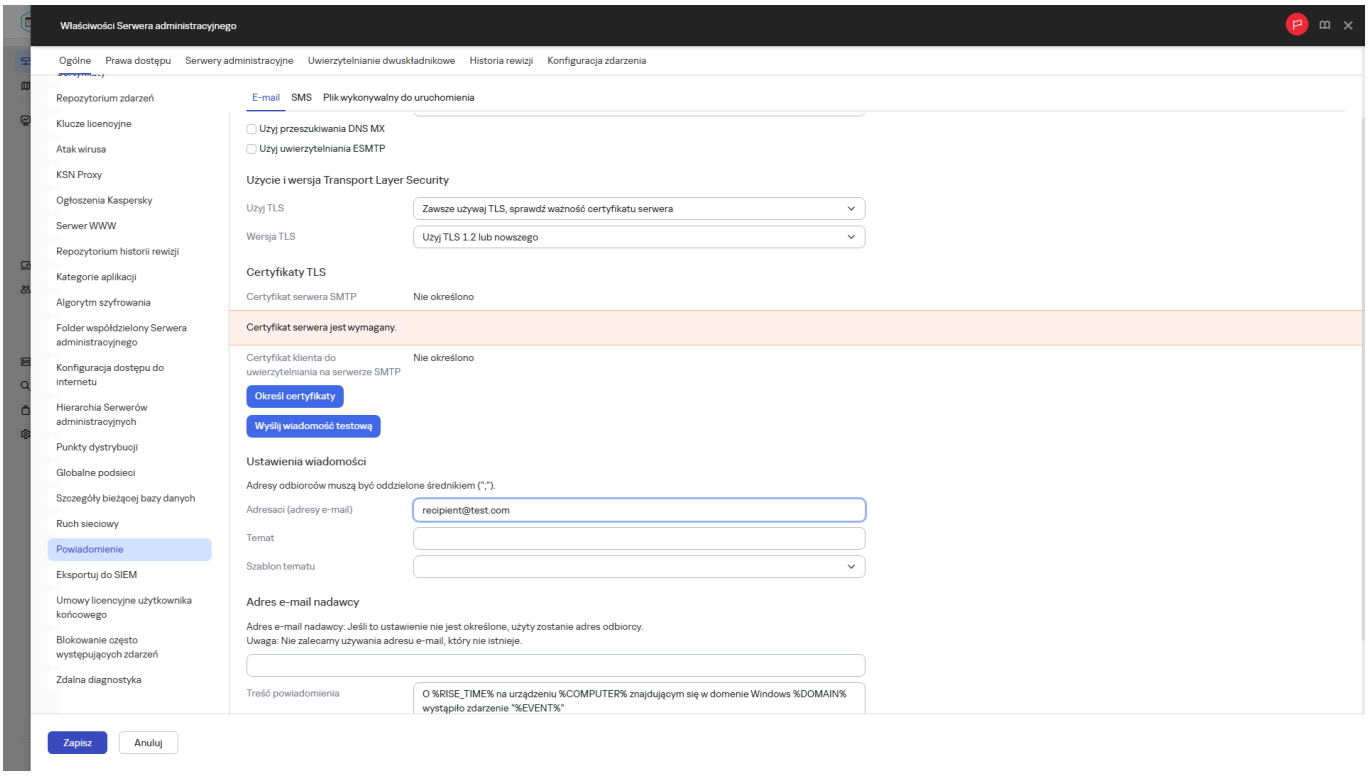
Kliknięcie odnośnika **Ustaw limit liczby powiadomień** umożliwia zdefiniowanie maksymalnej liczby powiadomień, które aplikacja może wysłać w określonym przedziale czasu.

- **Plik wykonywalny do uruchomienia**

  Jeśli wybrana jest ta metoda powiadamiania, w polu wejściowym określ aplikację, która zostanie uruchomiona, gdy wystąpi zdarzenie.

  W polu **Plik wykonywalny, który będzie uruchamiany na Serwerze administracyjnym w momencie wystąpienia zdarzenia** określ folder i nazwę pliku, który ma zostać uruchomiony. Przed określeniem pliku przygotuj plik i określ symbole zastępcze, które definiują szczegóły zdarzeń, które mają zostać wysłane w treści powiadomienia. Folder i plik, który określasz, muszą znajdować się na Serwerze administracyjnym.

  Kliknięcie odnośnika **Ustaw limit liczby powiadomień** umożliwia zdefiniowanie maksymalnej liczby powiadomień, które aplikacja może wysłać w określonym przedziale czasu.



Wybieranie metody powiadamiania

3. Na zakładce zdefiniuj ustawienia powiadamiania.

4. Kliknij **Zapisz**, aby zapisać zmiany i zamknąć okno właściwości Serwera administracyjnego.

   Zapisane ustawienia dostarczania powiadomień zostaną zastosowane do wszystkich zdarzeń, które występują w Kaspersky Security Center Linux.

Możesz zastąpić ustawienia dostarczania powiadomień dla pewnych zdarzeń w sekcji **Konfiguracja zdarzenia** ustawień Serwera administracyjnego, ustawień zasady lub ustawień aplikacji.

Sprawdzanie opcji wysyłania powiadomień

Aby sprawdzić, czy powiadomienia o zdarzeniach są dostarczane, aplikacja używa powiadomień o wykryciu na urządzeniach klienckich wirusa testowego EICAR.

W celu sprawdzenia opcji wysyłania powiadomień o zdarzeniach:

1. Zatrzymaj zadanie ochrony systemu plików w czasie rzeczywistym na urządzeniu klienckim, a następnie skopiuj na nie wirusa testowego EICAR. Następnie, włącz ponownie ochronę w czasie rzeczywistym systemu plików.

2. Uruchom zadanie skanowania dla urządzeń klienckich w grupie administracyjnej lub dla określonych urządzeń, uwzględniając urządzenie zawierające wirusa testowego EICAR.

   Jeżeli zadanie skanowania jest skonfigurowane poprawnie, wirus testowy zostanie wykryty. Jeżeli powiadomienia są skonfigurowane poprawnie, zostaniesz powiadomiony o wykryciu wirusa.

Aby otworzyć zapis wykrycia wirusa testowego:

1. W menu głównym przejdź do **Monitorowanie** → **Wybory zdarzeń**.
2. Kliknij nazwę wyboru **Ostatnie zdarzenia**.

   W oknie, które zostanie otwarte, wyświetlone zostanie powiadomienie o wirusie testowym.

Wirus testowy EICAR nie zawiera kodu, który mógłby zaszkodzić urządzeniu. Jednak większość aplikacji zabezpieczających wykrywa ten plik jako wirusa. Wirusa testowego możesz pobrać z oficjalnej strony EICAR.

Wyświetlanie powiadomień o zdarzeniach po uruchomieniu pliku wykonywalnego

Kaspersky Security Center Linux może powiadamiać administratora o zdarzeniach na urządzeniach klienckich poprzez uruchomienie pliku wykonywalnego. Plik wykonywalny musi zawierać inny plik wykonywalny ze zmiennymi środowiskowymi zdarzenia przekazywanymi administratorowi (patrz poniższa tabela).

Zmienne środowiskowe opisujące zdarzenie

Zmienna środowiskowa	Opis zmiennej środowiskowej
$SEVERITY	Priorytet zdarzenia. Możliwe wartości: • **Informacja** • **Ostrzeżenie** • **Błąd** • **Krytyczny**
$COMPUTER	Nazwa urządzenia, na którym wystąpiło zdarzenie. Maksymalna długość nazwy urządzenia wynosi 256 znaków.
$DOMAIN	Nazwa domeny urządzenia, na którym wystąpiło zdarzenie.
$EVENT	Nazwa typu zdarzenia. Maksymalna długość nazwy typu zdarzenia wynosi 50 znaków.
$DESCR	Opis zdarzenia. Maksymalna długość opisu wynosi 1000 znaków.
$RISE_TIME	Czas utworzenia zdarzenia.
$KLCSAK_EVENT_TASK_DISPLAY_NAME	Nazwa zadania. Maksymalna długość nazwy zadania wynosi 100 znaków.
$KL_PRODUCT	Nazwa aplikacji.
$KL_VERSION	Numer wersji aplikacji.
$KLCSAK_EVENT_SEVERITY_NUM	Numer priorytetu zdarzenia. Możliwe wartości: • 1—**Informacja** • 2—**Ostrzeżenie** • 3—**Błąd** • 4—**Krytyczny**
$HOST_IP	Adres IP urządzenia, na którym wystąpiło zdarzenie.
$HOST_CONN_IP	Adres IP połączenia urządzenia, na którym wystąpiło zdarzenie.

Na przykład:
Powiadomienia o zdarzeniach są wysyłane przez plik wykonywalny (na przykład script1.bat), w którym uruchomiony jest inny plik wykonywalny (na przykład script2.bat) ze zmienną środowiskową $COMPUTER. Po wystąpieniu zdarzenia, plik script1.bat jest uruchamiany na urządzeniu administratora, który uruchamia plik script2.bat ze zmienną środowiskową $COMPUTER. Administrator uzyska nazwę urządzenia, na którym wystąpiło zdarzenie.

Ogłoszenia firmy Kaspersky

W tej sekcji opisano, jak używać, konfigurować i wyłączać ogłoszenia Kaspersky.

Informacje o ogłoszeniach firmy Kaspersky

Sekcja Zapowiedzi firmy Kaspersky (**Monitorowanie** → **Zapowiedzi firmy Kaspersky**) zawiera informacje dotyczące Twojej wersji Kaspersky Security Center Linux i zarządzanych aplikacji, zainstalowanych na zarządzanych urządzeniach. Kaspersky Security Center Linux okresowo aktualizuje informacje w sekcji, usuwając nieaktualne ogłoszenia i dodając nowe informacje.

Kaspersky Security Center Linux wyświetla tylko te ogłoszenia Kaspersky, które odnoszą się do aktualnie podłączonego Serwera administracyjnego i aplikacji Kaspersky zainstalowanych na zarządzanych urządzeniach tego Serwera administracyjnego. Ogłoszenia są wyświetlane indywidualnie dla dowolnego typu Serwera administracyjnego — głównego, podrzędnego lub wirtualnego.

Serwer administracyjny musi mieć połączenie z internetem, aby otrzymywać ogłoszenia Kaspersky.

Ogłoszenia zawierają informacje następujących typów:

- Ogłoszenia związane z bezpieczeństwem

  Ogłoszenia związane z bezpieczeństwem mają na celu zapewnienie aktualności i pełnej funkcjonalności aplikacji Kaspersky zainstalowanych w Twojej sieci. Ogłoszenia mogą zawierać informacje o krytycznych aktualizacjach aplikacji Kaspersky, poprawkach znalezionych luk w zabezpieczeniach i sposobach rozwiązania innych problemów w aplikacjach Kaspersky. Domyślnie ogłoszenia związane z bezpieczeństwem są włączone. Jeśli nie chcesz otrzymywać ogłoszeń, możesz wyłącz tę funkcję.

  Aby wyświetlić informacje odpowiadające konfiguracji ochrony sieci, Kaspersky Security Center Linux wysyła dane do serwerów Kaspersky w chmurze i odbiera tylko te powiadomienia, które odnoszą się do aplikacji Kaspersky zainstalowanych w Twojej sieci. Zestaw danych, które mogą być wysyłane na serwery, opisano w Umowie licencyjnej użytkownika końcowego, którą akceptujesz podczas instalowania Serwera administracyjnego.

- Ogłoszenia marketingowe

  Ogłoszenia marketingowe obejmują informacje o specjalnych ofertach dla aplikacji Kaspersky, reklamach i nowościach od Kaspersky. Ogłoszenia marketingowe są domyślnie wyłączone. Otrzymujesz tego typu powiadomienia tylko wtedy, gdy włączyłeś Kaspersky Security Network (KSN). Możesz wyłączyć ogłoszenia marketingowe, wyłączając KSN.

  Aby wyświetlać tylko istotne informacje, które mogą być pomocne w ochronie urządzeń sieciowych i wykonywaniu codziennych zadań, Kaspersky Security Center Linux wysyła dane do serwerów Kaspersky w chmurze i odbiera odpowiednie ogłoszenia. Zestaw danych, które można wysłać do serwerów, opisano w sekcji Przetwarzane dane w Oświadczeniu KSN.

Nowe informacje są podzielone na następujące kategorie według ważności:

1. Krytyczne informacje
2. Ważne wiadomości

3. Ostrzeżenie

4. Informacja

Jeśli w sekcji Ogłoszenia firmy Kaspersky pojawią się nowe informacje, konsola Kaspersky Security Center Web Console wyświetli etykietę powiadomienia odpowiadającą istotności ogłoszeń. Możesz kliknąć etykietę, aby wyświetlić to ogłoszenie w sekcji Ogłoszenia firmy Kaspersky.

Możesz określić Ustawienia ogłoszeń firmy Kaspersky, w tym kategorie ogłoszeń, które chcesz przeglądać, i gdzie wyświetlać etykietę powiadomienia. Jeśli nie chcesz otrzymywać ogłoszeń, możesz wyłącz tę funkcję.

Określanie ustawień ogłoszeń Kaspersky

W sekcji Ogłoszenia firmy Kaspersky możesz określić ustawienia ogłoszeń firmy Kaspersky, w tym kategorie ogłoszeń, które chcesz przeglądać, i gdzie wyświetlać etykietę powiadomienia.

W celu skonfigurowania ogłoszeń Kaspersky:

1. W menu głównym przejdź do **Monitorowanie** → **Ogłoszenia Kaspersky**.

2. Kliknij odnośnik **Ustawienia**.

   Zostanie otwarte okno ustawień ogłoszeń Kaspersky.

3. Określ następujące ustawienia:

   - Wybierz poziom istotności ogłoszeń, które chcesz przejrzeć. Ogłoszenia z innych kategorii nie będą wyświetlane.

   - Wybierz, gdzie chcesz widzieć etykietę powiadomienia. Etykieta może być wyświetlana we wszystkich sekcjach konsoli lub w sekcji **Monitorowanie** i jego podsekcjach.

4. Kliknij przycisk **OK**.

   Zostaną określone ustawienia ogłoszeń firmy Kaspersky.

Wyłączanie ogłoszeń Kaspersky

Sekcja Zapowiedzi firmy Kaspersky (**Monitorowanie** → **Zapowiedzi firmy Kaspersky**) zawiera informacje dotyczące Twojej wersji Kaspersky Security Center Linux i zarządzanych aplikacji, zainstalowanych na zarządzanych urządzeniach. Jeśli nie chcesz otrzymywać ogłoszeń firmy Kaspersky, możesz wyłączyć tę funkcję.

Ogłoszenia firmy Kaspersky obejmują dwa rodzaje informacji: ogłoszenia związane z bezpieczeństwem oraz ogłoszenia marketingowe. Możesz wyłączyć ogłoszenia każdego typu osobno.

W celu wyłączenia ogłoszeń związanych z bezpieczeństwem:

1. W menu głównym kliknij nazwę Serwera administracyjnego.

   Zostanie otwarte okno właściwości Serwera administracyjnego.

2. Na zakładce **Ogólne** wybierz sekcję **Ogłoszenia firmy Kaspersky**.

3. Przełącz przycisk przełączania na pozycję **Ogłoszenia związane z bezpieczeństwem są wyłączone**.

4. Kliknij przycisk **Zapisz**.

   Ogłoszenia firmy Kaspersky są wyłączone.

Ogłoszenia marketingowe są domyślnie wyłączone. Otrzymujesz ogłoszenia marketingowe tylko wtedy, gdy włączyłeś Kaspersky Security Network (KSN). Możesz wyłączyć tego typu ogłoszenia, wyłączając KSN.

W celu wyłączenia ogłoszeń marketingowych:

1. W menu głównym kliknij nazwę Serwera administracyjnego.

   Zostanie otwarte okno właściwości Serwera administracyjnego.

2. Na zakładce **Ogólne** wybierz sekcję **Ustawienia KSN Proxy**.

3. Wyłącz opcję **Użyj Kaspersky Security Network Włączono**.

4. Kliknij przycisk **Zapisz**.

   Ogłoszenia marketingowe są wyłączone.

Przeglądanie informacji dotyczących wykrycia zagrożeń

Możesz włączyć lub wyłączyć wyświetlanie informacji o alertach.

Po aktywowaniu Serwera administracyjnego przy użyciu licencji Kaspersky Extended Detection and Response Optimum lub Kaspersky Next XDR Optimum konsola Kaspersky Security Center Web Console automatycznie wyświetla podsekcję **Alerty** w sekcji **Monitorowanie** menu głównego.

*W celu włączenia lub wyłączenia sekcji **Alerty** w menu głównym:*

1. W menu głównym przejdź do sekcji **Ustawienia** → **Opcje interfejsu**.

2. Włącz lub wyłącz opcję **Pokaż alerty EDR**.

3. Kliknij **Zapisz**.

Gdy opcja **Pokaż alerty EDR** jest włączona, konsola wyświetla podsekcję **Alerty** w sekcji **Monitorowanie** menu głównego. W podsekcji **Alerty** możesz przejrzeć informacje dotyczące wykrycia zagrożeń na urządzeniach końcowych.

Dodatkowo, możesz dodać widżet, który wyświetla informacje o alertach.

Aby poprawnie wyświetlać szczegółowe informacje o wykrytych zagrożeniach na karcie alertu, należy zainstalować wtyczkę Kaspersky Endpoint Agent oraz zgodną wersja wtyczki Kaspersky Endpoint Security (Kaspersky Endpoint Security for Linux w wersji 12.1 lub nowszej, Kaspersky Endpoint Security for Mac w wersji 12.1 lub nowszej albo Kaspersky Endpoint Security for Windows w wersji 12.6 lub nowszej).

Użyj menu **Filtr**, aby filtrować alerty według daty i wartości pól.

Pole **Typ obiektu** zawiera następujące wartości:

- nieznany
- Łącze wykorzystywane do phishingu
- wirus
- Trojan
- szkodliwe narzędzie
- backdoor
- robak
- inna aplikacja
- Adware
- Pornware
- Niebezpieczny spakowany program
- Niebezpieczne zachowanie

Pole **Odpowiedź automatyczna** zawiera następujące wartości:

- Wykryto szkodliwy obiekt
- Obiekt usunięty
- Obiekt wyleczony
- Wyleczenie obiektu nie powiodło się
- Obiekt przeniesiono do Kwarantanny
- Wykryto archiwum zabezpieczone hasłem
- Wykryto wirusa

Integracje umożliwiające reagowanie na alerty

Jeśli posiadasz licencję Kaspersky Next XDR Optimum, możesz skonfigurować integracje z następującymi rozwiązaniami w celu reagowania na zagrożenia:

- Kaspersky Automated Security Awareness Platform
- Kaspersky Threat Intelligence Portal Sandbox
- Active Directory

Te integracje są dostępne, jeśli aktywowano Serwer administracyjny przy użyciu licencji Kaspersky Next XDR Optimum.
Aby wykonywać działania reagowania, należy wdrożyć klucz licencyjny Kaspersky Next XDR Optimum w zarządzanych aplikacjach.
Podczas korzystania z funkcjonalności Kaspersky Next XDR Optimum w ramach licencji próbnej, najpierw musisz dodać podrzędny fizyczny Serwer administracyjny, następnie aktywować ten podrzędny Serwer administracyjny w ramach licencji próbnej i wdrożyć klucz licencyjny na urządzenia zarządzane przez ten Serwer administracyjny.

Jeśli korzystasz z licencji Kaspersky Next EDR Optimum, nie musisz aktywować aplikacji zainstalowanych na zarządzanych urządzeniach w ramach licencji Kaspersky Next XDR Optimum. Należy to zrobić tylko dla nowych urządzeń, o ile takie istnieją.

Ponieważ licencja Kaspersky Next XDR Optimum wspiera wielodostęp, możesz centralnie dystrybuować klucz licencyjny do zarządzanych aplikacji. Automatyczna dystrybucja licencji do podrzędnych i wirtualnych Serwerów administracyjnych nie jest obsługiwana.

Aby skonfigurować integracje, musisz mieć uprawnienia do **odczytu** i **zapisu** w obszarze funkcjonalnym **Funkcje ogólne: Integracja aplikacji**.

Konfigurowanie integracji z usługą Active Directory w celu wykonywania działań reagowania

Integracja z usługą Active Directory umożliwia wykonywanie działań reagowania dla użytkowników usługi Active Directory objętych alertem lub w niego zaangażowanych.

Aby skonfigurować integrację z usługą Active Directory w celu reagowania na alerty, należy używać Serwera administracyjnego Kaspersky Security Center Linux w wersji 15.4 lub nowszej.

Integracja z usługą Active Directory w celu reagowania na alerty oraz ustawienia skanowania kontrolera domeny usługi Active Directory (adres i poświadczenia użytkownika kontrolera domeny) określone podczas konfigurowania przeszukiwania kontrolera domeny to dwa różne ustawienia. Ponieważ musisz mieć pewność, że użytkownik, dla którego ma zostać wykonane działanie reagowania, ma konto w usłudze Active Directory, musisz skonfigurować obie integracje: dla skanowania i dla reagowania. Kolejność nie ma znaczenia.

Ustawienia integracji nie są dziedziczone i mają zastosowanie wyłącznie do Serwera administracyjnego (fizycznego lub wirtualnego), na którym konfigurujesz te ustawienia.

Aby skonfigurować integrację z usługą Active Directory w celu reagowania na alerty:

1. W menu głównym kliknij nazwę Serwera administracyjnego.

   Okno właściwości Serwera administracyjnego zostanie otwarte na zakładce **Ogólne**.

2. Wykonaj jedną z poniższych czynności:

   - Wybierz sekcję **Punkty dystrybucji**, kliknij nazwę wymaganego punktu dystrybucji, a następnie w otwartym oknie właściwości wybierz sekcję **Active Directory**.
   - Wybierz sekcję **Odpowiedź Active Directory**.

3. W prawym panelu włącz przełącznik **Integracja Active Directory**.

   Jeśli później zechcesz wyłączyć integrację, będziesz mógł to zrobić jedynie dla wszystkich połączeń, dezaktywując przełącznik **Integracja Active Directory**. Nie można wyłączyć integracji dla oddzielnego połączenia. Zamiast tego można usunąć połączenie.

   > Po włączeniu lub wyłączeniu przełącznika **Integracja Active Directory** ustawienie to zostanie zastosowane zarówno do sekcji **Odpowiedź Active Directory**, jak i do sekcji **Punkty dystrybucji**.

4. Utwórz połączenie z kontrolerem domeny Active Directory, klikając przycisk **Dodaj**.

5. W otwartym oknie określ następujące parametry dla połączenia:

   - **Adres sterownika domeny**

     Nazwa komputera, na przykład: `server.mycompany.com`.

     Możesz podać kilka adresów. Wszystkie kontrolery domeny, których adresy podasz, muszą należeć do tej samej domeny.

   - **Nazwa domeny Active Directory**

     W pełni kwalifikowana nazwa domeny DNS, na przykład: `mycompany.com`

     Możesz również określić nazwę SAM lub NetBIOS, na przykład: `mycompany`

     Używaj małych liter. Jeżeli tworzysz kilka połączeń dla Serwera administracyjnego lub punktu dystrybucji, podaj inną nazwę dla każdego połączenia.

     > Aby wykonać działania reagowania, nazwa domeny Active Directory podana w tym polu musi być zgodna z nazwą domeny Active Directory podaną w alercie.

   - **Login**

     Zaloguj się na konto Active Directory z uprawnieniami administratora, na podstawie których mają zostać wykonane działania reagowania.

   - **Hasło**

     Hasło konta Active Directory z uprawnieniami administratora, na podstawie którego mają zostać wykonane działania reagowania.

6. Jeśli chcesz sprawdzić stan połączenia, kliknij przycisk **Sprawdź połączenie**.

   Jeżeli połączenie zostanie nawiązane pomyślnie, zostanie wyświetlony status **Połączono**. W przeciwnym wypadku status będzie ustawiony na **Niepowodzenie** i zostanie wyświetlony komunikat o błędzie z nazwami kontrolerów domeny, z którymi nie udało się nawiązać połączenia.

Należy wziąć pod uwagę sposób łączenia się z usługą Active Directory: **z urządzenia z systemem Linux czy z urządzenia z systemem Windows**.

Łączenie się z urządzenia z systemem Linux

Domyślnie podczas łączenia się z kontrolerem domeny i uwierzytelniania go z poziomu urządzenia Linux logika jest następująca:

1. Serwer administracyjny lub punkt dystrybucji próbuje połączyć się z kontrolerem domeny poprzez protokół LDAPS.

   Wymagana jest silna weryfikacja certyfikatu serwera LDAP.

2. Aby zweryfikować certyfikat, umieszczasz publiczną część certyfikatu kontrolera domeny w repozytorium certyfikatów systemu.

   Aby uzyskać dostęp do łańcucha certyfikatów, używana jest ścieżka zależna od systemu operacyjnego do urzędu certyfikacji (CA).

   Na przykład:

   - /etc/ssl/certs/ca-certificates.crt — Ścieżka dla systemów operacyjnych opartych na Debianie (Debian, Ubuntu, Astra).
   - /etc/pki/ca-trust/extracted/pem/tls-ca-bundle.pem — ścieżka dla CentOS lub Red Hat.

3. Jeżeli połączenie LDAPS się nie powiedzie, pojawi się błąd i nie zostanie użyty żaden inny protokół połączenia.

   W przypadku problemów z LDAPS możesz skontaktować się z Pomocą techniczną Kaspersky.

Jeśli nie chcesz instalować certyfikatu w repozytorium certyfikatów systemu, możesz użyć flagi KLNAG_LDAP_SSL_CACERT, aby ustawić ścieżkę do certyfikatu kontrolera domeny. Aby to zrobić należy uruchomić polecenie:

```
klscflag -fset -pv klnagent -n KLNAG_LDAP_SSL_CACERT -t s -v "</path/to/domain-controller/cert>"
```

gdzie `</path/to/domain-controller/cert>` jest ścieżką do publicznej części certyfikatu kontrolera domeny.

Na przykład, jeśli ścieżka to `"/var/opt/kaspersky/ldap_cert.crt"`, polecenie wygląda następująco:
```
klscflag -fset -pv klnagent -n KLNAG_LDAP_SSL_CACERT -t s -v "/var/opt/kaspersky/ldap_cert.crt"
```

Łączenie z urządzenia z systemem Windows

Podczas łączenia się z kontrolerem domeny i uwierzytelniania go z poziomu urządzenia z systemem Windows ustawienia połączenia są definiowane przez domenę.

Musisz tylko upewnić się, że:

- Protokół LDAPS jest włączony, a port 636 jest dostępny na urządzeniu.
- Zezwalasz na połączenia z kontrolerem domeny poprzez zaporę sieciową lub serwer proxy.

7. Kliknij przycisk **Zapisz**.

Okno zostanie zamknięte, a połączenie zostanie wyświetlone w tabeli połączeń.

W tabeli połączeń możesz wykonać następujące czynności:

- Edytuj parametry połączenia.

  Aby tego dokonać, kliknij odnośnik z parametrem **Adres sterownika domeny** dla wymaganego połączenia. W oknie, które zostanie otwarte, dodaj niezbędne źródła, a następnie kliknij przycisk **Zapisz**.

  Możesz edytować tylko parametry **Login** i **Hasło**.

- Usuń połączenia.

  Aby to zrobić, zaznacz pole wyboru obok połączenia, które chcesz usunąć, kliknij przycisk **Usuń** na pasku narzędzi, a następnie potwierdź usunięcie połączenia.

Konfigurowanie integracji z platformą Kaspersky Automated Security Awareness Platform

Integracja z Kaspersky Automated Security Awareness Platform (dalej również KASAP) umożliwia przypisanie kursów edukacyjnych KASAP do użytkowników powiązanych z alertami.

Ustawienia integracji nie są dziedziczone i mają zastosowanie wyłącznie do Serwera administracyjnego (fizycznego lub wirtualnego), na którym konfigurujesz te ustawienia.

> Przed skonfigurowaniem integracji w Kaspersky Security Center Web Console należy utworzyć token autoryzacji i uzyskać adres URL dla żądań API w KASAP.

Aby skonfigurować integrację z platformą Kaspersky Automated Security Awareness Platform:

1. W menu głównym kliknij nazwę Serwera administracyjnego.

   Okno właściwości Serwera administracyjnego zostanie otwarte na zakładce **Ogólne**.

2. Wybierz sekcję **KASAP**.

3. W prawym panelu włącz przełącznik **Integracja KASAP**.

4. Określ ustawienia, które mają być użyte do połączenia z KASAP:

   - **Token API**—token utworzony w celu uzyskania dostępu do KASAP Open API.
   - **Adres URL**—adres URL żądań API, który uzyskałeś podczas tworzenia tokenu API.
   - **Użyj serwera proxy**—przełącznik, który włącza korzystanie z serwera proxy podczas łączenia się z KASAP.

     Domyślnie przełącznik ten jest wyłączony.

5. W razie potrzeby zweryfikuj określone ustawienia, klikając przycisk **Sprawdź połączenie**.

   Wyświetlany jest status połączenia.

6. Kliknij przycisk **Zapisz**.

Skonfigurowano integrację z Kaspersky Automated Security Awareness Platform.

Po zapisaniu ustawień integracji KASAP możesz wyświetlić listę grup edukacyjnych KASAP, klikając przycisk **Wyświetl grupy**.

Jeżeli to konieczne, po wyświetleniu listy grup możesz ją zaktualizować, klikając przycisk **Odśwież grupy**.

> Po otwarciu listy nie można jej ukryć. Jeśli wyłączysz przełącznik **Integracja KASAP**, lista grup KASAP nie będzie wyświetlana.

Konfigurowanie integracji z Kaspersky Threat Intelligence Portal Sandbox

Integracja z Kaspersky Threat Intelligence Portal (dalej również zwanym Kaspersky TIP) umożliwia wykonywanie plików przeniesionych do sekcji **Kwarantanna** przy użyciu Kaspersky Sandbox—bezpieczne środowisko odizolowane od sieci korporacyjnej.

Ustawienia integracji nie są dziedziczone i mają zastosowanie wyłącznie do Serwera administracyjnego (fizycznego lub wirtualnego), na którym konfigurujesz te ustawienia.

> Przed skonfigurowaniem integracji należy uzyskać token autoryzacyjny dla żądań API w Kaspersky TIP.

Aby skonfigurować integrację z Kaspersky TIP Sandbox:

1. W menu głównym kliknij nazwę Serwera administracyjnego.

   Okno właściwości Serwera administracyjnego zostanie otwarte na zakładce **Ogólne**.

2. Wybierz **Kaspersky TIP**.

3. W prawym panelu włącz przełącznik **Integracja**.

   Zostaną wyświetlone ustawienia połączenia z Kaspersky TIP.

   > Jeżeli po skonfigurowaniu i zapisaniu ustawień integracji wyłączysz przełącznik **Integracja**, ustawienia nie zostaną usunięte, ale nie będzie można wykonać działania reagowania.

4. Kliknij przycisk **Dodaj token** i w oknie, które zostanie otwarte, wskaż token, który wcześniej uzyskałeś w Kaspersky TIP, a następnie kliknij przycisk **Dodaj**.

   Okno zostanie zamknięte, a token API zostanie dodany.

5. Jeśli chcesz używać serwera proxy podczas łączenia się z Kaspersky TIP, włącz przełącznik **Użyj serwera proxy**.

   Domyślnie przełącznik ten jest wyłączony.

6. Kliknij przycisk **Zapisz**.

Integracja z Kaspersky TIP Sandbox została skonfigurowana.

Teraz możesz wysyłać pliki z sekcji **Kwarantanna** do Kaspersky TIP Sandbox w celu analizy zagrożeń. Maksymalny rozmiar pliku wynosi 100 MB.

Ponieważ licencja Kaspersky Next XDR Optimum obsługuje wielodostęp, pliki umieszczone w **Kwarantanna** są podzielone według dzierżawców. Podział na poziomie dzierżawcy obowiązuje również podczas przesyłania plików do Kaspersky TIP Sandbox i wyświetlania wyników, jeśli administrator używa dedykowanego konta TIP i tokena API powiązanego z każdym dzierżawcą. Centralne zarządzanie sekcją **Kwarantanna** dla wszystkich dzierżawców nie jest jednak możliwe, ponieważ lista kwarantanny nie wyświetla obiektów zgodnie z hierarchią serwera.

Grupowanie alertów według atrybutów

Agregacja alertów pomaga identyfikować alerty, które mogą dotyczyć tego samego incydentu, co upraszcza proces dochodzenia.

Aby włączyć funkcję agregacji alertów, należy wykonać następujące czynności:

- Włącz podsekcję **Alerty** w menu głównym.
- Aktywuj Serwer administracyjny w ramach licencji Kaspersky Next XDR Optimum, a następnie zainstaluj klucz licencyjny Kaspersky Next XDR Optimum w zarządzanych aplikacjach.

  Podczas korzystania z funkcjonalności Kaspersky Next XDR Optimum w ramach licencji próbnej w trybie testowym, najpierw musisz dodać podrzędny fizyczny Serwer administracyjny, a następnie aktywować ten serwer na podstawie tej licencji.

Jeśli korzystasz z licencji Kaspersky Next EDR Optimum, nie musisz aktywować aplikacji zainstalowanych na zarządzanych urządzeniach w ramach licencji Kaspersky Next XDR Optimum. Należy to zrobić tylko dla nowych urządzeń, o ile takie istnieją.
Ponieważ licencja Kaspersky Next XDR Optimum obsługuje wielodostęp, można centralnie dystrybuować klucz licencyjny do zarządzanych aplikacji. Automatyczna dystrybucja licencji do podrzędnych i wirtualnych Serwerów administracyjnych nie jest obsługiwana.

Możesz agregować alerty według nazwy urządzenia, konta lub nazwy skrótu (SHA256).

Alerty są agregowane według atrybutu tylko wtedy, gdy atrybut ten nie jest pusty.

Alerty są agregowane, jeśli mają przynajmniej jeden wspólny atrybut i występują w ciągu 24 godzin od wystąpienia jakiegokolwiek innego alertu w grupie.

Aby agregować alerty według atrybutów:

1. W menu głównym przejdź do **Monitorowanie** → **Alerty**.
2. Wykonaj jedną z poniższych czynności:
   - Włącz przełącznik **Agregacja alertów**, a następnie wybierz jeden lub więcej atrybutów, według których chcesz agregować alerty:
     - **Nazwa urządzenia**
     - **Konto**
     - **Hash pliku (SHA256)**

     Atrybuty **Nazwa urządzenia** i **Konto** są wybierane domyślnie.
   - Kliknij ikonę ustawienia (⚙). W panelu **Ustawienia tabeli**, który się otworzy, przejdź do zakładki **Grupowanie**. Wybierz **ID grupy agregacji** i kliknij **Zastosuj**.

   Po włączeniu agregacji alerty są sortowane według **Czas zdarzenia** od najnowszych do najstarszych. Dodatkowe opcje sortowania nie są obsługiwane. Wybranie innej opcji grupowania spowoduje wyłączenie agregacji.

   Tabela wyświetla alerty zagregowane według atrybutów. Alerty, które nie są zagregowane są wyświetlane na dole tabeli.

Każdy alert po agregacji jest przypisywany tylko do jednej grupy.

Cloud Discovery

Kaspersky Security Center Linux umożliwia monitorowanie korzystania z usług w chmurze na zarządzanych urządzeniach z systemem Windows i blokowanie dostępu do usług w chmurze, które użytkownik uważa za niepożądane. Program Cloud Discovery śledzi próby uzyskania dostępu do tych usług przez użytkowników zarówno za pośrednictwem przeglądarek, jak i aplikacji komputerowych. Śledzi także próby uzyskania przez użytkownika dostępu do usług w chmurze za pośrednictwem połączeń nieszyfrowanych (na przykład przy użyciu protokołu HTTP). Ta funkcja pomaga wykryć i zatrzymać korzystanie z usług w chmurze przez Shadow IT.

Możliwość blokowania jest dostępna tylko wtedy, gdy aktywowano Kaspersky Security Center Linux w ramach licencji Kaspersky Next EDR Optimum lub Kaspersky Next XDR Expert.

Możliwość blokowania jest dostępna tylko w przypadku korzystania z Kaspersky Endpoint Security 11.2 for Windows lub nowszego. Wcześniejsze wersje aplikacji zabezpieczającej umożliwiają tylko monitorowanie korzystania z usług w chmurze.

Możesz włączyć funkcję Cloud Discovery i wybrać zasady lub profile bezpieczeństwa, dla których chcesz włączyć tę funkcję. Możesz także włączyć lub wyłączyć tę funkcję oddzielnie w każdej zasadzie lub profilu bezpieczeństwa. Możesz zablokować dostęp do usług w chmurze, do których nie chcesz, aby użytkownicy mieli dostęp.

Aby móc zablokować dostęp do niechcianych usług w chmurze, upewnij się, że zostały spełnione następujące warunki:

- Używasz Kaspersky Endpoint Security 11.2 for Windows lub nowszego. Wcześniejsze wersje aplikacji zabezpieczającej umożliwiają tylko monitorowanie korzystania z usług w chmurze.
- Posiadasz warstwę licencji Kaspersky Next, która zapewnia możliwość blokowania dostępu do niechcianych usług w chmurze. Aby uzyskać szczegółowe informacje, zobacz Pomoc Kaspersky Next.

Widżet Cloud Discovery i raporty Cloud Discovery wyświetlają informacje o udanych i zablokowanych próbach uzyskania dostępu do usług w chmurze. Widżet wyświetla także poziom ryzyka każdej usługi w chmurze. Kaspersky Security Center Linux pobiera informacje o korzystaniu z usług w chmurze ze wszystkich zarządzanych urządzeń, które są chronione wyłącznie przez zasady i profile bezpieczeństwa, które mają włączoną tę funkcję.

Włączanie funkcji Cloud Discovery za pomocą widżetu

Funkcja Cloud Discovery pozwala uzyskać informacje o korzystaniu z usług w chmurze ze wszystkich zarządzanych urządzeń chronionych wyłącznie przez zasady bezpieczeństwa, które mają włączoną tę funkcję. Możesz włączyć lub wyłączyć Cloud Discovery tylko dla zasady Kaspersky Endpoint Security for Windows.

Istnieją dwa sposoby włączenia funkcji Cloud Discovery:

- Za pomocą widżetu Cloud Discovery.
- We właściwościach zasady Kaspersky Endpoint Security for Windows.

  Szczegółowe informacje na temat włączania funkcji Cloud Discovery we właściwościach zasady Kaspersky Endpoint Security for Windows można znaleźć w sekcji Cloud Discovery pomocy Kaspersky Endpoint Security for Windows.

Pamiętaj, że funkcję Cloud Discovery możesz wyłączyć wyłącznie w parametrach zasady Kaspersky Endpoint Security for Windows.

Aby włączyć Cloud Discovery, musisz mieć uprawnienia do **Zapis** w obszarze funkcjonalnym **Funkcje ogólne: funkcjonalność podstawowa**.

Aby włączyć funkcję Cloud Discovery za pomocą widżetu Cloud Discovery:

1. Przejdź do Kaspersky Security Center Linux.
2. W menu głównym przejdź do **Monitorowanie** → **Pulpit nawigacyjny**.
3. W widżecie **Cloud Discovery** kliknij przycisk **Włącz**.

   Jeśli masz zainstalowany program Kaspersky Endpoint Security for Windows w wersji 12.4, włącz funkcję Cloud Discovery we właściwościach zasady Kaspersky Endpoint Security for Windows. Aby uzyskać szczegółowe informacje, zobacz Cloud Discovery w sekcji pomocy Kaspersky Endpoint Security for Windows.

Jeżeli posiadasz Kaspersky Endpoint Security for Windows w wersji starszej niż 12.4, zaktualizuj wtyczkę Kaspersky Endpoint Security for Windows do wersji 12.5.

4. W otwartym oknie **Włącz Cloud Discovery** wybierz zasady zabezpieczeń, dla których chcesz włączyć tę funkcję, a następnie kliknij przycisk **Włącz**.

   Następujące ustawienia zasad zostaną włączone automatycznie: **Wprowadź skrypt do ruchu internetowego w celu interakcji ze stronami internetowymi**, **Monitor sesji internetowej** i **Skanowanie połączeń szyfrowanych**.

Funkcja Cloud Discovery jest włączona, a widżet zostaje dodany do pulpitu nawigacyjnego.

Dodanie widżetu Cloud Discovery do pulpitu nawigacyjnego

Do panelu kontrolnego możesz dodać widżet **Cloud Discovery**, aby monitorować wykorzystanie usług w chmurze na zarządzanych urządzeniach.

Aby dodać widżet Cloud Discovery do pulpitu nawigacyjnego, musisz mieć uprawnienie do **Zapis** w obszarze funkcjonalnym **Funkcje ogólne: funkcjonalność podstawowa**.

Aby dodać widżet Cloud Discovery do pulpitu nawigacyjnego:

1. Przejdź do Kaspersky Security Center Linux.
2. W menu głównym przejdź do **Monitorowanie** → **Pulpit nawigacyjny**.
3. Kliknij przycisk **Dodaj lub przywróć widżet sieciowy**.
4. Na liście dostępnych widżetów kliknij ikonę jodełki (>) obok kategorii **Inny**.
5. Wybierz widżet **Cloud Discovery**, a następnie kliknij przycisk **Dodaj**.

   Jeśli funkcja Cloud Discovery jest wyłączona, postępuj zgodnie z instrukcjami w sekcji Włączanie Cloud Discovery przy użyciu widżetu.

Wybrany widżet zostanie dodany na końcu pulpitu nawigacyjnego.

Przeglądanie informacji o korzystaniu z usług w chmurze

Możesz wyświetlić widżet **Cloud Discovery**, który wyświetla informacje o próbach uzyskania dostępu do usług w chmurze. Widżet wyświetla także poziom ryzyka każdej usługi w chmurze. Kaspersky Security Center Linux pobiera informacje o korzystaniu z usług w chmurze ze wszystkich zarządzanych urządzeń, które są chronione wyłącznie przez profile bezpieczeństwa, które mają włączoną tę funkcję.

Przed obejrzeniem upewnij się, że:

- Do pulpitu nawigacyjnego dodano widżet Cloud Discovery.
- Funkcja Cloud Discovery jest włączona.
- Masz uprawnienia do **Odczyt** w obszarze funkcjonalnym **Funkcje ogólne: podstawowa funkcjonalność**.

Aby wyświetlić widżet Cloud Discovery:

1. Przejdź do Kaspersky Security Center Linux.
2. W menu głównym przejdź do **Monitorowanie** → **Pulpit nawigacyjny**.

   Widżet **Cloud Discovery** zostanie wyświetlony na pulpicie nawigacyjnym.
3. Po lewej stronie widżetu **Cloud Discovery** wybierz kategorię usług w chmurze.

   W tabeli po prawej stronie widżetu wyświetlanych jest maksymalnie pięć usług z wybranej kategorii, do których użytkownicy najczęściej starają się uzyskać dostęp. Liczone są zarówno próby udane, jak i zablokowane.
4. Po prawej stronie widżetu wybierz konkretną usługę.

   Poniższa tabela przedstawia aż dziesięć urządzeń, które najczęściej podejmują próbę uzyskania dostępu do usługi. W tej tabeli można wygenerować dwa rodzaje raportów: raport dotyczący udanych prób dostępu i raport dotyczący zablokowanych prób dostępu.

   Dodatkowo w tej tabeli możesz zablokować dostęp do usługi w chmurze dla określonego urządzenia.

Widżet wyświetla żądane informacje.

W wyświetlonym widżecie możesz wykonać następujące czynności:

- Przejdź do sekcji **Monitorowanie** → **Raporty**, aby wyświetlić raporty Cloud Discovery.
- Zablokuj lub zezwól na dostęp do wybranej usługi w chmurze.

Możliwość blokowania jest dostępna tylko wtedy, gdy aktywowano Kaspersky Security Center Linux w ramach licencji Kaspersky Next EDR Optimum lub Kaspersky Next XDR Expert.

Możliwość blokowania jest dostępna tylko w przypadku korzystania z Kaspersky Endpoint Security 11.2 for Windows lub nowszego. Wcześniejsze wersje aplikacji zabezpieczającej umożliwiają tylko monitorowanie korzystania z usług w chmurze.

Poziom ryzyka usługi w chmurze

Dla każdej usługi w chmurze Cloud Discovery zapewnia informację o poziomie ryzyka. Poziom ryzyka pomaga określić, które usługi nie spełniają wymagań bezpieczeństwa Twojej organizacji. Na przykład możesz chcieć wziąć pod uwagę poziom ryzyka przy podejmowaniu decyzji o zablokowaniu dostępu do określonej usługi.

Poziom ryzyka jest wskaźnikiem szacunkowym i nie mówi nic o jakości usługi w chmurze ani o jej producencie. Poziom ryzyka to po prostu zalecenie ekspertów z Kaspersky.

Poziomy ryzyka usług w chmurze wyświetlane są w widżecie Cloud Discovery oraz na liście wszystkich monitorowanych usług w chmurze.

Blokowanie dostępu do niechcianych usług w chmurze

Możesz zablokować dostęp do usług w chmurze, do których nie chcesz, aby użytkownicy mieli dostęp. Możesz także zezwolić na dostęp do usług w chmurze, które zostały wcześniej zablokowane.

Decydując o zablokowaniu dostępu do określonej usługi, możesz między innymi wziąć pod uwagę poziom ryzyka.

Możesz zablokować lub zezwolić na dostęp do usług w chmurze w ramach zasady lub profilu bezpieczeństwa.

Istnieją dwa sposoby blokowania dostępu do niechcianych usług w chmurze:

- Za pomocą widżetu Cloud Discovery.

  W takim wypadku możesz po kolei blokować dostęp do poszczególnych usług.

- We właściwościach zasady Kaspersky Endpoint Security for Windows.

  W takim przypadku możesz blokować dostęp do usług pojedynczo lub od razu blokować całą kategorię.

  Szczegółowe informacje na temat włączania funkcji Cloud Discovery we właściwościach zasady Kaspersky Endpoint Security for Windows można znaleźć w sekcji Cloud Discovery pomocy Kaspersky Endpoint Security for Windows.

Aby zablokować lub zezwolić na dostęp do usługi w chmurze za pomocą widżetu:

1. Otwórz widżet Cloud Discovery, a następnie wybierz wymaganą usługę w chmurze.

2. Na **10 najpopularniejszych urządzeń korzystających z usługi** znajdź zasadę lub profil bezpieczeństwa, dla którego chcesz zablokować usługę lub zezwolić na nią.

3. W wymaganym wierszu, w kolumnie **Status dostępu w zasadach lub profilu** wykonaj dowolną z następujących czynności:

   - Aby zablokować usługę, wybierz **Zablokowano** z listy rozwijanej.

   - Aby zezwolić na usługę, wybierz z listy rozwijanej opcję **Dozwolony**.

4. Kliknij przycisk **Zapisz**.

Dostęp do wybranej usługi jest zablokowany lub dozwolony przez zasadę lub profil bezpieczeństwa.

Eksportowanie zdarzeń do systemów SIEM

Ta sekcja opisuje sposób skonfigurowania eksportowania zdarzeń do systemów SIEM.

Konfigurowanie eksportowania zdarzeń do systemów SIEM

Kaspersky Security Center Linux umożliwia skonfigurowanie eksportu zdarzeń do systemów SIEM przy użyciu jednej z następujących metod: eksport do dowolnego systemu SIEM korzystającego z formatu Syslog, eksport do systemów Kaspersky SIEM, QRadar, Splunk i ArcSight SIEM korzystających z formatów LEEF i CEF lub eksport zdarzeń do systemów SIEM bezpośrednio z bazy danych Kaspersky Security Center. Po zakończeniu tego scenariusza Serwer administracyjny automatycznie wysyła zdarzenia do systemu SIEM.

Wymagania wstępne

Zanim rozpoczniesz konfigurowanie eksportowania zdarzeń w Kaspersky Security Center Linux:

- Dowiedz się więcej o metodach eksportowania zdarzeń.
- Upewnij się, że posiadasz wartości ustawień systemowych.

Możesz wykonać kroki tego scenariusza w dowolnej kolejności.

Proces eksportowania zdarzeń do systemu SIEM obejmuje następujące kroki:

- **Konfigurowanie systemu SIEM do odbierania zdarzeń z Kaspersky Security Center Linux**

  Instrukcja: Konfigurowanie eksportowania zdarzeń w systemie SIEM

- **Wybieranie zdarzeń, które chcesz wyeksportować do systemu SIEM**

  Zaznacz zdarzenia, które chcesz wyeksportować do systemu SIEM. Najpierw zaznacz ogólne zdarzenia, które występują we wszystkich zarządzanych aplikacjach Kaspersky. Następnie możesz oznaczyć zdarzenia dla określonych zarządzanych aplikacji Kaspersky.

- **Konfiguracja eksportu zdarzeń do systemu SIEM**

  Można eksportować zdarzenia przy użyciu jednej z następujących metod:

  - Korzystanie z protokołów TCP, UDP lub TLS przez protokoły TCP
  - Używanie eksportowania zdarzeń bezpośrednio z bazy danych Kaspersky Security Center (zestaw widoków publicznych jest dostępny w bazie danych Kaspersky Security Center; opis tych widoków publicznych można znaleźć w dokumencie klakdb.chm)

Wyniki

Po skonfigurowaniu eksportowania zdarzeń do systemu SIEM możesz przeglądać wyniki eksportu, jeśli wybrano zdarzenia, które chcesz wyeksportować.

Czynności niezbędne do wykonania przed rozpoczęciem pracy

Podczas konfigurowania automatycznego eksportowania zdarzeń w Kaspersky Security Center Linux musisz określić niektóre ustawienia systemu SIEM. Zalecane jest wcześniejsze sprawdzenie tych ustawień w celu przygotowania do konfiguracji Kaspersky Security Center Linux.

W celu pomyślnego skonfigurowania automatycznego wysyłania zdarzeń do systemu SIEM należy znać następujące ustawienia:

- **Adres serwera systemu SIEM**

  Adres IP serwera, na którym zainstalowany jest aktualnie używany system SIEM. Sprawdź wartość tego ustawienia w ustawieniach systemu SIEM.

- **Port serwera systemu SIEM**

  Numer portu używanego do nawiązania połączenia pomiędzy Kaspersky Security Center Linux a serwerem Twojego systemu SIEM. Tę wartość należy określić w ustawieniach Kaspersky Security Center Linux i w ustawieniach odbiornika Twojego systemu SIEM.

- **Protokół**

  Protokół używany do przesyłania wiadomości z Kaspersky Security Center Linux do Twojego systemu SIEM. Tę wartość należy określić w ustawieniach Kaspersky Security Center Linux i w ustawieniach odbiornika Twojego systemu SIEM.

Informacje o eksportowaniu zdarzeń

Kaspersky Security Center Linux umożliwia otrzymywanie informacji o zdarzeniach występujących podczas działania Serwera administracyjnego i aplikacji firmy Kaspersky zainstalowanych na zarządzanych urządzeniach. Informacje o zdarzeniach są zapisywane w bazie danych Serwera administracyjnego.

Eksportowanie zdarzeń może być używane w obrębie scentralizowanych systemów, które zajmują się problemami z bezpieczeństwem na poziomie organizacyjnym i technicznym, zapewniają usługi monitorowania ochrony oraz skonsolidowane informacje z różnych rozwiązań. To są systemy SIEM, które oferują przeprowadzania w czasie rzeczywistym analizy alertów o zagrożeniach i zdarzeń zabezpieczeń, wygenerowanych przez aplikacje i sprzęt w sieci, lub Security Operation Centers (SOCs).

Te systemy otrzymują dane z wielu źródeł, w tym sieci, ochrony, serwerów, baz danych i aplikacji. Systemy SIEM oferują także funkcjonalność konsolidowania monitorowanych danych, aby pomóc w uniknięciu przeoczenia zdarzeń krytycznych. Dodatkowo, systemy przeprowadzają zautomatyzowaną analizę powiązanych zdarzeń i alertów w celu powiadomienia administratorów o nagłych problemach z bezpieczeństwem. Wysyłanie alertów może zostać zaimplementowane poprzez pulpit nawigacyjny lub wysyłanie ostrzeżeń może się odbywać poprzez kanały firm trzecich, na przykład pocztę elektroniczną.

Proces eksportowania zdarzeń z Kaspersky Security Center Linux do zewnętrznych systemów SIEM składa się na dwie części: nadawca zdarzenia – Kaspersky Security Center Linux oraz odbiorca zdarzenia – system SIEM. Aby pomyślnie eksportować zdarzenia, należy skonfigurować tę funkcję w posiadanym systemie SIEM i w Konsoli administracyjnej Kaspersky Security Center Linux. Nie ma znaczenia, która strona zostanie skonfigurowana jako pierwsza. Możesz skonfigurować przesyłanie zdarzeń w Kaspersky Security Center Linux, a następnie skonfigurować odbieranie zdarzeń przez system SIEM lub na odwrót.

Metody wysyłania zdarzeń z Kaspersky Security Center Linux

Dostępne są trzy metody wysyłania zdarzeń z Kaspersky Security Center Linux do systemów zewnętrznych:

- Wysyłanie zdarzeń po protokole Syslog do dowolnego systemu SIEM

  Korzystając z protokołu Syslog, możesz przekazywać wszelkie zdarzenia, które występują na Serwerze administracyjnym oraz w aplikacjach Kaspersky zainstalowanych na zarządzanych urządzeniach. Protokół Syslog jest standardowym protokołem rejestrowania wiadomości. Możesz go użyć do eksportowania zdarzeń do systemu SIEM.

  W tym celu należy zaznaczyć zdarzenia, które chcemy przekazać do systemu SIEM. Możesz zaznaczyć zdarzenia w konsoli Kaspersky Security Center Web Console. Tylko zaznaczone zdarzenia będą przekazywane do systemu SIEM. Jeśli nic nie zaznaczysz, żadne zdarzenia nie zostaną przekazane.

- Wysyłanie zdarzeń za pośrednictwem protokołów CEF i LEEF do systemów Kaspersky SIEM, QRadar, Splunk i ArcSight

  Możesz używać protokołów CEF i LEEF do eksportowania zdarzeń ogólnych. Podczas eksportowania zdarzeń po protokołach CEF i LEEF nie masz możliwości wyboru określonych zdarzeń do wyeksportowania. Eksportowane są wszystkie zdarzenia ogólne. Aby skonwertować zdarzenia Kaspersky Security Center Linux na zdarzenia w formacie CEF i LEEF, możesz użyć pliku siem_conversion_rules.xml. Ten plik zawiera listę atrybutów zdarzeń Kaspersky Security Center Linux i odpowiadających im atrybutów zdarzeń w formacie CEF i LEEF. Ponadto plik siem_conversion_rules.xml zawiera reguły generowania komunikatów odpowiadających zdarzeniom. To narzędzie znajduje się w pakiecie dystrybucyjnym Kaspersky Security Center Linux.

  W przeciwieństwie do protokołu Syslog, protokoły CEF i LEEF nie są uniwersalne. Protokoły CEF i LEEF są przeznaczone dla odpowiednich systemów SIEM (Kaspersky SIEM, QRadar, Splunk i ArcSight). Dlatego też, jeśli wybierzesz eksportowanie zdarzeń poprzez jeden z tych protokołów, użyjesz parsera w systemie SIEM.

- Bezpośrednio z bazy danych Kaspersky Security Center Linux do dowolnego systemu SIEM

  Ta metoda eksportowania zdarzeń może zostać użyta do odbierania zdarzeń bezpośrednio z widoków publicznych bazy danych przy użyciu zapytań SQL. Wyniki zapytań są zapisywane do pliku XML, który może zostać użyty jako dane wejściowe systemu zewnętrznego. Tylko zdarzenia dostępne w widokach publicznych mogą być eksportowane bezpośrednio z bazy danych.

Odbieranie zdarzeń przez system SIEM

System SIEM musi odbierać i poprawnie analizować zdarzenia otrzymywane z Kaspersky Security Center Linux. W tym celu należy odpowiednio skonfigurować system SIEM. Konfiguracja zależy od specyfiki używanego systemu SIEM. Jednakże istnieje kilka ogólnych kroków w konfiguracji wszystkich systemów SIEM, takie jak konfigurowanie odbiorcy i analizatora.

Informacje o konfigurowaniu eksportowania zdarzeń w systemie SIEM

Proces eksportowania zdarzeń z Kaspersky Security Center Linux do zewnętrznych systemów SIEM składa się na dwie części: nadawca zdarzenia – Kaspersky Security Center Linux oraz odbiorca zdarzenia – system SIEM. Należy skonfigurować eksportowanie zdarzeń w posiadanym systemie SIEM i w Kaspersky Security Center Linux.

Ustawienia określane w systemie SIEM zależą od określonego systemu, którego używasz. Zazwyczaj dla wszystkich systemów SIEM należy skonfigurować odbiorcę i, opcjonalnie, analizatora wiadomości do analizowania otrzymanych zdarzeń.

Konfigurowanie odbiorcy

Aby otrzymywać zdarzenia wysyłane przez Kaspersky Security Center Linux, należy skonfigurować odbiorcę w swoim systemie SIEM. W systemie SIEM powinny zostać określone następujące ustawienia:

- **Protokół eksportu**

  Protokół przesyłania komunikatów, UDP, TCP lub TLS, przez TCP. Ten protokół musi być taki sam, jak protokół, który określono w Kaspersky Security Center Linux.

- **Port**

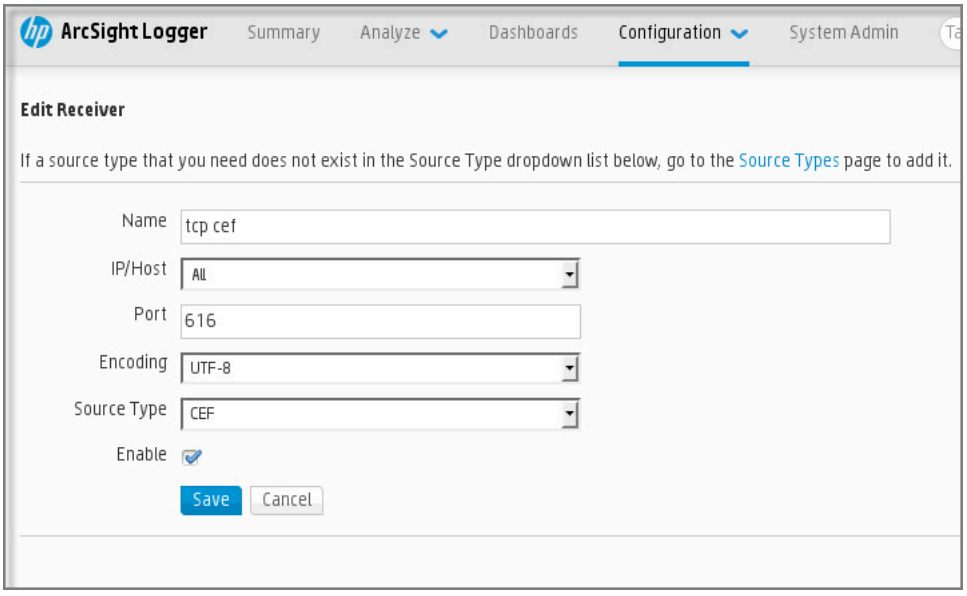
  Określ numer portu do nawiązana połączenia z Kaspersky Security Center Linux. Ten port musi być taki sam, jak port określony w Kaspersky Security Center Linux podczas konfiguracji z systemem SIEM.

- **Format danych**

  Określ format Syslog, CEF lub LEEF.

W zależności od używanego systemu SIEM, konieczne może być określenie niektórych dodatkowych ustawień odbiorcy.

Poniższy rysunek przedstawia okno konfiguracji odbiorcy w ArcSight.



Konfiguracja odbiorcy w ArcSight

Analizator wiadomości

Wyeksportowane zdarzenia są przekazywane do systemu SIEM jako wiadomości. Te wiadomości muszą być odpowiednio przeanalizowane, aby informacje na temat zdarzeń mogły być użyte przez system SIEM. Analizatory wiadomości są częścią systemu SIEM; są używane do podzielenia zawartości wiadomości na odpowiednie pola, takie jak: identyfikator zdarzenia, priorytet, opis, parametry itd. Umożliwia to systemowi SIEM przetworzenie zdarzeń otrzymanych z Kaspersky Security Center Linux tak, aby mogły być przechowywane w bazie danych systemu SIEM.

Informacje dotyczące eksportowania zdarzeń przy użyciu formatów CEF i LEEF

Możesz użyć formatów CEF i LEEF, aby wyeksportować do systemów SIEM ogólne zdarzenia, zdarzenia dotyczące zmian zasad oraz zdarzenia przesyłane przez aplikacje Kaspersky do Serwera administracyjnego. Zestaw eksportowanych zdarzeń jest predefiniowany i nie możesz wybrać zdarzeń do wyeksportowania. Przed wysłaniem zdarzeń do systemu SIEM (Kaspersky SIEM, QRadar, ArcSight lub Splunk) należy przekonwertować zdarzenia Kaspersky Security Center Linux na zdarzenia w formatach CEF i LEEF przy użyciu reguł określonych w pliku siem_conversion_rules.xml.

Wybierz format eksportowania w oparciu o używany system SIEM. Poniższa tabela wyświetla systemy SIEM i odpowiadające im formaty eksportu.

Formaty eksportowania zdarzenia do systemu SIEM

System SIEM	Format eksportu
Kaspersky SIEM	CEF
ArcSight	CEF
Splunk	CEF
QRadar	LEEF

- LEEF (Log Event Extended Format) - dostosowany format zdarzeń dla IBM Security QRadar SIEM. QRadar może integrować, identyfikować i przetwarzać zdarzenia LEEF. Zdarzenia LEEF muszą używać kodowania UTF-8. Szczegółowe informacje na temat protokołu LEEF można znaleźć w Centrum wiedzy IBM.

- CEF (Common Event Format)—standard zarządzania dziennikami, który ulepsza współdziałanie zdarzeń dotyczących bezpieczeństwa między różnymi urządzeniami i aplikacjami sieciowymi i zabezpieczającymi. CEF umożliwia korzystanie z podstawowego formatu dziennika zdarzeń, co ułatwia integrowanie i gromadzenie danych do analizy przez system zarządzania korporacji. Zdarzenia CEF muszą używać kodowania UTF-8.

Automatyczne eksportowanie oznacza, że Kaspersky Security Center Linux wysyła ogólne zdarzenia do systemu SIEM. Automatyczne eksportowanie zdarzeń rozpoczyna się od razu po włączeniu tej opcji. Ta sekcja szczegółowo wyjaśnia, jak włączyć automatyczne eksportowanie zdarzeń.

Konwersja zdarzeń do formatu CEF lub LEEF

Przed wysłaniem zdarzeń do systemu SIEM (Kaspersky SIEM, QRadar, ArcSight lub Splunk) należy przekształcić zdarzenia Kaspersky Security Center Linux w zdarzenia w formacie CEF i LEEF przy użyciu reguł określonych w pliku siem_conversion_rules.xml. To narzędzie znajduje się w pakiecie dystrybucyjnym Kaspersky Security Center Linux.

Plik siem_conversion_rules.xml zawiera predefiniowane reguły interpretacji umożliwiające konwersję zdarzeń do formatu CEF i LEEF. Jeśli chcesz użyć dodatkowych reguł interpretacji zdarzeń, możesz dodać je do pliku ręcznie.

Plik siem_conversion_rules.xml zawiera następujące sekcje:

- `<product name="SP_QRADAR" vendor="IBM">`

  Ta sekcja zawiera reguły generowania zdarzeń w formacie LEEF, które można wyeksportować do systemu QRadar SIEM.

- `<product name="SP_ARCSIGHT" vendor="HP">`.

  Ta sekcja zawiera reguły generowania zdarzeń w formacie CEF, które można wyeksportować do systemu ArcSight lub Splunk SIEM.

- `<product name="Kaspersky SIEM" vendor="Kaspersky">`.

  Ta sekcja zawiera reguły generowania zdarzeń w formacie CEF, które można wyeksportować do KUMA.

Każda sekcja ma podsekcję `<common>`, w której znajdują się atrybuty zdarzeń Kaspersky Security Center Linux i odpowiadające im atrybuty zdarzeń w formacie LEEF. Te wspólne atrybuty są używane dla wszystkich typów zdarzeń, które można eksportować.

Ponadto każda sekcja ma podsekcje `<event>`. Każda podsekcja `<event>` zawiera dodatkowe atrybuty, które są dodawane do tych wymienionych w sekcji `<common>`.

Możesz ręcznie dodać nową regułę generowania zdarzeń do pliku siem_conversion_rules.xml.

Aby dodać nową regułę generowania zdarzeń:

1. Dodaj nową podsekcję `<event>` do sekcji `<product name="SP_QRADAR" vendor="IBM">`, `<product name="SP_QRADAR" vendor="IBM">` lub `<product name="Kaspersky SIEM" vendor="Kaspersky">`, a następnie w razie potrzeby określ dodatkowe atrybuty zdarzenia.

2. Jeżeli zdarzenie składa się wyłącznie ze wspólnych atrybutów, podsekcja `<event>` będzie pusta.

siem_conversion_rules.xml

```
<conversion_rules>
    <product name="SP_QRADAR" vendor="IBM">
        <common> <!-- Common Kaspersky Security Center Linux event attributes and corresponding LEEF event
attributes -->
            <param name="KLSPLG_HOST_DISP_NAME" type="STRING_T">
                <attr name="EVC_EV_DISP_HOST_NAME" type="AT_STRING" limit="255"/>
            </param>
            ...
        </common>
        <event id="GNRL_EV_VIRUS_FOUND"> <!-- Generation rule for the GNRL_EV_VIRUS_FOUND event with additional
attributes -->
            <param name="GNRL_EA_PARAM_1" type="STRING_T">
                <attr name="EVC_EV_SHA256" type="AT_STRING" limit="255"/>
            </param>
            ...
        </event>
...
</product>
    <product name="SP_ARCSIGHT" vendor="HP">
        <common> <!-- Common Kaspersky Security Center Linux event attributes and corresponding LEEF event
attributes -->
            <param name="KLSPLG_HOST_DISP_NAME" type="STRING_T">
                <attr name="dhost" type="AT_STRING" limit="1023"/>
            </param>
            ...
        </common>
        <event id="GNRL_EV_VIRUS_FOUND">
            <param name="GNRL_EA_PARAM_1" type="STRING_T">
                <attr name="cs4" type="AT_STRING" limit="255"/>
```

```
                <attr name="cs4Label" type="AT_STRING" val="SHA256"/>
            </param>
            ...
</product>
    <product name="Kaspersky SIEM" vendor="Kaspersky">
        <common> <!-- Common Kaspersky Security Center Linux event attributes and corresponding LEEF event
attributes -->
            <param name="KLSPLG_HOST_DISP_NAME" type="STRING_T">
                <attr name="dhost" type="AT_STRING" limit="1023"/>
            </param>
            ...
        </common>
        <event id="GNRL_EV_VIRUS_FOUND">
            <param name="GNRL_EA_PARAM_1" type="STRING_T">
                <attr name="cs4" type="AT_STRING" limit="255"/>
                <attr name="cs4Label" type="AT_STRING" val="SHA256"/>
            </param>
            ...
</product>
</conversion_rules>
```

Oznaczenie zdarzeń do wyeksportowania do systemów SIEM w formacie Syslog

Po włączeniu automatycznego eksportowania zdarzeń, należy wskazać zdarzenia, które zostaną wyeksportowane do zewnętrznego systemu SIEM.

Możesz skonfigurować eksportowanie zdarzeń w formacie Syslog do zewnętrznego systemu w oparciu o jeden z następujących warunków:

- Oznaczanie zdarzeń ogólnych. Jeśli zdarzenia do wyeksportowania oznaczysz w zasadzie, w ustawieniach zdarzenia lub w ustawieniach Serwera administracyjnego system SIEM otrzyma oznaczone zdarzenia, które wystąpiły we wszystkich aplikacjach zarządzanych przez określoną zasadę. Jeśli wyeksportowane zdarzenia były wybrane w zasadzie, nie będziesz mógł ich ponownie zdefiniować dla aplikacji zarządzanej przez tą zasadę.

- Oznaczanie zdarzeń dla zarządzanej aplikacji. Jeśli oznaczysz zdarzenia do wyeksportowania dla zarządzanej aplikacji, zainstalowanej na zarządzanym urządzeniu, system SIEM otrzyma tylko zdarzenia, które wystąpiły w tej aplikacji.

W przypadku zdarzeń zmiany zasady możesz tylko włączyć lub wyłączyć eksportowanie wszystkich takich zdarzeń do systemu SIEM.

Oznaczanie zdarzeń aplikacji Kaspersky do eksportowania w formacie Syslog

Jeśli chcesz wyeksportować zdarzenia, które wystąpiły w określonej zarządzanej aplikacji, zainstalowanej na zarządzanych urządzeniach, w zasadzie aplikacji oznacz zdarzenia do wyeksportowania. W takim przypadku zaznaczone zdarzenia są eksportowane ze wszystkich urządzeń objętych zakresem zasady.

W celu oznaczenia zdarzeń do wyeksportowania dla określonej zarządzanej aplikacji:

1. W menu głównym przejdź do **Zarządzanie zasobami** → **Zasady**.

2. Kliknij zasadę aplikacji, dla której chcesz oznaczyć zdarzenia.

   Zostanie otwarte okno ustawień zasady.

3. Przejdź do sekcji **Konfiguracja zdarzenia**.

4. Zaznacz pola obok zdarzeń, które chcesz wyeksportować do systemu SIEM.

5. Kliknij przycisk **Zaznacz do eksportu do systemu SIEM poprzez Dziennik systemowy**.

   Możesz także oznaczyć zdarzenie do wyeksportowania do systemu SIEM w sekcji **Rejestracja zdarzenia**, która zostanie otwarta po kliknięciu odnośnika zdarzenia.

6. Znacznik (✓) pojawi się w kolumnie **Dziennik systemowy** zdarzenia lub zdarzeń, które oznaczyłeś do wyeksportowania do systemu SIEM.

7. Kliknij przycisk **Zapisz**.

Oznaczone zdarzenia z zarządzanej aplikacji są gotowe do wyeksportowania do systemu SIEM.

Możesz zaznaczyć, które zdarzenia wyeksportować do systemu SIEM dla określonego zarządzanego urządzenia. Jeśli poprzednio wyeksportowane zdarzenia były oznaczone w zasadzie aplikacji, nie będziesz mógł ponownie zdefiniować oznaczonych zdarzeń dla zarządzanego urządzenia.

W celu oznaczenia zdarzeń do wyeksportowania dla zarządzanego urządzenia:

1. W menu głównym przejdź do **Zarządzanie zasobami** → **Zasoby (urządzenia)**.

   Zostanie wyświetlona lista zarządzanych urządzeń.

2. Kliknij odnośnik z nazwą żądanego urządzenia na liście zarządzanych urządzeń.

   Zostanie wyświetlone okno właściwości wybranego urządzenia.

3. Przejdź do sekcji **Aplikacje**.

4. Kliknij odnośnik z nazwą żądanej aplikacji na liście aplikacji.

5. Przejdź do sekcji **Konfiguracja zdarzenia**.

6. Zaznacz pola obok zdarzeń, które chcesz wyeksportować do SIEM.

7. Kliknij przycisk **Zaznacz do eksportu do systemu SIEM poprzez Dziennik systemowy**.

   Dodatkowo, możesz oznaczyć zdarzenie do wyeksportowania do systemu SIEM w sekcji **Rejestracja zdarzenia**, która zostanie otwarta po kliknięciu odnośnika zdarzenia.

8. Znacznik (✓) pojawi się w kolumnie **Dziennik systemowy** zdarzenia lub zdarzeń, które oznaczyłeś do wyeksportowania do systemu SIEM.

Od tego momentu Serwer administracyjny wysyła do systemu SIEM oznaczone zdarzenia, jeśli eksportowanie do systemu SIEM zostało skonfigurowane.

Oznaczanie ogólnych zdarzeń do eksportu w formacie Syslog

Możesz oznaczyć zdarzenia ogólne, które Serwer administracyjny wyeksportuje do systemów SIEM przy użyciu formatu Syslog.

W celu oznaczenia zdarzeń ogólnych do wyeksportowania do systemu SIEM:

1. W menu głównym wykonaj jedną z następujących czynności:
   - Kliknij nazwę Serwera administracyjnego.
   - W menu głównym przejdź do **Zarządzanie zasobami** → **Zasady**, a następnie kliknij odnośnik do zasady.
2. W otwartym oknie przejdź na zakładkę **Konfiguracja zdarzenia**.
3. Kliknij **Zaznacz do eksportu do systemu SIEM poprzez Dziennik systemowy**.

   Dodatkowo, możesz oznaczyć zdarzenie do wyeksportowania do systemu SIEM w sekcji **Rejestracja zdarzenia**, która zostanie otwarta po kliknięciu odnośnika zdarzenia.

4. Znacznik (✓) pojawi się w kolumnie **Dziennik systemowy** zdarzenia lub zdarzeń, które oznaczyłeś do wyeksportowania do systemu SIEM.

Od tego momentu Serwer administracyjny wysyła do systemu SIEM oznaczone zdarzenia, jeśli eksportowanie do systemu SIEM zostało skonfigurowane.

Informacje dotyczące eksportowania zdarzeń przy użyciu formatu Syslog

Możesz użyć formatu Syslog do wyeksportowania do systemów SIEM zdarzeń, które występują na Serwerze administracyjnym i w innych aplikacjach firmy Kaspersky, zainstalowanych na zarządzanych urządzeniach.

Protokół Syslog jest standardowym protokołem rejestrowania wiadomości. Pozwala on na rozdzielenie oprogramowania, które generuje wiadomości, systemu, które je przechowuje, oraz oprogramowania, które raportuje i analizuje te wiadomości. Do każdej wiadomości przypisywany jest kod funkcji, wskazujący typ oprogramowania, które generuje wiadomość, oraz priorytet.

Format Syslog jest definiowany przez dokumenty RFC (Request for Comments — prośba o komentarze), publikowane przez Internet Engineering Task Force (standardy internetowe). Standard RFC 5424 jest używany do eksportowania zdarzeń z Kaspersky Security Center Linux do systemów zewnętrznych.

W Kaspersky Security Center Linux możesz skonfigurować eksportowanie zdarzeń do systemów zewnętrznych przy użyciu formatu Syslog.

Proces eksportowania składa się z dwóch etapów:

1. Włączanie automatycznego eksportowania zdarzeń. W tym kroku program Kaspersky Security Center Linux jest konfigurowany tak, aby wysyłał zdarzenia do systemu SIEM. Kaspersky Security Center Linux rozpoczyna wysyłanie zdarzeń natychmiast po włączeniu automatycznego eksportowania.
2. Wybieranie zdarzeń eksportowanych do systemu zewnętrznego. W tym kroku wybierasz zdarzenia, które będą eksportowane do systemu SIEM.

Konfigurowanie Kaspersky Security Center Linux do wyeksportowania zdarzeń do systemu SIEM

Aby wyeksportować zdarzenia do systemu SIEM, musisz skonfigurować proces eksportu w Kaspersky Security Center Linux.

Przed wysłaniem zdarzeń do systemu SIEM (Kaspersky SIEM, QRadar, ArcSight lub Splunk) należy przekształcić zdarzenia Kaspersky Security Center Linux w zdarzenia w formacie CEF i LEEF przy użyciu reguł określonych w pliku siem_conversion_rules.xml.

W celu skonfigurowania eksportowania do systemów SIEM w Kaspersky Security Center Web Console:

1. W menu głównym kliknij nazwę Serwera administracyjnego.

   Zostanie otwarte okno właściwości Serwera administracyjnego.

2. Na karcie **Ogólne** wybierz sekcję **Eksportuj do SIEM**.

3. Kliknij odnośnik **Ustawienia**.

   Zostanie otwarta sekcja **Eksportuj ustawienia**.

4. W sekcji **Eksportuj ustawienia** określ ustawienia:

   - **Adres serwera systemu SIEM**

     Adres IP serwera, na którym zainstalowany jest aktualnie używany system SIEM. Sprawdź wartość tego ustawienia w ustawieniach systemu SIEM.

   - **Port systemu SIEM**

     Numer portu używanego do nawiązania połączenia pomiędzy Kaspersky Security Center Linux a serwerem Twojego systemu SIEM. Tę wartość należy określić w ustawieniach Kaspersky Security Center Linux i w ustawieniach odbiornika Twojego systemu SIEM.

   - **Protokół**

     Wybierz protokół, który będzie używany do przesyłania wiadomości do systemu SIEM. Możesz wybrać protokół TCP, UDP lub TLS poprzez protokół TCP.

     Określ następujące ustawienia TLS, jeśli wybierzesz TLS poprzez protokół TCP:

     - **Uwierzytelnianie serwera**

W polu **Uwierzytelnianie serwera** możesz wybrać wartości **Zaufane certyfikaty** lub **Odciski palców SHA**:

- **Zaufane certyfikaty**. Możesz otrzymać kompletny łańcuch certyfikatów (włącznie z certyfikatem głównym) od zaufanych urzędów certyfikacji (CA) i przesłać plik do Kaspersky Security Center Linux. Kaspersky Security Center Linux sprawdza, czy łańcuch certyfikatów serwera systemu SIEM jest również podpisany przez zaufany urząd certyfikacji, czy nie.

  Aby dodać zaufany certyfikat, kliknij przycisk **Przeglądaj w poszukiwaniu pliku certyfikatów urzędu certyfikacji**, a następnie prześlij certyfikat.

- **Odciski palców SHA**. Możesz określić odciski palców SHA1 całego łańcucha certyfikatów systemu SIEM (w tym certyfikatu głównego) w Kaspersky Security Center Linux. Aby dodać odcisk palca SHA1, wprowadź go w polu **Odciski kciuka** palców, a następnie kliknij przycisk **Dodaj**.

Korzystając z ustawienia **Dodaj uwierzytelnianie klienta**, możesz wygenerować certyfikat do uwierzytelnienia Kaspersky Security Center Linux. W ten sposób będziesz używać certyfikatu z podpisem własnym wystawionego przez Kaspersky Security Center Linux. W takim przypadku do uwierzytelnienia serwera systemu SIEM można użyć zarówno zaufanego certyfikatu, jak i odcisku palca SHA.

- **Dodaj nazwę podmiotu / nazwę alternatywną podmiotu**

  Nazwa podmiotu to nazwa domeny, dla której otrzymano certyfikat. Kaspersky Security Center Linux nie może połączyć się z serwerem systemu SIEM, jeśli nazwa domeny serwera systemu SIEM nie jest zgodna z nazwą podmiotu certyfikatu serwera systemu SIEM. Jednak serwer systemu SIEM może zmienić swoją nazwę domeny, jeśli zmieniła się nazwa w certyfikacie. W takim przypadku można określić nazwy podmiotów w polu **Dodaj nazwę podmiotu / nazwę alternatywną podmiotu**. Jeśli dowolna z podanych nazw podmiotów odpowiada nazwie podmiotu certyfikatu systemu SIEM, Kaspersky Security Center Linux zweryfikuje certyfikat serwera systemu SIEM.

- **Dodaj uwierzytelnianie klienta**

  W celu uwierzytelnienia klienta możesz wstawić swój certyfikat lub wygenerować go w Kaspersky Security Center Linux.

  - **Wstaw certyfikat**. Możesz użyć certyfikatu otrzymanego z dowolnego źródła, na przykład, z dowolnego zaufanego urzędu certyfikacji. Musisz określić certyfikat i jego klucz prywatny, używając jednego z następujących typów certyfikatów:

    - **Certyfikat X.509 PEM**. Prześlij plik z certyfikatem w polu **Plik z certyfikatem** oraz plik z kluczem prywatnym w polu **Plik z kluczem**. Oba pliki nie są od siebie zależne, a kolejność wczytywania plików nie ma znaczenia. Po przesłaniu obu plików określ hasło do dekodowania klucza prywatnego w polu **Weryfikacja hasła lub certyfikatu**. Hasło może mieć pustą wartość, jeśli klucz prywatny nie jest zakodowany.

    - **Certyfikat X.509 PKCS12**. Prześlij pojedynczy plik zawierający certyfikat i jego klucz prywatny w polu **Plik z certyfikatem**. Po przesłaniu pliku określ hasło do dekodowania klucza prywatnego w polu **Weryfikacja hasła lub certyfikatu**. Hasło może mieć pustą wartość, jeśli klucz prywatny nie jest zakodowany.

  - **Generuj klucz**. Możesz wygenerować certyfikat z podpisem własnym w Kaspersky Security Center Linux. W rezultacie Kaspersky Security Center Linux przechowuje wygenerowany certyfikat z podpisem własnym i możesz przekazać publiczną część certyfikatu lub odcisk palca SHA1 do systemu SIEM.

- **Format danych**

  Możesz wybrać formaty Kaspersky SIEM, IBM QRadar SIEM, ArcSight, Splunk lub dziennik systemowy, w zależności od wymagań systemu SIEM.

  Jeśli wybierzesz Format danych dziennika systemu, musisz określić **Maksymalny rozmiar wiadomości, w bajtach**

  Określ maksymalny rozmiar (w bajtach) jednej wiadomości przekazywanej do systemu SIEM. Każde zdarzenie jest przesyłane w jednej wiadomości. Jeśli rzeczywisty rozmiar wiadomości przekracza określoną wartość, wiadomość jest skracana i dane mogą zostać utracone. Domyślny rozmiar to 2048 bajtów. To pole jest dostępne tylko wtedy, gdy w polu **Protokół** wybrałeś format System log.

5. Jeśli chcesz, możesz wyeksportować zarchiwizowane zdarzenia z bazy danych Serwera administracyjnego i ustawić datę początkową, od której chcesz rozpocząć eksport zarchiwizowanych zdarzeń:

   a. Kliknij łącze **Wybierz datę rozpoczęcia eksportu** łącza.

   b. W otwartej sekcji określ datę rozpoczęcia w polu **Data rozpoczęcia eksportu od**.

   c. Kliknij przycisk **OK**.

6. Włącz opcję **Eksportuj zdarzenia do SIEM**.

7. Aby wysyłać zdarzenia dotyczące zmian zasad do systemu SIEM, włącz opcję **Eksportuj rozszerzone zdarzenia dla zmian zasady do SIEM**. Dla każdego zmienionego ustawienia zasady zostanie wysłane do SIEM osobne zdarzenie.

8. Aby sprawdzić, czy połączenie z systemem SIEM zostało skonfigurowane, kliknij przycisk **Sprawdź połączenie**.

   Nawiązywane jest połączenie z serwerem systemu SIEM i wysyłane jest zdarzenie testowe. Zostanie wyświetlony stan połączenia.

9. Kliknij przycisk **Zapisz**.

Eksportowanie do systemu SIEM zostało skonfigurowane. Od teraz, jeśli skonfigurowano odbieranie zdarzeń w systemie SIEM, Serwer administracyjny eksportuje zaznaczone zdarzenia lub zdarzenia dotyczące zmian zasad do systemu SIEM. Jeśli ustawisz datę rozpoczęcia eksportu, Serwer administracyjny wyeksportuje również zaznaczone zdarzenia przechowywane w bazie danych Serwera administracyjnego od określonej daty.

Monitorowanie zmian zasad i profilów zasad

Gdy ustawienie zasady zostanie zmienione, generowane jest zdarzenie zmiany zasady, które można następnie wyeksportować do systemu SIEM, aby monitorować zmiany zasady i generować alerty. Dostęp do zdarzeń zmiany zasad można uzyskać wyłącznie za pośrednictwem systemu SIEM.

Zdarzenia zmiany zasad nie są przechowywane w bazie danych Serwera administracyjnego po wygenerowaniu i nie można ich wyświetlać w sekcji **Monitorowanie** → **Wybory zdarzeń** Kaspersky Security Center Web Console. Nie można również określić ustawień powiadomień ani ustawień przechowywania dla tych zdarzeń na karcie **Konfiguracja zdarzenia**.

Podczas tworzenia zasady dla każdego jej ustawienia generowane jest zdarzenie zmiany zasady. Po zmianie zasady zdarzenie zmiany zasady jest generowane dla każdego zmienionego ustawienia tej zasady. Usunięcie zasady generuje jedno zdarzenie. Na przykład utworzenie zasady Kaspersky Security Center generuje około 1000 zdarzeń, a utworzenie zasady Kaspersky Endpoint Security — ponad 7000 zdarzeń.

Warunki generowania zdarzeń zmiany zasad

Zdarzenia zmiany zasad są tworzone w następujących przypadkach:

- Utworzenie, zmodyfikowanie lub usunięcie zasad dla następujących aplikacji:
  - Agent sieciowy Kaspersky Security Center
  - Serwer administracyjny Kaspersky Security Center
  - Kaspersky Endpoint Security for Windows 14.1
  - Kaspersky Endpoint Security for Linux 12.5
  - Kaspersky Endpoint Security for Linux 12.4
  - Kaspersky Endpoint Security for Mac 12.2.1
- Opcja **Eksportuj rozszerzone zdarzenia dla zmian zasady do SIEM** we właściwościach Serwera administracyjnego jest włączona.
- Zasada jest modyfikowana ręcznie za pomocą interfejsu Kaspersky Security Center Web Console.

Zdarzenia zmiany zasad nie są tworzone w następujących przypadkach:

- Ogólne ustawienia zasady są modyfikowane.
- Ustawienia zasady odziedziczone z zasady nadrzędnej są modyfikowane.
- Ustawienia zasady są modyfikowane za pośrednictwem Kaspersky Security Center OpenAPI.
- Ustawienia aplikacji Kaspersky są modyfikowane bezpośrednio w aplikacji.

Pola zdarzeń zmiany zasad

Poniższa tabela przedstawia zestaw pól zdarzeń zmiany zasad. Sposób przedstawienia tych pól zależy od formatu zdarzenia wyjściowego (na przykład Syslog, CEF lub LEEF). Dokładne nazwy pól i szablony zdarzeń można znaleźć w pliku siem_conversion_rules.xml. Parametry zdarzeń są dostępne tylko w języku angielskim.

Pole zdarzenia	Typ danych	Opis
`eventType`	ciąg znaków	Typ zdarzenia. Umożliwia tworzenie reguł korelacji dla określonego typu zdarzenia. Możliwe wartości: „Utworzono zasadę”, „Zmodyfikowano zasadę”, „Usunięto zasadę”.
`srvName`	ciąg znaków	Nazwa Serwera administracyjnego.
`eventTime`	data i godzina	Data i godzina zdarzenia (w UTC).
`eventGroupID`	liczba całkowita	Identyfikator grupy zdarzeń modyfikacji.

`objectID`	liczba całkowita	Wewnętrzny identyfikator obiektu.
`objectName`	ciąg znaków	Wyświetlana nazwa zasady.
`objectGroup`	ciąg znaków	Pełna ścieżka i nazwa grupy administracyjnej zawierającej zasadę.
`user`	ciąg znaków	Nazwa użytkownika, który wprowadził modyfikację.
`operation`	ciąg znaków	Typ modyfikacji parametru. Możliwe wartości: „Added”, „Removed”, „Changed”.
`path`	ciąg znaków	Ścieżka parametru. Zawiera ścieżkę do węzła nadrzędnego parametru końcowego. Ścieżka jest tworzona na podstawie nazw sekcji i podsekcji zasady. Struktura ścieżki jest identyczna ze strukturą opisaną w sekcjach Ustawienia zasady Agenta sieciowego, Ogólne ustawienia zasady i Porównywanie wersji zasady.
`parameter`	ciąg znaków	Nazwa parametru końcowego.
`oldValue`	ciąg znaków	Stara wartość parametru końcowego.
`newValue`	ciąg znaków	Nowa wartość parametru końcowego.

Eksportowanie zdarzeń bezpośrednio z bazy danych

Zdarzenia można otrzymywać bezpośrednio z bazy danych Kaspersky Security Center Linux bez konieczności korzystania z interfejsu Kaspersky Security Center Linux. Możesz wykonać zapytanie bezpośrednio do widoków publicznych i pobrać dane zdarzenia lub utworzyć swoje własne widoki w oparciu o istniejące widoki publiczne i adresować je w celu otrzymania żądanych danych.

Widoki publiczne

Dla Twojej wygody, w bazie danych Kaspersky Security Center Linux dostępny jest zestaw widoków publicznych. Opis tych widoków publicznych można znaleźć w dokumentacji klakdb.chm.

Widok publiczny v_akpub_ev_event zawiera zestaw pól, które reprezentują parametry zdarzenia w bazie danych. W dokumencie klakdb.chm możesz także znaleźć informacje dotyczące widoków publicznych odpowiadających innym obiektom Kaspersky Security Center Linux, na przykład: urządzeniom, aplikacjom lub użytkownikom. Możesz użyć tych informacji w swoich zapytaniach.

Ta sekcja zawiera instrukcje dotyczące tworzenia zapytania SQL przy użyciu narzędzia klsql2 oraz przykłady zapytań.

Aby utworzyć zapytania SQL lub widoki bazy danych, możesz także użyć innego dowolnego programu do pracy z bazami danych. Informacje dotyczące przeglądania parametrów połączenia z bazą danych Kaspersky Security Center Linux, takich jak nazwa instancji i nazwa bazy danych, znajdują się w odpowiedniej sekcji.

Tworzenie zapytania SQL przy użyciu narzędzia klsql2

W tym artykule opisano sposób korzystania z narzędzia klsql2 i tworzenia zapytania SQL z użyciem tego narzędzia. Użyj wersji narzędzia klsql2 zawartej w zainstalowanej wersji Kaspersky Security Center Linux.

W celu użycia narzędzia klsql2:

1. Przejdź do katalogu, w którym zainstalowany jest Serwer administracyjny. Domyślna ścieżka instalacji to /opt/kaspersky/ksc64/sbin.

2. W tym katalogu utwórz pusty plik z rozszerzeniem .sql.

3. Otwórz utworzony plik .sql w dowolnym edytorze tekstu.

4. W pliku .sql wpisz typ żądanego zapytania SQL, a następnie zapisz plik.

5. Na urządzeniu z zainstalowanym Serwerem administracyjnym, w wierszu polecenia wpisz następujące polecenie do uruchomienia zapytania SQL z pliku .sql i zapisz wyniki do pliku result.xml:
   ```
   sudo ./klsql2 -i src.sql -u <nazwa użytkownika> -p <hasło> -o result.xml
   ```
   gdzie `<nazwa użytkownika>` i `<hasło>` to poświadczenia konta użytkownika, który ma dostęp do bazy danych.

6. W razie potrzeby wprowadź login i hasło konta użytkownika, który ma dostęp do bazy danych.

7. Otwórz nowo utworzony plik result.xml, aby wyświetlić wyniki zapytania SQL.

Możesz zmodyfikować plik .sql i utworzyć dowolne zapytanie SQL do widoków publicznych. Następnie, z poziomu wiersza poleceń, wykonaj zapytanie i zapisz wyniki do pliku.

Przykład zapytania SQL w narzędziu klsql2

W tej sekcji przedstawiono przykład zapytania SQL tworzonego przy użyciu narzędzia klsql2.

Poniższe przykłady ilustrują otrzymanie zdarzeń, które wystąpiły na urządzeniach w ciągu ostatnich siedmiu dni, oraz wyświetlenie zdarzeń według czasu ich wystąpienia. Najnowsze zdarzenia są wyświetlane jako pierwsze.

Przykład dla PostgreSQL:

```
SELECT
  /* identyfikator zdarzenia */
  "e"."nId",

  /* godzina wystąpienia zdarzenia */
  "e"."tmRiseTime",

  /* wewnętrzna nazwa typu zdarzenia */
  "e"."strEventType",

  /* wyświetlona nazwa zdarzenia */
  "e"."wstrEventTypeDisplayName",

  /* wyświetlony opis zdarzenia */
  "e"."wstrDescription",

  /* wyświetlony opis zdarzenia */
  "e"."wstrGroupName",

  /* wyświetlona nazwa urządzenia, na którym wystąpiło zdarzenie */
  "h"."wstrDisplayName",
  (
    CAST((("h"."nIp" / 16777216 )& 255 ) AS VARCHAR(4)) || '.' ||
    CAST((("h"."nIp" / 65536 )& 255 ) AS VARCHAR(4)) || '.' ||
    CAST((("h"."nIp" / 256 )& 255 ) AS VARCHAR(4)) || '.' ||

    /* adres IP urządzenia, na którym wystąpiło zdarzenie */
    CAST(("h"."nIp" )& 255 ) AS VARCHAR(4))
  ) AS "strIp"
FROM "v_akpub_ev_event" AS "e"
  INNER JOIN "v_akpub_host" AS "h" ON "h"."nId" = "e"."nHostId"
WHERE "e"."tmRiseTime" >= NOW() AT TIME ZONE 'utc' + make_interval(days => CAST(-7 AS INT))
ORDER BY "e"."tmRiseTime" DESC ;
```

Przykład dla MySQL lub MariaDB:

```
SELECT

  /* identyfikator zdarzenia */
  `e`.`nId`,

  /* godzina wystąpienia zdarzenia */
  `e`.`tmRiseTime`,

  /* wewnętrzna nazwa typu zdarzenia */
  `e`.`strEventType`,

  /* wyświetlona nazwa zdarzenia */
  `e`.`wstrEventTypeDisplayName`,

  /* wyświetlony opis zdarzenia */
  `e`.`wstrDescription`,

  /* nazwa grupy urządzeń */
  `e`.`wstrGroupName`,

  /* wyświetlona nazwa urządzenia, na którym wystąpiło zdarzenie */
  `h`.`wstrDisplayName`,
  CONCAT(
    LEFT(CAST((`h`.`nIp` DIV 1677721) & 255) AS CHAR), 4), '.',
    LEFT(CAST((`h`.`nIp` DIV 65536) & 255) AS CHAR), 4), '.',
    LEFT(CAST((`h`.`nIp` DIV 256) & 255) AS CHAR), 4), '.',

    /* adres IP urządzenia, na którym wystąpiło zdarzenie */
    LEFT(CAST((`h`.`nIp`) & 255) AS CHAR), 4)
  ) AS `strIp`
FROM `v_akpub_ev_event` AS `e`
  INNER JOIN `v_akpub_host` AS `h` ON `h`.`nId` = `e`.`nHostId`
WHERE `e`.`tmRiseTime` >= ADDDATE( UTC_TIMESTAMP( ) , INTERVAL -7 DAY)
ORDER BY `e`.`tmRiseTime` DESC ;
```

Sprawdzanie nazwy bazy danych Kaspersky Security Center Linux

Jeśli chcesz uzyskać dostęp do bazy danych Kaspersky Security Center Linux przy użyciu narzędzi do zarządzania serwerem MySQL lub bazą danych MySQL lub MariaDB, musisz znać nazwę bazy danych, aby nawiązać z nią połączenie z poziomu swojego edytora skryptów SQL.

W celu wyświetlenia nazwy bazy danych Kaspersky Security Center Linux:

1. W menu głównym kliknij nazwę Serwera administracyjnego.

   Zostanie otwarte okno właściwości Serwera administracyjnego.

2. Na karcie **Ogólne** wybierz sekcję **Szczegóły bieżącej bazy danych**.

   Nazwa bazy danych jest określona w polu **Nazwa bazy danych**. Użyj nazwy bazy danych, aby adresować bazę danych w swoich zapytaniach SQL.

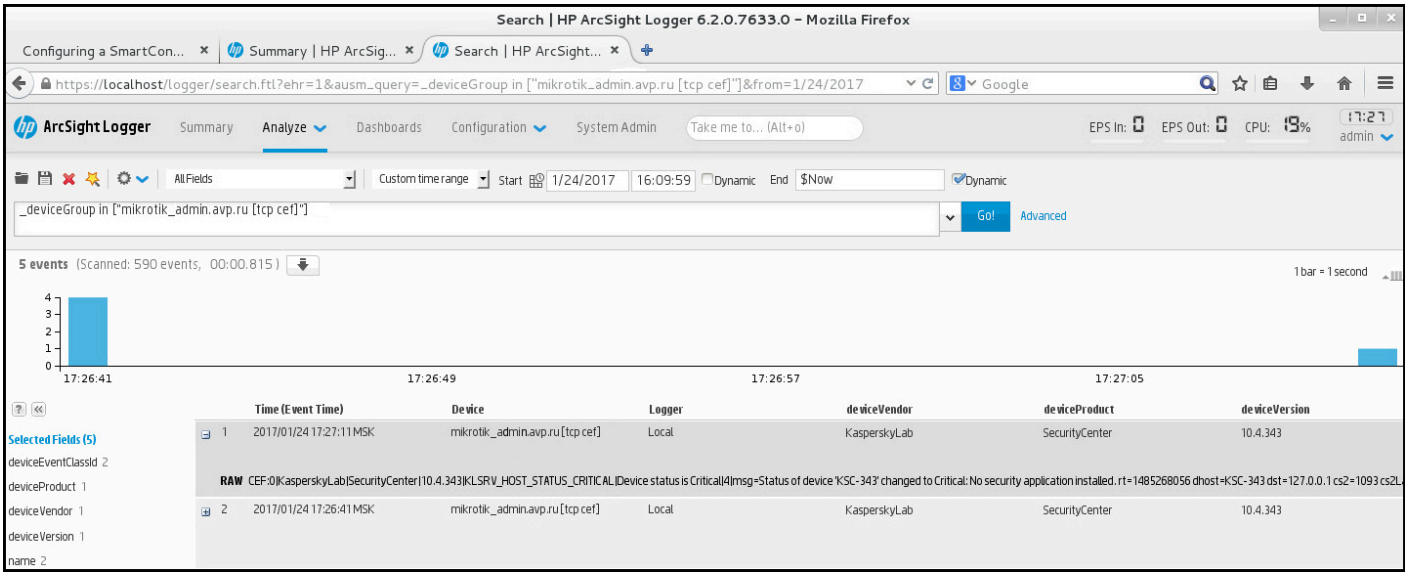
Przeglądanie wyników eksportowania

Możesz kontrolować pomyślne zakończenie procedury eksportowania zdarzeń. W tym celu sprawdź, czy wiadomości z eksportowanymi zdarzeniami są otrzymywane przez Twój system SIEM.

Jeśli zdarzenia wysłane z Kaspersky Security Center Linux są odbierane i poprawnie analizowane przez Twój system SIEM, konfiguracja po obu stronach została przeprowadzona właściwie. Jeśli jest inaczej, sprawdź ustawienia, które określono w Kaspersky Security Center Linux, porównując je z konfiguracją w Twoim systemie SIEM.

Poniższy rysunek przedstawia zdarzenia wyeksportowane do ArcSight. Na przykład, pierwsze zdarzenie jest krytycznym zdarzeniem Serwera administracyjnego: „*Urządzenie posiada stan Krytyczny*".

Reprezentacja eksportowania zdarzeń w systemie SIEM różni się w zależności od tego, którego systemu SIEM używasz.



Przykład zdarzeń

Zarządzanie rewizjami obiektów

Ta sekcja zawiera informacje dotyczące zarządzania rewizjami obiektów. Kaspersky Security Center Linux umożliwia śledzenie modyfikacji obiektów. Za każdym razem, gdy zapisujesz zmiany wprowadzone w obiekcie, tworzona jest *rewizja*. Każda rewizja posiada numer.

Obiekty, które obsługują zarządzanie rewizjami, obejmują:

- Właściwości Serwera administracyjnego
- Zasady
- Zadania
- Grupy administracyjne
- Konta użytkowników
- Pakiety instalacyjne

Na rewizjach obiektów możesz wykonać następujące działania:

- Wyświetlić wybraną rewizję (opcja dostępna tylko w przypadku zasad)
- Wycofać zmiany wprowadzone w obiekcie dla wybranej rewizji
- Zapisać wersje jako plik JSON (opcja dostępna tylko w przypadku zasad)

W oknie właściwości dowolnego obiektu obsługującego zarządzanie rewizjami sekcja **Historia rewizji** wyświetla listę rewizji obiektów z następującymi szczegółami:

- **Zmiana** — Numer rewizji obiektu.
- **Czas** — Data i godzina modyfikacji obiektu.
- **Użytkownik** — Nazwa użytkownika, który zmodyfikował obiekt.
- **Adres IP urządzenia użytkownika** — Adres IP urządzenia, z którego obiekt został zmodyfikowany.
- **Adres IP Web Console** — Adres IP Kaspersky Security Center Web Console, za pomocą którego obiekt został zmodyfikowany.
- **Akcja** — Działanie wykonane na obiekcie.
- **Opis** — Opis rewizji związanej ze zmianą wprowadzoną w ustawieniach obiektu.

  Domyślnie, pole opisu rewizji obiektu jest puste. Aby dodać opis do rewizji, wybierz żądaną rewizję i kliknij przycisk **Edytuj opis**. W otwartym oknie wprowadź tekst opisu rewizji.

Wyświetlanie i zapisywanie rewizji zasady

Kaspersky Security Center Linux umożliwia sprawdzenie, jakie modyfikacje zostały wprowadzone w zasadzie w określonym przedziale czasu, a także zapisanie informacji o tych modyfikacjach w pliku.

Przeglądanie i zapisywanie rewizji zasad jest możliwe, jeśli odpowiednia wtyczka webowa do zarządzania obsługuje tę funkcję.

Aby wyświetlić rewizję zasad:

1. W menu głównym przejdź do **Zarządzanie zasobami** → **Zasady**.
2. Kliknij zasadę dotyczącą wersji, którą chcesz wyświetlić, a następnie przejdź do sekcji **Historia rewizji**.
3. Na liście rewizji zasad kliknij numer rewizji, którą chcesz wyświetlić.

   Jeśli rozmiar rewizji jest większy niż 10 MB, nie będzie można jej wyświetlić przy użyciu Kaspersky Security Center Web Console. Wyświetlony zostanie monit o zapisanie wybranej wersji w pliku JSON.

   Jeżeli rozmiar rewizji nie przekracza 10 MB, wyświetlony zostanie raport w formacie HTML z ustawieniami wybranej rewizji zasady. Ponieważ raport jest wyświetlany w wyskakującym oknie, upewnij się, że w Twojej przeglądarce dozwolone są wyskakujące okienka.

W przypadku zasad Kaspersky Endpoint Security for Windows i Kaspersky Endpoint Security for Mac raport nie będzie zawierał informacji o profilach zasad.

Aby zapisać rewizję zasady w pliku JSON,

Na liście rewizji zasad wybierz rewizję, którą chcesz zapisać, a następnie kliknij **Zapisz do pliku**.

Rewizja zostanie zapisana w pliku JSON.

W razie potrzeby możesz porównać rewizje zasad. Ta opcja jest dostępna dla zasad Serwera administracyjnego, Agenta sieciowego, Kaspersky Endpoint Security for Windows (od wersji 14.0 wtyczki webowej) oraz Kaspersky Endpoint Security for Mac (od wersji 12.2.1 z poprawką A wtyczki webowej).

Porównanie rewizji zasad

Możesz porównać poprzednie rewizje zasady z jej bieżącą rewizją, porównać różne rewizje wybrane z listy lub porównać rewizję jednej zasady z rewizją innej zasady. Opcje są dostępne dla zasad Serwera administracyjnego, Agenta sieciowego, Kaspersky Endpoint Security for Windows (od wersji 14.0 wtyczki webowej) i Kaspersky Endpoint Security for Mac (od wersji 12.2.1 z poprawką A wtyczki webowej).

Aby wyświetlić rewizję zasad:

1. W menu głównym przejdź do **Zarządzanie zasobami** → **Zasady**.
2. Kliknij zasadę, której rewizje chcesz porównać.

   Zostanie otwarte okno ustawień zasady.
3. Przejdź do zakładki **Historia rewizji**, a następnie zaznacz pola wyboru obok rewizji, które chcesz porównać.
4. Na pasku narzędzi kliknij przycisk **Porównaj**, a następnie z listy rozwijanej wybierz jedną z następujących opcji:
   - **Z bieżącą rewizją**, jeśli chcesz porównać rewizją wybraną w kroku 3 z ostatnią zapisaną rewizją tej samej zasady.
   - **Wybrane rewizje**, jeśli chcesz porównać dwie rewizje, których pola wyboru zaznaczyłeś w kroku 3.

     Kolejność zaznaczania pól wyboru nie wpływa na wyniki porównania. Domyślnie, wcześniejsza rewizja wybranej rewizji jest porównywana z najnowszą rewizją. Na przykład, jeśli zaznaczysz pola wyboru obok rewizji 5 i 1, rewizja 1 zostanie porównywana z rewizją 5. Raport będzie zawierał informacje o ustawieniach w rewizji 1, które zostały dodane, usunięte lub zmienione w porównaniu z rewizją 5.
   - **W przypadku innej rewizji zasady**, jeśli chcesz porównać rewizje dwóch różnych zasad.

     W prawej części okna wykonaj jedną z następujących czynności:

     a. W polu **Nazwa aplikacji** wybierz zasadę, która chcesz porównać: Agenta sieciowego czy Serwera administracyjnego.

     b. W polu **Nazwa zasady** określ nazwę zasady, której rewizję chcesz porównać z tą wybraną w kroku 3.

     Zostanie wyświetlona lista istniejących zasad.

     c. Wybierz wymaganą rewizję, a następnie kliknij przycisk **Porównaj**.

Raport z porównania rewizji zostanie wyświetlony w formacie HTML na nowej karcie przeglądarki.

Jeśli wynik porównania przekroczy 10 MB, zostanie wyświetlone odpowiednie okno dialogowe. Możesz kliknąć przycisk **Zapisz do pliku**, aby zapisać raport jako plik, lub anulować operację.

Raport zostanie wyświetlony w języku interfejsu Kaspersky Security Center Web Console. Możesz rozwinąć niektóre sekcje raportu, klikając ikonę strzałki w dół (▼) obok sekcji lub zwinąć sekcję, klikając ikonę strzałkę w górę (▲).

Raport zawiera następujące informacje:

- Logo Kaspersky.
- Nazwa raportu.
- Data i godzina utworzenia raportu.
- Nazwa zasady, Serwer administracyjny i grupa administracyjna obejmująca zasadę (zasady), których rewizje zostały porównane.

- Przycisk **Zapisz jako HTML**. Po kliknięciu przycisku raport zostanie zapisany na komputerze.
- Sekcja **Podsumowanie**, która wyświetla ogólne informacje o porównywanych rewizjach: nazwa zasady (zasad), numer rewizji, czas i data zapisania rewizji, użytkownik, który zapisał rewizję, oraz opis rewizji.

  W przypadku odziedziczonych zasad użytkownik nie jest wyświetlany.

- Różnice między porównywanymi rewizjami. Różnice są wyświetlane w następujących sekcjach:
  - **Dodane ustawienia**
  - **Usunięte ustawienia**
  - **Zmienione ustawienia**
  - Ustawienia **dostępne tylko dla obiektu 1** (jeśli porównałeś rewizje dwóch różnych zasad)
  - **Ustawienia dostępne tylko dla obiektu 2** (jeśli porównałeś rewizje dwóch różnych zasad)

  Sekcja nie jest wyświetlana, jeśli nie zawiera danych.

W przypadku zasad Kaspersky Endpoint Security for Windows i Kaspersky Endpoint Security for Mac raport z porównania rewizji nie będzie zawierał informacji o profilach zasad.

Przywracanie poprzedniej wersji obiektu

Jeśli to konieczne, możesz wycofać zmiany wprowadzone w obiekcie. Na przykład, konieczne może być przywrócenie ustawień zasady z określonego dnia.

W celu wycofania zmian wprowadzonych w obiekcie:

1. W oknie właściwości obiektu otwórz zakładkę **Historia rewizji**.
2. Na liście rewizji obiektu wybierz rewizję, do której chcesz wycofać zmiany.
3. Kliknij przycisk **Wycofaj**.
4. Kliknij **OK**, aby potwierdzić działanie.

   Obiekt zostanie wycofany do wybranej rewizji. Lista rewizji obiektu wyświetla wpis dotyczący podjętego działania. Opis rewizji wyświetla informacje o numerze rewizji, do której wycofałeś obiekt.

Operacja wycofywania jest dostępna tylko w przypadku obiektów zasad i zadań.

Aktywne zagrożenia

Informacje o nieprzetworzonych plikach wykrytych na urządzeniach klienckich są przechowywane w sekcji **Repozytoria**, w podsekcji **Aktywne zagrożenia**.

Odroczone przetwarzanie i leczenie plików jest wykonywane przez aplikację antywirusową na żądanie lub po wystąpieniu określonego zdarzenia. Możesz skonfigurować odroczone przetwarzanie.

Leczenie nieprzetworzonego pliku

W celu uruchomienia leczenia nieprzetworzonego pliku:

1. W menu głównym przejdź do **Repozytoria** → **Aktywne zagrożenia**.
2. Wykonaj jedną z poniższych czynności:
   - Zaznacz pole obok pliku, który musisz wyleczyć.
   - Kliknij nazwę pliku, który musisz wyleczyć.
3. Rozpocznij leczenie pliku, klikając przycisk **Wylecz**.

   Podjęta zostanie próba wyleczenia wybranego pliku.

Jeśli plik zostanie wyleczony, aplikacja antywirusowa, zainstalowana na urządzeniu klienckim, przywróci go do oryginalnego folderu. Wpis dotyczący pliku zostanie usunięty z listy w sekcji **Aktywne zagrożenia**. Jeśli pliku nie można wyleczyć, aplikacja antywirusowa, zainstalowana na urządzeniu, usunie go z tego urządzenia. Wpis dotyczący pliku zostanie usunięty z listy w sekcji **Aktywne zagrożenia**.

> Możliwości leczenia i usuwania plików mogą się różnić w zależności od zainstalowanej aplikacji zabezpieczającej, jej wersji i ustawień.

Pobieranie nieprzetworzonego pliku

Kaspersky Security Center umożliwia pobieranie kopii nieprzetworzonych plików, wykrytych na urządzeniach klienckich. Odnosi się to do plików przetwarzanych lub usuwanych przez aplikację. Pliki są pobierane do określonego folderu na urządzeniu, na którym jest zainstalowany Kaspersky Security Center Linux.

Możesz pobierać kopie plików jeżeli pliki zostały usunięte lub zmodyfikowane podczas leczenia, a ich kopie są przechowywane w magazynie Kaspersky Endpoint Security for Linux na zarządzanym urządzeniu.

W celu pobrania kopii nieprzetworzonego pliku:

1. W menu głównym przejdź do **Repozytoria** → **Aktywne zagrożenia**.
2. Wykonaj jedną z poniższych czynności:
   - Zaznacz pola obok pliku, który musisz pobrać.
   - Kliknij nazwę pliku, który musisz pobrać.
3. Rozpocznij pobieranie, klikając przycisk **Pobierz**.

Aplikacja zabezpieczająca, zainstalowana na urządzeniu klienckim, na którym wykryto nieprzetworzony plik, pobierze kopię tego pliku do określonego folderu.

Usuwanie plików z sekcji „Aktywne zagrożenia”

*Aby usunąć plik z sekcji **Aktywne zagrożenia**:*

1. W menu głównym przejdź do **Repozytoria** → **Aktywne zagrożenia**.
2. Wykonaj jedną z poniższych czynności:
   - Zaznacz pole obok pliku, który musisz usunąć.
   - Kliknij nazwę pliku, który musisz usunąć.
3. Usuń pliki, klikając przycisk **Usuń**.
4. W otwartym oknie kliknij przycisk **Usuń**.

   Aplikacje zabezpieczające, które umieściły pliki w repozytoriach na urządzeniach klienckich, usuną te same pliki z tych repozytoriów. Wpisy dotyczące plików zostaną usunięte z listy w sekcji **Aktywne zagrożenia**.

Usuwanie obiektów

W tej sekcji znajdują się informacje dotyczące usuwania obiektów.

Możesz usuwać obiekty, w tym:

- Zasady
- Zadania
- Pakiety instalacyjne
- Wirtualne Serwery administracyjne
- Użytkownicy

- Grupy bezpieczeństwa
- Grupy administracyjne

W celu usunięcia obiektu:

1. Otwórz wymaganą sekcję Kaspersky Security Center Web Console, a następnie wybierz obiekt.
2. Na pasku narzędzi kliknij przycisk **Usuń**.
3. W otwartym oknie kliknij **OK**, aby potwierdzić swój wybór.

   Wybrany obiekt zostanie usunięty.

Jeśli usuniesz obiekt, informacje o nim pozostaną w bazie danych. Okres przechowywania informacji o usuniętych obiektach jest taki sam, jak okres przechowywania rewizji obiektu (zalecany okres wynosi 90 dni). Możesz zmienić okres przechowywania tylko wtedy, gdy posiadasz uprawnienie **Modyfikacja** w obszarze uprawnień **Usunięte obiekty**.

Informacje o usuwaniu urządzeń klienckich

Gdy usuniesz urządzenie zarządzane z grupy administracyjnej, aplikacja przeniesie je do grupy Urządzenia nieprzypisane. Po usunięciu urządzenia zainstalowane aplikacje Kaspersky — Agent sieciowy i dowolna aplikacja zabezpieczająca, na przykład Kaspersky Endpoint Security — pozostają na urządzeniu.

Kaspersky Security Center Linux obsługuje urządzenia w grupie Nieprzypisane urządzenia zgodnie z następującymi regułami:

- Jeśli skonfigurowałeś reguły przenoszenia urządzeń i urządzenie spełnia kryteria reguły przenoszenia, urządzenie jest automatycznie przenoszone do grupy administracyjnej zgodnie z regułą.
- Urządzenie jest przechowywane w grupie Urządzenia nieprzypisane i automatycznie usuwane z grupy zgodnie z regułami przechowywania urządzeń.

  Reguły przechowywania urządzeń nie mają wpływu na urządzenia, które mają jeden lub więcej napędów zaszyfrowanych za pomocą pełnego szyfrowania dysku. Takie urządzenia nie są usuwane automatycznie — można je usunąć tylko ręcznie. Jeśli chcesz usunąć urządzenie z zaszyfrowanym dyskiem, najpierw odszyfruj dysk, a następnie usuń urządzenie.

  > Przy usuwaniu urządzenia z zaszyfrowanym dyskiem dane wymagane do odszyfrowania dysku są również usuwane. Jeżeli zaznaczysz pole **Rozumiem ryzyko i chcę usunąć wybrane urządzenia** w oknie potwierdzenia otwierającym się po usunięciu takich urządzeń (z grupy **Urządzenia nieprzypisane** lub z grupy **Zarządzane urządzenia**), oznacza to, że masz świadomość związanego z tym usunięcia danych.

Aby odszyfrować dysk, muszą zostać spełnione następujące warunki:

- Urządzenie zostaje ponownie podłączone do Serwera administracyjnego w celu przywrócenia danych wymaganych do odszyfrowania dysku.
- Użytkownik urządzenia zapamięta hasło do odszyfrowania.
- Aplikacja zabezpieczająca, która została użyta do zaszyfrowania dysku, na przykład Kaspersky Endpoint Security for Windows, jest nadal zainstalowana na urządzeniu.

Jeśli dysk został zaszyfrowany przy użyciu technologii Kaspersky Disk Encryption, możesz również spróbować odzyskiwania danych przy użyciu narzędzia FDERT Restore Utility.

W przypadku VDI, jeśli masz urządzenie z zaszyfrowanymi dyskami, informacje na zaszyfrowanym dysku zostaną usunięte po usunięciu urządzenia.

Gdy ręcznie usuniesz urządzenie z grupy Urządzenia nieprzypisane, aplikacja usunie je z listy. Po usunięciu urządzenia zainstalowane aplikacje Kaspersky (jeśli istnieją) pozostają na urządzeniu. Następnie, jeśli urządzenie jest nadal widoczne dla Serwera administracyjnego i przeprowadzona została regularna konfiguracja przeszukiwania sieci Kaspersky Security Center Linux wykrywa urządzenie podczas przeszukiwania sieci i dodaje je z powrotem do grupy Urządzenia nieprzypisane. Dlatego rozsądne jest ręczne usunięcie urządzenia tylko wtedy, gdy jest ono niewidoczne dla Serwera administracyjnego.

Pobieranie i usuwanie plików z Kwarantanny i Kopie zapasowe plików

Ta sekcja zawiera informacje na temat pobierania i usuwania plików z Kwarantanny i Kopie zapasowe plików w Kaspersky Security Center Web Console.

Pobieranie plików z Kwarantanny i Kopii zapasowej

Pliki można pobierać z kwarantanny lub kopii zapasowej tylko wtedy, gdy spełniony jest jeden z dwóch warunków: albo opcja **Nie odłączaj od Serwera administracyjnego** jest włączona w ustawieniach urządzenia lub używana jest brama połączenia. W przeciwnym razie pobieranie nie będzie możliwe.

W celu zapisania kopii pliku z Kwarantanny lub Kopie zapasowe plików na dysku twardym:

1. Wykonaj jedną z poniższych czynności:

   - Jeśli chcesz zapisać kopię pliku z Kwarantanny, w menu głównym przejdź do **Operacje** → **Repozytoria** → **Kwarantanna**.

   - Jeśli chcesz zapisać kopię pliku z Kopii zapasowej, w menu głównym przejdź do **Operacje** → **Repozytoria** → **Kopie zapasowe plików**.

2. W otwartym oknie wybierz plik, który chcesz pobrać, i kliknij **Pobierz**.

   Rozpocznie się pobieranie. Kopia pliku, który został umieszczony w Kwarantannie na urządzeniu klienckim, jest zapisywana w określonym folderze.

Informacje o usuwaniu obiektów z repozytoriów Kwarantanny, Kopii zapasowej plików lub Aktywnych zagrożeń

Jeśli aplikacje zabezpieczające firmy Kaspersky zainstalowane na urządzeniach klienckich umieszczają obiekty w repozytoriach Kwarantanny, Kopii zapasowej lub Aktywnych zagrożeniach, wysyłają informacje o obiektach dodanych do sekcji **Kwarantanna**, **Kopie zapasowe plików** lub **Aktywne zagrożenia** w Kaspersky Security Center Linux. Po otwarciu jednej z tych sekcji możesz usunąć wymagany obiekt.

W sekcji **Kopie zapasowe plików** lub **Aktywne zagrożenia** wybierz obiekt z listy i kliknij przycisk **Usuń**.

W sekcji **Kwarantanna** możesz wykonać jedną z następujących czynności:

- Zaznacz pole wyboru obok nazwy obiektu, który chcesz usunąć, a następnie kliknij przycisk **Usuń** na pasku narzędzi.

- Kliknij nazwę obiektu, który chcesz usunąć, a następnie w otwartym oknie szczegółów na pasku narzędzi kliknij przycisk **Usuń**.

  W takim przypadku obiekt zostanie usunięty, na ekranie wyświetli się odpowiednie powiadomienie, a okno szczegółów zostanie zamknięte.

Kaspersky Security Center Linux usuwa wybrany obiekt z listy lub z repozytorium. Akcja do wykonania jest definiowana przez aplikację Kaspersky, która umieściła wybrany obiekt w repozytorium. Aplikacja Kaspersky jest określona w polu **Wpis dodany przez**.

Szczegółowe informacje na temat czynności, która ma być wykonana można znaleźć w dokumentacji aplikacji Kaspersky.

Zarządzanie aplikacją przez SNMP

Ta sekcja opisuje sposób pobierania informacji z Serwera administracyjnego przy użyciu protokołu SNMP (Simple Network Management Protocol) w systemie Linux.

SNMP to protokół do zarządzania urządzeniami sieciowymi.

Aby działać przez SNMP, Kaspersky Security Center Linux używa usługi snmpd zawartej w systemie operacyjnym oraz agenta SNMP do monitorowania wydajności Serwera administracyjnego i wysyłania danych do aplikacji pobocznych za pomocą identyfikatorów OID. Kaspersky Security Center Linux może wysyłać te informacje w formie statystyk lub pułapek SNMP, które są powiadomieniami o zdarzeniach aplikacji.

Protokół SNMP umożliwia dostęp do następujących informacji o aplikacji:

- Informacje ogólne
- Statystyki Kaspersky Security Center Linux od momentu instalacji aplikacji
- Informacje o zdarzeniach Kaspersky Security Center Linux

Udzielany jest dostęp tylko do odczytu.

Informacje o pułapkach SNMP i statystykach wysyłanych przez SNMP są przechowywane w pliku adminkit.mib. Domyślnie plik adminkit.mib znajduje się w folderze /opt/kaspersky/ksc64/share/snmp/.

Lokalna usługa snmpd na każdym węźle klastra służy jako serwer SNMP odbierający statystyki. Interakcja z zewnętrznym serwerem SNMP nie jest obsługiwana. Pułapki SNMP można odbierać lokalnie za pomocą usługi snmptrapd na każdym węźle klastra lub przekierowywać je do serwera zewnętrznego.

W przypadku operacji wykonywanych za pośrednictwem protokołu SNMP należy wstępnie skonfigurować usługę snmpd w systemie operacyjnym na każdym węźle klastra.

Konfigurowanie usługi snmpd w systemie operacyjnym

Przed konfiguracją upewnij się, że usługa snmpd jest zainstalowana w systemie operacyjnym.

Tworzenie konta użytkownika w celu uzyskania dostępu do danych

Przed utworzeniem konta zatrzymaj usługę snmpd, uruchamiając następujące polecenie:

```
bash
sudo systemctl stop snmpd
```

Aby zapewnić bezpieczeństwo dostępu do danych przez SNMPv3 z uwierzytelnianiem i szyfrowaniem, musisz utworzyć konto użytkownika po stronie usługi snmpd z następującymi informacjami:

- Nazwa użytkownika (uwzględnianie wielkości liter)
- Algorytm uwierzytelniania (MD5 lub SHA, zalecany jest SHA)
- Hasło uwierzytelniania

- Algorytm szyfrowania (obsługiwany jest tylko AES)
- Hasło szyfrowania

Konto użytkownika możesz utworzyć w następujący sposób:

- Za pomocą narzędzia net-snmp-create-v3-user, jeśli jest dostępne w systemie operacyjnym.
- Ręcznie, dodając odpowiednią dyrektywę do pliku konfiguracyjnego usługi snmpd.

Aby utworzyć konto użytkownika za pomocą narzędzia net-snmp-create-v3-user, uruchom następujące polecenie:

```
net-snmp-create-v3-user -ro -a <algorytm uwierzytelniania> -x <algorytm szyfrowania> <nazwa użytkownika>
```

Hasła uwierzytelniania i szyfrowania są żądane interaktywnie.

Na przykład:

```
net-snmp-create-v3-user -ro -a SHA -x AES MonitoringUser
```

W celu ręcznego utworzenia roli użytkownika:

1. Utwórz plik konfiguracyjny /var/lib/snmp/snmpd.conf, uruchamiając następujące polecenie:

   ```
   touch /var/lib/snmp/snmpd.conf
   ```

2. Dodaj następujące wiersze do pliku konfiguracyjnego:

   ```
   createUser <nazwa użytkownika> <algorytm uwierzytelniania> "<hasło uwierzytelniania>" <algorytm szyfrowania> "
   <hasło szyfrowania>"
   ```

   Na przykład:

   ```
   createUser MonitoringUser SHA "MonitoringAuthSecret" AES "MonitoringPrivSecret"
   ```

Tworzenie konta użytkownika do odbierania pułapek SNMP

Aby odbierać pułapki SNMP przez protokół SNMPv3 z uwierzytelnianiem i szyfrowaniem, należy utworzyć konto po stronie systemu monitorującego w kontekście odpowiedniej usługi (zwykle usługi snmptrapd).

Konto musi zawierać następujące informacje:

- Nazwa użytkownika
- Algorytm uwierzytelniania
- Hasło uwierzytelniania

- Algorytm szyfrowania
- Hasło szyfrowania

Ze względów bezpieczeństwa należy używać oddzielnych kont użytkowników do dostępu do danych i do odbierania pułapek SNMP.

Instrukcje dotyczące tworzenia konta użytkownika do odbierania pułapek SNMP można znaleźć w dokumentacji systemu monitorującego.

Konfigurowanie usługi snmpd

Konfiguracja usługi snmpd jest przechowywana w pliku /etc/snmp/snmpd.conf. Można dodać niezbędne informacje do istniejącego pliku konfiguracyjnego lub utworzyć nowy plik konfiguracyjny i dodać wiersze wymienione poniżej w podanej kolejności.

Jeżeli wybierzesz opcję utworzenia nowego pliku konfiguracyjnego, upewnij się, że wyłącznie superużytkownik ma do niego dostęp. Jeśli wymagane uprawnienia dostępu nie są ustawione, skonfiguruj je, uruchamiając następujące polecenia w podanej kolejności:

```
chown root:root /etc/snmp/snmpd.conf
chmod 600 /etc/snmp/snmpd.conf
```

Aby skonfigurować usługę snmpd:

1. W pliku konfiguracyjnym określ protokół, adres interfejsu sieciowego i numer portu, na których usługa snmpd ma nasłuchiwać żądań przychodzących.

   - Jeśli chcesz nasłuchiwać żądań na wszystkich interfejsach sieciowych, dodaj następujące wiersze do pliku konfiguracyjnego:

     ```
     agentAddress udp:161
     ```

   - Jeśli chcesz nasłuchiwać żądań tylko na lokalnym interfejsie sieciowym, na przykład, jeśli system monitorujący jest zainstalowany na tym samym komputerze, dodaj następujące wiersze do pliku konfiguracyjnego:

     ```
     agentAddress udp:127.0.0.1:161
     ```

2. Skonfiguruj interakcję między programem Kaspersky Security Center Linux a usługą snmpd. Możesz użyć gniazda UNIX lub TCP.

   - Jeśli używasz gniazda UNIX:

     a. Określ ścieżkę i uprawnienia dla gniazda UNIX. W tym celu, do pliku dodaj następujące wiersze:

     ```
     master agentx
     agentXSocket unix:/var/run/agentx-master.socket
     agentXPerms 770 770 kluser klusers
     ```

     b. Dodaj grupę klusers jako grupę uzupełniającą dla konta {'KLSRV_UNATT_KLSVCUSER'}.

   - Jeśli używasz gniazda TCP, określ port i adres gniazda TCP. W tym celu, do pliku konfiguracyjnego dodaj następujące wiersze:

     ```
     master agentx
     agentXSocket tcp:127.0.0.1:705,tcp6:[::1]:705
     ```

3. Ustaw minimalny limit czasu odpowiedzi na co najmniej 30 sekund. W tym celu, do pliku dodaj następujące wiersze:

   ```
   agentxTimeout 30
   ```

4. W razie potrzeby możesz podać opis serwera, na którym skonfigurowano SNMP, lokalizację systemu oraz adres kontaktowy administratora. W tym celu, do pliku dodaj następujące wiersze:

   ```
   sysDescr <opis serwera>
   sysLocation <lokalizacja serwera>
   sysContact <adres kontaktowy administratora>
   sysServices 72
   ```

5. Określ zakres drzewa OID, które ma być dostępne dla systemu monitorowania za pośrednictwem protokołu SNMP. W tym celu, dodaj następujące wiersze do pliku konfiguracyjnego:

   ```
   view monitoring included .1.3.6.1.4.1.23668.1093.1

   view systemonly included .1.3.6.1.4.1.23668.1093.1
   ```

6. W razie potrzeby możesz dodatkowo określić zakres drzewa OID zawierający informacje o systemie operacyjnym przechowywanym przez usługę snmpd. Zakres ten będzie dostępny dla systemu monitorowania.

Informacje o systemie operacyjnym obejmują na przykład informacje o wykorzystaniu procesora i RAM, wolne miejsce na partycjach dysku, obciążenie interfejsów sieciowych; listę zainstalowanego oprogramowania; listę otwartych połączeń sieciowych; oraz listę uruchomionych procesów. Część tych informacji może być poufna.

- Jeśli chcesz zezwolić na dostęp tylko do ogólnych informacji o systemie oraz informacji o wykorzystaniu RAM, procesora i urządzeń dyskowych, dodaj następujące wiersze do pliku konfiguracyjnego:

```
# SNMPv2-MIB - Basic system information
view monitoring included .1.3.6.1.2.1.1
# HOST-RESOURCES-MIB - CPU, Memory, Filesystems
view monitoring included .1.3.6.1.2.1.25.1
view monitoring included .1.3.6.1.2.1.25.2
view monitoring included .1.3.6.1.2.1.25.3
view monitoring included .1.3.6.1.2.1.25.5
# UCD-SNMP-MIB - Memory and CPU usage
view monitoring included .1.3.6.1.4.1.2021.4
view monitoring included .1.3.6.1.4.1.2021.10
view monitoring included .1.3.6.1.4.1.2021.11
# UCD-SNMP-DISKIO-MIB - Block devices I/O statistics
view monitoring included .1.3.6.1.4.1.2021.13
# IF-MIB - Network interfaces I/O statistics
view monitoring included .1.3.6.1.2.1.2
view monitoring included .1.3.6.1.2.1.31
```

- Jeśli chcesz zezwolić na dostęp do wszystkich informacji o systemie, dodaj następujące wiersze do pliku konfiguracyjnego:

```
view monitoring included .1
```

7. Określ tryb dostępu i zakres informacji dla utworzonego konta użytkownika. W tym celu, dodaj następujące wiersze do pliku konfiguracyjnego:

```
rouser <user name> priv -V monitoring
```

8. Aby wysyłać pułapki SNMP, określ adres IP systemu monitorującego i poświadczenia użytkownika do odbierania pułapek. W tym celu, dodaj następujące wiersze do pliku konfiguracyjnego:

```
trapsess -Ci -v3 -t0.1 -r1 -l authPriv -u <nazwa użytkownika do odbierania pułapek> -a <algorytm
uwierzytelniania> -A "<hasło użytkownika do odbierania pułapek>" -x <algorytm szyfrowania> -X "<hasło
szyfrowania>" udp:<adres IP>:162
```

Usługa snmpd jest skonfigurowana.

Aby zintegrować ją z wieloma systemami monitorowania, utwórz osobne konto użytkownika dla każdego systemu, określ zakres dostępnych informacji dla każdego konta użytkownika (dyrektywy 'view' i 'rouser') oraz skonfiguruj wysyłanie pułapek SNMP (dyrektywa 'trapsess').

Uruchomienie usługi snmpd z nową konfiguracją

Aby zastosować nową konfigurację:

1. Uruchom ponownie usługę snmpd:

   ```
   systemctl restart snmpd
   ```

2. Sprawdź status usługi snmpd:

   ```
   systemctl status snmpd
   ```

   Status musi być `running`.

3. Zezwól na automatyczne uruchamianie usługi przy starcie systemu operacyjnego:

   ```
   systemctl enable snmpd
   ```

4. Jeśli używasz zapory sieciowej w systemie operacyjnym lub sprzęcie sieciowym, dodaj reguły, aby przepuszczać pakiety SNMP.

Usługa snmpd jest uruchomiona.

Jeśli usługa klcssnmp była uruchomiona w momencie konfiguracji usługi snmpd, uruchom ponownie również usługę klcssnmp.

Sprawdzanie stanu usługi snmpd

Aby przetestować usługę snmpd, skonfiguruj korzystanie z protokołu SNMP w Kaspersky Security Center Linux i zażądaj danych SNMP za pomocą narzędzia snmpwalk.

Aby uzyskać zakresy danych SNMP udostępniane przez Kaspersky Security Center Linux,

uruchom następujące polecenie:

```
snmpwalk -v3 -l authPriv -u <nazwa użytkownika> -a <algorytm uwierzytelniania> -A "<hasło uwierzytelniania>" -x
<algorytm szyfrowania> -X "<hasło szyfrowania>" <adres IP> .1.3.6.1.4.1.23668.1093.1
```

Na przykład:

```
snmpwalk -v3 -l authPriv -u MonitoringUser -a SHA -A "MonitoringAuthSecret" -x AES -X "MonitoringPrivSecret"
127.0.0.1 .1.3.6.1.4.1.23668.1093.1
```

Włączanie i wyłączanie powiadomień przez SNMP

Kaspersky Security Center Linux wysyła powiadomienia o zdarzeniach Serwera administracyjnego w formie pułapek SNMP.

Domyślnie powiadomienia SNMP dla zdarzeń Kaspersky Security Center Linux są wyłączone.

Aby włączyć lub wyłączyć powiadomienia przez SNMP dla zdarzeń Kaspersky Security Center Linux:

1. W menu głównym kliknij nazwę Serwera administracyjnego.

   Zostanie otwarte okno **Właściwości Serwera administracyjnego**.

2. Na zakładce **Konfiguracja zdarzenia** w oknie właściwości kliknij typ zdarzenia, dla którego chcesz otrzymywać powiadomienia SNMP.

3. W otwartym panelu włącz lub wyłącz przełącznik **Powiadom przez SNMP**.

   Ta opcja jest dostępna tylko wtedy, gdy włączona jest opcja **Wyślij statystyki przy użyciu SNMP**.

Powiadomienia SNMP o zdarzeniach programu Kaspersky Security Center Linux są włączane lub wyłączane w zależności od dokonanego wyboru.

Włączanie i wyłączanie protokołu SNMP w Kaspersky Security Center Linux

Domyślnie wysyłanie statystyk przez protokół SNMP jest włączone. Aby wysyłać pułapki SNMP, należy skonfigurować usługę snmpd.

Aby włączyć lub wyłączyć wysyłanie statystyk przez protokół SNMP:

1. W menu głównym kliknij nazwę Serwera administracyjnego.

   Zostanie otwarte okno **Właściwości Serwera administracyjnego**.

2. Na zakładce **Ogólne** wybierz sekcję **SNMP**.

3. Włącz lub wyłącz przełącznik **Wyślij statystyki przy użyciu SNMP**.

4. Kliknij **Zapisz**.

Wysyłanie statystyk przez protokół SNMP jest włączane lub wyłączane w zależności od dokonanego wyboru.

Wartości identyfikatorów obiektów dla SNMP

Poniższa tabela przedstawia wartości i opisy identyfikatorów obiektów (OID), które są używane do przesyłania informacji o działaniu Serwera administracyjnego do aplikacji firm trzecich.

Wartość identyfikatora obiektu	Typ danych numerycznych	Identyfikator OID	Opis
`deploymentStatus`	`INTEGER { ok(0), info(1), warning(2), critical(3) }`	.1.3.6.1.4.1.23668.1093.1.1.1	Stan wdrożenia. Stan może być jednym z następujących: • **Informacja**. Licencja nie jest już ważna dla N urządzeń. • **Ostrzeżenie**. Jeden z następujących: Istnieje M urządzeń z aplikacjami Kaspersky zainstalowanymi na łącznie N urządzeniach w grupach Serwera administracyjnego (N > M). Licencja L utraci ważność na N urządzeniach za M dni. Zadanie T instalacji aplikacji zostało pomyślnie zakończone na N urządzeniach, dla M urządzeń konieczne jest ponowne uruchomienie. • **Krytyczne**. Licencja utraciła ważność dla N urządzeń. • **OK**. Żadne z powyższych.
`noAntivirusSoftware`	`INTEGER { off(0), on(1) }`	.1.3.6.1.4.1.23668.1093.1.1.2.1	`deploymentStatus` wskazuje, że grupa Serwera administracyjnego zawiera zbyt wiele urządzeń bez zarządzanych aplikacji. Wartość jest równa 1 w przypadku wykrycia kilku urządzeń bez zarządzanych aplikacji, i 0 w innym przypadku.
`remoteInstallTaskFailed`	`INTEGER { off(0), on(1) }`	.1.3.6.1.4.1.23668.1093.1.1.2.2	`deploymentStatus` wskazuje, że zadanie zdalnej instalacji nie powiodło się na niektórych urządzeniach. Liczbę tych urządzeń można uzyskać za pośrednictwem wartości `hostsRemoteInstallFailed`.
`licenceExpiring`	`INTEGER { off(0), on(1) }`	.1.3.6.1.4.1.23668.1093.1.1.2.3	`deploymentStatus` wskazuje, że istnieją urządzenia, dla których licencja utraci ważność w ciągu następnych 7 dni. Liczbę tych urządzeń można uzyskać za pośrednictwem wartości `hostsLicenseExpiring`.
`licenceExpired`	`INTEGER { off(0), on(1) }`	.1.3.6.1.4.1.23668.1093.1.1.2.4	`deploymentStatus` wskazuje, że istnieją urządzenia z licencją, która utraciła ważność. Liczbę tych urządzeń można uzyskać za pośrednictwem `hostsLicenseExpired`.
`hostsInGroups`	`Counter32`	.1.3.6.1.4.1.23668.1093.1.1.3	Liczba urządzeń w grupach Serwera administracyjnego.
`hostsWithAntivirus`	`Counter32`	.1.3.6.1.4.1.23668.1093.1.1.4	Liczba urządzeń w grupach Serwera administracyjnego z zainstalowanymi zarządzanymi aplikacjami.
`hostsRemoteInstallFailed`	`Counter32`	.1.3.6.1.4.1.23668.1093.1.1.5	Liczba urządzeń, na których zadanie zdalnej instalacji nie powiodło się.
`licenceExpiringSerial`	`OCTET STRING`	.1.3.6.1.4.1.23668.1093.1.1.6	Identyfikator klucza licencyjnego, który utraci ważność za mniej niż 7 dni.
`licenceExpiredSerial`	`OCTET STRING`	.1.3.6.1.4.1.23668.1093.1.1.7	Identyfikator wygasłego klucza licencyjnego.
`licenceExpiringDays`	`Unsigned32`	.1.3.6.1.4.1.23668.1093.1.1.8	Liczba dni pozostałych do utraty ważności licencji. Dla tego parametru okres licencji uważa się za wygasły, jeśli do daty wygaśnięcia pozostało mniej niż 7 dni. Jeśli do daty wygaśnięcia pozostało więcej niż 7 dni, wartość wynosi 0.
`hostsLicenceExpiring`	`Counter32`	.1.3.6.1.4.1.23668.1093.1.1.9	Liczba urządzeń z licencją, która wygaśnie za mniej niż 7 dni.
`hostsLicenceExpired`	`Counter32`	.1.3.6.1.4.1.23668.1093.1.1.10	Liczba urządzeń z licencją, która utraciła ważność.

Wartość identyfikatora obiektu	Typ danych numerycznych	Identyfikator OID	Opis
`updatesStatus`	`INTEGER { ok(0), info(1), warning(2), critical(3) }`	.1.3.6.1.4.1.23668.1093.1.2.1	Aktualny stan aktualizacji antywirusowych baz danych. Stan może być jednym z następujących: • **Informacja**. Bazy antywirusowe na serwerze administracyjnym lub na urządzeniach nie były aktualizowane dłużej niż 1 dzień, a od instalacji aplikacji upłynął mniej niż 1 dzień. • **Ostrzeżenie**. Bazy antywirusowe na serwerze administracyjnym lub na urządzeniach nie były aktualizowane dłużej niż 3 dni. Wartość tę można zmienić w ustawieniach grupy. • **Krytyczne**. Bazy antywirusowe na serwerze administracyjnym lub na urządzeniach nie były aktualizowane dłużej niż 7 dni. Wartość tę można zmienić w ustawieniach grupy. • **OK**. Żadne z powyższych.
`serverNotUpdated`	`INTEGER { off(0), on(1) }`	.1.3.6.1.4.1.23668.1093.1.2.2.1	Serwer administracyjny nie był aktualizowany przez długi czas. Okres uważany za długi jest określony w wartości `updatesStatus`.
`notUpdatedHosts`	`INTEGER { off(0), on(1) }`	.1.3.6.1.4.1.23668.1093.1.2.2.2	Niektóre urządzenia nie były aktualizowane przez długi czas (domyślnie 7 dni lub więcej w przypadkach **krytycznych** i 3 dni w przypadku **ostrzeżenia**). Liczbę tych urządzeń można uzyskać za pośrednictwem `hostsNotUpdated`.
`lastServerUpdateTime`	`Hex-STRING`	.1.3.6.1.4.1.23668.1093.1.2.3	Ostatni raz, kiedy antywirusowe bazy danych zostały zaktualizowane na Serwerze administracyjnym.
`hostsNotUpdated`	`Counter32`	.1.3.6.1.4.1.23668.1093.1.2.4	Liczba urządzeń zawierających bazy antywirusowe, które nie były aktualizowane przez długi czas (domyślnie 7 dni lub więcej w przypadkach **krytycznych** i 3 dni w przypadkach **ostrzeżeń**). Jeśli istnieją urządzenia ze statusem aktualizacji **krytycznych**, zliczane są tylko te urządzenia. Stan aktualizacji można uzyskać za pomocą `updatesStatus`.
`protectionStatus`	`INTEGER { ok(0), warning(2), critical(3) }`	.1.3.6.1.4.1.23668.1093.1.3.1	Stan ochrony w czasie rzeczywistym. Jeden z następujących: • **Ostrzeżenie**. Jeden z następujących: Wykryto naruszenie zabezpieczeń na urządzeniu należącym do grupy Serwera administracyjnego. Błędy szyfrowania spowodowały, że niektóre urządzenia zmieniły stan ochrony. Pełne skanowanie nie było wykonywane przez długi czas. • **Krytyczne**. Ochrona antywirusowa nie działa na niektórych urządzeniach w grupach Serwera administracyjnego. • **OK**. Żadne z powyższych.
`antivirusNotRunning`	`INTEGER { off(0), on(1) }`	.1.3.6.1.4.1.23668.1093.1.3.2.1	Aplikacja zabezpieczająca nie działa na niektórych urządzeniach. Liczbę tych urządzeń można uzyskać za pośrednictwem `hostsAntivirusNotRunning`.
`realtimeNotRunning`	`INTEGER { off(0), on(1) }`	.1.3.6.1.4.1.23668.1093.1.3.2.2	Ochrona w czasie rzeczywistym nie działa na niektórych urządzeniach. Liczbę tych urządzeń można uzyskać za pośrednictwem `hostsRealtimeNotRunning`.
`psRealtimeLevelChanged`	`INTEGER { off(0), on(1) }`	.1.3.6.1.4.1.23668.1093.1.3.2.3	Poziom ochrony w czasie wykonywania różni się od poziomu ustawionego przez administratora na N komputerach w grupach administracyjnych.
`notCuredFound`	`INTEGER { off(0), on(1) }`	.1.3.6.1.4.1.23668.1093.1.3.2.4	Istnieją urządzenia zawierające niewyleczone obiekty. Liczbę tych urządzeń można uzyskać za pośrednictwem `hostsNotCuredObject`.
`tooManyThreats`	`INTEGER { off(0), on(1) }`	.1.3.6.1.4.1.23668.1093.1.3.2.5	Na niektórych urządzeniach wykryto zagrożenia. Liczbę tych urządzeń można uzyskać za pośrednictwem `hostsTooManyThreats`.

Wartość identyfikatora obiektu	Typ danych numerycznych	Identyfikator OID	Opis
`virusOutbreak`	`INTEGER { off(0), on(1) }`	.1.3.6.1.4.1.23668.1093.1.3.2.6	Stan ataku wirusa w systemie. Wartość wynosi 1, jeśli pewna liczba wirusów została znaleziona w określonym czasie, i 0 w przeciwnym wypadku. Liczba wirusów i ilość czasu są określane na Serwerze administracyjnym przy użyciu ustawień `Virus attack`.
`psVulnerabilitiesFound`	`INTEGER { off(0), on(1) }`	.1.3.6.1.4.1.23668.1093.1.3.2.7	Wykryto luki w zabezpieczeniach.
`psEncryptionFaultsFound`	`INTEGER { off(0), on(1) }`	.1.3.6.1.4.1.23668.1093.1.3.2.8	Wykryto błędy szyfrowania, które zmieniły stan ochrony urządzenia.
`psVulnerableHostsFound`	`INTEGER { off(0), on(1) }`	.1.3.6.1.4.1.23668.1093.1.3.2.9	Na niektórych urządzeniach wykryto luki w zabezpieczeniach.
`psNotScannedLately`	`INTEGER { off(0), on(1) }`	.1.3.6.1.4.1.23668.1093.1.3.2.10	Wykryto urządzenia bez pełnego skanowania przez dłuższy czas.
`psNagentsNotRunningUntilReboot`	`INTEGER { off(0), on(1) }`	.1.3.6.1.4.1.23668.1093.1.3.2.11	Wykryto urządzenia, na których Agent sieciowy uruchamia się dopiero po ponownym uruchomieniu.
`hostsAntivirusNotRunning`	`Counter32`	.1.3.6.1.4.1.23668.1093.1.3.3	Liczba urządzeń z niedziałającymi aplikacjami zabezpieczającymi.
`hostsRealtimeNotRunning`	`Counter32`	.1.3.6.1.4.1.23668.1093.1.3.4	Liczba urządzeń z niedziałającą ochroną w czasie rzeczywistym.
`hostsRealtimeLevelChanged`	`Counter32`	.1.3.6.1.4.1.23668.1093.1.3.5	Liczba urządzeń z niedopuszczalnym poziomem ochrony w czasie rzeczywistym.
`hostsNotCuredObject`	`Counter32`	.1.3.6.1.4.1.23668.1093.1.3.6	Liczba urządzeń zawierających niewyleczone obiekty.
`hostsTooManyThreats`	`Counter32`	.1.3.6.1.4.1.23668.1093.1.3.7	Liczba urządzeń zawierających zagrożenia.
`fullscanStatus`	`INTEGER { ok(0), info(1), warning(2), critical(3) }`	.1.3.6.1.4.1.23668.1093.1.4.1	Stan pełnego skanowania antywirusowego jest jednym z następujących: • **Informacja**. Od momentu instalacji aplikacji minęło mniej niż 7 dni. • **Ostrzeżenie**. Pełne skanowanie antywirusowe nie było wykonywane od ponad 7 dni od momentu instalacji aplikacji. • **Krytyczne**. Pełne skanowanie antywirusowe nie było wykonywane od ponad 14 dni od momentu instalacji aplikacji. • **OK**. Żadne z powyższych.
`notScannedLately`	`INTEGER { off(0), on(1) }`	.1.3.6.1.4.1.23668.1093.1.4.2.1	Niektóre urządzenia nie były skanowane przez określony czas. Liczbę tych urządzeń można uzyskać za pośrednictwem `hostsNotScannedLately`. Ilość czas jest określona w wartości `fullScanStatus`.
`hostsNotScannedLately`	`Counter32`	.1.3.6.1.4.1.23668.1093.1.4.3	Liczba urządzeń, które nie były skanowane przez określony czas. Ilość czas jest określona w wartości `fullScanStatus`.
`logicalNetworkStatus`	`INTEGER { ok(0), warning(1), critical(2) }`	.1.3.6.1.4.1.23668.1093.1.5.1	Stan sieci logicznej Serwera administracyjnego. Jeden z następujących: • **Ostrzeżenie**. Jeśli istnieją urządzenia ze stanem ostrzeżenia, do których nie można uzyskać dostępu, lub jeśli istnieją urządzenia, które nie należą do żadnej grupy Serwera administracyjnego. • **Krytyczne**. Jeśli istnieją urządzenia, nad którymi kontrola została utracona przez Serwer administracyjny, lub jeśli istnieją urządzenia o stanie krytycznym, do których nie można uzyskać dostępu. • **OK**. Żadne z powyższych.

Wartość identyfikatora obiektu	Typ danych numerycznych	Identyfikator OID	Opis
`notConnectedLongTime`	`INTEGER { off(0), on(1) }`	.1.3.6.1.4.1.23668.1093.1.5.2.1	Niektóre urządzenia nie były połączone z Serwerem administracyjnym przez długi czas (7 lub więcej dni w przypadku urządzenia o stanie **Ostrzeżenie** i 4 dni w przypadku urządzenia o stanie **Krytyczne**). Liczbę tych urządzeń można uzyskać za pośrednictwem `hostsNotConnectedLongTime`.
`controlLost`	`INTEGER { off(0), on(1) }`	.1.3.6.1.4.1.23668.1093.1.5.2.2	Istnieją urządzenia, nad którymi kontrola została utracona przez Serwer administracyjny. Liczbę tych urządzeń można uzyskać za pośrednictwem `hostsControlLost`.
`hostsFound`	`Counter32`	.1.3.6.1.4.1.23668.1093.1.5.3	Liczba urządzeń znalezionych przez Serwer administracyjny, które nie należą do żadnej grupy Serwera administracyjnego.
`groupsCount`	`Counter32`	.1.3.6.1.4.1.23668.1093.1.5.4	Liczba grup na Serwerze administracyjnym.
`hostsNotConnectedLongTime`	`Counter32`	.1.3.6.1.4.1.23668.1093.1.5.5	Liczba urządzeń, które nie były połączone z Serwerem administracyjnym od dłuższego czasu. Okres uważany za długi jest określony w wartości `notConnectedLongTime`.
`hostsControlLost`	`Counter32`	.1.3.6.1.4.1.23668.1093.1.5.6	Liczba urządzeń, które nie są kontrolowane przez Serwer administracyjny.
`eventsStatus`	`INTEGER { ok(0), info(1), warning(2), critical(3) }`	.1.3.6.1.4.1.23668.1093.1.6.1	Stan podsystemu zdarzeń jest jednym z następujących: • **Ostrzeżenie**. Jeden z następujących: Urządzenia grupy Serwera administracyjnego nie wyszukiwały aktualizacji systemu Windows przez długi czas. Istnieją urządzenia z problemami ze stanem. • **Krytyczne**. Jeden z następujących: Wystąpiło zdarzenie „Krytyczne" na co najmniej jednym urządzeniu. Wystąpiło zdarzenie „Błąd" na co najmniej jednym urządzeniu. Istnieje zdarzenie zadania zakończonego niepomyślnie na co najmniej jednym urządzeniu. Urządzenia grupy Serwera administracyjnego nie wyszukiwały aktualizacji systemu Windows przez długi czas. Istnieją urządzenia z problemami ze stanem. • **Informacja.** Jeden z następujących: Minął mniej niż tydzień od ostatniego pełnego skanowania antywirusowego wszystkich urządzeń. Zadania instalacji zdalnej zostały ukończone i żadne urządzenie nie wymaga ponownego uruchomienia. Minął mniej niż tydzień od ostatniej aktualizacji Serwera administracyjnego. Serwer administracyjny nie był aktualizowany od dłuższego czasu, ale aktualizacja jest obecnie w toku. • **OK**. Żadne z powyższych.
`criticalEventOccured`	`INTEGER { off(0), on(1) }`	.1.3.6.1.4.1.23668.1093.1.6.2.1	`eventsStatus` wskazuje, że na Serwerze administracyjnym istnieją zdarzenia krytyczne. Liczbę tych zdarzeń można uzyskać, korzystając z funkcji `criticalEventsCount`. Wartość jest równa 1, jeśli na dowolnym urządzeniu występuje co najmniej jedno zdarzenie krytyczne, i 0 w innym przypadku.
`criticalEventsCount`	`Counter32`	.1.3.6.1.4.1.23668.1093.1.6.3	Liczba zdarzeń krytycznych na Serwerze administracyjnym.

Praca z Kaspersky Security Center Linux w ramach licencji Kaspersky Next XDR Optimum

Jeśli zakupiłeś licencję na Kaspersky Next XDR Optimum w ramach licencji aplikacji EPP i licencji Kaspersky Security Center Linux, będziesz mógł korzystać z funkcjonalności Kaspersky Next XDR Optimum po wykonaniu konfiguracji początkowej.

Jeśli zakupiłeś licencję na Kaspersky Next XDR Optimum osobno jako rozszerzenie wcześniej zakupionej licencji po zainstalowaniu i aktywowaniu aplikacji Kaspersky na urządzeniach, musisz ponownie aktywować Kaspersky Security Center Linux na urządzeniach, korzystając z nowego kodu aktywacyjnego lub pliku klucza, w zależności od sposobu zakupu licencji na Kaspersky Next XDR Optimum. Następnie wykonaj konfigurację początkową.

Możesz również korzystać z funkcjonalności Kaspersky Next XDR Optimum w trybie testowym. Aby to zrobić, najpierw musisz dodać podrzędny fizyczny Serwer administracyjny, a następnie aktywować ten serwer w ramach swojej próbnej licencji Kaspersky Next XDR Optimum. Funkcjonalność Kaspersky Next XDR Optimum będzie dostępna na serwerze podrzędnym przez cały okres ważności licencji próbnej.

Po aktywowaniu Serwera administracyjnego w ramach Twojej licencji Kaspersky Next XDR Optimum i wdrożeniu klucza licencyjnego na urządzeniach zarządzanych przez odpowiedni Serwer administracyjny możesz wykonać następujące czynności:

- Reaguj na zagrożenia, korzystając z integracji z Kaspersky Automated Security Awareness Platform, Kaspersky Threat Intelligence Portal Sandbox i Active Directory.
- Grupuj alerty według atrybutów.

Aby uzyskać więcej informacji o funkcjach włączonych dzięki licencji Kaspersky Next XDR Optimum, zapoznaj się z pomocą techniczną Kaspersky Endpoint Detection and Response Optimum.

Integracje umożliwiające reagowanie na alerty

Jeśli posiadasz licencję Kaspersky Next XDR Optimum, możesz skonfigurować integracje z następującymi rozwiązaniami w celu reagowania na zagrożenia:

- Kaspersky Automated Security Awareness Platform
- Kaspersky Threat Intelligence Portal Sandbox
- Active Directory

Te integracje są dostępne, jeśli aktywowano Serwer administracyjny przy użyciu licencji Kaspersky Next XDR Optimum.
Aby wykonywać działania reagowania, należy wdrożyć klucz licencyjny Kaspersky Next XDR Optimum w zarządzanych aplikacjach.
Podczas korzystania z funkcjonalności Kaspersky Next XDR Optimum w ramach licencji próbnej, najpierw musisz dodać podrzędny fizyczny Serwer administracyjny, następnie aktywować ten podrzędny Serwer administracyjny w ramach licencji próbnej i wdrożyć klucz licencyjny na urządzenia zarządzane przez ten Serwer administracyjny.

Jeśli korzystasz z licencji Kaspersky Next EDR Optimum, nie musisz aktywować aplikacji zainstalowanych na zarządzanych urządzeniach w ramach licencji Kaspersky Next XDR Optimum. Należy to zrobić tylko dla nowych urządzeń, o ile takie istnieją.

Ponieważ licencja Kaspersky Next XDR Optimum wspiera wielodostęp, możesz centralnie dystrybuować klucz licencyjny do zarządzanych aplikacji. Automatyczna dystrybucja licencji do podrzędnych i wirtualnych Serwerów administracyjnych nie jest obsługiwana.

Aby skonfigurować integracje, musisz mieć uprawnienia do **odczytu** i **zapisu** w obszarze funkcjonalnym **Funkcje ogólne: Integracja aplikacji**.

Konfigurowanie integracji z usługą Active Directory w celu wykonywania działań reagowania

Integracja z usługą Active Directory umożliwia wykonywanie działań reagowania dla użytkowników usługi Active Directory objętych alertem lub w niego zaangażowanych.

Aby skonfigurować integrację z usługą Active Directory w celu reagowania na alerty, należy używać Serwera administracyjnego Kaspersky Security Center Linux w wersji 15.4 lub nowszej.

Integracja z usługą Active Directory w celu reagowania na alerty oraz ustawienia skanowania kontrolera domeny usługi Active Directory (adres i poświadczenia użytkownika kontrolera domeny) określone podczas konfigurowania przeszukiwania kontrolera domeny to dwa różne ustawienia. Ponieważ musisz mieć pewność, że użytkownik, dla którego ma zostać wykonane działanie reagowania, ma konto w usłudze Active Directory, musisz skonfigurować obie integracje: dla skanowania i dla reagowania. Kolejność nie ma znaczenia.

Ustawienia integracji nie są dziedziczone i mają zastosowanie wyłącznie do Serwera administracyjnego (fizycznego lub wirtualnego), na którym konfigurujesz te ustawienia.

Aby skonfigurować integrację z usługą Active Directory w celu reagowania na alerty:

1. W menu głównym kliknij nazwę Serwera administracyjnego.

   Okno właściwości Serwera administracyjnego zostanie otwarte na zakładce **Ogólne**.

2. Wykonaj jedną z poniższych czynności:

   - Wybierz sekcję **Punkty dystrybucji**, kliknij nazwę wymaganego punktu dystrybucji, a następnie w otwartym oknie właściwości wybierz sekcję **Active Directory**.
   - Wybierz sekcję **Odpowiedź Active Directory**.

3. W prawym panelu włącz przełącznik **Integracja Active Directory**.

   Jeśli później zechcesz wyłączyć integrację, będziesz mógł to zrobić jedynie dla wszystkich połączeń, dezaktywując przełącznik **Integracja Active Directory**. Nie można wyłączyć integracji dla oddzielnego połączenia. Zamiast tego można usunąć połączenie.

   > Po włączeniu lub wyłączeniu przełącznika **Integracja Active Directory** ustawienie to zostanie zastosowane zarówno do sekcji **Odpowiedź Active Directory**, jak i do sekcji **Punkty dystrybucji**.

4. Utwórz połączenie z kontrolerem domeny Active Directory, klikając przycisk **Dodaj**.

5. W otwartym oknie określ następujące parametry dla połączenia:

- **Adres sterownika domeny**

  Nazwa komputera, na przykład: `server.mycompany.com`.

  Możesz podać kilka adresów. Wszystkie kontrolery domeny, których adresy podasz, muszą należeć do tej samej domeny.

- **Nazwa domeny Active Directory**

  W pełni kwalifikowana nazwa domeny DNS, na przykład: `mycompany.com`

  Możesz również określić nazwę SAM lub NetBIOS, na przykład: `mycompany`

  Używaj małych liter. Jeżeli tworzysz kilka połączeń dla Serwera administracyjnego lub punktu dystrybucji, podaj inną nazwę dla każdego połączenia.

  > Aby wykonać działania reagowania, nazwa domeny Active Directory podana w tym polu musi być zgodna z nazwą domeny Active Directory podaną w alercie.

- **Login**

  Zaloguj się na konto Active Directory z uprawnieniami administratora, na podstawie których mają zostać wykonane działania reagowania.

- **Hasło**

  Hasło konta Active Directory z uprawnieniami administratora, na podstawie którego mają zostać wykonane działania reagowania.

6. Jeśli chcesz sprawdzić stan połączenia, kliknij przycisk **Sprawdź połączenie**.

   Jeżeli połączenie zostanie nawiązane pomyślnie, zostanie wyświetlony status **Połączono**. W przeciwnym wypadku status będzie ustawiony na **Niepowodzenie** i zostanie wyświetlony komunikat o błędzie z nazwami kontrolerów domeny, z którymi nie udało się nawiązać połączenia.

   > Należy wziąć pod uwagę sposób łączenia się z usługą Active Directory: **z urządzenia z systemem Linux czy z urządzenia z systemem Windows**.

Łączenie się z urządzenia z systemem Linux

Domyślnie podczas łączenia się z kontrolerem domeny i uwierzytelniania go z poziomu urządzenia Linux logika jest następująca:

1. Serwer administracyjny lub punkt dystrybucji próbuje połączyć się z kontrolerem domeny poprzez protokół LDAPS.

   Wymagana jest silna weryfikacja certyfikatu serwera LDAP.

2. Aby zweryfikować certyfikat, umieszczasz publiczną część certyfikatu kontrolera domeny w repozytorium certyfikatów systemu.

   Aby uzyskać dostęp do łańcucha certyfikatów, używana jest ścieżka zależna od systemu operacyjnego do urzędu certyfikacji (CA).

Na przykład:

- /etc/ssl/certs/ca-certificates.crt — Ścieżka dla systemów operacyjnych opartych na Debianie (Debian, Ubuntu, Astra).
- /etc/pki/ca-trust/extracted/pem/tls-ca-bundle.pem — ścieżka dla CentOS lub Red Hat.

3. Jeżeli połączenie LDAPS się nie powiedzie, pojawi się błąd i nie zostanie użyty żaden inny protokół połączenia.

> W przypadku problemów z LDAPS możesz skontaktować się z Pomocą techniczną Kaspersky.

Jeśli nie chcesz instalować certyfikatu w repozytorium certyfikatów systemu, możesz użyć flagi KLNAG_LDAP_SSL_CACERT, aby ustawić ścieżkę do certyfikatu kontrolera domeny. Aby to zrobić należy uruchomić polecenie:

```
klscflag -fset -pv klnagent -n KLNAG_LDAP_SSL_CACERT -t s -v "</path/to/domain-controller/cert>"
```

gdzie `</path/to/domain-controller/cert>` jest ścieżką do publicznej części certyfikatu kontrolera domeny.

Na przykład, jeśli ścieżka to `"/var/opt/kaspersky/ldap_cert.crt"`, polecenie wygląda następująco:
`klscflag -fset -pv klnagent -n KLNAG_LDAP_SSL_CACERT -t s -v "/var/opt/kaspersky/ldap_cert.crt"`

Łączenie z urządzenia z systemem Windows

Podczas łączenia się z kontrolerem domeny i uwierzytelniania go z poziomu urządzenia z systemem Windows ustawienia połączenia są definiowane przez domenę.

Musisz tylko upewnić się, że:

- Protokół LDAPS jest włączony, a port 636 jest dostępny na urządzeniu.
- Zezwalasz na połączenia z kontrolerem domeny poprzez zaporę sieciową lub serwer proxy.

7. Kliknij przycisk **Zapisz**.

Okno zostanie zamknięte, a połączenie zostanie wyświetlone w tabeli połączeń.

W tabeli połączeń możesz wykonać następujące czynności:

- Edytuj parametry połączenia.

  Aby tego dokonać, kliknij odnośnik z parametrem **Adres sterownika domeny** dla wymaganego połączenia. W oknie, które zostanie otwarte, dodaj niezbędne źródła, a następnie kliknij przycisk **Zapisz**.

  Możesz edytować tylko parametry **Login** i **Hasło**.

- Usuń połączenia.

  Aby to zrobić, zaznacz pole wyboru obok połączenia, które chcesz usunąć, kliknij przycisk **Usuń** na pasku narzędzi, a następnie potwierdź usunięcie połączenia.

Konfigurowanie integracji z platformą Kaspersky Automated Security Awareness Platform

Integracja z Kaspersky Automated Security Awareness Platform (dalej również KASAP) umożliwia przypisanie kursów edukacyjnych KASAP do użytkowników powiązanych z alertami.

Ustawienia integracji nie są dziedziczone i mają zastosowanie wyłącznie do Serwera administracyjnego (fizycznego lub wirtualnego), na którym konfigurujesz te ustawienia.

Przed skonfigurowaniem integracji w Kaspersky Security Center Web Console należy utworzyć token autoryzacji i uzyskać adres URL dla żądań API w KASAP.

Aby skonfigurować integrację z platformą Kaspersky Automated Security Awareness Platform:

1. W menu głównym kliknij nazwę Serwera administracyjnego.

   Okno właściwości Serwera administracyjnego zostanie otwarte na zakładce **Ogólne**.

2. Wybierz sekcję **KASAP**.

3. W prawym panelu włącz przełącznik **Integracja KASAP**.

4. Określ ustawienia, które mają być użyte do połączenia z KASAP:

   - **Token API**—token utworzony w celu uzyskania dostępu do KASAP Open API.
   - **Adres URL**—adres URL żądań API, który uzyskałeś podczas tworzenia tokenu API.
   - **Użyj serwera proxy**—przełącznik, który włącza korzystanie z serwera proxy podczas łączenia się z KASAP.

     Domyślnie przełącznik ten jest wyłączony.

5. W razie potrzeby zweryfikuj określone ustawienia, klikając przycisk **Sprawdź połączenie**.

   Wyświetlany jest status połączenia.

6. Kliknij przycisk **Zapisz**.

Skonfigurowano integrację z Kaspersky Automated Security Awareness Platform.

Po zapisaniu ustawień integracji KASAP możesz wyświetlić listę grup edukacyjnych KASAP, klikając przycisk **Wyświetl grupy**.

Jeżeli to konieczne, po wyświetleniu listy grup możesz ją zaktualizować, klikając przycisk **Odśwież grupy**.

Po otwarciu listy nie można jej ukryć. Jeśli wyłączysz przełącznik **Integracja KASAP**, lista grup KASAP nie będzie wyświetlana.

Konfigurowanie integracji z Kaspersky Threat Intelligence Portal Sandbox

Integracja z Kaspersky Threat Intelligence Portal (dalej również zwanym Kaspersky TIP) umożliwia wykonywanie plików przeniesionych do sekcji **Kwarantanna** przy użyciu Kaspersky Sandbox—bezpieczne środowisko odizolowane od sieci korporacyjnej.

Ustawienia integracji nie są dziedziczone i mają zastosowanie wyłącznie do Serwera administracyjnego (fizycznego lub wirtualnego), na którym konfigurujesz te ustawienia.

Przed skonfigurowaniem integracji należy uzyskać token autoryzacyjny dla żądań API w Kaspersky TIP.

Aby skonfigurować integrację z Kaspersky TIP Sandbox:

1. W menu głównym kliknij nazwę Serwera administracyjnego.

   Okno właściwości Serwera administracyjnego zostanie otwarte na zakładce **Ogólne**.

2. Wybierz **Kaspersky TIP**.

3. W prawym panelu włącz przełącznik **Integracja**.

   Zostaną wyświetlone ustawienia połączenia z Kaspersky TIP.

   Jeżeli po skonfigurowaniu i zapisaniu ustawień integracji wyłączysz przełącznik **Integracja**, ustawienia nie zostaną usunięte, ale nie będzie można wykonać działania reagowania.

4. Kliknij przycisk **Dodaj token** i w oknie, które zostanie otwarte, wskaż token, który wcześniej uzyskałeś w Kaspersky TIP, a następnie kliknij przycisk **Dodaj**.

   Okno zostanie zamknięte, a token API zostanie dodany.

5. Jeśli chcesz używać serwera proxy podczas łączenia się z Kaspersky TIP, włącz przełącznik **Użyj serwera proxy**.

   Domyślnie przełącznik ten jest wyłączony.

6. Kliknij przycisk **Zapisz**.

Integracja z Kaspersky TIP Sandbox została skonfigurowana.

Teraz możesz wysyłać pliki z sekcji **Kwarantanna** do Kaspersky TIP Sandbox w celu analizy zagrożeń. Maksymalny rozmiar pliku wynosi 100 MB.

Ponieważ licencja Kaspersky Next XDR Optimum obsługuje wielodostęp, pliki umieszczone w **Kwarantanna** są podzielone według dzierżawców. Podział na poziomie dzierżawcy obowiązuje również podczas przesyłania plików do Kaspersky TIP Sandbox i wyświetlania wyników, jeśli administrator używa dedykowanego konta TIP i tokena API powiązanego z każdym dzierżawcą. Centralne zarządzanie sekcją **Kwarantanna** dla wszystkich dzierżawców nie jest jednak możliwe, ponieważ lista kwarantanny nie wyświetla obiektów zgodnie z hierarchią serwera.

Grupowanie alertów według atrybutów

Agregacja alertów pomaga identyfikować alerty, które mogą dotyczyć tego samego incydentu, co upraszcza proces dochodzenia.

Aby włączyć funkcję agregacji alertów, należy wykonać następujące czynności:

- Włącz podsekcję **Alerty** w menu głównym.
- Aktywuj Serwer administracyjny w ramach licencji Kaspersky Next XDR Optimum, a następnie zainstaluj klucz licencyjny Kaspersky Next XDR Optimum w zarządzanych aplikacjach.

  Podczas korzystania z funkcjonalności Kaspersky Next XDR Optimum w ramach licencji próbnej w trybie testowym, najpierw musisz dodać podrzędny fizyczny Serwer administracyjny, a następnie aktywować ten serwer na podstawie tej licencji.

Jeśli korzystasz z licencji Kaspersky Next EDR Optimum, nie musisz aktywować aplikacji zainstalowanych na zarządzanych urządzeniach w ramach licencji Kaspersky Next XDR Optimum. Należy to zrobić tylko dla nowych urządzeń, o ile takie istnieją.
Ponieważ licencja Kaspersky Next XDR Optimum obsługuje wielodostęp, można centralnie dystrybuować klucz licencyjny do zarządzanych aplikacji. Automatyczna dystrybucja licencji do podrzędnych i wirtualnych Serwerów administracyjnych nie jest obsługiwana.

Możesz agregować alerty według nazwy urządzenia, konta lub nazwy skrótu (SHA256).

> Alerty są agregowane według atrybutu tylko wtedy, gdy atrybut ten nie jest pusty.

Alerty są agregowane, jeśli mają przynajmniej jeden wspólny atrybut i występują w ciągu 24 godzin od wystąpienia jakiegokolwiek innego alertu w grupie.

Aby agregować alerty według atrybutów:

1. W menu głównym przejdź do **Monitorowanie** → **Alerty**.
2. Wykonaj jedną z poniższych czynności:
   - Włącz przełącznik **Agregacja alertów**, a następnie wybierz jeden lub więcej atrybutów, według których chcesz agregować alerty:
     - **Nazwa urządzenia**
     - **Konto**
     - **Hash pliku (SHA256)**

     Atrybuty **Nazwa urządzenia** i **Konto** są wybierane domyślnie.
   - Kliknij ikonę ustawienia (⚙). W panelu **Ustawienia tabeli**, który się otworzy, przejdź do zakładki **Grupowanie**. Wybierz **ID grupy agregacji** i kliknij **Zastosuj**.

Po włączeniu agregacji alerty są sortowane według **Czas zdarzenia** od najnowszych do najstarszych. Dodatkowe opcje sortowania nie są obsługiwane. Wybranie innej opcji grupowania spowoduje wyłączenie agregacji.

Tabela wyświetla alerty zagregowane według atrybutów. Alerty, które nie są zagregowane są wyświetlane na dole tabeli.

Każdy alert po agregacji jest przypisywany tylko do jednej grupy.

Interakcja Kaspersky Security Center Web Console i innych rozwiązań Kaspersky

W tej sekcji opisano, jak skonfigurować dostęp z Kaspersky Security Center Web Console do innej aplikacji Kaspersky, takiej jak Kaspersky Managed Detection and Response. W tej sekcji opisano również, jak skonfigurować eksport do systemów SIEM.

Nawiązywanie połączenia w tle

Aby skonfigurować interakcję między Kaspersky Security Center Linux a inną aplikacją lub rozwiązaniem Kaspersky, na przykład Kaspersky Managed Detection and Response (nazywane również MDR), musisz ustanowić połączenie w tle pomiędzy konsolą Kaspersky Security Center Web Console a Serwerem administracyjnym. Możesz nawiązać to połączenie tylko wtedy, jeśli Twoje konto ma uprawnienie Modyfikuj listy ACL obiektów w obszarze funkcyjnym **Cechy ogólne: Uprawnienia użytkownika**.

> Możesz skonfigurować interakcję tylko między Kaspersky Managed Detection and Response a wersją Kaspersky Security Center dla systemu Windows.

Aby nawiązać połączenie w tle:

1. W menu głównym przejdź do sekcji **Ustawienia** → **Integracja**.
2. Wybierz zakładkę **Ustawienia serwera proxy Web Console**.
3. W sekcji **Integracja**, ustaw przycisk przełącznika do nawiązywania połączenia w tle w pozycji: **Połączenie w tle w celu integracji Włączone**.
4. W otwartej sekcji **Włącz połączenie w tle** kliknij przycisk **OK**.

Połączenie w tle pomiędzy konsolą Kaspersky Security Center Web Console i Serwerem administracyjnym jest nawiązywane. Serwer administracyjny tworzy konto dla połączenia w tle, które jest używane jako konto usługi do utrzymywania interakcji między Kaspersky Security Center Linux a inną aplikacją lub rozwiązaniem Kaspersky. Nazwa tego konta usługi zawiera przedrostek NWCSvcUser. Serwer administracyjny automatycznie zmienia hasło do konta usługi co 30 dni ze względów bezpieczeństwa. Nie możesz usunąć konta usługi ręcznie. Serwer administracyjny automatycznie usuwa to konto po wyłączeniu połączenia między usługami. Serwer administracyjny tworzy jedno konto usługi dla każdej Kaspersky Security Center Web Console i Konsoli Administracyjnej i przypisuje wszystkie konta usług do grupy bezpieczeństwa o nazwie ServiceNwcGroup. Serwer administracyjny tworzy grupę zabezpieczeń automatycznie podczas procesu instalacji Kaspersky Security Center Linux. Nie możesz usunąć tej grupy zabezpieczeń ręcznie.

Konfigurowanie połączenia z serwerem proxy

Aby skonfigurować połączenie z serwerem proxy dla Kaspersky Security Center Web Console i wtyczek webowych:

1. W menu głównym przejdź do sekcji **Ustawienia** → **Integracja**.
2. Wybierz zakładkę **Ustawienia serwera proxy Web Console**.
3. Włącz opcję **Użyj serwera proxy**.
4. Określ ustawienia połączenia serwera proxy:
   - **Adres serwera proxy**
   - **Numer portu**
   - **Uwierzytelnianie na serwerze proxy**
   - **Nazwa użytkownika** (wymagana, jeśli włączysz opcję **Uwierzytelnianie serwera proxy**)
   - **Hasło** (wymagane, jeśli włączysz opcję **Uwierzytelnianie serwera proxy**)
5. Kliknij **Zapisz**, aby zapisać ustawienia połączenia serwera proxy.

Jeśli masz hierarchię Serwerów administracyjnych, ustawienia połączenia serwera proxy nie są propagowane do Web Console, które zarządzają podrzędnymi Serwerami administracyjnymi. Musisz skonfigurować połączenie serwera proxy osobno dla każdej Kaspersky Security Center Web Console.

Zdalna diagnostyka urządzeń klienckich

Możesz użyć zdalnej diagnostyki do zdalnego wykonania następujących operacji na urządzeniach klienckich z systemem Windows i z systemem Linux:

- Włączania i wyłączania śledzenia, zmieniania poziomu śledzenia i pobierania pliku śledzenia
- Pobierania informacji o systemie i ustawień aplikacji
- Pobierania dzienników zdarzeń
- Generowania pliku zrzutu dla aplikacji
- Uruchamiania diagnostyki i pobierania jej raportów
- Uruchamianie, zatrzymywanie i ponowne uruchamianie aplikacji

Możesz użyć dzienników zdarzeń i raportów diagnostycznych pobranych z urządzenia klienckiego do samodzielnego rozwiązania problemów. Dodatkowo, jeśli skontaktujesz się z działem pomocy technicznej Kaspersky, specjalista z pomocy technicznej może poprosić o pobranie plików śledzenia, plików zrzutu pamięci, dzienników zdarzeń, a także raportów diagnostycznych z urządzenia klienckiego w celu przeprowadzenia dalszej analizy w Kaspersky.

Otwieranie okna zdalnej diagnostyki

Aby przeprowadzić zdalną diagnostykę na urządzeniach klienckich z systemem Windows i systemem Linux, należy najpierw otworzyć okno zdalnej diagnostyki.

W celu otwarcia okna zdalnej diagnostyki:

1. W celu wybrania urządzenia, dla którego chcesz otworzyć okno zdalnej diagnostyki, wykonaj jedną z następujących czynności:
   - Jeśli urządzenie należy do grupy administracyjnej, w menu głównym przejdź do **Zarządzanie zasobami** → **Zasoby (urządzenia)**.
   - Jeśli urządzenie należy do grupy Urządzenia nieprzypisane, w menu głównym przejdź do **Zarządzanie zasobami** → **Urządzenia nieprzypisane**.
2. Kliknij nazwę żądanego urządzenia.
3. W otwartym oknie właściwości urządzenia wybierz zakładkę **Zaawansowane**.
4. W zakładce **Zaawansowane** kliknij **Zdalna diagnostyka**.

   Spowoduje to otwarcie okna **Zdalna diagnostyka** urządzenia klienckiego. Jeżeli połączenie między Serwerem administracyjnym a urządzeniem klienckim nie zostanie nawiązane, zostanie wyświetlony komunikat o błędzie.

Alternatywnie, jeśli chcesz uzyskać jednocześnie wszystkie informacje diagnostyczne na temat urządzenia klienckiego z systemem Linux, możesz uruchomić na tym urządzeniu skrypt collect.sh.

Włączanie i wyłączanie śledzenia dla aplikacji

Możesz włączyć i wyłączyć śledzenie aplikacji, w tym śledzenie Xperf.

Włączanie i wyłączanie śledzenia

W celu włączenia lub wyłączenia śledzenia na zdalnym urządzeniu:

1. Otwórz okno do zdalnej diagnostyki urządzenia klienckiego.
2. W oknie zdalnej diagnostyki wybierz kartę **Aplikacje Kaspersky**.

   W sekcji **Zarządzanie aplikacjami** wyświetlana jest lista aplikacji Kaspersky zainstalowanych na urządzeniu.
3. Na liście aplikacji wybierz aplikację, dla której chcesz włączyć lub wyłączyć śledzenie.

   Zostanie otwarta lista opcji zdalnej diagnostyki.
4. Jeśli chcesz włączyć śledzenie:

   a. W sekcji **Śledzenie** kliknij **Włącz śledzenie**.

   b. W otwartym oknie **Modyfikuj poziom śledzenia** zalecane jest zachowanie domyślnych wartości ustawień. Jeśli jest to wymagane, specjalista z pomocy technicznej przeprowadzi Cię przez proces konfiguracji. Dostępne są następujące ustawienia:

   - **Poziom śledzenia**

     Poziom śledzenia definiuje ilość szczegółów, jaką plik śledzenia zawiera.

   - **Śledzenie na podstawie rotacji**

     Aplikacja nadpisuje informacje o śledzeniu, aby zapobiec nadmiernemu zwiększeniu rozmiaru pliku śledzenia. Określ maksymalną liczbę plików, jaka będzie używana do przechowywania informacji o śledzeniu, a także maksymalny rozmiar każdego pliku. Jeśli zostanie zapisana maksymalna liczba plików śledzenia o maksymalnym rozmiarze, najstarszy plik śledzenia zostanie usunięty, aby mógł zostać zapisany nowy plik śledzenia.

     To ustawienie jest dostępne tylko dla Kaspersky Endpoint Security.

   c. Kliknij **Zapisz**.

   Śledzenie jest włączone dla wybranej aplikacji. W niektórych przypadkach, aby włączyć śledzenie, konieczne jest ponowne uruchomienie aplikacji zabezpieczającej i jej zadania.

> Na urządzeniach klienckich z systemem Linux śledzenie dla komponentu Updater of Network Agent jest regulowane przez ustawienia Agenta sieciowego. Dlatego opcje **Włącz śledzenie** i **Modyfikuj poziom śledzenia** są wyłączone dla tego modułu na urządzeniach klienckich z systemem Linux.

5. Jeśli chcesz wyłączyć śledzenie dla wybranej aplikacji, kliknij przycisk **Wyłącz śledzenie**.

   Śledzenie jest wyłączone dla wybranej aplikacji.

Włączanie śledzenia Xperf

W przypadku Kaspersky Endpoint Security specjalista z pomocy technicznej może poprosić o włączenie śledzenia Xperf dla informacji o działaniu systemu.

Aby włączyć i skonfigurować śledzenie Xperf lub je wyłączyć:

1. Otwórz okno do zdalnej diagnostyki urządzenia klienckiego.

2. W oknie zdalnej diagnostyki wybierz kartę **Aplikacje Kaspersky**.

   W sekcji **Zarządzanie aplikacjami** wyświetlana jest lista aplikacji Kaspersky zainstalowanych na urządzeniu.

3. Na liście aplikacji wybierz Kaspersky Endpoint Security for Windows.

   Zostanie wyświetlona lista opcji zdalnej diagnostyki dla Kaspersky Endpoint Security for Windows.

4. W sekcji **Śledzenie Xperf** kliknij opcję **Włącz śledzenie Xperf**.

   Jeśli śledzenie Xperf jest już włączone, zamiast tego zostanie wyświetlony przycisk **Wyłącz śledzenie Xperf**. Kliknij ten przycisk, jeśli chcesz wyłączyć śledzenie Xperf dla Kaspersky Endpoint Security for Windows.

5. W otwartym oknie **Zmień poziom śledzenia Xperf**, w zależności od odpowiedzi od specjalisty z pomocy technicznej, wykonaj jedną z następujących czynności:

   a. Wybierz jeden z następujących poziomów śledzenia:

   - **Niski**

     Plik śledzenia tego typu zawiera minimalną ilość informacji o systemie.

     Domyślnie opcja ta jest zaznaczona.

   - **Głęboki**

     Plik śledzenia tego typu zawiera bardziej szczegółowe informacje niż pliki śledzenia typu *Niski* i specjaliści z pomocy technicznej mogą poprosić o nie, gdy plik śledzenia typu *Niski* nie jest wystarczający do oceny działania. *Głęboki* plik śledzenia zawiera informacje techniczne o systemie, w tym informacje o sprzęcie, systemie operacyjnym, listę uruchomionych i zakończonych procesów i aplikacji, zdarzeń użytych do oceny działania, a także zdarzeń z Narzędzia do oceny wydajności systemu Windows.

   b. Wybierz jeden z następujących typów śledzenia Xperf:

   - **Podstawowy**

     Informacje o śledzeniu są otrzymywane podczas działania aplikacji Kaspersky Endpoint Security.

     Domyślnie opcja ta jest zaznaczona.

   - **Po ponownym uruchomieniu**

     Informacje o śledzeniu są otrzymywane, gdy system operacyjny jest uruchamiany na zarządzanym urządzeniu. Ten typ śledzenia jest efektywny, gdy problem, który wpływa na działanie systemu, pojawi się po włączeniu urządzenia, a przed uruchomieniem Kaspersky Endpoint Security.

Możesz także zostać poproszony o włączenie opcji **Rozmiar pliku, po którym nastąpi nadpisanie, w MB**, aby zapobiec nadmiernemu zwiększeniu rozmiaru pliku śledzenia. Następnie określ maksymalny rozmiar pliku śledzenia. Jeśli plik osiągnie maksymalny rozmiar, najstarsze informacje śledzenia zostaną nadpisane nowymi informacjami.

c. Zdefiniuj rozmiar pliku rotacji.

d. Kliknij **Zapisz**.

Śledzenie Xperf jest włączone i skonfigurowane.

6. Jeśli chcesz wyłączyć śledzenie Xperf dla Kaspersky Endpoint Security for Windows, kliknij opcję **Wyłącz śledzenie Xperf** w sekcji **Śledzenie Xperf**.

   Śledzenie Xperf jest wyłączone.

Pobieranie plików śledzenia aplikacji

W celu pobrania pliku śledzenia aplikacji:

1. Otwórz okno do zdalnej diagnostyki urządzenia klienckiego.

2. W oknie zdalnej diagnostyki wybierz kartę **Aplikacje Kaspersky**.

   W sekcji **Zarządzanie aplikacjami** wyświetlana jest lista aplikacji Kaspersky zainstalowanych na urządzeniu.

3. Na liście aplikacji wybierz aplikację, dla której chcesz pobrać plik śledzenia.

4. W sekcji **Śledzenie** kliknij przycisk **Pliki śledzenia**.

   To spowoduje otwarcie okna **Dzienniki śledzenia urządzenia**, w którym wyświetlana jest lista plików śledzenia.

5. Z listy plików śledzenia wybierz plik, który chcesz pobrać.

6. Wykonaj jedną z poniższych czynności:

   - Pobierz wybrany plik, klikając **Pobierz**. Możesz wybrać jeden lub kilka plików do pobrania.

   - Pobierz porcję wybranego pliku:

     a. Kliknij **Pobierz część**.

     Nie można jednocześnie pobierać części kilku plików. Jeśli wybierzesz więcej niż jeden plik śledzenia, przycisk **Pobierz część** będzie nieaktywny.

     b. W otwartym oknie określ nazwę i fragment pliku do pobrania, zgodnie ze swoimi potrzebami.

     W przypadku urządzeń z systemem Linux edytowanie nazwy części pliku nie jest dostępne.

     c. Kliknij **Pobierz**.

Wybrany plik lub jego porcja zostają pobrane do lokalizacji, którą określiłeś.

Usuwanie plików śledzenia

Możesz usunąć pliki śledzenia, które nie są już potrzebne.

W celu usunięcia pliku śledzenia:

1. Otwórz okno do zdalnej diagnostyki urządzenia klienckiego.
2. W otwartym oknie zdalnej diagnostyki wybierz kartę **Dzienniki zdarzeń**.
3. W sekcji **Pliki śledzenia** kliknij opcję **Raporty usługi Windows Update** lub **Raporty zdalnej instalacji** w zależności od plików śledzenia, które chcesz usunąć.

   Odnośnik **Raporty usługi Windows Update** jest dostępny tylko dla urządzeń klienckich z systemem Windows.

   To spowoduje otwarcie okna **Dzienniki śledzenia urządzenia**, w którym wyświetlana jest lista plików śledzenia.
4. Z listy plików śledzenia wybierz jeden lub większą liczbę plików, które chcesz usunąć.
5. Kliknij przycisk **Usuń**.

Wybrane pliki śledzenia zostaną usunięte.

Pobierania ustawień aplikacji

W celu pobrania ustawień aplikacji z urządzenia klienckiego:

1. Otwórz okno do zdalnej diagnostyki urządzenia klienckiego.
2. W oknie zdalnej diagnostyki wybierz kartę **Aplikacje Kaspersky**.
3. W sekcji **Ustawienia aplikacji** kliknij przycisk **Pobierz**, aby pobrać informacje o ustawieniach aplikacji zainstalowanych na urządzeniu klienckim.

Archiwum ZIP z informacjami zostanie pobrane do określonej lokalizacji.

Pobieranie informacji systemowych z urządzenia klienckiego

W celu pobrania informacji o systemie z urządzenia klienckiego:

1. Otwórz okno do zdalnej diagnostyki urządzenia klienckiego.
2. W oknie zdalnej diagnostyki wybierz kartę **Informacje o systemie**.

3. Kliknij przycisk **Pobierz**, aby pobrać informacje o systemie urządzenia klienckiego.

   Jeśli uzyskasz informacje o systemie urządzenia z systemem Linux, do pliku wynikowego zostanie dodany plik zrzutu dla aplikacji zakończonych awaryjnie.

   > Archiwum może zawierać poufne dane (na przykład klucze i hasła) w postaci zwykłego tekstu. Zalecamy przejrzenie plików w archiwum i usunięcie takich danych przed wysłaniem archiwum do Pomocy technicznej Kaspersky.

Plik z informacjami zostanie pobrany do określonej lokalizacji.

Pobierania dzienników zdarzeń

W celu pobrania dziennika zdarzeń ze zdalnego urządzenia:

1. Otwórz okno do zdalnej diagnostyki urządzenia klienckiego.
2. W oknie zdalnej diagnostyki, na karcie **Dzienniki zdarzeń** kliknij **Wszystkie dzienniki urządzenia**.
3. W oknie **Wszystkie dzienniki urządzenia** wybierz jeden lub kilka dzienników.
4. Wykonaj jedną z poniższych czynności:
   - Pobierz wybrany plik, klikając **Pobierz cały plik**.
   - Pobierz porcję wybranego dziennika:
     a. Kliknij **Pobierz część**.

     Nie można jednocześnie pobierać części kilku dzienników. Jeśli wybierzesz więcej niż jeden dziennik zdarzeń, przycisk **Pobierz część** będzie nieaktywny.

     b. W otwartym oknie określ nazwę i część pliku do pobrania, odpowiednio do potrzeb.

     W przypadku urządzeń z systemem Linux funkcja edytowania nazwy części dziennika nie jest dostępna.

     c. Kliknij **Pobierz**.

Wybrany dziennik zdarzeń lub jego część zostają pobrane do określonej lokalizacji.

Uruchamianie, zatrzymywanie, ponowne uruchamianie aplikacji

Aplikację można uruchomić, zatrzymać lub uruchomić ponownie.

W celu uruchomienia, zatrzymania lub ponownego uruchomienia aplikacji:

1. Otwórz okno do zdalnej diagnostyki urządzenia klienckiego.
2. W oknie zdalnej diagnostyki wybierz kartę **Aplikacje Kaspersky**.

   W sekcji **Zarządzanie aplikacjami** wyświetlana jest lista aplikacji Kaspersky zainstalowanych na urządzeniu.
3. Na liście aplikacji wybierz aplikację, którą chcesz uruchomić, zatrzymać lub uruchomić ponownie.
4. Wybierz akcję, klikając jeden z następujących przycisków:

   - **Zatrzymaj aplikację**

     Ten przycisk jest dostępny tylko wtedy, gdy aplikacja jest aktualnie uruchomiona.
   - **Uruchom aplikację ponownie**

     Ten przycisk jest dostępny tylko wtedy, gdy aplikacja jest aktualnie uruchomiona.
   - **Uruchom aplikację**

     Ten przycisk jest dostępny tylko wtedy, gdy aplikacja nie jest aktualnie uruchomiona.

   W zależności od wybranej akcji, wymagana aplikacja zostanie uruchomiona, zatrzymana lub uruchomiona ponownie na urządzeniu klienckim.

Jeśli uruchomisz ponownie Agenta sieciowego, zostanie wyświetlona wiadomość informująca, że bieżące połączenie urządzenia z Serwerem administracyjnym zostanie utracone.

Uruchamianie zdalnej diagnostyki Agenta sieciowego Kaspersky Security Center Linux i pobieranie wyników

Aby rozpocząć diagnostykę Agenta sieciowego Kaspersky Security Center Linux na urządzeniu zdalnym i pobrać wyniki:

1. Otwórz okno do zdalnej diagnostyki urządzenia klienckiego.
2. W oknie zdalnej diagnostyki wybierz kartę **Aplikacje Kaspersky**.

   W sekcji **Zarządzanie aplikacjami** wyświetlana jest lista aplikacji Kaspersky zainstalowanych na urządzeniu.
3. Na liście aplikacji wybierz opcję **Agent sieciowy Kaspersky Security Center Linux**.

   Zostanie otwarta lista opcji zdalnej diagnostyki.
4. W sekcji **Raport diagnostyczny** kliknij przycisk **Uruchom diagnostykę**.

   Spowoduje to uruchomienie procesu zdalnej diagnostyki i wygenerowanie raportu diagnostycznego. Po zakończeniu procesu diagnostyki, przycisk **Pobierz raport diagnostyczny** stanie się dostępny.
5. Kliknij przycisk **Pobierz raport diagnostyczny**, aby pobrać raport.

Raport zostanie pobrany do określonej lokalizacji.

Uruchamianie aplikacji na urządzeniu klienckim

Konieczne może być uruchomienie aplikacji na urządzeniu klienckim, jeśli specjalista z pomocy technicznej firmy Kaspersky poprosi o to. Nie trzeba instalować aplikacji na tym urządzeniu.

Jeśli chcesz uruchomić niestandardowy skrypt na urządzeniu klienckim, możesz użyć zmiennej środowiskowej `KLACDT_SAVE_SETTING` w celu określenia ścieżki, w której zostaną zapisane wyniki wykonania. Na przykład:

- W przypadku urządzenia z systemem Windows:

  ```
  @echo some result > %KLACDT_SAVE_SETTING%\res.log
  ```

- W przypadku urządzenia z systemem Linux:

  ```
  echo some result > $KLACDT_SAVE_SETTING/res.log
  ```

W celu uruchomienia aplikacji na urządzeniu klienckim:

1. Otwórz okno do zdalnej diagnostyki urządzenia klienckiego.
2. W oknie zdalnej diagnostyki wybierz kartę **Uruchamianie aplikacji zdalnej**.
3. W polu **Typ obiektu** wybierz typ obiektu, który chcesz przesłać:
   - Wybierz **Plik**, aby przesłać plik wykonywalny.
   - Wybierz **Folder**, aby przesłać folder zawierający aplikację, którą chcesz uruchomić na urządzeniu klienta.

     Jeżeli wybierzesz ten typ obiektu, pojawi się pole **Nazwa pliku wykonywalnego do uruchomienia**. W tym polu należy podać nazwę pliku wykonywalnego w folderze. Można również określić ścieżkę względną do pliku.
   - Wybierz **Archiwum**, aby przesłać archiwum ZIP zawierające aplikację, którą chcesz uruchomić na urządzeniu klienta.

     Jeżeli wybierzesz ten typ obiektu, pojawi się pole **Nazwa pliku wykonywalnego do uruchomienia**. W tym polu należy podać nazwę pliku wykonywalnego w folderze. Można również określić ścieżkę względną do pliku.

     > Archiwum ZIP musi zawierać folder z narzędziami. Ten folder zawiera plik wykonywalny do uruchomienia na urządzeniu zdalnym.
4. Prześlij obiekt, wybierając go w oknie systemowym lub przeciągając do pola przesyłania.
5. W razie potrzeby w polu **Argumenty wiersza polecenia** określ argumenty wiersza polecenia, które mają zostać przekazane podczas uruchamiania pliku wykonywalnego.
6. Kliknij przycisk **Wczytaj i uruchom**, aby uruchomić wybraną aplikację na urządzeniu klienta.

7. Po pomyślnym ukończeniu wykonywania aplikacji można pobrać wyniki wykonania, klikając przycisk **Pobierz wyniki wykonania aplikacji**.

   Wyniki wykonania aplikacji są przechowywane do momentu uruchomienia nowej diagnostyki lub zamknięcia okna.

Zdalna diagnostyka urządzenia klienta przy użyciu aplikacji została ukończona.

Uruchamianie zdalnej diagnostyki na urządzeniu klienckim z systemem Linux

Kaspersky Security Center Linux umożliwia pobranie podstawowych informacji diagnostycznych z urządzenia klienckiego. Alternatywnie możesz uzyskać informacje diagnostyczne na temat urządzenia z systemem Linux, korzystając ze skryptu collect.sh firmy Kaspersky. Ten skrypt jest uruchamiany na urządzeniu klienckim z systemem Linux, które wymaga diagnozy, a następnie generuje plik zawierający informacje diagnostyczne, informacje o systemie o tym urządzeniu, pliki śledzenia aplikacji, dzienniki urządzenia i plik zrzutu dla aplikacji zakończonych awaryjnie.

Zalecamy użycie skryptu collect.sh w celu jednoczesnego uzyskania wszystkich informacji diagnostycznych na temat urządzenia klienckiego z systemem Linux. Jeśli pobierasz informacje diagnostyczne zdalnie poprzez Kaspersky Security Center Linux, będziesz musiał przejść przez wszystkie sekcje interfejsu zdalnej diagnostyki. Prawdopodobnie nie zostaną uzyskane w całości informacje diagnostyczne dla urządzenia opartego na systemie Linux.

Jeśli chcesz wysłać wygenerowany plik z informacjami diagnostycznymi do pomocy technicznej Kaspersky, przed wysłaniem pliku usuń wszystkie poufne informacje.

Aby pobrać informacje diagnostyczne z urządzenia klienckiego z systemem Linux za pomocą skryptu collect.sh:

1. Pobierz skryptcollect.sh spakowane w archiwum collect.tar.gz.
2. Skopiuj pobrane archiwum na urządzenie klienckie z systemem Linux, które wymaga diagnozy.
3. Uruchom następujące polecenie, aby rozpakować archiwum collect.tar.gz:

   ```
   # tar -xzf collect.tar.gz
   ```

4. Uruchom następujące polecenie, aby określić uprawnienia do wykonywania skryptu:

   ```
   # chmod +x collect.sh
   ```

5. Uruchom skrypt collect.sh, korzystając z konta z uprawnieniami administratora:

   ```
   # ./collect.sh
   ```

Generowany jest plik z informacjami diagnostycznymi, który jest zapisywany w folderze /tmp/$HOST_NAME-collect.tar.gz.

Zarządzanie aplikacjami i plikami wykonywalnymi firm trzecich na urządzeniach klienckich

Ta sekcja opisuje funkcje Kaspersky Security Center Linux, które dotyczą zarządzania uruchamianiem aplikacji i plików wykonywalnych firm trzecich na urządzeniach klienckich.

Korzystanie z Kontroli aplikacji do zarządzania plikami wykonywalnymi

Możesz użyć komponentu Kontrola aplikacji, aby zezwolić lub zablokować uruchamianie plików wykonywalnych na urządzeniach użytkowników. Komponent Kontrola aplikacji obsługuje systemy operacyjne oparte na systemie Windows i Linux.

W przypadku systemów operacyjnych opartych na systemie Linux komponent Kontrola aplikacji jest dostępny począwszy od Kaspersky Endpoint Security 11.2 for Linux.

Wymagania wstępne

- Kaspersky Security Center Linux zostanie wdrożony w Twojej organizacji.
- Zasada Kaspersky Endpoint Security for Linux lub Kaspersky Endpoint Security for Windows została utworzona i jest aktywna. W tej zasadzie włączony jest komponent Kontrola aplikacji.

Etapy

Scenariusz korzystania z Kontroli aplikacji podzielony jest na etapy:

1. **Tworzenie i przeglądanie listy plików wykonywalnych na urządzeniach klienckich**

   Ten etap pomaga w odnalezieniu plików wykonywalnych, które znajdują się na zarządzanych urządzeniach. Przejrzyj listę plików wykonywalnych i porównaj ją z listami dozwolonych i zabronionych plików wykonywalnych. Ograniczenia dotyczące użycia plików wykonywalnych mogą być związane z polityką bezpieczeństwa informacji, obowiązującej w Twojej organizacji.

   Jak to zrobić: Uzyskiwanie i przeglądanie listy plików wykonywalnych przechowywanych na urządzeniach klienckich

2. **Tworzenie kategorii dla plików wykonywalnych używanych w Twojej organizacji**

Przeanalizuj listy plików wykonywalnych, przechowywanych na zarządzanych urządzeniach. Na podstawie analizy utwórz kategorie dla plików wykonywalnych. Zalecane jest utworzenie kategorii „Aplikacje do pracy", która obejmuje standardowy zestaw plików wykonywalnych używanych w Twojej organizacji. Jeśli różne grupy bezpieczeństwa używają własnych zestawów plików wykonywalnych w swojej pracy, oddzielna kategoria może zostać utworzona dla każdej grupy bezpieczeństwa.

Uruchamianie plików wykonywalnych, których ustawienia nie odpowiadają żadnym regułom Kontroli aplikacji, jest regulowane przez wybrany tryb działania komponentu:

- *Lista zablokowanych*. Tryb jest używany, jeśli chcesz zezwolić na uruchamianie wszystkich plików wykonywalnych, za wyjątkiem plików określonych w regułach blokowania. Ten tryb jest wybrany domyślnie.
- *Lista zezwolonych*. Tryb jest używany, jeśli chcesz zablokować uruchamianie wszystkich plików wykonywalnych, z wyjątkiem plików określonych w regułach zezwalania.

Reguły Kontroli aplikacji są implementowane poprzez kategorie plików wykonywalnych. W Kaspersky Security Center Linux istnieją trzy typy kategorii plików wykonywalnych:

- Ręcznie dodana kategoria z zawartością. Definiujesz warunki, na przykład metadane plików, kod hashu pliku, certyfikat pliku, ścieżkę do pliku, aby uwzględniać pliki wykonywalne w kategorii.
- Kategoria zawierająca pliki wykonywalne z wybranych urządzeń. Określasz urządzenie, którego pliki wykonywalne są automatycznie uwzględniane w kategorii.
- Kategoria zawierająca pliki wykonywalne z wybranego folderu. Określasz folder, z którego pliki wykonywalne mają zostać automatycznie uwzględnione w kategorii.

3. **Konfigurowanie Kontroli aplikacji w zasadzie Kaspersky Endpoint Security**

   Skonfiguruj komponent Kontrola aplikacji w zasadzie Kaspersky Endpoint Security for Linux, korzystając z kategorii, które utworzono w poprzednim kroku.

   Wskazówki jak to zrobić: Konfigurowanie Kontroli aplikacji w zasadzie Kaspersky Endpoint Security for Windows

4. **Włączanie komponentu Kontrola aplikacji w trybie testowym**

   Aby zapewnić, że reguły Kontroli aplikacji nie będą blokowały plików wykonywalnych wymaganych do pracy użytkownika, zalecane jest włączenie testowania reguł Kontroli aplikacji i analizowanie ich działania po utworzeniu nowych reguł. Po włączeniu testowania, Kaspersky Endpoint Security for Windows nie zablokuje plików wykonywalnych, których uruchamianie jest zablokowane przez reguły Kontroli aplikacji, ale zamiast tego wyśle powiadomienia o ich uruchomieniu do Serwera administracyjnego.

   Podczas testowania reguł Kontroli aplikacji zalecane jest wykonanie następujących działań:

   - Określenie okresu testowania. Okres testowania może wahać się od siedmiu dni do dwóch miesięcy.
   - Sprawdź zdarzenia wynikające z testowania działania Kontroli aplikacji.

   Wskazówki jak postępować dla Kaspersky Security Center Web Console: Konfigurowanie komponentu Kontrola aplikacji w zasadzie Kaspersky Endpoint Security for Windows. Postępuj zgodnie z tymi instrukcjami i włącz opcję **Tryb testowy** w procesie konfiguracji.

5. **Zmienianie ustawień komponentu Kontrola aplikacji**

   Jeśli to konieczne, wprowadź zmiany w ustawieniach Kontroli aplikacji. W oparciu o wyniki testu, możesz dodać pliki wykonywalne związane ze zdarzeniami komponentu Kontrola aplikacji do kategorii z zawartością dodaną ręcznie.

   Wskazówki jak to zrobić: Kaspersky Security Center Web Console: Dodawanie plików wykonywalnych dotyczących zdarzeń do kategorii aplikacji

6. **Stosowanie reguł Kontroli aplikacji w trybie działania**

   Po przetestowaniu reguł Kontroli aplikacji i zakończeniu konfiguracji kategorii możesz zastosować reguły Kontroli aplikacji w trybie działania.

   Wskazówki jak postępować dla Kaspersky Security Center Web Console: Konfigurowanie komponentu Kontrola aplikacji w zasadzie Kaspersky Endpoint Security for Windows. Postępuj zgodnie z tymi instrukcjami i wyłącz opcję **Tryb testowy** w procesie konfiguracji.

7. **Weryfikowanie konfiguracji Kontroli aplikacji**

   Upewnij się, że wykonałeś następujące czynności:

   - Utworzono kategorie dla plików wykonywalnych.
   - Skonfigurowano Kontrolę aplikacji przy użyciu kategorii.
   - Zastosowałeś reguły Kontroli aplikacji w trybie działania.

Wyniki

Po zakończeniu scenariusza uruchamianie plików wykonywalnych na zarządzanych urządzeniach jest kontrolowane. Użytkownicy mogą uruchamiać tylko te pliki wykonywalne, które są dozwolone w Twojej organizacji, a nie mogą uruchamiać plików wykonywalnych, które są zabronione w Twojej organizacji.

Aby uzyskać szczegółowe informacje na temat Kontroli aplikacji, zapoznaj się z Pomocą Kaspersky Endpoint Security for Linux oraz Kaspersky Endpoint Security for Windows Pomoc.

Uzyskiwanie i przeglądanie listy plików wykonywalnych przechowywanych na urządzeniach klienckich

Listę plików wykonywalnych przechowywanych na urządzeniach klienckich można uzyskać w jeden z następujących sposobów:

- Włączenie powiadomień o uruchomieniu aplikacji w zasadach Kaspersky Endpoint Security.
- Tworzenie zadania inwentaryzacji.

Włączenie powiadomień o uruchomieniu aplikacji w zasadach Kaspersky Endpoint Security

Aby włączyć powiadomienia o uruchomieniu aplikacji:

1. Otwórz ustawienia zasad Kaspersky Endpoint Security, a następnie przejdź do **Ustawienia ogólne** → **Raporty i pliki danych**.

2. W grupie ustawień **Przesyłania danych do Serwera administracyjnego** zaznacz pole wyboru **Informacje o uruchomionych aplikacjach** i zapisz zmiany.

   Gdy użytkownik próbuje uruchomić pliki wykonywalne, informacje o tych plikach są dodawane do listy plików wykonywalnych na urządzeniu klienckim. Kaspersky Endpoint Security wysyła te informacje do Agenta sieciowego, a następnie Agent sieciowy wysyła je do Serwera administracyjnego.

Tworzenie zadania inwentaryzacji

Dla Kaspersky Endpoint Security for Linux funkcja inwentaryzacji plików wykonywalnych jest dostępna nie wcześniej niż w wersji 11.2.

Możesz zmniejszyć obciążenie bazy danych, jednocześnie uzyskując informacje o zainstalowanych aplikacjach. Aby zaoszczędzić miejsce, uruchom zadanie inwentaryzacji na urządzeniach referencyjnych, na których jest zainstalowany standardowy zestaw oprogramowania. Preferowana liczba urządzeń to od 1 do 3.

W celu utworzenia zadania dla plików wykonywalnych na urządzeniach klienckich:

1. W menu głównym przejdź do **Zadania**.

   Zostanie wyświetlona lista zadań.

2. Kliknij przycisk **Dodaj**.

   Zostanie uruchomiony Kreator tworzenia nowego zadania. Postępuj zgodnie z krokami kreatora.

3. Na stronie **Ustawienia nowych zadań**, z listy rozwijanej **Aplikacja** wybierz Kaspersky Endpoint Security for Linux lub Kaspersky Endpoint Security for Windows, w zależności od systemu operacyjnego urządzeń klienckich.

4. Z listy rozwijalnej **Typ zadania** wybierz **Inwentaryzacja**.

5. Na stronie **Zakończ tworzenie zadania** kliknij przycisk **Zakończ**.

   Po zakończeniu działania Kreatora tworzenia nowego zadania, zostaje utworzone i skonfigurowane zadanie **Inwentaryzacja**. Jeśli chcesz, możesz zmienić ustawienia dla utworzonego zadania. Nowo utworzone zadanie będzie wyświetlane na liście zadań.

Szczegółowy opis zadania inwentaryzacji znajduje się w pomocy Kaspersky Endpoint Security for Linux oraz Pomoc Kaspersky Endpoint Security for Windows.

Po wykonaniu zadania **Inwentaryzacja**, zostaje utworzona lista plików wykonywalnych przechowywanych na zarządzanych urządzeniach i możesz przejrzeć listę.

Podczas inwentaryzacji mogą zostać wykryte pliki wykonywalne w następujących formatach (w zależności od opcji wybranej we właściwościach zadania inwentaryzacji): MZ, COM, PE, NE, SYS, CMD, BAT, PS1, JS, VBS, REG, MSI, CPL, DLL, JAR i HTML.

Przeglądanie listy plików wykonywalnych, przechowywanych na zarządzanych urządzeniach

W celu przejrzenia listy plików wykonywalnych przechowywanych na urządzeniach klienckich:

W menu głównym przejdź do **Zarządzanie oprogramowaniem** → **Aplikacje innych firm** → **Pliki wykonywalne**.

Strona wyświetla listę plików wykonywalnych przechowywanych na urządzeniach klienckich.

W razie potrzeby możesz wysłać plik wykonywalny zarządzanego urządzenia na urządzenie, na którym otwarta jest Kaspersky Security Center Web Console.

Aby wysłać plik wykonywalny:

1. W menu głównym przejdź do **Zarządzanie oprogramowaniem** → **Aplikacje innych firm** → **Pliki wykonywalne**.
2. Zaznacz odnośnik do pliku wykonywalnego, który chcesz wysłać.
3. W oknie, które zostanie otwarte, przejdź do sekcji **Urządzenia**, a następnie zaznacz pole wyboru zarządzanego urządzenia, z którego chcesz wysłać plik wykonywalny.

   Przed wysłaniem pliku wykonywalnego upewnij się, że zarządzane urządzenie ma bezpośrednie połączenie z Serwerem administracyjnym, zaznaczając pole wyboru **Nie odłączaj od Serwera administracyjnego**.

4. Kliknij przycisk **Wyślij**.

   Wybrany plik wykonywalny zostanie pobrany w celu dalszego wysłania na urządzenie, na którym otwarta jest Kaspersky Security Center Web Console.

Tworzenie kategorii aplikacji z zawartością dodaną ręcznie

Możesz określić zestaw kryteriów jako szablon plików wykonywalnych, dla których chcesz zezwolić na lub zablokować uruchamianie w Twojej organizacji. W oparciu o pliki wykonywalne odpowiadające kryteriom, możesz utworzyć kategorię aplikacji i użyć jej w konfiguracji komponentu Kontrola aplikacji.

W celu utworzenia kategorii aplikacji z zawartością dodaną ręcznie:

1. W menu głównym przejdź do **Zarządzanie oprogramowaniem** → **Aplikacje innych firm** → **Kategorie aplikacji**.

   Zostanie wyświetlona strona z listą kategorii aplikacji.

2. Kliknij przycisk **Dodaj**.

   Zostanie uruchomiony Kreator tworzenia nowej kategorii. Przejdź przez kroki kreatora, korzystając z przycisku **Dalej**.

3. W kroku **Wybierz metodę tworzenia kategorii** kreatora określ nazwę kategorii aplikacji i wybierz opcję **Kategoria z zawartością dodaną ręcznie. Dane plików wykonywalnych są dodawane do tej kategorii ręcznie**.

4. W kroku **Warunki** kliknij przycisk **Add**, aby dodać kryterium warunku do uwzględnienia plików w tworzonej kategorii.

5. W kroku **Kryteria warunku** wykonaj następujące czynności:

   a. Wybierz typ reguły tworzenia kategorii:

   - **Z kategorii KL**

     Jeśli ta opcja jest zaznaczona, możesz określić kategorię aplikacji Kaspersky jako warunek dodania aplikacji do kategorii użytkownika. Aplikacje z określonej kategorii Kaspersky zostaną dodane do kategorii użytkownika dla aplikacji.

   - **Wybierz certyfikat z repozytorium**

     Jeśli ta opcja jest zaznaczona, możesz określić certyfikaty z repozytorium. Warunek kategorii obejmuje tylko pliki wykonywalne podpisane określonym certyfikatem.

     Certyfikaty są dodawane do repozytorium, jeśli utworzono i uruchomiono zadanie inwentaryzacji lub zaznaczono pole wyboru **Informacje o uruchomionych aplikacjach** w profilu Kaspersky Endpoint Security. Możesz wykonać obie czynności.

     > Informacje o certyfikatach można wyodrębnić tylko z plików wykonywalnych w formacie PE (.exe, .dll, .sys).

   - **Określ ścieżkę do aplikacji (maski są obsługiwane)**

     Jeżeli ta opcja zostanie zaznaczona, możesz określić ścieżkę do folderu na urządzeniu klienckim zawierający pliki wykonywalne, które zostaną dodane do kategorii użytkownika dla aplikacji.

   - **Dysk wymienny**

     Jeżeli ta opcja jest zaznaczona, możesz określić typ nośnika (dowolny dysk lub dysk wymienny), na którym aplikacja jest uruchomiona. Aplikacje, które były uruchomione na wybranym typie urządzenia, zostaną dodane do kategorii użytkownika dla aplikacji.

   - **Suma kontrolna, metadane lub certyfikat**:

     - **Wybierz z listy plików wykonywalnych**

       Jeśli ta opcja jest zaznaczona, możesz wskazać na liście plików wykonywalnych na urządzeniu klienckim te aplikacje, które chcesz dodać do kategorii.

     - **Wybierz z rejestru aplikacji**

Jeśli ta opcja jest wybrana, zostanie wyświetlony rejestr aplikacji. Po wybraniu aplikacji z rejestru otwiera się okno z parametrami wypełnionymi metadanymi wybranej aplikacji:

- Nazwa pliku.
- Wersja pliku. Możesz określić dokładną wartość wersji lub opisać warunek, na przykład „większy niż 5.0”.
- Nazwa aplikacji.
- Wersja aplikacji. Możesz określić dokładną wartość wersji lub opisać warunek, na przykład „większy niż 5.0”.
- Producent.

Należy pamiętać, że zablokowane zostanie wyłącznie uruchomienie plików wykonywalnych spełniających określone parametry, a nie uruchomienie wybranej aplikacji. Jeśli wybrane metadane aplikacji odpowiadają metadanym pliku wykonywalnego uruchamianego po uruchomieniu aplikacji, możesz przejść do następnego kroku. W przeciwnym razie należy ręcznie zmienić wartości, aby odpowiadały metadanym pliku wykonywalnego.

- **Określ ręcznie**

  Jeśli ta opcja jest zaznaczona, możesz określić hash pliku lub metadane lub certyfikat jako warunek dodawania aplikacji do kategorii użytkownika.

  Hash pliku

  W zależności od wersji aplikacji zabezpieczającej zainstalowanej na urządzeniach w sieci musisz wybrać algorytm obliczania wartości sumy kontrolnej przez Kaspersky Security Center Linux dla plików w tej kategorii. Informacje o wartościach sumy kontrolnej obliczonych przez funkcje skrótu są przechowywane w bazie danych Serwera administracyjnego.

  SHA256 jest kryptograficzną funkcją skrótu: w algorytmie nie znaleziono luk, dlatego jest obecnie najbardziej aktualną funkcją kryptograficzną. Kaspersky Endpoint Security for Linux obsługuje obliczenia SHA256.

  Wybierz jedną z opcji obliczania wartości sumy kontrolnej przez Kaspersky Security Center Linux dla plików w kategorii:

  - Jeśli wszystkie instancje aplikacji zabezpieczających zainstalowane w Twojej sieci to Kaspersky Endpoint Security for Linux, zaznacz pole **SHA256**.
  - Zaznacz pole **Suma kontrolna MD5** tylko wtedy, gdy korzystasz z Kaspersky Endpoint Security for Windows. Kaspersky Endpoint Security for Linux nie obsługuje funkcji skrótu MD5.

  Metadane

  Jeśli ta opcja jest wybrana, możesz określić metadane pliku jako nazwę pliku, wersję pliku, producenta. Warunek kategorii obejmuje tylko pliki wykonywalne z takimi samymi metadanymi.

  Certyfikat

  Jeśli ta opcja jest zaznaczona, możesz określić certyfikaty z repozytorium. Warunek kategorii obejmuje tylko pliki wykonywalne podpisane określonym certyfikatem.

  Certyfikaty są dodawane do repozytorium, jeśli utworzono i uruchomiono zadanie inwentaryzacji lub zaznaczono pole wyboru **Informacje o uruchomionych aplikacjach** w profilu Kaspersky Endpoint Security. Możesz wykonać obie czynności.

- **Z zarchiwizowanego folderu**

Jeśli ta opcja jest zaznaczona, możesz określić plik zarchiwizowanego folderu, a następnie wybrać warunek, którego chcesz użyć do dodania aplikacji do kategorii użytkownika. Zarchiwizowany folder zostanie rozpakowany, a wybrane warunki zostaną zastosowane do plików w folderze. Jako warunek możesz wybrać jedno z następujących kryteriów:

- **Hash pliku**

  Wybierz funkcję skrótu (MD5 lub SHA256), której chcesz użyć do obliczenia wartości skrótu. Aplikacje, które mają tę samą wartość kontrolną co pliki w zarchiwizowanym folderze, zostaną dodane do kategorii aplikacji użytkownika.

  Wybierz funkcję skrótu MD5 tylko wtedy, gdy korzystasz z Kaspersky Endpoint Security for Windows. Kaspersky Endpoint Security for Linux nie obsługuje funkcji skrótu MD5.

- **Metadane**

  Ty wybierasz, których metadanych chcesz użyć jako kryteriów. Pliki wykonywalne, które zawierają te same metadane, zostaną dodane do kategorii użytkownika.

- **Certyfikat**

  Wybierz właściwości certyfikatu (podmiot certyfikatu, odcisk palca lub wystawca), których chcesz użyć jako kryteriów. Pliki wykonywalne, które zostały podpisane certyfikatami o tych samych właściwościach, zostaną dodane do kategorii użytkownika.

Metadane i kryteria **Certyfikat** należy określić ręcznie po przesłaniu pliku archiwum lub folderu, jeśli chcesz użyć tych kryteriów.

Jeśli ta opcja jest zaznaczona, możesz określić plik zarchiwizowanego folderu, a następnie wybrać warunek, którego chcesz użyć do dodania aplikacji do kategorii użytkownika. Zarchiwizowany folder zostanie rozpakowany, a wybrane warunki zostaną zastosowane do plików w folderze. Jako warunek możesz wybrać jedno z następujących kryteriów:

- **Hash pliku**

  Wybierz funkcję skrótu (MD5 lub SHA256), której chcesz użyć do obliczenia wartości skrótu. Aplikacje, które mają tę samą wartość kontrolną co pliki w zarchiwizowanym folderze, zostaną dodane do kategorii aplikacji użytkownika.

  Wybierz funkcję skrótu MD5 tylko wtedy, gdy korzystasz z Kaspersky Endpoint Security for Windows. Kaspersky Endpoint Security for Linux nie obsługuje funkcji skrótu MD5.

- **Metadane**

  Ty wybierasz, których metadanych chcesz użyć jako kryteriów. Pliki wykonywalne, które zawierają te same metadane, zostaną dodane do kategorii użytkownika.

- **Certyfikat**

  Wybierz właściwości certyfikatu (podmiot certyfikatu, odcisk palca lub wystawca), których chcesz użyć jako kryteriów. Pliki wykonywalne, które zostały podpisane certyfikatami o tych samych właściwościach, zostaną dodane do kategorii użytkownika.

Metadane i kryteria **Certyfikat** należy określić ręcznie po przesłaniu pliku archiwum lub folderu, jeśli chcesz użyć tych kryteriów.

b. W razie potrzeby dodaj komentarz w polu **Opis**. Liczba symboli nie może przekroczyć 1000.

Później możesz edytować lub usunąć komentarz, otwierając kartę **Warunki** we właściwościach kategorii aplikacji, a następnie w kolumnie **Kryterium warunku** kliknij łącze z warunkiem, dla którego chcesz edytować lub usunąć komentarz.

> Wybierając typ reguły **Z kategorii KL**, możesz dodać jeden komentarz dla wszystkich warunków, które mają zostać utworzone na podstawie tego typu reguły. Możesz edytować lub usunąć komentarz dla każdego warunku osobno.

Wybrane kryterium zostanie dodane do listy warunków.

Możesz dodać dowolną liczbę kryteriów dla tworzonej kategorii aplikacji.

6. W kroku **Wykluczenia** kliknij przycisk **Add**, aby dodać kryterium warunku wykluczenia w celu wykluczenia plików z tworzonej kategorii.

   W razie potrzeby możesz dodać komentarz w polu **Opis**. Liczba symboli nie może przekroczyć 1000.

   Później możesz edytować lub usunąć komentarz, otwierając zakładkę **Wykluczenia** w oknie właściwości kategorii aplikacji, a następnie w kolumnie **Kryterium warunku** kliknij odnośnik z warunkiem, dla którego chcesz edytować lub usunąć komentarz.

7. W kroku **Kryteria warunku** wybierz typ reguły z listy w taki sam sposób, w jaki wybierałeś typ reguły dla tworzenia kategorii.

Po zakończeniu działania kreatora kategoria aplikacji zostanie utworzona i wyświetlona na liście kategorii aplikacji. Po skonfigurowaniu Kontroli aplikacji możesz użyć utworzonej kategorii aplikacji.

Aby uzyskać szczegółowe informacje na temat Kontroli aplikacji, zapoznaj się z Pomocą Kaspersky Endpoint Security for Linux oraz Kaspersky Endpoint Security for Windows Pomoc.

Tworzenie kategorii aplikacji, która zawiera pliki wykonywalne z wybranych urządzeń

Możesz użyć plików wykonywalnych z wybranych urządzeń jako szablonu plików wykonywalnych, które chcesz zablokować lub na które chcesz zezwolić. W oparciu o pliki wykonywalne z wybranych urządzeń, możesz utworzyć kategorię aplikacji i użyć jej w konfiguracji komponentu Kontrola aplikacji.

Upewnij się, że spełnione są następujące wymagania wstępne:

- Komponent Kontrola aplikacji jest włączony w zasadzie Kaspersky Endpoint Security.
- Uzyskano listę plików wykonywalnych przechowywanych na zarządzanych urządzeniach.

W celu utworzenia kategorii aplikacji, która zawiera pliki wykonywalne z wybranych urządzeń:

1. W menu głównym przejdź do sekcji **Zarządzanie oprogramowaniem** → **Aplikacje innych firm** → **Kategorie aplikacji**.

   Wyświetlona zostanie strona z listą kategorii plików wykonywalnych.

2. Kliknij przycisk **Dodaj**.

   Zostanie uruchomiony Kreator tworzenia nowej kategorii. Przejdź przez kroki kreatora, korzystając z przycisku **Next**.

3. W kroku **Wybierz metodę tworzenia kategorii** określ nazwę kategorii i wybierz **Kategoria zawierająca pliki wykonywalne znajdujące się na wybranych urządzeniach. Takie pliki wykonywalne są przetwarzane automatycznie, a ich metryki są dodawane do kategorii**.

4. Kliknij **Dodaj**.

5. W otwartym oknie wybierz urządzenie lub urządzenia, których pliki wykonywalne będą używane do tworzenia kategorii aplikacji.

6. Określ następujące ustawienia:

   - **Algorytm obliczania wartości sumy kontrolnej**

     W zależności od wersji aplikacji zabezpieczającej zainstalowanej na urządzeniach w sieci musisz wybrać algorytm obliczania wartości sumy kontrolnej przez Kaspersky Security Center Linux dla plików w tej kategorii. Informacje o wartościach sumy kontrolnej obliczonych przez funkcje skrótu są przechowywane w bazie danych Serwera administracyjnego.

     SHA256 jest kryptograficzną funkcją skrótu: w algorytmie nie znaleziono luk, dlatego jest obecnie najbardziej aktualną funkcją kryptograficzną. Kaspersky Endpoint Security for Linux obsługuje obliczenia SHA256.

     Wybierz jedną z opcji obliczania wartości sumy kontrolnej przez Kaspersky Security Center Linux dla plików w kategorii:

     - Jeśli wszystkie instancje aplikacji zabezpieczających zainstalowane w Twojej sieci to Kaspersky Endpoint Security for Linux, zaznacz pole **SHA256**.

     Zaznacz pole **Suma kontrolna MD5** tylko wtedy, gdy korzystasz z Kaspersky Endpoint Security for Windows. Kaspersky Endpoint Security for Linux nie obsługuje funkcji skrótu MD5.

     Pole **Oblicz SHA256 plików należących do tej kategorii (obsługiwane przez Kaspersky Endpoint Security 10 Service Pack 2 for Windows i nowsze wersje)** jest zaznaczone domyślnie.

     Pole **Przelicz sumę kontrolną MD5 dla plików z tej kategorii (obsługiwane w wersjach starszych niż Kaspersky Endpoint Security 10 Service Pack 2 for Windows)** jest odznaczone domyślnie.

   - **Synchronizuj dane z repozytorium Serwera administracyjnego**

     Wybierz tę opcję, jeśli chcesz, żeby Serwer administracyjny okresowo sprawdzał zmiany w określonym folderze (lub folderach).

     Domyślnie opcja ta jest wyłączona.

     Jeśli włączysz tę opcję, określ przedział czasu (w godzinach), aby sprawdzić zmiany w określonym folderze (folderach). Domyślnie przedział czasu skanowania wynosi 24 godziny.

   - **Typ pliku**

     W tej sekcji możesz określić typ pliku, który jest używany do tworzenia kategorii aplikacji.

     Wszystkie pliki. Wszystkie pliki są brane pod uwagę podczas tworzenia kategorii. Domyślnie opcja ta jest zaznaczona.

     Tylko pliki spoza kategorii aplikacji. Tylko pliki poza kategoriami aplikacji są brane pod uwagę podczas tworzenia kategorii.

   - **Foldery**

     W tej sekcji możesz określić, które foldery z wybranego urządzenia (urządzeń) zawierają pliki używane do tworzenia kategorii aplikacji.

     Wszystkie foldery. Wszystkie foldery są brane pod uwagę podczas tworzenia kategorii. Domyślnie opcja ta jest zaznaczona.

Określony folder. Tylko określony folder jest brany pod uwagę podczas tworzenia kategorii. Jeśli wybierzesz tę opcję, musisz określić ścieżkę do folderu.

Po zakończeniu działania kreatora tworzona jest kategoria plików wykonywalnych. Jest wyświetlana na liście kategorii. W przypadku konfigurowania Kontroli aplikacji możesz użyć utworzonej kategorii.

Tworzenie kategorii aplikacji, która zawiera pliki wykonywalne z wybranego folderu

Możesz użyć plików wykonywalnych z wybranego folderu jako standardu plików wykonywalnych, które chcesz zablokować lub na które chcesz zezwolić w swojej organizacji. W oparciu o pliki wykonywalne z wybranego folderu, możesz utworzyć kategorię aplikacji i użyć jej w konfiguracji komponentu Kontrola aplikacji.

W celu utworzenia kategorii, która zawiera pliki wykonywalne z wybranego folderu:

1. W menu głównym przejdź do sekcji **Zarządzanie oprogramowaniem** → **Aplikacje innych firm** → **Kategorie aplikacji**.

   Zostanie wyświetlona strona z listą kategorii.

2. Kliknij przycisk **Dodaj**.

   Zostanie uruchomiony Kreator tworzenia nowej kategorii. Przejdź przez kroki kreatora, korzystając z przycisku **Next**.

3. W kroku **Wybierz metodę tworzenia kategorii** kreatora określ nazwę kategorii i wybierz opcję **Kategoria, która zawiera pliki wykonywalne z określonego folderu. Pliki wykonywalne aplikacji skopiowane do określonego folderu są przetwarzane automatycznie, a ich metryki są dodawane do kategorii**.

4. Określ folder, którego pliki wykonywalne zostaną użyte do utworzenia kategorii.

5. Określ następujące ustawienia:

   - **Uwzględnij w tej kategorii biblioteki dołączane dynamicznie (DLL)**

     Kategoria aplikacji zawiera biblioteki dołączane dynamicznie (pliki w formacie DLL), a składnik Kontrola aplikacji rejestruje akcje takich bibliotek działających w systemie. Włączenie plików DLL do kategorii może obniżyć wydajność Kaspersky Security Center Linux.

     Domyślnie pole to nie jest zaznaczone.

   - **Uwzględnij w tej kategorii dane skryptów**

     Kategoria aplikacji zawiera dane o skryptach, a skrypty nie są blokowane przez moduł Ochrona WWW. Włączenie danych skryptów do kategorii może obniżyć wydajność Kaspersky Security Center Linux.

     Domyślnie pole to nie jest zaznaczone.

   - **Algorytm obliczania wartości sumy kontrolnej**: **Oblicz sumy SHA256 plików należących do tej kategorii (obsługiwane przez Kaspersky Endpoint Security 10 Service Pack 2 for Windows i nowsze) / Oblicz sumę kontrolną MD5 dla plików z tej kategorii (obsługiwane przez starsze wersje niż Kaspersky Endpoint Security 10 Service Pack 2 for Windows)**

     W zależności od wersji aplikacji zabezpieczającej zainstalowanej na urządzeniach w sieci musisz wybrać algorytm obliczania wartości sumy kontrolnej przez Kaspersky Security Center Linux dla plików w tej kategorii. Informacje o wartościach sumy kontrolnej obliczonych przez funkcje skrótu są przechowywane w bazie danych Serwera administracyjnego.

SHA256 jest kryptograficzną funkcją skrótu: w algorytmie nie znaleziono luk, dlatego jest obecnie najbardziej aktualną funkcją kryptograficzną. Kaspersky Endpoint Security for Linux obsługuje obliczenia SHA256.

Wybierz jedną z opcji obliczania wartości sumy kontrolnej przez Kaspersky Security Center Linux dla plików w kategorii:

- Jeśli wszystkie instancje aplikacji zabezpieczających zainstalowane w Twojej sieci to Kaspersky Endpoint Security for Linux, zaznacz pole **SHA256**.

Zaznacz pole **Suma kontrolna MD5** tylko wtedy, gdy korzystasz z Kaspersky Endpoint Security for Windows. Kaspersky Endpoint Security for Linux nie obsługuje funkcji skrótu MD5.

Pole **Oblicz SHA256 plików należących do tej kategorii (obsługiwane przez Kaspersky Endpoint Security 10 Service Pack 2 for Windows i nowsze wersje)** jest zaznaczone domyślnie.

Pole **Oblicz MD5 plików należących do tej kategorii (obsługiwane w wersjach starszych niż Kaspersky Endpoint Security 10 Service Pack 2 for Windows)** jest odznaczone domyślnie.

- **Wymuś skanowanie folderu pod kątem zmian**

  Jeśli ta opcja jest włączona, aplikacja regularnie sprawdza folder dodawania zawartości kategorii na obecność zmian. Możesz określić częstotliwość skanowań (w godzinach) w polu wejściowym znajdującym się obok pola do zaznaczenia. Domyślnie przedział czasu między wymuszonymi skanowaniami wynosi 24 godziny.

  Jeśli ta opcja jest wyłączona, aplikacja nie wymusza skanowania folderu. Serwer podejmie próbę uzyskania dostępu do plików, jeśli zostały zmodyfikowane, dodane lub usunięte.

  Domyślnie opcja ta jest wyłączona.

Po zakończeniu działania kreatora tworzona jest kategoria plików wykonywalnych. Jest wyświetlana na liście kategorii. Podczas konfiguracji Kontroli aplikacji możesz użyć kategorii.

Aby uzyskać szczegółowe informacje na temat Kontroli aplikacji, zapoznaj się z Pomocą Kaspersky Endpoint Security for Linux oraz Kaspersky Endpoint Security for Windows Pomoc.

Przeglądanie listy kategorii aplikacji

Możesz przejrzeć listę konfigurowanych kategorii plików wykonywalnych i ustawień każdej kategorii.

W celu przejrzenia listy kategorii aplikacji:

W menu głównym przejdź do sekcji **Zarządzanie oprogramowaniem** → **Aplikacje innych firm** → **Kategorie aplikacji**.

Zostanie wyświetlona strona z listą kategorii.

W celu przejrzenia właściwości kategorii aplikacji:

Kliknij nazwę kategorii.

Zostanie wyświetlone okno właściwości kategorii. Właściwości zostaną pogrupowane na kilku zakładkach.

Dodawanie plików wykonywalnych dotyczących zdarzeń do kategorii aplikacji

Po skonfigurowaniu Kontroli aplikacji w zasadach Kaspersky Endpoint Security, na liście zdarzeń zostaną wyświetlone następujące zdarzenia:

- **Zablokowano uruchomienie aplikacji** (zdarzenie *Krytyczne*). To zdarzenie jest wyświetlane, jeśli skonfigurowałeś Kontrolę aplikacji do stosowania reguł.
- **Zablokowane uruchomienie aplikacji w trybie testowym** (zdarzenie *Informacje*). To zdarzenie jest wyświetlane, jeśli skonfigurowałeś Kontrolę aplikacji do testowania reguł.
- **Wiadomość do administratora o zakazie uruchamiania aplikacji** (zdarzenie *ostrzegawcze*). To zdarzenie jest wyświetlane, jeśli skonfigurowałeś Kontrolę aplikacji do stosowania reguł i użytkownik zażądał dostępu do aplikacji, która jest zablokowana podczas uruchamiania.

Zalecane jest utworzenie wyborów zdarzeń, aby przeglądać zdarzenia dotyczące działania Kontroli aplikacji.

Możesz dodać pliki wykonywalne dotyczące zdarzeń Kontroli aplikacji do istniejącej kategorii aplikacji lub do nowej kategorii aplikacji. Możesz dodać pliki wykonywalne tylko do kategorii aplikacji z zawartością dodaną ręcznie.

W celu dodania plików wykonywalnych związanych ze zdarzeniami Kontroli aplikacji do kategorii aplikacji:

1. W menu głównym przejdź do **Monitorowanie** → **Wybory zdarzeń**.

   Zostanie wyświetlona lista wyborów zdarzeń.

2. Wybierz wybór zdarzeń, aby przeglądać zdarzenia związane z Kontrolą aplikacji oraz uruchomić ten wybór zdarzeń.

   Jeśli nie utworzyłeś wyboru zdarzeń dotyczącego Kontroli aplikacji, możesz wybrać i uruchomić predefiniowany wybór, na przykład, **Ostatnie zdarzenia**.

   Zostanie wyświetlona lista zdarzeń.

3. Wybierz zdarzenia, których skojarzone pliki wykonywalne chcesz dodać do kategorii aplikacji, a następnie kliknij przycisk **Przypisz do kategorii**.

   Zostanie uruchomiony Kreator tworzenia nowej kategorii. Przejdź przez kroki kreatora, korzystając z przycisku **Next**.

4. W kroku kreatora określ odpowiednie ustawienia:

   - W sekcji **Akcja na pliku wykonywalnym związanym ze zdarzeniem** wybierz jedną z następujących opcji:

     - **Dodaj do nowej kategorii aplikacji**

       Wybierz tę opcję, jeśli chcesz utworzyć nową kategorię aplikacji w oparciu o pliki wykonywalne dotyczące zdarzeń.

       Domyślnie opcja ta jest zaznaczona.

       Jeśli wybrałeś tę opcję, określ nową nazwę kategorii.

- **Dodaj do istniejącej kategorii aplikacji**

  Wybierz tę opcję, jeśli chcesz dodać pliki wykonywalne dotyczące zdarzeń do istniejącej kategorii aplikacji.

  Domyślnie ta opcja nie jest zaznaczona.

  Jeśli wybrałeś tę opcję, wybierz kategorię aplikacji z zawartością dodaną ręcznie, do której chcesz dodać pliki wykonywalne.

- W sekcji **Typ reguły** wybierz jedną z następujących opcji:

  - **Reguły dodawania do włączeń**

  - **Reguły dodawania do wykluczeń**

- W sekcji **Parametr użyty jako warunek** wybierz jedną z następujących opcji:

  - **Szczegóły certyfikatu (lub sumy kontrolne SHA256 dla plików bez certyfikatu)**

    Pliki mogą być podpisane certyfikatem. Kilka plików może być podpisanych tym samym certyfikatem. Na przykład, różne wersje tej samej aplikacji mogą być podpisane tym samym certyfikatem lub kilka różnych aplikacji od tego samego producenta może być podpisanych tym samym certyfikatem. Jeśli wybierzesz certyfikat, kilka wersji aplikacji lub kilka aplikacji od tego samego producenta może zostać przydzielonych do kategorii.

    Każdy plik posiada swoją unikatową funkcję skrótu SHA256. Jeśli wybierzesz funkcję skrótu SHA256, tylko jeden odpowiadający plik, na przykład, zdefiniowana wersja aplikacji, zostanie przydzielony do kategorii.

    Wybierz tę opcję, jeśli chcesz dodać do reguł kategorii szczegóły certyfikatu pliku wykonywalnego (lub funkcję skrótu SHA256 dla plików bez certyfikatu).

    Domyślnie opcja ta jest zaznaczona.

  - **Szczegóły certyfikatu (pliki bez certyfikatu zostaną pominięte)**

    Pliki mogą być podpisane certyfikatem. Kilka plików może być podpisanych tym samym certyfikatem. Na przykład, różne wersje tej samej aplikacji mogą być podpisane tym samym certyfikatem lub kilka różnych aplikacji od tego samego producenta może być podpisanych tym samym certyfikatem. Jeśli wybierzesz certyfikat, kilka wersji aplikacji lub kilka aplikacji od tego samego producenta może zostać przydzielonych do kategorii.

    Wybierz tę opcję, jeśli chcesz dodać szczegóły certyfikatu pliku wykonywalnego do reguł kategorii. Jeśli plik wykonywalny nie posiada certyfikatu, ten plik zostanie pominięty. Do kategorii nie zostaną dodane żadne informacje o tym pliku.

  - **Tylko SHA256 (pliki bez sumy kontrolnej zostaną pominięte)**

    Każdy plik posiada swoją unikatową funkcję skrótu SHA256. Jeśli wybierzesz funkcję skrótu SHA256, tylko jeden odpowiadający plik, na przykład, zdefiniowana wersja aplikacji, zostanie przydzielony do kategorii.

    Wybierz tę opcję, jeśli chcesz dodać tylko szczegóły funkcji skrótu SHA256 pliku wykonywalnego.

  - **Tylko MD5 (tryb wycofany, wyłącznie dla wersji Kaspersky Endpoint Security 10 Service Pack 1)**

    > Wybierz tę opcję tylko wtedy, gdy korzystasz z Kaspersky Endpoint Security for Windows. Kaspersky Endpoint Security for Linux nie obsługuje funkcji skrótu MD5.

    Każdy plik posiada swoją unikatową funkcję skrótu MD5. Jeśli wybierzesz funkcję skrótu MD5, tylko jeden odpowiadający plik, na przykład, zdefiniowana wersja aplikacji, zostanie przydzielony do kategorii.

5. Kliknij **OK**.

   Jeśli kreator zakończy działanie, pliki wykonywalne dotyczące zdarzeń Kontroli aplikacji są dodawane do istniejącej kategorii aplikacji lub do nowej kategorii aplikacji. Możesz przejrzeć ustawienia kategorii aplikacji, które zmodyfikowałeś lub utworzyłeś.

Aby uzyskać szczegółowe informacje na temat Kontroli aplikacji, zapoznaj się z Pomocą Kaspersky Endpoint Security for Linux oraz Kaspersky Endpoint Security for Windows Pomoc.

Konfigurowanie Kontroli aplikacji w zasadzie Kaspersky Endpoint Security for Windows

Po utworzeniu kategorii Kontroli aplikacji możesz użyć ich do konfigurowania Kontroli aplikacji w zasadach Kaspersky Endpoint Security for Windows.

W celu skonfigurowania Kontroli aplikacji w zasadzie Kaspersky Endpoint Security for Windows:

1. W menu głównym przejdź do **Zarządzanie zasobami** → **Zasady**.

   Zostanie wyświetlona lista zasad.

2. Kliknij zasadę **Kaspersky Endpoint Security for Windows**.

   Zostanie otwarte okno ustawień zasady.

3. Przejdź do **Ustawienia aplikacji** → **Kontrola bezpieczeństwa** → Kontrola **aplikacji**.

   Zostanie wyświetlone okno **Kontrola aplikacji** z ustawieniami Kontroli aplikacji.

4. Opcja **Kontrola aplikacji** jest domyślnie włączona. Przełącz przycisk przełączania **Kontrola aplikacji WYŁĄCZONA**, aby wyłączyć tę opcję.

5. W ustawieniach blokowania **Ustawienia Kontroli aplikacji** włącz tryb działania, aby zastosować reguły Kontroli aplikacji i zezwól Kaspersky Endpoint Security for Windows na blokowanie uruchamiania aplikacji.

   Jeśli chcesz przetestować reguły Kontroli aplikacji, w sekcji **Ustawienia Kontroli aplikacji** włącz tryb testowy. W trybie testowym Kaspersky Endpoint Security for Windows nie blokuje uruchamiania aplikacji, ale rejestruje informacje o wyzwolonych regułach w raporcie. Kliknij łącze **Wyświetl raport**, aby wyświetlić te informacje.

6. Włącz opcję **Kontrola wczytywania modułów DLL**, jeśli chcesz, żeby program Kaspersky Endpoint Security for Windows monitorował wczytywanie modułów DLL, gdy aplikacje są uruchamiane przez użytkowników.

   Informacje o module i aplikacji, która wczytuje moduł, zostaną zapisane w raporcie.

   Kaspersky Endpoint Security for Windows monitoruje tylko moduły DLL i sterowniki wczytywane po wybraniu opcji **Kontrola wczytywania modułów DLL**. Uruchom ponownie urządzenie po wybraniu opcji **Kontrola wczytywania modułów DLL**, jeśli chcesz, żeby program Kaspersky Endpoint Security for Windows monitorował wszystkie moduły DLL i sterowniki, w tym te wczytywane przed uruchomieniem Kaspersky Endpoint Security for Windows.

7. (Opcjonalne) W sekcji **Szablony wiadomości** zmień szablon wiadomości, która jest wyświetlana po zablokowaniu możliwości uruchomienia aplikacji, oraz szablon wiadomości e-mail, która jest wysyłana do Ciebie.

8. W ustawieniach sekcji **Tryb Kontroli aplikacji** wybierz tryb **Lista zablokowanych** lub **Lista zezwolonych**.

   Domyślnie, wybrany jest tryb **Lista zablokowanych**.

9. Kliknij odnośnik **Ustawienia list reguł**.

   Zostanie otwarte okno **Lista zablokowanych i lista zezwolonych**, w którym można dodać kategorię aplikacji. Domyślnie, wybrana jest zakładka **Lista zablokowanych**, jeśli wybrany jest tryb **Lista zablokowanych** lub wybrana jest zakładka **Lista zezwolonych**, jeśli wybrany jest tryb **Lista zezwolonych**.

10. W oknie **Lista zablokowanych i lista zezwolonych** kliknij przycisk **Dodaj**.

    Zostanie otwarte okno **Reguła Kontroli aplikacji**.

11. Kliknij łącze **Wybierz kategorię**.

    Zostanie otwarte okno **Kategoria aplikacji**.

12. Dodaj kategorię (lub kategorie) aplikacji, które utworzyłeś wcześniej.

    Możesz edytować ustawienia utworzonej kategorii, klikając przycisk **Edytuj**.

    Możesz utworzyć nową kategorię, klikając przycisk **Dodaj**.

    Możesz usunąć kategorię z listy, klikając przycisk **Usuń**.

13. Po zakończeniu tworzenia listy kategorii aplikacji, kliknij przycisk **OK**.

    Okno **Kategoria aplikacji** zostanie zamknięte.

14. W oknie reguły **Kontrola aplikacji**, w sekcji **Użytkownicy i ich uprawnienia** utwórz listę użytkowników i grup użytkowników do zastosowania reguły Kontroli aplikacji.

15. Aby zapisać ustawienia i zamknąć okno **Reguła Kontroli aplikacji**, kliknij przycisk **OK**.

16. Aby zapisać ustawienia i zamknąć okno **Lista zablokowanych i lista zezwolonych**, kliknij przycisk **OK**.

17. Aby zapisać ustawienia i zamknąć okno **Kontrola aplikacji**, kliknij przycisk **OK**.

18. Zamknij okno z ustawieniami zasady Kaspersky Endpoint Security for Windows.

Kontrola aplikacji została skonfigurowana. Po przeniesieniu zasady na urządzenia klienckie, możliwe jest zarządzanie uruchamianiem plików wykonywalnych.

Aby uzyskać szczegółowe informacje na temat Kontroli aplikacji, zapoznaj się z Pomocą Kaspersky Endpoint Security for Linux oraz Kaspersky Endpoint Security for Windows Pomoc.

Uzyskiwanie i przeglądanie listy aplikacji zainstalowanych na urządzeniach klienckich

Kaspersky Security Center Linux przeprowadza inwentaryzację wszystkich programów zainstalowanych na zarządzanych urządzeniach klienckich działających pod kontrolą systemu Linux i Windows.

Agent sieciowy tworzy listę aplikacji zainstalowanych na urządzeniu, a następnie wysyła ją do Serwera administracyjnego. Aktualizacja listy aplikacji przez Agenta sieciowego zajmuje około 10–15 minut.

W przypadku urządzeń klienckich z systemem Windows Agent sieciowy otrzymuje większość informacji o zainstalowanych aplikacjach z rejestru systemu Windows. W przypadku urządzeń klienckich opartych na systemie Linux menedżery pakietów dostarczają Agentowi sieciowemu informacje o zainstalowanych aplikacjach.

W celu przejrzenia listy aplikacji zainstalowanych na zarządzanych urządzeniach:

1. W menu głównym przejdź do **Operacje** → **Aplikacje innych firm** → **Rejestr aplikacji**.

   Strona wyświetla tabelę z aplikacjami zainstalowanymi na zarządzanych urządzeniach. Wybierz aplikację, aby wyświetlić jej właściwości, na przykład nazwę dostawcy, numer wersji, listę plików wykonywalnych, listę urządzeń, na których aplikacja jest zainstalowana.

2. Możesz grupować i filtrować dane tabeli z zainstalowanymi aplikacjami w następujący sposób:

   - Kliknij ikonę ustawień ( ) w prawym górnym rogu tabeli.

     W wywołanym menu **Ustawienia kolumn** wybierz kolumny, które mają być wyświetlane w tabeli. Aby wyświetlić typ systemu operacyjnego urządzeń klienckich, na których zainstalowana jest aplikacja, wybierz kolumnę **Typ systemu operacyjnego**.

   - Kliknij ikonę filtra ( ) w prawym górnym rogu tabeli, a następnie określić i zastosować kryterium filtrowania w wywołanym menu.

     Zostanie wyświetlona przefiltrowana tabela zainstalowanych aplikacji.

Aby wyświetlić listę aplikacji zainstalowanych na określonym zarządzanym urządzeniu,

W menu głównym przejdź do **Zarządzanie zasobami** → **Zasoby (urządzenia)** → **<nazwa urządzenia>** → **Zaawansowane** → **Rejestr aplikacji**. Z tego menu możesz wyeksportować listę aplikacji do pliku CSV lub pliku TXT.

Aby uzyskać szczegółowe informacje na temat Kontroli aplikacji, zapoznaj się z Pomocą Kaspersky Endpoint Security for Linux oraz Kaspersky Endpoint Security for Windows Pomoc.

Informacje o aplikacjach innych firm

Kaspersky Security Center Linux może pomóc w aktualizacji oprogramowania firm trzecich, zainstalowanego na urządzeniach klienckich, a także w naprawianiu luk w oprogramowaniu firm trzecich. Kaspersky Security Center Linux może aktualizować oprogramowanie innych firm tylko z bieżącej wersji do najnowszej wersji.

> Listę oprogramowania innych firm można zmieniać i jest ona aktualizowana na bieżąco. Możesz sprawdzić, czy możesz zaktualizować oprogramowanie innych firm (zainstalowane na urządzeniach użytkowników) za pomocą Kaspersky Security Center Linux poprzez przejrzenie listy dostępnych aktualizacji w Kaspersky Security Center Web Console.

Opisana poniżej procedura służy wyłącznie do przeglądania listy oprogramowania innych firm, które można aktualizować za pomocą Kaspersky Security Center Linux. Poniższe kroki mają na celu uzyskanie dostępu do odpowiednich informacji bez konieczności inicjowania jakichkolwiek zadań.

Aby wyświetlić listę oprogramowania innych firm, które można aktualizować za pomocą Kaspersky Security Center Linux:

1. W menu głównym przejdź do **Zadania**.

2. Kliknij **Dodaj**.

   Zostanie uruchomiony Kreator tworzenia nowego zadania. Przejdź przez kroki kreatora, korzystając z przycisku **Dalej**.

3. W kroku **Ustawienia nowych zadań** kreatora określ następujące ustawienia:

   a. Z listy rozwijanej **Aplikacja** wybierz **Kaspersky Security Center Linux**.

   b. W polu **Typ zadania** wybierz **Zainstaluj wymagane aktualizacje i napraw luki**.

4. W kroku **Zakres zadania** kreatora wybierz opcję **Zarządzane urządzenia**.

5. W kroku **Określ reguły instalacji aktualizacji** kreatora kliknij przycisk **Dodaj**.

   Zostanie uruchomiony Kreator tworzenia reguły. Przejdź przez kroki kreatora, korzystając z przycisku **Dalej**.

6. W kroku **Wybierz typ reguły** kreatora wybierz opcję **Reguła dla aktualizacji firm trzecich**.

7. W kroku **Kryteria ogólne** kreatora wybierz opcję **Zainstaluj wszystkie aktualizacje (za wyjątkiem odrzuconych)**, a następnie kliknij przycisk **Dalej**.

Wyświetlana jest lista oprogramowania innych firm.

Instalowanie aktualizacji oprogramowania firm trzecich

Kaspersky Security Center Linux umożliwia zarządzanie aktualizacjami oprogramowania innych firm zainstalowanymi na zarządzanych urządzeniach i naprawianie luk w zabezpieczeniach takiego oprogramowania poprzez instalację wymaganych aktualizacji.

Kaspersky Security Center Linux wyszukuje aktualizacje za pośrednictwem zadania *Wyszukiwanie luk i wymaganych aktualizacji*. Jeśli to zadanie zostanie zakończone, Serwer administracyjny pobierze listy wykrytych luk i żądanych aktualizacji dla oprogramowania firm trzecich zainstalowanego na urządzeniach, które określiłeś we właściwościach zadania. Po przejrzeniu informacji o dostępnych aktualizacjach, możesz zainstalować je na urządzeniach.

Kaspersky Security Center Linux aktualizuje niektóre aplikacje poprzez usunięcie poprzedniej wersji aplikacji i instalację nowej.

Interakcja użytkownika może być wymagana podczas aktualizacji aplikacji innej firmy lub naprawy luki w aplikacji innej firmy na zarządzanym urządzeniu. Na przykład, użytkownik może zostać poproszony o zamknięcie aplikacji innej firmy, jeśli jest ona aktualnie otwarta.

Ze względów bezpieczeństwa wszelkie aktualizacje oprogramowania innych firm, które instalujesz za pomocą funkcji Zarządzanie lukami i poprawkami, są automatycznie skanowane w poszukiwaniu szkodliwego oprogramowania przez technologie firmy Kaspersky. Technologie te są używane do automatycznego sprawdzania plików i obejmują skanowanie antywirusowe, analizę statyczną, analizę dynamiczną, analizę zachowania w środowisku sandbox i uczenie maszynowe.

Eksperci firmy Kaspersky nie przeprowadzają ręcznej analizy aktualizacji oprogramowania innych firm, które są instalowane przez funkcję Zarządzanie lukami i poprawkami. Ponadto eksperci z firmy Kaspersky nie wyszukują luk (znanych lub nieznanych) ani nieudokumentowanych funkcji w takich aktualizacjach, a także nie przeprowadzają innych rodzajów analizy aktualizacji innych, niż określone w powyższym akapicie.

Jeśli metadane aktualizacji oprogramowania firm trzecich są pobierane do repozytorium, możesz zainstalować aktualizacje na urządzeniach klienckich, korzystając z zadania *Zainstaluj wymagane aktualizacje i napraw luki*.

> Zadanie *Zainstaluj wymagane aktualizacje i napraw luki* może zostać utworzone tylko wtedy, gdy masz licencję dla funkcji Zarządzanie lukami i poprawkami.

Jeśli to zadanie zostanie zakończone, aktualizacje zostaną automatycznie zainstalowane na zarządzanych urządzeniach. Jeśli metadane nowych aktualizacji zostaną pobrane do repozytorium Serwera administracyjnego, Kaspersky Security Center Linux sprawdzi, czy aktualizacje spełniają kryteria określone w regułach aktualizacji. Wszystkie nowe aktualizacje, które spełniają kryteria, zostaną pobrane i zainstalowane automatycznie przy kolejnym uruchomieniu zadania.

Scenariusz: Aktualizowanie oprogramowania innej firmy

Ta sekcja oferuje scenariusz aktualizacji oprogramowania innej firmy, zainstalowanego na urządzeniach klienckich. Oprogramowanie innej firmy obejmuje aplikacje innych sprzedawców oprogramowania.

Wymagania wstępne

Aby móc zainstalować aktualizacje oprogramowania innych firm, Serwer administracyjny musi być podłączony do Internetu.

Etapy

Aktualizowanie oprogramowania firm trzecich odbywa się w etapach:

1. **Wyszukiwanie wymaganych aktualizacji**

   Aby odnaleźć aktualizacje oprogramowania firm trzecich dla zarządzanych urządzeń, uruchom zadanie *Wyszukiwanie luk i wymaganych aktualizacji*. Jeśli to zadanie zostanie zakończone, Kaspersky Security Center Linux pobierze listy wykrytych luk i żądanych aktualizacji dla oprogramowania firm trzecich zainstalowanego na urządzeniach, które określiłeś we właściwościach zadania.

   Zadanie *Wyszukiwanie luk i wymaganych aktualizacji* jest tworzone automatycznie przez Kreator wstępnej konfiguracji Serwera administracyjnego. Jeśli nie uruchomiono kreatora, utwórz zadanie *Wyszukiwanie luk i wymaganych aktualizacji* lub uruchom Kreator wstępnej konfiguracji teraz.

   > Zadanie *Wyszukiwanie luk i wymaganych aktualizacji* możesz utworzyć tylko dla urządzeń z systemem Windows. Nie można utworzyć tego zadania dla urządzeń działających na innych systemach operacyjnych.

2. **Przeglądanie listy wykrytych aktualizacji**

   Wyświetl informacje o dostępnych aktualizacjach oprogramowania innych firm i zdecyduj, które aktualizacje chcesz zainstalować. Aby przejrzeć szczegółowe informacje o każdej aktualizacji, kliknij nazwę aktualizacji na liście. Dla każdej aktualizacji na liście możesz także przejrzeć statystyki dotyczące instalacji aktualizacji na urządzeniach klienckich.

3. **Konfigurowanie instalacji aktualizacji**

   Jeśli Kaspersky Security Center Linux odebrał listę aktualizacji oprogramowania firm trzecich, możesz zainstalować je na urządzeniach klienckich przez utworzenie zadania *Zainstaluj wymagane aktualizacje i napraw luki*.

   > Zadanie *Zainstaluj wymagane aktualizacje i napraw luki* możesz utworzyć tylko dla urządzeń z systemem Windows. Nie można utworzyć tego zadania dla urządzeń działających na innych systemach operacyjnych.

Zadanie *Zainstaluj wymagane aktualizacje i napraw luki* jest używane do zainstalowania aktualizacji dla aplikacji firmy Microsoft, w tym aktualizacji dostarczonych przez usługę Windows Update, a także aktualizacji oprogramowania innych producentów. Należy zauważyć, że zadanie *Zainstaluj wymagane aktualizacje i napraw luki* może zostać utworzone tylko wtedy, gdy masz licencję dla funkcji Zarządzanie lukami i poprawkami.

Aby zainstalować niektóre aktualizacje oprogramowania, należy zaakceptować Umowę licencyjną użytkownika końcowego do zainstalowania oprogramowania. Jeśli odrzucisz Umowę licencyjną użytkownika końcowego, aktualizacja oprogramowania nie zostanie zainstalowana.

Możesz uruchomić zadanie instalacji aktualizacji zgodnie z terminarzem. Podczas określania terminarza zadania upewnij się, że zadanie instalacji aktualizacji jest uruchamiane po zakończeniu zadania *Wyszukiwanie luk i wymaganych aktualizacji*.

4. **Konfigurowanie terminarza zadań**

   Aby upewnić się, że lista aktualizacji jest zawsze aktualna, skonfiguruj zadanie *Wyszukiwanie luk i wymaganych aktualizacji* tak, aby było uruchamiane automatycznie od czasu do czasu. Domyślnie, zadanie *Wyszukiwanie luk i wymaganych aktualizacji* jest ustawione na uruchamianie ręczne.

   Jeśli utworzyłeś zadanie *Zainstaluj wymagane aktualizacje i napraw luki*, możesz skonfigurować terminarz tak, aby zadanie było uruchamiane z tą samą częstotliwością co zadanie *Wyszukiwanie luk i wymaganych aktualizacji* lub rzadziej.

   Jeśli konfigurujesz terminarz uruchamiania zadań, upewnij się, że zadanie instalacji aktualizacji zostanie uruchomione po zakończeniu zadania *Wyszukiwanie luk i wymaganych aktualizacji*.

5. **Zatwierdzanie oraz odrzucanie aktualizacji oprogramowania firm trzecich (opcja)**

   Jeśli utworzyłeś zadanie *Zainstaluj wymagane aktualizacje i napraw luki*, możesz określić reguły instalacji aktualizacji we właściwościach zadania.

   Dla każdej reguły możesz zdefiniować aktualizacje do zainstalowania w zależności od stanu aktualizacji: *Nie zdefiniowano*, *Zatwierdzono* lub *Odrzucono*. Na przykład, możesz utworzyć określone zadanie dla serwerów i ustawić regułę dla tego zadania, aby zezwolić na instalację tylko tych aktualizacji, które posiadają stan *Zatwierdzono*. Po ręcznym ustawieniu stanu *Zatwierdzono* dla tych aktualizacji, które chcesz zainstalować. W tym przypadku aktualizacje, które posiadają stan *Nie zdefiniowano* lub *Odrzucono*, nie będą zainstalowane na serwerach, które określiłeś w zadaniu.

   Używanie stanu *Zatwierdzono* do zarządzania instalacją aktualizacji jest wystarczające dla małej ilości uaktualnień. Aby zainstalować kilka aktualizacji, użyj reguł, które możesz skonfigurować w zadaniu *Zainstaluj wymagane aktualizacje i napraw luki*. Zalecane jest ustawienie stanu *Zatwierdzono* tylko dla tych określonych aktualizacji, które nie spełniają kryteriów określonych w regułach. Jeśli ręcznie zatwierdzisz dużą liczbę aktualizacji, wydajność Serwera administracyjnego spadnie, co może prowadzić do przeciążenia Serwera administracyjnego.

   Domyślnie pobrane uaktualnienia oprogramowania posiadają stan *Nie zdefiniowano*. Możesz zmienić stan na *Zatwierdzono* lub *Odrzucono* na liście **Aktualizacje oprogramowania** list (**Operacje** → **Zarządzanie poprawkami** → **Aktualizacje oprogramowania**).

   Aby uzyskać więcej informacji, zapoznaj się z instrukcjami dotyczącymi zatwierdzania i odrzucania aktualizacji oprogramowania innych firm.

6. **Uruchamianie zadania instalacji aktualizacji**

   Tworzenie zadania *Zainstaluj wymagane aktualizacje i napraw luki*. Jeśli uruchamiasz to zadanie, aktualizacje są pobierane i instalowane na zarządzanych urządzeniach. Po zakończeniu zadania, upewnij się, że na liście zadań posiada stan *Pomyślnie zakończone*.

7. **Utwórz raport o wynikach instalacji aktualizacji (opcja)**

   Aby wyświetlić szczegółowe statystyki dotyczące instalacji aktualizacji, utwórz Raport z wynikami instalacji aktualizacji oprogramowania firm trzecich.

Wyniki

Jeśli utworzyłeś i skonfigurowałeś zadanie *Zainstaluj wymagane aktualizacje i napraw luki*, aktualizacje są automatycznie instalowane na zarządzanych urządzeniach. Jeśli nowe aktualizacje zostaną pobrane do repozytorium Serwera administracyjnego, Kaspersky Security Center Linux sprawdzi, czy spełniają kryteria określone w regułach aktualizacji. Wszystkie nowe aktualizacje, które spełniają kryteria, zostaną zainstalowane automatycznie przy kolejnym uruchomieniu zadania.

Opcje instalacji aktualizacji oprogramowania innej firmy

Aktualizacje oprogramowania innych firm i aktualizacje z witryny Windows Update można instalować na zarządzanych urządzeniach, tworząc i uruchamiając zadanie *Zainstaluj wymagane aktualizacje i napraw luki*. Zadanie *Zainstaluj wymagane aktualizacje i napraw luki* może zostać utworzone tylko wtedy, gdy masz licencję dla funkcji Zarządzanie lukami i poprawkami. Możesz użyć tego zadania, aby zainstalować aktualizacje oprogramowania innych dostawców.

> Interakcja użytkownika może być wymagana podczas aktualizacji aplikacji innej firmy lub naprawy luki w aplikacji innej firmy na zarządzanym urządzeniu. Na przykład, użytkownik może zostać poproszony o zamknięcie aplikacji innej firmy, jeśli jest ona aktualnie otwarta.

Opcjonalnie możesz utworzyć zadanie instalacji wymaganych aktualizacji w następujący sposób:

- Otwierając listę aktualizacji, a następnie określając aktualizacje do zainstalowania.

  W rezultacie tworzone jest nowe zadanie instalacji wybranych aktualizacji. Istnieje możliwość dodania wybranych aktualizacji do istniejącego zadania.

- Uruchamiając kreator instalacji aktualizacji.

  > kreator instalacji aktualizacji jest dostępny tylko dla licencji Zarządzanie lukami i poprawkami.

  Kreator upraszcza tworzenie i konfigurację zadania instalacji aktualizacji i pozwala wyeliminować tworzenie zbędnych zadań zawierających te same aktualizacje do zainstalowania.

Instalowanie aktualizacji oprogramowania innych firm przy użyciu listy aktualizacji

W celu zainstalowania aktualizacji oprogramowania firm trzecich, korzystając z listy aktualizacji:

1. Otwórz listę aktualizacji, korzystając z jednej z następujących ścieżek:

   - **Zarządzanie oprogramowaniem** → **Zarządzanie poprawkami** → **Aktualizacje oprogramowania**.
   - **Zarządzanie zasobami** → **Zasoby (urządzenia)** → <nazwa urządzenia> → **Zaawansowane** → **Dostępne aktualizacje**.
   - **Zarządzanie oprogramowaniem** → **Aplikacje innych firm** → **Rejestr aplikacji** → <nazwa aplikacji> → **Dostępne aktualizacje**.

Zostaje wyświetlona lista dostępnych aktualizacji.

2. Zaznacz pola obok aktualizacji, które chcesz zainstalować.

3. Kliknij przycisk **Zainstaluj aktualizacje**. Jeśli ten przycisk nie jest widoczny, kliknij przycisk wielokropka, a następnie z listy rozwijanej wybierz opcję **Zainstaluj aktualizacje**.

   Aby zainstalować niektóre aktualizacje oprogramowania, należy zaakceptować Umowę licencyjną użytkownika końcowego. Jeśli odrzucisz Umowę licencyjną użytkownika końcowego, aktualizacja oprogramowania nie zostanie zainstalowana.

4. Wybierz jedną z następujących opcji:

   - **Nowe zadanie**

     Zostanie uruchomiony Kreator tworzenia nowego zadania. Jeśli masz licencję Zarządzania lukami i poprawkami, domyślnie wybrany jest typ zadania *Zainstaluj wymagane aktualizacje i napraw luki*. Aby zakończyć tworzenie zadania, postępuj zgodnie z instrukcjami kreatora.

   - **Zainstaluj aktualizację (dodaj regułę do określonego zadania)**

     Wybierz zadanie, do którego chcesz dodać wybrane aktualizacje. Jeśli masz licencję Zarządzania lukami i poprawkami, wybierz zadanie *Zainstaluj wymagane aktualizacje i napraw luki*. Nowa reguła instalacji wybranych aktualizacji zostaje automatycznie dodana do wybranego zadania. Wybrane aktualizacje zostają dodane do właściwości zadania.

     Zostanie otwarte okno właściwości zadania. Kliknij przycisk **Zapisz**, aby zapisać zmiany.

Jeśli wybrałeś utworzenie nowego zadania, zadanie zostanie utworzone i wyświetlone na liście zadań w sekcji **Zadania**. Jeśli wybrałeś dodanie aktualizacji do istniejącego zadania, aktualizacje zostaną zapisane we właściwościach zadania.

Aby zainstalować aktualizacje oprogramowania innych firm, musisz uruchomić zadanie *Zainstaluj wymagane aktualizacje i napraw luki*. Możesz uruchomić to zadanie klikając przycisk **Uruchom** na liście zadań lub określając ustawienia harmonogramu we właściwościach uruchamianego zadania. Podczas określania terminarza zadania upewnij się, że zadanie instalacji aktualizacji jest uruchamiane po zakończeniu zadania *Wyszukiwanie luk i wymaganych aktualizacji*.

Instalowanie aktualizacji oprogramowania innych firm za pomocą Kreator naprawiania luk

kreator instalacji aktualizacji jest dostępny tylko dla licencji Zarządzanie lukami i poprawkami.

W celu utworzenia zadania instalacji aktualizacji oprogramowania firm trzecich, korzystając z Kreator naprawiania luk:

1. W menu głównym przejdź do **Zarządzanie oprogramowaniem** → **Zarządzanie poprawkami** → **Aktualizacje oprogramowania**.

   Zostanie wyświetlona lista dostępnych aktualizacji.

2. Zaznacz pole obok aktualizacji, którą chcesz zainstalować.

3. Kliknij przycisk **Uruchom kreatora instalacji aktualizacji**.

Zostanie uruchomiony kreator instalacji aktualizacji. Strona **Wybierz zadanie instalacji aktualizacji** wyświetla listę wszystkich istniejących zadań następujących typów:

- *Zainstaluj wymagane aktualizacje i napraw luki*
- *Napraw luki*

4. Jeśli chcesz, aby kreator wyświetlał tylko te zadania, które instalują wybraną aktualizację, włącz opcję **Wyświetl tylko zadania instalujące tę aktualizację**.

5. Wybierz, co chcesz zrobić:

   - Aby rozpocząć istniejące zadanie, zaznacz pole wyboru obok zadania *Zainstaluj wymagane aktualizacje i napraw luki*, a następnie kliknij przycisk **Uruchom**.

     Zadanie zakończy się w tle. Dalsze działania nie są wymagane.

   - Aby dodać nową regułę do istniejącego zadania:

     a. Zaznacz pole obok nazwy zadania i kliknij przycisk **Dodaj regułę**.

     > Jeśli wybierzesz więcej niż jedno zadanie, przycisk **Dodaj regułę** jest nieaktywny.

     Nie można dodać reguły do zadania *Napraw luki*. Jeśli wybierzesz zadanie *Napraw luki*, pojawi się następujące powiadomienie: *„Aby zainstalować aktualizacje, użyj zadania „Zainstaluj wymagane aktualizacje i napraw luki””*.

     b. W kroku **Utwórz regułę instalacji aktualizacji** kreatora skonfiguruj nową regułę:

     - **Reguła instalacji dla aktualizacji tej istotności**

       Czasami aktualizacje oprogramowania mogą wpłynąć ujemnie na doświadczenie użytkownika z oprogramowaniem. W takich przypadkach możesz zdecydować się na zainstalowanie tylko tych aktualizacji, które są krytyczne dla działania oprogramowania, a na pominięcie innych aktualizacji.

       Jeśli ta opcja jest włączona, aktualizacje eliminują tylko te luki, dla których priorytet określony przez Kaspersky jest równy lub wyższy niż priorytet wybranej aktualizacji (**Średni**, **Wysoki** lub **Krytyczny**). Luki z priorytetem niższym niż wybrana wartość nie zostają wyeliminowane.

       Jeśli ta opcja jest wyłączona, aktualizacje eliminują wszystkie luki niezależnie od ich priorytetu.

       Domyślnie opcja ta jest wyłączona.

       Ta reguła nie jest wyświetlana, jeśli istotność wybranej aktualizacji jest *Nieznany*.

     - **Reguła instalacji aktualizacji tej istotności zgodnie z MSRC**

       Czasami aktualizacje oprogramowania mogą wpłynąć ujemnie na doświadczenie użytkownika z oprogramowaniem. W takich przypadkach możesz zdecydować się na zainstalowanie tylko tych aktualizacji, które są krytyczne dla działania oprogramowania, a na pominięcie innych aktualizacji.

       Jeśli ta opcja jest włączona (dostępna tylko dla aktualizacji systemu Windows Update), aktualizacje eliminują tylko te luki, dla których priorytet określony przez centrum Microsoft Security Response Center (MSRC) jest równy lub wyższy niż wartość wybrana na liście (**Niski**, **Średni**, **Wysoki** lub **Krytyczny**). Luki z priorytetem niższym niż wybrana wartość nie zostają wyeliminowane.

       Jeśli ta opcja jest wyłączona, aktualizacje eliminują wszystkie luki niezależnie od ich priorytetu.

       Domyślnie opcja ta jest wyłączona.

Ta reguła jest wyświetlana tylko w przypadku aktualizacji oprogramowania firmy Microsoft. Nie jest wyświetlana, jeśli istotność wybranej aktualizacji jest *Nieznany*.

- **Reguła instalacji dla aktualizacji tego dostawcy**

  Ta opcja jest dostępna tylko dla aktualizacji aplikacji innych firm. Kaspersky Security Center Linux instaluje tylko te aktualizacje, które odnoszą się do aplikacji stworzonych przez tego samego dostawcę co wybrana aktualizacja. Odrzucone aktualizacje i aktualizacje aplikacji stworzone przez innych dostawców nie są instalowane.

  Domyślnie opcja ta jest wyłączona.

  Ta reguła jest wyświetlana tylko w przypadku aktualizacji oprogramowania innych firm.

- **Reguła instalacji dla aktualizacji typu**

- **Reguła instalacji aktualizacji wybranej aplikacji**

  Ta reguła jest wyświetlana tylko w przypadku aktualizacji oprogramowania innych firm.

- **Reguła instalacji dla wybranej aktualizacji**

- **Zatwierdź wybrane aktualizacje**

  Instalacja wybranej aktualizacji zostanie zatwierdzona. Włącz tę opcję, jeśli niektóre stosowane reguły instalacji aktualizacji zezwalają tylko na instalację zaakceptowanych aktualizacji.

  Domyślnie opcja ta jest wyłączona.

- **Automatycznie zainstaluj wszystkie poprzednie aktualizacje aplikacji, jeśli są one niezbędne do zainstalowania wybranych aktualizacji**

  Pozostaw tę opcję włączoną, jeśli zgadzasz się na instalację tymczasowych wersji aplikacji, gdy jest to wymagane do zainstalowania wybranych aktualizacji.

  Jeśli ta opcja jest wyłączona, tylko wybrane wersje aplikacji są instalowane. Wybierz tę opcję, jeśli chcesz zaktualizować aplikacje w prosty sposób, bez próby zainstalowania kolejnych wersji. Jeśli zainstalowanie wybranych aktualizacji nie jest możliwe bez zainstalowania poprzednich wersji aplikacji, aktualizacja aplikacji nie powiedzie się.

  Na przykład, posiadasz wersję 3 aplikacji zainstalowanej na urządzeniu i chcesz zaktualizować ją do wersji 5, ale wersja 5 tej aplikacji może być zainstalowana tylko na wersji 4. Jeśli ta opcja jest włączona, oprogramowanie w pierwszej kolejności instaluje wersję 4, a następnie instaluje wersję 5. Jeśli ta opcja jest wyłączona, oprogramowanie nie zdoła zaktualizować aplikacji.

  Domyślnie opcja ta jest włączona.

c. Kliknij przycisk **Dodaj**.

Zostanie otwarte okno właściwości zadania. Nowa reguła została już dodana do właściwości zadania. Możesz przejrzeć lub zmodyfikować regułę lub ustawienia innego zadania. Kliknij przycisk **Zapisz**, aby zapisać zmiany.

- W celu utworzenia zadania:

  a. Kliknij przycisk **Nowe zadanie**.

  b. W kroku **Utwórz regułę instalacji aktualizacji** kreatora skonfiguruj nową regułę:

  - **Reguła instalacji dla aktualizacji tej istotności**

Czasami aktualizacje oprogramowania mogą wpłynąć ujemnie na doświadczenie użytkownika z oprogramowaniem. W takich przypadkach możesz zdecydować się na zainstalowanie tylko tych aktualizacji, które są krytyczne dla działania oprogramowania, a na pominięcie innych aktualizacji.

Jeśli ta opcja jest włączona, aktualizacje eliminują tylko te luki, dla których priorytet określony przez Kaspersky jest równy lub wyższy niż priorytet wybranej aktualizacji (**Średni**, **Wysoki** lub **Krytyczny**). Luki z priorytetem niższym niż wybrana wartość nie zostają wyeliminowane.

Jeśli ta opcja jest wyłączona, aktualizacje eliminują wszystkie luki niezależnie od ich priorytetu.

Domyślnie opcja ta jest wyłączona.

Ta reguła nie jest wyświetlana, jeśli istotność wybranej aktualizacji jest *Nieznany*.

- **Reguła instalacji aktualizacji tej istotności zgodnie z MSRC**

  Czasami aktualizacje oprogramowania mogą wpłynąć ujemnie na doświadczenie użytkownika z oprogramowaniem. W takich przypadkach możesz zdecydować się na zainstalowanie tylko tych aktualizacji, które są krytyczne dla działania oprogramowania, a na pominięcie innych aktualizacji.

  Jeśli ta opcja jest włączona (dostępna tylko dla aktualizacji systemu Windows Update), aktualizacje eliminują tylko te luki, dla których priorytet określony przez centrum Microsoft Security Response Center (MSRC) jest równy lub wyższy niż wartość wybrana na liście (**Niski**, **Średni**, **Wysoki** lub **Krytyczny**). Luki z priorytetem niższym niż wybrana wartość nie zostają wyeliminowane.

  Jeśli ta opcja jest wyłączona, aktualizacje eliminują wszystkie luki niezależnie od ich priorytetu.

  Domyślnie opcja ta jest wyłączona.

  Ta reguła jest wyświetlana tylko w przypadku aktualizacji oprogramowania firmy Microsoft. Nie jest wyświetlana, jeśli istotność wybranej aktualizacji jest *Nieznany*.

- **Reguła instalacji dla aktualizacji tego dostawcy**

  Ta opcja jest dostępna tylko dla aktualizacji aplikacji innych firm. Kaspersky Security Center Linux instaluje tylko te aktualizacje, które odnoszą się do aplikacji stworzonych przez tego samego dostawcę co wybrana aktualizacja. Odrzucone aktualizacje i aktualizacje aplikacji stworzone przez innych dostawców nie są instalowane.

  Domyślnie opcja ta jest wyłączona.

  Ta reguła jest wyświetlana tylko w przypadku aktualizacji oprogramowania innych firm.

- **Reguła instalacji dla aktualizacji typu**

- **Reguła instalacji aktualizacji wybranej aplikacji**

  Ta reguła jest wyświetlana tylko w przypadku aktualizacji oprogramowania innych firm.

- **Reguła instalacji dla wybranej aktualizacji**

- **Zatwierdź wybrane aktualizacje**

  Instalacja wybranej aktualizacji zostanie zatwierdzona. Włącz tę opcję, jeśli niektóre stosowane reguły instalacji aktualizacji zezwalają tylko na instalację zaakceptowanych aktualizacji.

  Domyślnie opcja ta jest wyłączona.

- **Automatycznie zainstaluj wszystkie poprzednie aktualizacje aplikacji, jeśli są one niezbędne do zainstalowania wybranych aktualizacji**

  Pozostaw tę opcję włączoną, jeśli zgadzasz się na instalację tymczasowych wersji aplikacji, gdy jest to wymagane do zainstalowania wybranych aktualizacji.

Jeśli ta opcja jest wyłączona, tylko wybrane wersje aplikacji są instalowane. Wybierz tę opcję, jeśli chcesz zaktualizować aplikacje w prosty sposób, bez próby zainstalowania kolejnych wersji. Jeśli zainstalowanie wybranych aktualizacji nie jest możliwe bez zainstalowania poprzednich wersji aplikacji, aktualizacja aplikacji nie powiedzie się.

Na przykład, posiadasz wersję 3 aplikacji zainstalowanej na urządzeniu i chcesz zaktualizować ją do wersji 5, ale wersja 5 tej aplikacji może być zainstalowana tylko na wersji 4. Jeśli ta opcja jest włączona, oprogramowanie w pierwszej kolejności instaluje wersję 4, a następnie instaluje wersję 5. Jeśli ta opcja jest wyłączona, oprogramowanie nie zdoła zaktualizować aplikacji.

Domyślnie opcja ta jest włączona.

c. Kliknij przycisk **Dodaj**.

Kontynuuj tworzenie zadania w kreatorze tworzenia nowego zadania. Nowa reguła dodana w kreatorze instalacji aktualizacji zostanie wyświetlona w kreatorze tworzenia nowego zadania. Po zakończeniu pracy kreatora, do listy zadań zostanie dodane zadanie *Zainstaluj wymagane aktualizacje i napraw luki*.

Ustawienia zadania Wyszukiwanie luk i wymaganych aktualizacji

Zadanie *Wyszukiwanie luk i wymaganych aktualizacji* jest tworzone automatycznie po uruchomieniu kreatora wstępnej konfiguracji. Jeśli nie uruchomiono kreatora, możesz utworzyć zadanie ręcznie.

Oprócz ogólnych ustawień zadania możesz określić następujące ustawienia podczas tworzenia zadania *Wyszukiwanie luk i wymaganych aktualizacji* lub później, podczas konfigurowania właściwości utworzonego zadania:

- **Wyszukaj luki i aktualizacje wymienione przez firmę Microsoft**

  Podczas wyszukiwania luk i aktualizacji program Kaspersky Security Center Linux używa informacji o stosowanych aktualizacjach firmy Microsoft ze źródła uaktualnień Microsoft, które są dostępne w danym momencie.

  Na przykład, możesz chcieć wyłączyć tę opcję, jeśli posiadasz różne zadania z różnymi ustawieniami aktualizacji Microsoft i aktualizacji aplikacji innych firm.

  Domyślnie opcja ta jest włączona.

  Informacje o opcjonalnych aktualizacjach Microsoft Windows nie są wysyłane do Serwera administracyjnego.

- **Połącz z serwerem aktualizacji, aby zaktualizować dane**

  Agent usługi Windows Update na zarządzanym urządzeniu nawiązuje połączenie ze źródłem uaktualnień Microsoft. Następujące serwery mogą pełnić rolę źródeł aktualizacji Microsoft:

  - System Windows Server wdrożony w sieci Twojej organizacji wraz z programem Microsoft Windows Server Update Services (WSUS)
  - Serwery aktualizacji Microsoft

  Jeśli ta opcja jest włączona, agent usługi Windows Update na zarządzanym urządzeniu nawiązuje połączenie ze źródłem aktualizacji firmy Microsoft, aby odświeżyć informacje o stosowanych aktualizacjach Microsoft Windows.

  Jeśli ta opcja jest wyłączona, agent usługi Windows Update na zarządzanym urządzeniu używa informacji o stosowanych aktualizacjach Microsoft Windows, które zostały pobrane ze źródła aktualizacji firmy Microsoft wcześniej i które są przechowywane w pamięci podręcznej urządzenia.

Nawiązywanie połączenia ze źródłem aktualizacji firmy Microsoft może zużywać dużo zasobów. Możesz chcieć wyłączyć tę opcję, jeśli ustawisz regularne nawiązywanie połączenia z tym źródłem uaktualnień w innym zadaniu lub we właściwościach zasady Agenta sieciowego, w sekcji **Aktualizacje oprogramowania i luki**. Jeśli nie chcesz wyłączyć tej opcji, następnie, aby zmniejszyć obciążenie Serwera, możesz skonfigurować terminarz zadania do losowego opóźnienia uruchomienia zadania w ciągu 360 minut.

Domyślnie opcja ta jest włączona.

Kombinacja następujących opcji ustawień zasady Agenta sieciowego definiuje tryb uzyskiwania aktualizacji:

- Agent usługi Windows Update na zarządzanym urządzeniu łączy się z serwerem aktualizacji w celu pobierania aktualizacji tylko wtedy, gdy opcja **Połącz z serwerem aktualizacji, aby zaktualizować dane** jest włączona we właściwościach zadania *Wyszukiwanie luk i wymaganych aktualizacji*, a opcja **Tryb wyszukiwania aktualizacji systemu Windows** jest ustawiona na **Aktywny** w ustawieniach zasady Agenta sieciowego.

- Jeśli nie potrzebujesz, aby Agent sieciowy nawiązał połączenie ze źródłem aktualizacji systemu Microsoft Windows i pobrał aktualizacje podczas wykonywania zadania *skanowania w poszukiwaniu luk*, możesz ustawić opcję **Tryb wyszukiwania aktualizacji systemu Windows** na **Pasywny**, a opcja **Połącz z serwerem aktualizacji, aby zaktualizować dane** musi pozostać włączona. Dzięki temu możesz zaoszczędzić zasoby i wykorzystać wcześniej pobrane aktualizacje systemu Windows do skanowania w poszukiwaniu luk w zabezpieczeniach. Możesz użyć trybu pasywnego, jeśli skonfigurujesz otrzymywanie aktualizacji systemu Microsoft Windows w inny sposób. Jeśli odbieranie aktualizacji systemu Microsoft Windows nie zostało skonfigurowane w inny sposób, nie należy ustawiać opcji **Tryb wyszukiwania aktualizacji systemu Windows** na **Pasywny**, ponieważ w takim przypadku informacje o aktualizacjach nigdy nie zostaną odebrane.

- Bez względu na stan opcji **Połącz z serwerem aktualizacji, aby zaktualizować dane** (włączona lub wyłączona), jeśli opcja **Tryb wyszukiwania aktualizacji systemu Windows** jest ustawiony na **Wyłączony**, Kaspersky Security Center Linux nie żąda żadnych informacji o aktualizacjach.

Jeśli w sieci Twojej organizacji używany jest serwer WSUS (lokalny serwer WSUS) i chcesz go używać razem z Serwerem administracyjnym Kaspersky Security Center, musisz najpierw upewnić się, że Serwer administracyjny Kaspersky Security Center nie jest używany jako serwer WSUS, a następnie wykonać następujące czynności:

1. Na swoich zarządzanych urządzeniach z systemem Windows, określ lokalny serwer WSUS dla usługi aktualizacji Windows Update. Możesz to zrobić ręcznie w rejestrze systemu Windows lub za pomocą zasad grupy systemu Windows.

2. Na lokalnym serwerze WSUS określ wymagane klasyfikacje aktualizacji oraz aplikacje, na których aktualizacje mają być dystrybuowane.

3. Zsynchronizuj serwer WSUS z serwerem nadrzędnym (może to być serwer Microsoft WSUS lub inny lokalny serwer nadrzędny WSUS).

Po uruchomieniu zadania *Wyszukiwanie luk i wymaganych aktualizacji* na urządzeniu, Agent sieciowy korzysta z usługi Windows Update, aby zainicjować żądanie dotyczące aktualizacji Windows Update odpowiednich dla urządzenia. Usługa Windows Update pobiera adres zewnętrznego serwera WSUS z rejestru i wyszukuje aktualizacje bezpośrednio na tym zewnętrznym serwerze WSUS. Następnie usługa Windows Update przekazuje tę listę do Serwera administracyjnego za pośrednictwem Agenta sieciowego. W ten sposób Serwer administracyjny ma aktualną bazę danych.

- **Wyszukaj luki i aktualizacje innych firm wymienione przez firmę Kaspersky**

  Jeśli ta opcja jest włączona, Kaspersky Security Center Linux wyszukuje luki i wymagane aktualizacje dla aplikacji firm trzecich (aplikacji producentów innych niż Kaspersky i Microsoft) w rejestrze systemu Windows i w folderach określonych pod **Określ ścieżki zaawansowanego wyszukiwania aplikacji w systemie plików**. Pełna lista obsługiwanych aplikacji firm trzecich jest zarządzana przez Kaspersky.

Jeśli ta opcja jest wyłączona, Kaspersky Security Center Linux nie szuka luk i wymaganych uaktualnień dla aplikacji firm trzecich. Na przykład, możesz chcieć wyłączyć tę opcję, jeśli posiadasz różne zadania z różnymi ustawieniami aktualizacji Microsoft Windows i aktualizacji aplikacji innych firm.

Domyślnie opcja ta jest włączona.

- **Określ ścieżki zaawansowanego wyszukiwania aplikacji w systemie plików**

  Foldery, w których Kaspersky Security Center Linux wyszukuje aplikacje firm trzecich, które wymagają naprawienia luk i zainstalowania aktualizacji. Możesz użyć zmiennych systemowych.

  Określ foldery, w których zostaną zainstalowane aplikacje. Domyślnie, lista zawiera foldery systemowe, w których instalowana jest większość aplikacji.

- **Włącz diagnostykę zaawansowaną**

  Jeśli ta funkcja jest włączona, Agent sieciowy zapisuje pliki śledzenia nawet wtedy, gdy zapisywanie plików śledzenia jest wyłączone dla Agenta sieciowego w Narzędziu zdalnej diagnostyki Kaspersky Security Center Linux. Śledzenie jest zapisywane do dwóch plików; całkowity rozmiar obu plików jest określany przez wartość **Maksymalny rozmiar plików zaawansowanej diagnostyki, w MB**. Jeśli oba pliki są pełne, Agent sieciowy ponownie uruchamia zapisywanie do tych plików. Pliki zawierające ślady są przechowywane w folderze %WINDIR%\Temp. Te pliki są dostępne w narzędziu do zdalnej diagnostyki – możesz je pobrać lub usunąć.

  Jeśli ta funkcja jest wyłączona, Agent sieciowy zapisuje śledzenie zgodnie z ustawieniami Narzędzia zdalnej diagnostyki Kaspersky Security Center Linux. Nie są zapisywane żadne dodatkowe pliki śledzenia.

  Jeśli tworzysz zadanie, nie musisz włączać zaawansowanej diagnostyki. Tej funkcji można użyć później, jeśli, na przykład, uruchomienie zadania nie powiedzie się na niektórych urządzeniach i chcesz uzyskać dodatkowe informacje podczas uruchamiania innego zadania.

  Domyślnie opcja ta jest wyłączona.

- **Maksymalny rozmiar plików zaawansowanej diagnostyki, w MB**

  Domyślna wartość to 100 MB, a dostępne wartości mieszczą się między 1 MB a 2048 MB. Specjalista z pomocy technicznej Kaspersky może poprosić o zmianę domyślnej wartości, jeśli informacje w plikach zaawansowanej diagnostyki, które wysłałeś, nie są wystarczające do rozwiązania problemu.

Zalecenia dotyczące terminarza zadania

Podczas tworzenia terminarza zadania *Wyszukiwanie luk i wymaganych aktualizacji* upewnij się, że włączone są dwie opcje: **Uruchom pominięte zadania** oraz **Używaj automatycznie losowego opóźnienia dla uruchamiania zadań**.

Domyślnie, zadanie *Wyszukiwanie luk i wymaganych aktualizacji* jest ustawione na uruchamianie ręczne. Jeśli zasady obowiązujące w organizacji nakazują wyłączenie wszystkich urządzeń w tym czasie, zadanie *Wyszukiwanie luk i wymaganych aktualizacji* zostanie uruchomione, gdy urządzenia znowu zostaną włączone, czyli następnego dnia rano. Takie działanie nie jest wskazane, ponieważ wykrywanie luk może zwiększać zużycie procesora i obciążenie podsystemów dysku. Terminarz dla tego zadania należy skonfigurować w oparciu o zasady obowiązujące w organizacji.

Tworzenie zadania Wyszukiwanie luk i wymaganych aktualizacji

Za pośrednictwem zadania *Wyszukiwanie luk i wymaganych aktualizacji* program Kaspersky Security Center Linux otrzymuje listy wykrytych luk i wymaganych aktualizacji dla oprogramowania firm trzecich, zainstalowanego na zarządzanych urządzeniach.

Zadanie *Wyszukiwanie luk i wymaganych aktualizacji* możesz utworzyć tylko dla urządzeń z systemem Windows. Nie można utworzyć tego zadania dla urządzeń działających na innych systemach operacyjnych.

Zadanie *Wyszukiwanie luk i wymaganych aktualizacji* jest tworzone automatycznie po uruchomieniu kreatora wstępnej konfiguracji. Jeśli nie uruchamiałeś kreatora, możesz utworzyć zadanie ręcznie.

W celu utworzenia zadania Wyszukiwanie luk i wymaganych aktualizacji:

1. W menu głównym przejdź do **Zadania**.
2. Kliknij **Dodaj**.

   Zostanie uruchomiony Kreator tworzenia nowego zadania. Przejdź przez kroki kreatora, korzystając z przycisku **Dalej**.
3. Dla aplikacji Kaspersky Security Center wybierz typ zadania **Wyszukiwanie luk i wymaganych aktualizacji**.
4. Określ nazwę tworzonego zadania. Nazwa zadania nie może zawierać więcej niż 100 znaków oraz nie może zawierać żadnych znaków specjalnych ("*<>?\:|).
5. Wybierz urządzenia, do których zadanie zostanie przypisane.
6. Określ metody skanowania w poszukiwaniu luk i aplikacji wymagających aktualizacji:

   - **Wyszukaj luki i aktualizacje wymienione przez firmę Microsoft**

     Podczas wyszukiwania luk i aktualizacji program Kaspersky Security Center Linux używa informacji o stosowanych aktualizacjach firmy Microsoft ze źródła uaktualnień Microsoft, które są dostępne w danym momencie.

     Na przykład, możesz chcieć wyłączyć tę opcję, jeśli posiadasz różne zadania z różnymi ustawieniami aktualizacji Microsoft i aktualizacji aplikacji innych firm.

     Domyślnie opcja ta jest włączona.

     Informacje o opcjonalnych aktualizacjach Microsoft Windows nie są wysyłane do Serwera administracyjnego.

     - **Połącz z serwerem aktualizacji, aby zaktualizować dane**

       Agent usługi Windows Update na zarządzanym urządzeniu nawiązuje połączenie ze źródłem uaktualnień Microsoft. Następujące serwery mogą pełnić rolę źródeł aktualizacji Microsoft:

       - System Windows Server wdrożony w sieci Twojej organizacji wraz z programem Microsoft Windows Server Update Services (WSUS)
       - Serwery aktualizacji Microsoft

Jeśli ta opcja jest włączona, agent usługi Windows Update na zarządzanym urządzeniu nawiązuje połączenie ze źródłem aktualizacji firmy Microsoft, aby odświeżyć informacje o stosowanych aktualizacjach Microsoft Windows.

Jeśli ta opcja jest wyłączona, agent usługi Windows Update na zarządzanym urządzeniu używa informacji o stosowanych aktualizacjach Microsoft Windows, które zostały pobrane ze źródła aktualizacji firmy Microsoft wcześniej i które są przechowywane w pamięci podręcznej urządzenia.

Nawiązywanie połączenia ze źródłem aktualizacji firmy Microsoft może zużywać dużo zasobów. Możesz chcieć wyłączyć tę opcję, jeśli ustawisz regularne nawiązywanie połączenia z tym źródłem uaktualnień w innym zadaniu lub we właściwościach zasady Agenta sieciowego, w sekcji **Aktualizacje oprogramowania i luki**. Jeśli nie chcesz wyłączyć tej opcji, następnie, aby zmniejszyć obciążenie Serwera, możesz skonfigurować terminarz zadania do losowego opóźnienia uruchomienia zadania w ciągu 360 minut.

Domyślnie opcja ta jest włączona.

Kombinacja następujących opcji ustawień zasady Agenta sieciowego definiuje tryb uzyskiwania aktualizacji:

- Agent usługi Windows Update na zarządzanym urządzeniu łączy się z serwerem aktualizacji w celu pobierania aktualizacji tylko wtedy, gdy opcja **Połącz z serwerem aktualizacji, aby zaktualizować dane** jest włączona we właściwościach zadania *Wyszukiwanie luk i wymaganych aktualizacji*, a opcja **Tryb wyszukiwania aktualizacji systemu Windows** jest ustawiona na **Aktywny** w ustawieniach zasady Agenta sieciowego.

- Jeśli nie potrzebujesz, aby Agent sieciowy nawiązał połączenie ze źródłem aktualizacji systemu Microsoft Windows i pobrał aktualizacje podczas wykonywania zadania *skanowania w poszukiwaniu luk*, możesz ustawić opcję **Tryb wyszukiwania aktualizacji systemu Windows** na **Pasywny**, a opcja **Połącz z serwerem aktualizacji, aby zaktualizować dane** musi pozostać włączona. Dzięki temu możesz zaoszczędzić zasoby i wykorzystać wcześniej pobrane aktualizacje systemu Windows do skanowania w poszukiwaniu luk w zabezpieczeniach. Możesz użyć trybu pasywnego, jeśli skonfigurujesz otrzymywanie aktualizacji systemu Microsoft Windows w inny sposób. Jeśli odbieranie aktualizacji systemu Microsoft Windows nie zostało skonfigurowane w inny sposób, nie należy ustawiać opcji **Tryb wyszukiwania aktualizacji systemu Windows** na **Pasywny**, ponieważ w takim przypadku informacje o aktualizacjach nigdy nie zostaną odebrane.

- Bez względu na stan opcji **Połącz z serwerem aktualizacji, aby zaktualizować dane** (włączona lub wyłączona), jeśli opcja **Tryb wyszukiwania aktualizacji systemu Windows** jest ustawiony na **Wyłączony**, Kaspersky Security Center Linux nie żąda żadnych informacji o aktualizacjach.

Jeśli w sieci Twojej organizacji używany jest serwer WSUS (lokalny serwer WSUS) i chcesz go używać razem z Serwerem administracyjnym Kaspersky Security Center, musisz najpierw upewnić się, że Serwer administracyjny Kaspersky Security Center nie jest używany jako serwer WSUS, a następnie wykonać następujące czynności:

1. Na swoich zarządzanych urządzeniach z systemem Windows, określ lokalny serwer WSUS dla usługi aktualizacji Windows Update. Możesz to zrobić ręcznie w rejestrze systemu Windows lub za pomocą zasad grupy systemu Windows.

2. Na lokalnym serwerze WSUS określ wymagane klasyfikacje aktualizacji oraz aplikacje, na których aktualizacje mają być dystrybuowane.

3. Zsynchronizuj serwer WSUS z serwerem nadrzędnym (może to być serwer Microsoft WSUS lub inny lokalny serwer nadrzędny WSUS).

Po uruchomieniu zadania *Wyszukiwanie luk i wymaganych aktualizacji* na urządzeniu, Agent sieciowy korzysta z usługi Windows Update, aby zainicjować żądanie dotyczące aktualizacji Windows Update odpowiednich dla urządzenia. Usługa Windows Update pobiera adres zewnętrznego serwera WSUS z rejestru i wyszukuje aktualizacje bezpośrednio na tym zewnętrznym serwerze WSUS. Następnie usługa Windows Update przekazuje tę listę do Serwera administracyjnego za pośrednictwem Agenta sieciowego. W ten sposób Serwer administracyjny ma aktualną bazę danych.

- **Wyszukaj luki i aktualizacje innych firm wymienione przez firmę Kaspersky**

  Jeśli ta opcja jest włączona, Kaspersky Security Center Linux wyszukuje luki i wymagane aktualizacje dla aplikacji firm trzecich (aplikacji producentów innych niż Kaspersky i Microsoft) w rejestrze systemu Windows i w folderach określonych pod **Określ ścieżki zaawansowanego wyszukiwania aplikacji w systemie plików**. Pełna lista obsługiwanych aplikacji firm trzecich jest zarządzana przez Kaspersky.

  Jeśli ta opcja jest wyłączona, Kaspersky Security Center Linux nie szuka luk i wymaganych uaktualnień dla aplikacji firm trzecich. Na przykład, możesz chcieć wyłączyć tę opcję, jeśli posiadasz różne zadania z różnymi ustawieniami aktualizacji Microsoft Windows i aktualizacji aplikacji innych firm.

  Domyślnie opcja ta jest włączona.

Możesz wyłączyć te opcje po utworzeniu zadania w zakładce **Ustawienia aplikacji** okna właściwości zadania.

7. **Określ ścieżki zaawansowanego wyszukiwania aplikacji w systemie plików**

   Foldery, w których Kaspersky Security Center Linux wyszukuje aplikacje firm trzecich, które wymagają naprawienia luk i zainstalowania aktualizacji. Możesz użyć zmiennych systemowych.

   Określ foldery, w których zostaną zainstalowane aplikacje. Domyślnie, lista zawiera foldery systemowe, w których instalowana jest większość aplikacji.

   Określone ścieżki możesz zmienić po utworzeniu zadania w zakładce **Ustawienia aplikacji** okna właściwości zadania.

8. W razie potrzeby **Włącz diagnostykę zaawansowaną**

   Jeśli ta funkcja jest włączona, Agent sieciowy zapisuje pliki śledzenia nawet wtedy, gdy zapisywanie plików śledzenia jest wyłączone dla Agenta sieciowego w Narzędziu zdalnej diagnostyki Kaspersky Security Center Linux. Śledzenie jest zapisywane do dwóch plików; całkowity rozmiar obu plików jest określany przez wartość **Maksymalny rozmiar plików zaawansowanej diagnostyki, w MB**. Jeśli oba pliki są pełne, Agent sieciowy ponownie uruchamia zapisywanie do tych plików. Pliki zawierające ślady są przechowywane w folderze %WINDIR%\Temp. Te pliki są dostępne w narzędziu do zdalnej diagnostyki – możesz je pobrać lub usunąć.

   Jeśli ta funkcja jest wyłączona, Agent sieciowy zapisuje śledzenie zgodnie z ustawieniami Narzędzia zdalnej diagnostyki Kaspersky Security Center Linux. Nie są zapisywane żadne dodatkowe pliki śledzenia.

   Jeśli tworzysz zadanie, nie musisz włączać zaawansowanej diagnostyki. Tej funkcji można użyć później, jeśli, na przykład, uruchomienie zadania nie powiedzie się na niektórych urządzeniach i chcesz uzyskać dodatkowe informacje podczas uruchamiania innego zadania.

   Domyślnie opcja ta jest wyłączona.

   Możesz wyłączyć tę opcję po utworzeniu zadania w zakładce **Ustawienia aplikacji** okna właściwości zadania.

9. Określ **Maksymalny rozmiar plików zaawansowanej diagnostyki, w MB**

   Domyślna wartość to 100 MB, a dostępne wartości mieszczą się między 1 MB a 2048 MB. Specjalista z pomocy technicznej Kaspersky może poprosić o zmianę domyślnej wartości, jeśli informacje w plikach zaawansowanej diagnostyki, które wysłałeś, nie są wystarczające do rozwiązania problemu.

   Musisz określić tę wartość, jeśli w poprzednim kroku włączono zaawansowaną diagnostykę. Możesz zmienić tę wartość po utworzeniu zadania w zakładce **Ustawienia aplikacji** okna właściwości zadania.

10. Jeśli chcesz zmodyfikować domyślne ustawienia zadania, włącz opcję **Otwórz szczegóły zadania po jego utworzeniu** na stronie **Zakończ tworzenie zadania**. Jeśli nie włączysz tej opcji, zadanie zostanie utworzone z domyślnymi ustawieniami. Możesz zmodyfikować domyślne ustawienia później w dowolnym momencie.

11. Kliknij przycisk **Zakończ**.

    Kreator tworzy zadanie. Jeśli włączyłeś opcję **Otwórz szczegóły zadania po jego utworzeniu**, automatycznie zostanie otwarte okno właściwości zadania. W tym oknie możesz określić ogólne ustawienia zadania oraz w razie potrzeby zmienić ustawienia określone podczas tworzenia zadania.

    Możesz także otworzyć okno właściwości zadania, klikając nazwę utworzonego zadania na liście zadań.

Zadanie zostało utworzone i skonfigurowane. Aby uruchomić zadanie, na liście zadań wybierz zadanie i kliknij przycisk **Uruchom**.

Zalecenia dotyczące harmonogramu zadania

Podczas tworzenia terminarza zadania *Wyszukiwanie luk i wymaganych aktualizacji* upewnij się, że włączone są dwie opcje: **Uruchom pominięte zadania** oraz **Używaj automatycznie losowego opóźnienia dla uruchamiania zadań**.

Domyślnie, zadanie *Wyszukiwanie luk i wymaganych aktualizacji* jest ustawione na uruchamianie ręczne.

Możesz także zaplanować rozpoczęcie zadania *Wyszukiwanie luk i wymaganych aktualizacji* o określonej godzinie. Na przykład możesz wybrać opcję **Co N godzin** zaplanowanego rozpoczęcia z listy rozwijanej **Uruchom zadanie** na karcie **Terminarz** w oknie właściwości zadania. Jeśli zasady obowiązujące w organizacji nakazują wyłączenie wszystkich urządzeń w tym czasie, zadanie *Wyszukiwanie luk i wymaganych aktualizacji* zostanie uruchomione, gdy urządzenia znowu zostaną włączone. Takie działanie nie jest wskazane, ponieważ wykrywanie luk może zwiększać zużycie procesora i obciążenie podsystemów dysku. Terminarz dla tego zadania należy skonfigurować w oparciu o zasady obowiązujące w organizacji.

Szczegółowy opis ustawień zaplanowanego uruchomienia znajduje się w ogólnych ustawieniach zadania.

Przeglądanie informacji o dostępnych aktualizacjach oprogramowania firm trzecich

Możesz przejrzeć listę dostępnych aktualizacji dla oprogramowania firm trzecich, w tym oprogramowania firmy Microsoft, zainstalowanego na urządzeniach klienckich.

W celu przejrzenia listy aktualizacji dostępnych dla aplikacji firm trzecich, zainstalowanych na urządzeniach klienckich,

W menu głównym przejdź do **Zarządzanie oprogramowaniem** → **Zarządzanie poprawkami** → **Aktualizacje oprogramowania**.

Zostaje wyświetlona lista dostępnych aktualizacji.

Możesz określić filtr przeglądania listy aktualizacji oprogramowania. Kliknij ikonę **Filtr** ( ) na liście aktualizacji oprogramowania w celu zarządzania filtrem. Możesz także wybrać jeden z predefiniowanych filtrów z listy rozwijalnej **Wstępnie ustawione filtry** nad listą luk w oprogramowaniu.

W celu przejrzenia właściwości aktualizacji:

1. Kliknij nazwę żądanej aktualizacji oprogramowania.

2. Zostanie otwarte okno właściwości aktualizacji, wyświetlające informacje pogrupowane na następujących zakładkach:

   - **Ogólne**

     Ta zakładka wyświetla ogólne szczegóły wybranej aktualizacji:

     - Stan zatwierdzenia aktualizacji (można zmienić ręcznie, wybierają nowy stan na liście rozwijalnej)
     - Data i godzina zarejestrowania aktualizacji
     - Data i godzina utworzenia aktualizacji
     - Istotność aktualizacji
     - Wymagania instalacyjne: nałożone przez aktualizację
     - Rodzina aplikacji, do której należy aktualizacja
     - Aplikacja, do której stosowana jest aktualizacja
     - Liczba rewizji aktualizacji

   - **Atrybuty**

     Ta zakładka wyświetla zestaw atrybutów, których możesz użyć do uzyskania większej ilości informacji na temat wybranej aktualizacji. Ten zestaw różni się w zależności od tego, czy aktualizacja jest publikowana przez firmę Microsoft lub innego producenta.

     Zakładka wyświetla następujące informacje dla aktualizacji firmy Microsoft:

     - Poziom ważności aktualizacji zgodny z Microsoft Security Response Center (MSRC)
     - Odnośnik do artykułu w Bazie wiedzy Microsoft Knowledge Base opisujący aktualizację
     - Odnośnik do artykułu w biuletynie Microsoft Security Bulletin opisujący aktualizację
     - Identyfikator aktualizacji (ID)

     Zakładka wyświetla następujące informacje dla aktualizacji innej firmy:

     - Czy aktualizacja jest poprawką lub pełnym pakietem dystrybucyjnym
     - Język lokalizacji aktualizacji
     - Czy aktualizacja jest instalowana automatycznie lub ręcznie
     - Czy aktualizacja została wycofana po zastosowaniu
     - Odnośnik do pobrania aktualizacji

- **Urządzenia**

  Ta zakładka wyświetla listę urządzeń, na których zainstalowano wybraną aktualizację.

- **Naprawione luki**

  Ta zakładka wyświetla listę luk, które mogą zostać usunięte przez wybraną aktualizację.

- **Podział aktualizacji**

  Ta zakładka wyświetla możliwe podziały między różnymi aktualizacjami opublikowanymi dla tej samej aplikacji, czyli czy wybrana aktualizacja może zastąpić inne aktualizacje lub czy mogą zostać zastąpione przez inne aktualizacje (dostępne tylko dla aktualizacji Microsoft).

- **Zadania instalacji tej aktualizacji**

  Ta zakładka wyświetla listę zadań, których obszar obejmuje instalację wybranej aktualizacji. Zakładka umożliwia także utworzenie nowego zadania zdalnej instalacji dla aktualizacji.

W celu przejrzenia statystyk dotyczących instalacji aktualizacji:

1. Zaznacz pole obok żądanej aktualizacji oprogramowania.

2. Kliknij przycisk **Statystyki stanów instalacji aktualizacji**.

Zostanie wyświetlony wykres stanów instalacji aktualizacji. Kliknięcie stanu powoduje otwarcie listę urządzeń, które mają wybrany stan.

Możesz przejrzeć informacje o dostępnych aktualizacjach oprogramowania dla programów firm trzecich, w tym programów firmy Microsoft, zainstalowanych na wybranym zarządzanym urządzeniu działającym pod kontrolą systemu Windows.

W celu przejrzenia listy aktualizacji dostępnych dla oprogramowania firm trzecich, zainstalowanych na wybranych zarządzanych urządzeniach:

1. W menu głównym przejdź do **Zarządzanie zasobami** → **Zasoby (urządzenia)**.

   Zostanie wyświetlona lista zarządzanych urządzeń.

2. Na liście zarządzanych urządzeń kliknij odnośnik z nazwą urządzenia, dla którego chcesz przejrzeć aktualizacje oprogramowania firm trzecich.

   Zostanie wyświetlone okno właściwości wybranego urządzenia.

3. W oknie właściwości wybranego urządzenia wybierz zakładkę **Zaawansowane**.

4. W lewej części okna wybierz sekcję **Dostępne aktualizacje**. Jeśli chcesz przejrzeć tylko zainstalowane aktualizacje, włącz opcję **Pokaż zainstalowane aktualizacje**.

Zostanie wyświetlona lista aktualizacji oprogramowania firm trzecich, dostępnych dla wybranego urządzenia.

Eksportowanie listy dostępnych aktualizacji oprogramowania do pliku

Możesz wyeksportować aktualizacje dla oprogramowania firm trzecich, w tym oprogramowania firmy Microsoft do plików CSV lub TXT. Możesz użyć tych plików, na przykład, do wysłania do swojego menedżera ds. bezpieczeństwa informacji lub przechowywać je w celach statystycznych.

W celu wyeksportowania do pliku tekstowego listy aktualizacji dostępnych dla oprogramowania firm trzecich, zainstalowanego na wszystkich zarządzanych urządzeniach:

1. W menu głównym przejdź do **Operacje** → **Zarządzanie poprawkami** → **Aktualizacje oprogramowania**.

   Zostaje wyświetlona lista dostępnych aktualizacji.

   Jeśli chcesz wyeksportować pełną listę aktualizacji oprogramowania, zostaną wyeksportowane tylko aktualizacje wyświetlone na bieżącej stronie.

   Jeśli chcesz wyeksportować tylko wybrane aktualizacje, zaznacz pola wyboru obok wymaganych aktualizacji na liście.

2. W zależności od preferowanego formatu eksportowania, kliknij przycisk **Eksportuj do pliku TXT** lub przycisk **Eksportuj do pliku CSV**. Jeśli którykolwiek z tych przycisków nie jest widoczny, kliknij przycisk wielokropka, a następnie wybierz żądaną opcję z listy rozwijanej.

Plik zawierający listę dostępnych aktualizacji oprogramowania firm trzecich, w tym oprogramowania firmy Microsoft, zostanie pobrany na Twoje bieżące urządzenie.

W celu wyeksportowania do pliku tekstowego listy aktualizacji dostępnych dla oprogramowania firm trzecich, zainstalowanego na wybranym zarządzanym urządzeniu:

1. Otwórz listę aktualizacji dostępnych dla oprogramowania firm trzecich na wybranym, zarządzanym urządzeniu.

   Zostaje wyświetlona lista dostępnych aktualizacji.

   Jeśli chcesz wyeksportować pełną listę aktualizacji oprogramowania, zostaną wyeksportowane tylko aktualizacje wyświetlone na bieżącej stronie.

   Jeśli chcesz wyeksportować tylko wybrane aktualizacje, zaznacz pola wyboru obok wymaganych aktualizacji na liście.

   Jeśli chcesz wyeksportować tylko zainstalowane aktualizacje, zaznacz pole **Pokaż zainstalowane aktualizacje**.

2. W zależności od preferowanego formatu eksportowania, kliknij przycisk **Eksportuj do pliku TXT** lub przycisk **Eksportuj do pliku CSV**. Jeśli którykolwiek z tych przycisków nie jest widoczny, kliknij przycisk wielokropka, a następnie wybierz żądaną opcję z listy rozwijanej.

Plik zawierający listę aktualizacji dostępnych dla oprogramowania firm trzecich, w tym oprogramowania firmy Microsoft, zainstalowanego na wybranym zarządzanym urządzeniu jest pobierany na Twoje bieżące urządzenie.

Zatwierdzanie oraz odrzucanie aktualizacji oprogramowania firm trzecich

Jeśli konfigurujesz zadanie *Zainstaluj wymagane aktualizacje i napraw luki*, możesz utworzyć regułę, która wymaga określonego stanu aktualizacji, które zostaną zainstalowane. Na przykład, reguła aktualizacji może zezwolić na instalację następujących elementów:

- Tylko zatwierdzonych aktualizacji
- Tylko zatwierdzonych i niezdefiniowanych aktualizacji
- Wszystkich aktualizacji niezależnie od stanu aktualizacji

Możesz zatwierdzić uaktualnienia, które muszą zostać zainstalowane, oraz odrzucić uaktualnienia, które nie muszą zostać zainstalowane.

Używanie stanu *Zatwierdzono* do zarządzania instalacją aktualizacji jest wystarczające dla małej liczby aktualizacji. Aby zainstalować kilka aktualizacji, użyj reguł, które możesz skonfigurować we właściwościach zadania *Zainstaluj wymagane aktualizacje i napraw luki*. Zalecane jest ustawienie stanu *Zatwierdzono* tylko dla tych aktualizacji, które nie spełniają kryteriów określonych w regułach. Kiedy ręcznie zatwierdzasz dużą liczbę aktualizacji, wydajność Serwera administracyjnego spada, co może prowadzić do jego przeciążenia.

W celu zatwierdzenia lub odrzucenia jednej lub kilku aktualizacji:

1. W menu głównym przejdź do **Zarządzanie oprogramowaniem** → **Zarządzanie poprawkami** → **Aktualizacje oprogramowania**.

   Zostanie wyświetlona lista dostępnych aktualizacji.

2. Wybierz uaktualnienia, które chcesz zatwierdzić lub odrzucić.

3. Kliknij przycisk **Zatwierdź,** aby zatwierdzić wybrane aktualizacje, lub przycisk **Odrzuć**, aby odrzucić wybrane aktualizacje. Jeśli którykolwiek z tych przycisków nie jest widoczny, kliknij przycisk wielokropka, a następnie wybierz żądaną opcję z listy rozwijanej.

   Domyślny stan aktualizacji to *Nie zdefiniowano*.

Wybrane aktualizacje posiadają stany, które zdefiniowałeś.

Istnieje również możliwość zmiany stanu zatwierdzenia we właściwościach określonej aktualizacji.

W celu zatwierdzenia lub odrzucenia aktualizacji w jej właściwościach:

1. W menu głównym przejdź do **Zarządzanie oprogramowaniem** → **Zarządzanie poprawkami** → **Aktualizacje oprogramowania**.

   Zostanie wyświetlona lista dostępnych aktualizacji.

2. Kliknij nazwę aktualizacji, którą chcesz zatwierdzić lub odrzucić.

   Zostanie otwarte okno właściwości aktualizacji.

3. W sekcji **Ogólne** wybierz stan dla aktualizacji z listy rozwijanej **Stan zatwierdzenia aktualizacji**. Możesz wybrać stan *Zatwierdzono*, *Odrzucono* lub *Nie zdefiniowano*.

4. Kliknij przycisk **Zapisz**, aby zapisać zmiany.

   Wybrana aktualizacja posiada stan, który zdefiniowałeś.

Jeśli ustawisz stan *Odrzucono* dla aktualizacji oprogramowania firm trzecich, te aktualizacje nie zostaną zainstalowane na urządzeniach, dla których planowane było ich zainstalowanie, ale jeszcze nie zostały zainstalowane. Uaktualnienia pozostaną na urządzeniach, na których zostały już zainstalowane. Jeśli to konieczne, możesz ręcznie usunąć je lokalnie.

Tworzenie zadania Zainstaluj wymagane aktualizacje i napraw luki

Zadanie *Zainstaluj wymagane aktualizacje i napraw luki* jest dostępne tylko dla licencji Zarządzanie lukami i poprawkami.

Zadanie *Zainstaluj wymagane aktualizacje i napraw luki* jest używane do aktualizacji i naprawy luk w oprogramowaniu firm trzecich zainstalowanym na zarządzanych urządzeniach. To zadanie umożliwia zainstalowanie kilku aktualizacji i naprawienie kilku luk zgodnie z regułami określonymi w ustawieniach zadania.

W celu zainstalowania aktualizacji lub wyeliminowania luk za pomocą zadania *Zainstaluj wymagane aktualizacje i napraw luki*, możesz wykonać jedną z następujących czynności:

- Uruchom kreator instalacji aktualizacji lub Kreator naprawiania luk.
- Utwórz zadanie *Zainstaluj wymagane aktualizacje i napraw luki*.
- Dodaj regułę instalacji aktualizacji do istniejącego pliku *Zainstaluj wymagane aktualizacje i napraw luki* zadanie.

Tworzenie zadania Zainstaluj wymagane aktualizacje i napraw luki:

1. W menu głównym przejdź do **Zadania**.

2. Kliknij **Dodaj**.

   Zostanie uruchomiony Kreator tworzenia nowego zadania. Przejdź przez kroki kreatora, korzystając z przycisku **Dalej**.

3. Z listy rozwijanej **Aplikacja** wybierz Kaspersky Security Center Linux.

4. Na liście **Typ zadania** wybierz typ zadania **Zainstaluj wymagane aktualizacje i napraw luki**.

   Jeśli zadanie nie jest wyświetlane, sprawdź, czy Twoje konto ma uprawnienia do **Odczytu**, **Zapisu** oraz **wykonaj** uprawnienia dla obszaru funkcjonalnego **Zarządzanie systemem**: **Zarządzanie lukami w zabezpieczeniach i poprawkami**. Bez tych praw dostępu nie można utworzyć ani skonfigurować zadania *Zainstaluj wymagane aktualizacje i napraw luki*.

5. W polu **Nazwa zadania** podaj nazwę nowego zadania.

   Nazwa zadania nie może zawierać więcej niż 100 znaków oraz nie może zawierać żadnych znaków specjalnych ("* <>?\:|).

6. Wybierz urządzenia, do których zadanie zostanie przypisane.

7. W kroku **Określ reguły instalacji aktualizacji** kreatora dodaj reguły instalacji aktualizacji.

   Te reguły są stosowane do instalacji aktualizacji na urządzeniach klienckich. Jeśli reguły nie zostały określone, zadanie nie zostanie wykonane. Informacje dotyczące działań wykonywanych na regułach znajdziesz w sekcji Reguły instalacji aktualizacji.

   Te reguły są stosowane do instalacji aktualizacji na urządzeniach klienckich. Jeśli nie określisz żadnych reguł, zadanie nie ma nic do wykonania.

8. Określ następujące ustawienia:

   - **Uruchom instalację podczas ponownego uruchamiania lub wyłączania urządzenia**

     Jeśli ta opcja jest włączona, aktualizacje są instalowane po ponownym uruchomieniu lub zamknięciu urządzenia. W innym przypadku aktualizacje są instalowane zgodnie z terminarzem.

     Użyj tej opcji, jeśli instalowanie aktualizacji może wpłynąć na działanie urządzenia.

     Domyślnie opcja ta jest wyłączona.

   - **Zainstaluj wymagane ogólne składniki systemu**

     Jeśli ta opcja jest włączona, przed zainstalowaniem aktualizacji aplikacja automatycznie instaluje wszystkie ogólne składniki systemu (wymagania wstępne), które są niezbędne do zainstalowania aktualizacji. Na przykład, tymi wymaganiami wstępnymi mogą być aktualizacje systemu operacyjnego.

     Jeśli ta opcja jest wyłączona, konieczne może być ręczne zainstalowanie wymagań wstępnych.

     Domyślnie opcja ta jest wyłączona.

   - **Zezwól na instalację nowych wersji aplikacji podczas aktualizacji**

     Jeśli ta opcja jest włączona, aktualizacje są dozwolone, gdy powodują zainstalowanie nowej wersji aplikacji.

     Jeśli ta opcja jest wyłączona, aplikacja nie zostanie zaktualizowana. W takiej sytuacji możesz ręcznie zainstalować nowe wersje aplikacji lub użyć w tym celu innego zadania. Na przykład, możesz użyć tej opcji, jeśli struktura Twojej firmy nie jest obsługiwana przez nową wersję aplikacji lub jeśli chcesz sprawdzić aktualizację w infrastrukturze testowej.

     Domyślnie opcja ta jest włączona.

     > Aktualizowanie aplikacji może spowodować problemy z działaniem powiązanych aplikacji zainstalowanych na urządzeniach klienckich.

   - **Pobierz aktualizacje na urządzenie, ale ich nie instaluj**

     Jeśli ta opcja jest włączona, aplikacja pobierze uaktualnienia na urządzenie, ale nie zainstaluje ich automatycznie. Możesz ręcznie zainstalować pobrane aktualizacje.

     Aktualizacje Microsoft są pobierane do folderu systemowego Windows. Aktualizacje aplikacji firm trzecich (aplikacje innych producentów niż Kaspersky i Microsoft) są pobierane do folderu określonego w polu **Pobierz uaktualnienia do**.

     Jeśli ta opcja jest wyłączona, aktualizacje są instalowane na urządzeniu automatycznie.

     Domyślnie opcja ta jest wyłączona.

     - **Pobierz uaktualnienia do**

       Ten folder jest używany do pobierania aktualizacji aplikacji innych firm (aplikacji innych producentów niż Kaspersky i Microsoft).

- **Włącz diagnostykę zaawansowaną**

  Jeśli ta funkcja jest włączona, Agent sieciowy zapisuje pliki śledzenia nawet wtedy, gdy zapisywanie plików śledzenia jest wyłączone dla Agenta sieciowego w Narzędziu zdalnej diagnostyki Kaspersky Security Center Linux. Śledzenie jest zapisywane do dwóch plików; całkowity rozmiar obu plików jest określany przez wartość **Maksymalny rozmiar plików zaawansowanej diagnostyki, w MB**. Jeśli oba pliki są pełne, Agent sieciowy ponownie uruchamia zapisywanie do tych plików. Pliki zawierające ślady są przechowywane w folderze %WINDIR%\Temp. Te pliki są dostępne w narzędziu do zdalnej diagnostyki – możesz je pobrać lub usunąć.

  Jeśli ta funkcja jest wyłączona, Agent sieciowy zapisuje śledzenie zgodnie z ustawieniami Narzędzia zdalnej diagnostyki Kaspersky Security Center Linux. Nie są zapisywane żadne dodatkowe pliki śledzenia.

  Jeśli tworzysz zadanie, nie musisz włączać zaawansowanej diagnostyki. Tej funkcji można użyć później, jeśli, na przykład, uruchomienie zadania nie powiedzie się na niektórych urządzeniach i chcesz uzyskać dodatkowe informacje podczas uruchamiania innego zadania.

  Domyślnie opcja ta jest wyłączona.

  - **Maksymalny rozmiar plików zaawansowanej diagnostyki, w MB**

    Domyślna wartość to 100 MB, a dostępne wartości mieszczą się między 1 MB a 2048 MB. Specjalista z pomocy technicznej Kaspersky może poprosić o zmianę domyślnej wartości, jeśli informacje w plikach zaawansowanej diagnostyki, które wysłałeś, nie są wystarczające do rozwiązania problemu.

Przejdź do następnego kroku kreatora.

9. Określ ustawienia ponownego uruchamiania systemu operacyjnego:

- **Nie uruchamiaj ponownie urządzenia**

  Urządzenia klienckie nie są automatycznie uruchamiane ponownie po działaniu. Aby zakończyć działanie, należy uruchomić urządzenie ponownie (na przykład ręcznie lub przy użyciu zadania zarządzania urządzeniem). Informacje o wymaganym ponownym uruchomieniu zostaną zapisane w wynikach zadania oraz w statusie urządzenia. Opcja ta jest odpowiednia dla zadań na serwerach i innych urządzeniach, na których działanie ciągłe jest krytyczne.

- **Uruchom urządzenie ponownie**

  Urządzenia klienckie są zawsze automatycznie uruchamiane ponownie, jeśli jest to wymagane do zakończenia działania. Opcja jest przydatna, gdy zadania są uruchamiane na urządzeniach, na których możliwe są regularne przerwy w działaniu (wyłączenie lub ponowne uruchomienie).

- **Pytaj użytkownika o akcję**

  Na urządzeniu klienckim wyświetlane jest przypomnienie o ręcznym ponownym uruchomieniu urządzenia. Dla tej opcji można zdefiniować pewne ustawienia zaawansowane: treść wyświetlanego komunikatu, częstotliwość wyświetlania wiadomości oraz przedział czasu, po upływie którego ponowne uruchomienie zostanie wymuszone (bez potwierdzenia ze strony użytkownika). Ta opcja jest najodpowiedniejsza dla stacji roboczych, na których użytkownicy muszą mieć możliwość wyboru odpowiedniej godziny ponownego uruchomienia.

  Domyślnie opcja ta jest zaznaczona.

- **Ponawiaj pytanie co (min)**

  Jeśli ta opcja jest włączona, aplikacja wyświetli pytanie o ponowne uruchomienie systemu operacyjnego z określoną częstotliwością.

  Domyślnie opcja ta jest włączona. Domyślnie przedział czasu wynosi 5 minut. Dostępne wartości znajdują się w zakresie od 1 do 1440 minut.

  Jeśli ta opcja jest wyłączona, monit zostaje wyświetlony tylko raz.

- **Uruchom ponownie po (min)**

  Po wyświetleniu monitu, aplikacja wymusza ponowne uruchomienie systemu operacyjnego po minięciu określonego przedziału czasu.

  Domyślnie opcja ta jest włączona. Domyślne opóźnienie wynosi 30 minut. Dostępne wartości znajdują się w zakresie od 1 do 1440 minut.

- **Czas oczekiwania przed wymuszeniem zamknięcia aplikacji dla zablokowanych sesji (min)**

  Wymuszone zamknięcie aplikacji ma miejsce, gdy urządzenie użytkownika jest zablokowane (automatycznie po określonym czasie nieaktywności lub ręcznie).

  Jeśli ta opcja jest włączona, wymuszone zamknięcie aplikacji na zablokowanym urządzeniu odbywa się po minięciu czasu określonego w polu wejściowym.

  Jeśli ta opcja jest wyłączona, aplikacje nie będą zamykane na zablokowanym urządzeniu.

  Domyślnie opcja ta jest wyłączona.

10. W kroku **Zakończ tworzenie zadania** kreatora, włącz opcję **Otwórz szczegóły zadania po jego utworzeniu**, aby zmodyfikować domyślne ustawienia zadania.

    Jeśli nie włączysz tej opcji, zadanie zostanie utworzone z domyślnymi ustawieniami. Możesz zmodyfikować domyślne ustawienia później.

11. Kliknij przycisk **Zakończ**.

    Kreator tworzenia nowego zadania tworzy zadanie. Jeśli włączyłeś opcję **Otwórz szczegóły zadania po jego utworzeniu**, automatycznie zostanie otwarte okno właściwości zadania. W tym oknie możesz określić ogólne ustawienia zadania oraz w razie potrzeby zmienić ustawienia określone podczas tworzenia zadania.

    > Możesz także otworzyć okno właściwości zadania, klikając nazwę utworzonego zadania na liście zadań.

    Zadanie zostanie utworzone, skonfigurowane i będzie wyświetlane na liście zadań.

12. Aby uruchomić zadanie, na liście zadań wybierz zadanie i kliknij przycisk **Uruchom**.

    Możesz także ustawić harmonogram uruchamiania zadania na karcie **Terminarz** w oknie właściwości zadania.

    Szczegółowy opis ustawień zaplanowanego uruchomienia znajduje się w ogólnych ustawieniach zadania.

Po zakończeniu zadania instalowane są wymagane aktualizacje i naprawiane są luki w zabezpieczeniach.

Jeżeli w sieci organizacji używany jest serwer WSUS (lokalny serwer WSUS) i ma on być używany razem z Serwerem administracyjnym, najpierw upewnij się, że Serwer administracyjny nie jest używany jako serwer WSUS, a następnie wykonaj następujące czynności:

a. Na swoich zarządzanych urządzeniach z systemem Windows, określ lokalny serwer WSUS dla usługi aktualizacji Windows Update. Możesz to zrobić ręcznie w rejestrze systemu Windows lub za pomocą zasad grupy systemu Windows.

b. Na lokalnym serwerze WSUS określ wymagane klasyfikacje aktualizacji oraz aplikacje, na których aktualizacje mają być dystrybuowane.

c. Zsynchronizuj serwer WSUS z serwerem nadrzędnym (może to być serwer Microsoft WSUS lub inny lokalny serwer nadrzędny WSUS).

Po uruchomieniu zadania *Zainstaluj wymagane aktualizacje i napraw luki w zabezpieczeniach* na urządzeniu, Agent sieciowy używa usługi Windows Update do zainstalowania aktualizacji systemu Windows. Usługa Windows Update pobiera adres zewnętrznego serwera WSUS z rejestru i pobiera aktualizacje bezpośrednio z tego serwera zewnętrznego.

Dodawanie reguł dla instalacji aktualizacji

Ta funkcja jest dostępna tylko w ramach licencji na Zarządzanie lukami i poprawkami.

Podczas instalowania aktualizacji oprogramowania lub naprawiania luk w oprogramowaniu przy użyciu zadania *Zainstaluj wymagane aktualizacje i napraw luki* należy określić zasady instalacji aktualizacji. Te reguły określają aktualizacje do zainstalowania oraz luki do wyeliminowania.

Dokładne ustawienia zależą od tego, czy dodajesz regułę dla wszystkich aktualizacji, aktualizacji Windows Update lub aktualizacji aplikacji firm trzecich (aplikacje stworzone przez producentów oprogramowania innych niż Kaspersky i Microsoft). Podczas dodawania reguły dla aktualizacji Windows Update lub aktualizacji aplikacji firm trzecich możesz wybrać określone aplikacje oraz wersje aplikacji, dla których chcesz zainstalować uaktualnienia. Podczas dodawania reguły dla wszystkich aktualizacji możesz wybrać określone uaktualnienia, które chcesz zainstalować, oraz luki, które chcesz naprawić poprzez zainstalowanie aktualizacji.

Regułę instalacji aktualizacji można dodać w następujący sposób:

- Dodając regułę podczas tworzenia nowego zadania *Zainstaluj wymagane aktualizacje i napraw luki*.
- Dodając regułę w zakładce **Ustawienia aplikacji** w oknie właściwości istniejącego zadania *Zainstaluj wymagane aktualizacje i napraw luki*.
- Za pomocą kreatora instalacji aktualizacji lub kreatora naprawiania luk.

Dodawanie reguł do wszystkich aktualizacji

W celu dodania nowej reguły dla wszystkich aktualizacji:

1. Kliknij przycisk **Dodaj**.

   Zostanie uruchomiony Kreator tworzenia reguły. Przejdź przez kroki kreatora, korzystając z przycisku **Dalej**.

2. W kroku **Wybierz typ reguły** kreatora wybierz opcję **Reguła dla wszystkich aktualizacji**.

3. W kroku **Kryteria ogólne** kreatora określ następujące ustawienia:

- **Zbiór aktualizacji do zainstalowania**

  Wybierz aktualizacje, które muszą być zainstalowane na urządzeniach klienckich:

  - **Zainstaluj tylko zatwierdzone aktualizacje**. Spowoduje to zainstalowanie tylko zatwierdzonych aktualizacji.

  - **Zainstaluj wszystkie aktualizacje (za wyjątkiem odrzuconych)**. Spowoduje to zainstalowanie aktualizacji posiadających stan *Zatwierdzono* lub *Nie zdefiniowano*.

  - **Zainstaluj wszystkie aktualizacje (wraz z odrzuconymi)**. Spowoduje to zainstalowanie wszystkich aktualizacji niezależnie od ich stanu zatwierdzenia. Tę opcję należy wybierać z rozwagą. Na przykład, użyj tej opcji, jeśli chcesz sprawdzić instalację niektórych odrzuconych aktualizacji w infrastrukturze testowej.

- **Napraw luki z priorytetem równym lub większym niż**

  Czasami aktualizacje oprogramowania mogą wpłynąć ujemnie na doświadczenie użytkownika z oprogramowaniem. W takich przypadkach możesz zdecydować się na zainstalowanie tylko tych aktualizacji, które są krytyczne dla działania oprogramowania, a na pominięcie innych aktualizacji.

  Jeśli ta opcja jest włączona, aktualizacje eliminują tylko te luki, dla których priorytet określony przez Kaspersky jest równy lub wyższy niż wartość wybrana na liście (**Średni**, **Wysoki** lub **Krytyczny**). Luki z priorytetem niższym niż wybrana wartość nie zostają wyeliminowane.

  Jeśli ta opcja jest wyłączona, aktualizacje eliminują wszystkie luki niezależnie od ich priorytetu.

  Domyślnie opcja ta jest wyłączona.

Przejdź do następnego kroku kreatora.

4. Wybieranie aktualizacji do zainstalowania:

- **Zainstaluj wszystkie pasujące aktualizacje**

  Zainstaluj aktualizacje oprogramowania, które spełniają kryteria określone w kroku **Kryteria ogólne**. Ta opcja jest wybrana domyślnie.

- **Zainstaluj tylko aktualizacje z listy**

  Instalowane są tylko te aktualizacje oprogramowania, które wybierzesz ręcznie z listy. Ta lista zawiera wszystkie dostępne aktualizacje oprogramowania.

  Na przykład, możesz wybrać określone aktualizacje w następujących przypadkach: aby sprawdzić ich instalację w środowisku testowym, aby zaktualizować tylko krytyczne aplikacje lub aby zaktualizować tylko określone aplikacje.

  - **Automatycznie zainstaluj wszystkie poprzednie aktualizacje aplikacji, jeśli są one niezbędne do zainstalowania wybranych aktualizacji**

    Pozostaw tę opcję włączoną, jeśli zgadzasz się na instalację tymczasowych wersji aplikacji, gdy jest to wymagane do zainstalowania wybranych aktualizacji.

    Jeśli ta opcja jest wyłączona, tylko wybrane wersje aplikacji są instalowane. Wybierz tę opcję, jeśli chcesz zaktualizować aplikacje w prosty sposób, bez próby zainstalowania kolejnych wersji. Jeśli zainstalowanie wybranych aktualizacji nie jest możliwe bez zainstalowania poprzednich wersji aplikacji, aktualizacja aplikacji nie powiedzie się.

Na przykład, posiadasz wersję 3 aplikacji zainstalowanej na urządzeniu i chcesz zaktualizować ją do wersji 5, ale wersja 5 tej aplikacji może być zainstalowana tylko na wersji 4. Jeśli ta opcja jest włączona, oprogramowanie w pierwszej kolejności instaluje wersję 4, a następnie instaluje wersję 5. Jeśli ta opcja jest wyłączona, oprogramowanie nie zdoła zaktualizować aplikacji.

Domyślnie opcja ta jest włączona.

Przejdź do następnego kroku kreatora.

5. Wybierz luki, które zostaną wyeliminowane poprzez zainstalowanie wybranych aktualizacji:

   - **Napraw wszystkie luki spełniające inne kryteria**

     Wyeliminuj wszystkie luki, które spełniają kryteria określone w kroku **Kryteria ogólne** kreatora. Ta opcja jest wybrana domyślnie.

   - **Napraw tylko luki z listy**

     Naprawione zostaną tylko te luki, które ręcznie wybierzesz z listy. Ta lista zawiera wszystkie wykryte luki.

     Na przykład, możesz wybrać określone luki w następujących przypadkach: aby sprawdzić ich eliminację w środowisku testowym, aby wyeliminować luki tylko w krytycznych aplikacjach lub aby wyeliminować luki tylko w określonych aplikacjach.

   Przejdź do następnego kroku kreatora.

6. Określ nazwę dodawanej reguły. W późniejszym czasie możesz zmienić tę nazwę w zakładce **Ustawienia aplikacji** właściwości utworzonego zadania.

Nowa reguła zostanie utworzona, skonfigurowana i wyświetlona w tabeli reguł Kreator tworzenia nowego zadania.

Dodawanie reguł dla aktualizacji z Windows Update

W celu dodania nowej reguły dla aktualizacji Windows Update:

1. Kliknij przycisk **Dodaj**.

   Zostanie uruchomiony Kreator tworzenia reguły. Przejdź przez kroki kreatora, korzystając z przycisku **Dalej**.

2. Wybierz opcję **Reguła dla aktualizacji systemu Windows**.

   Przejdź do następnego kroku kreatora.

3. W kroku **Kryteria ogólne** kreatora określ następujące ustawienia:

   - **Zbiór uaktualnień do zainstalowania**

     Wybierz aktualizacje, które muszą być zainstalowane na urządzeniach klienckich:

     - **Zainstaluj tylko zatwierdzone aktualizacje**. Spowoduje to zainstalowanie tylko zatwierdzonych aktualizacji.

     - **Zainstaluj wszystkie aktualizacje (za wyjątkiem odrzuconych)**. Spowoduje to zainstalowanie aktualizacji posiadających stan *Zatwierdzono* lub *Nie zdefiniowano*.

     - **Zainstaluj wszystkie aktualizacje (wraz z odrzuconymi)**. Spowoduje to zainstalowanie wszystkich aktualizacji niezależnie od ich stanu zatwierdzenia. Tę opcję należy wybierać z rozwagą. Na przykład, użyj tej opcji, jeśli chcesz sprawdzić instalację niektórych odrzuconych aktualizacji w infrastrukturze testowej.

   - **Napraw luki z priorytetem równym lub większym niż**

     Czasami aktualizacje oprogramowania mogą wpłynąć ujemnie na doświadczenie użytkownika z oprogramowaniem. W takich przypadkach możesz zdecydować się na zainstalowanie tylko tych aktualizacji, które są krytyczne dla działania oprogramowania, a na pominięcie innych aktualizacji.

     Jeśli ta opcja jest włączona, aktualizacje eliminują tylko te luki, dla których priorytet określony przez Kaspersky jest równy lub wyższy niż wartość wybrana na liście (**Średni**, **Wysoki** lub **Krytyczny**). Luki z priorytetem niższym niż wybrana wartość nie zostają wyeliminowane.

     Jeśli ta opcja jest wyłączona, aktualizacje eliminują wszystkie luki niezależnie od ich priorytetu.

     Domyślnie opcja ta jest wyłączona.

   - **Napraw luki z priorytetem MSRC równym lub większym niż**

     Czasami aktualizacje oprogramowania mogą wpłynąć ujemnie na doświadczenie użytkownika z oprogramowaniem. W takich przypadkach możesz zdecydować się na zainstalowanie tylko tych aktualizacji, które są krytyczne dla działania oprogramowania, a na pominięcie innych aktualizacji.

     Jeśli ta opcja jest włączona, aktualizacje eliminują tylko te luki, dla których priorytet określony przez centrum Microsoft Security Response Center (MSRC) jest równy lub wyższy niż wartość wybrana na liście (**Niski**, **Średni**, **Wysoki** lub **Krytyczny**). Luki z priorytetem niższym niż wybrana wartość nie zostają wyeliminowane.

     Jeśli ta opcja jest wyłączona, aktualizacje eliminują wszystkie luki niezależnie od ich priorytetu.

     Domyślnie opcja ta jest wyłączona.

4. W kroku **Aplikacje** wybierz aplikacje i wersje aplikacji, dla których chcesz zainstalować aktualizacje. Domyślnie, zaznaczone są wszystkie aplikacje.

5. W kroku **Kategorie aktualizacji** wybierz kategorie aktualizacji, które mają zostać zainstalowane. Te kategorie są takie same, jak w Microsoft Update Catalog. Domyślnie, zaznaczone są wszystkie kategorie.

6. W kroku **Nazwa** określ nazwę dla reguły, którą dodajesz. W późniejszym czasie możesz zmienić tę nazwę w sekcji **Ustawienia** okna właściwości utworzonego zadania.

Po zakończeniu działania kreatora tworzenia reguły, nowa reguła zostanie dodana i wyświetlona na liście reguł kreatora tworzenia nowego zadania lub we właściwościach zadania.

Dodanie reguł aktualizacji aplikacji firm trzecich

W celu dodania nowej reguły dla aktualizacji aplikacji firm trzecich:

1. Kliknij przycisk **Dodaj**.

   Zostanie uruchomiony Kreator tworzenia reguły. Przejdź przez kroki kreatora, korzystając z przycisku **Dalej**.

2. W kroku **Wybierz typ reguły** kreatora wybierz opcję **Reguła dla aktualizacji firm trzecich**.

3. W kroku **Kryteria ogólne** kreatora określ następujące ustawienia:

   - **Zbiór uaktualnień do zainstalowania**

     Wybierz aktualizacje, które muszą być zainstalowane na urządzeniach klienckich:

     - **Zainstaluj tylko zatwierdzone aktualizacje**. Spowoduje to zainstalowanie tylko zatwierdzonych aktualizacji.

     - **Zainstaluj wszystkie aktualizacje (za wyjątkiem odrzuconych)**. Spowoduje to zainstalowanie aktualizacji posiadających stan *Zatwierdzono* lub *Nie zdefiniowano*.

     - **Zainstaluj wszystkie aktualizacje (wraz z odrzuconymi)**. Spowoduje to zainstalowanie wszystkich aktualizacji niezależnie od ich stanu zatwierdzenia. Tę opcję należy wybierać z rozwagą. Na przykład, użyj tej opcji, jeśli chcesz sprawdzić instalację niektórych odrzuconych aktualizacji w infrastrukturze testowej.

   - **Napraw luki z priorytetem równym lub większym niż**

     Czasami aktualizacje oprogramowania mogą wpłynąć ujemnie na doświadczenie użytkownika z oprogramowaniem. W takich przypadkach możesz zdecydować się na zainstalowanie tylko tych aktualizacji, które są krytyczne dla działania oprogramowania, a na pominięcie innych aktualizacji.

     Jeśli ta opcja jest włączona, aktualizacje eliminują tylko te luki, dla których priorytet określony przez Kaspersky jest równy lub wyższy niż wartość wybrana na liście (**Średni**, **Wysoki** lub **Krytyczny**). Luki z priorytetem niższym niż wybrana wartość nie zostają wyeliminowane.

     Jeśli ta opcja jest wyłączona, aktualizacje eliminują wszystkie luki niezależnie od ich priorytetu.

     Domyślnie opcja ta jest wyłączona.

   Przejdź do następnego kroku kreatora.

4. Wybierz aplikacje i wersje aplikacji, dla których chcesz zainstalować aktualizacje.

   Domyślnie, zaznaczone są wszystkie aplikacje.

   Przejdź do następnego kroku kreatora.

5. Określ nazwę dodawanej reguły. W późniejszym czasie możesz zmienić tę nazwę w zakładce **Ustawienia aplikacji** właściwości utworzonego zadania.

Nowa reguła zostanie utworzona, skonfigurowana i wyświetlona w tabeli reguł Kreator tworzenia nowego zadania.

Ustawienia zadania Zainstaluj wymagane aktualizacje i napraw luki określone po utworzeniu zadania

Po utworzeniu zadania *Zainstaluj wymagane aktualizacje i napraw luki* możesz określić następujące ustawienia w zakładce **Ustawienia aplikacji** okna właściwości zadania:

- W sekcji **Instalacja testowa**:

  - **Nie skanuj**. Wybierz tę opcję, jeśli nie chcesz przeprowadzać testowej instalacji aktualizacji.

  - **Uruchom skanowanie na wybranych urządzeniach**. Wybierz tę opcję, jeśli chcesz przetestować instalację aktualizacji na wybranych urządzeniach. Kliknij przycisk **Dodaj**, a następnie wybierz urządzenia, na których chcesz przeprowadzić testową instalację aktualizacji.

  - **Uruchom skanowanie na urządzeniach w określonej grupie**. Wybierz tę opcję, jeśli chcesz przetestować instalację aktualizacji na grupach urządzeń. W polu **Określ grupę testową** określ grupę urządzeń, na których chcesz przeprowadzić instalację testową.

  - **Uruchom skanowanie na określonym procencie urządzeń**. Wybierz tę opcję, jeśli chcesz przetestować instalację aktualizacji na pewnym odsetku urządzeń. W polu **Procentowy udział urządzeń testowych z wszystkich urządzeń docelowych** określ procentową ilość urządzeń, na których chcesz przeprowadzić testową instalację aktualizacji.

  Po wybraniu dowolnej opcji innej niż **Nie skanuj**, w polu **Czas na podjęcie decyzji, jeśli instalacja ma być kontynuowana, w godzinach** określ liczbę godzin, jaka powinna upłynąć od testowej instalacji aktualizacji do momentu uruchomienia instalacji aktualizacji na wszystkich urządzeniach.

- W sekcji **Aktualizacje do zainstalowania** możesz przejrzeć listę aktualizacji instalowanych przez zadanie. Wyświetlane są tylko aktualizacje, które odpowiadają zastosowanych ustawieniom zadania.

Pełny opis ustawień zadania znajduje się w ogólnych ustawieniach zadania.

Automatyczne aktualizowanie aplikacji innych firm

Niektóre aplikacje innych firm mogą być aktualizowane automatycznie. Producent aplikacji definiuje, czy aplikacja obsługuje funkcję automatycznej aktualizacji. Jeśli aplikacja innej firmy, zainstalowana na zarządzanym urządzeniu, obsługuje automatyczną aktualizację, możesz określić ustawienie automatycznej aktualizacji we właściwościach aplikacji. Po zmianie ustawienia automatycznej aktualizacji Agenty sieciowe stosują nowe ustawienie na każdym zarządzanym urządzeniu, na którym jest zainstalowana aplikacja.

Ustawienie automatycznej aktualizacji jest niezależne od innych obiektów i ustawień funkcji Zarządzanie lukami i poprawkami. Na przykład, to ustawienie nie zależy od stanu zatwierdzenia aktualizacji ani od zadań instalacji aktualizacji, takich jak *Zainstaluj wymagane aktualizacje i napraw luki* oraz *Napraw luki*.

W celu skonfigurowania ustawienia automatycznej aktualizacji dla aplikacji innej firmy:

1. W menu głównym przejdź do **Zarządzanie oprogramowaniem** → **Aplikacje innych firm** → **Rejestr aplikacji**.

2. Kliknij nazwę aplikacji, dla której chcesz zmienić ustawienie automatycznej aktualizacji.

Aby uprościć wyszukiwanie, możesz przefiltrować listę według kolumny **Stan aktualizacji automatycznych** i **Zarządzaj aktualizacjami automatycznymi**.

Zostanie otwarte okno właściwości aplikacji.

3. W sekcji **Ogólne** wybierz wartość dla następującego ustawienia:

   Stan aktualizacji automatycznych.

   Wybierz jedną z następujących opcji:

   - **Nie zdefiniowano**

     Funkcja automatycznej aktualizacji jest wyłączona. Kaspersky Security Center Linux instaluje aktualizacje aplikacji innej firmy, korzystając z zadań: *Zainstaluj wymagane aktualizacje i napraw luki* i *Napraw luki*.

   - **Dozwolony**

     Jak tylko wydawca opublikuje aktualizację dla aplikacji, ta aktualizacja jest automatycznie instalowana na zarządzanych urządzeniach. Dodatkowe działania nie są wymagane.

   - **Zablokowano**

     Aktualizacje aplikacji nie są instalowane automatycznie. Kaspersky Security Center Linux instaluje aktualizacje aplikacji innej firmy, korzystając z zadań: *Zainstaluj wymagane aktualizacje i napraw luki* i *Napraw luki*.

4. Kliknij przycisk **Zapisz**, aby zapisać zmiany.

Ustawienie automatycznej aktualizacji jest stosowane do wybranej aplikacji.

Eliminowanie luk w oprogramowaniu innych firm

Ta sekcja opisuje funkcje Kaspersky Security Center Linux, które dotyczą eliminowania luk w oprogramowaniu zainstalowanym na zarządzanych urządzeniach.

Informacje o wyszukiwaniu i eliminowaniu luk w oprogramowaniu

Kaspersky Security Center Linux wykrywa i naprawia luki w oprogramowaniu na zarządzanych urządzeniach działających pod kontrolą systemów operacyjnych Microsoft Windows. Luki są wykrywane w systemie operacyjnym i w oprogramowaniu innych firm, w tym w oprogramowaniu firmy Microsoft.

Aktualizuje funkcje (obejmuje aktualizacje sygnatur wirusów oraz aktualizacje bazy kodu), przy czym funkcja KSN może nie być dostępna w oprogramowaniu na terytorium Stanów Zjednoczonych.

Wyszukiwanie luk w oprogramowaniu

Aby znaleźć luki w oprogramowaniu, Kaspersky Security Center Linux wykorzystuje znaki charakterystyczne z bazy danych znanych zagrożeń. Ta baza danych została utworzona i jest aktualizowana przez specjalistów z firmy Kaspersky. Zawiera informacje o lukach, takie jak opis luki, data wykrycia luki, priorytet luki. Szczegóły dotyczące luk w oprogramowaniu można znaleźć na stronie internetowej Kaspersky.

Kaspersky Security Center Linux wykorzystuje zadanie *Wyszukiwanie luk i wymaganych aktualizacji* do wykrywania luk w oprogramowaniu.

Naprawianie luk w oprogramowaniu

Aby naprawić luki w oprogramowaniu, Kaspersky Security Center Linux używa aktualizacji oprogramowania opublikowanych przez producentów oprogramowania. Metadane aktualizacji oprogramowania są pobierane do repozytorium Serwera administracyjnego w wyniku uruchomienia zadania *Pobierz aktualizacje do repozytorium Serwera administracyjnego*. To zadanie jest przeznaczone do pobrania metadanych aktualizacji oprogramowania Kaspersky i innych firm. To zadanie jest tworzone automatycznie przez Kreator wstępnej konfiguracji Kaspersky Security Center Linux. Możesz ręcznie utworzyć zadanie *Pobierz aktualizacje do repozytorium Serwera administracyjnego*.

Aktualizacje oprogramowania eliminujące luki mogą być w postaci pełnych pakietów dystrybucyjnych lub poprawek. Aktualizacje oprogramowania, które eliminują luki w oprogramowaniu, nazywane są *poprawkami*. *Zalecane poprawki* to takie poprawki, które są zalecane do zainstalowania przez specjalistów z Kaspersky. *Poprawki użytkownika* to takie poprawki, które są ręcznie określane do zainstalowania przez użytkowników. Aby zainstalować poprawkę użytkownika, należy utworzyć pakiet instalacyjny zawierający tę poprawkę.

Jeśli posiadasz licencję dla Kaspersky Security Center Linux z funkcją Zarządzanie lukami i poprawkami, aby usunąć luki w oprogramowaniu, możesz użyć zadania *Zainstaluj wymagane aktualizacje i napraw luki*. To zadanie automatycznie eliminuje kilka luk poprzez zainstalowanie zalecanych poprawek. Dla tego zadania można ręcznie skonfigurować pewne reguły do naprawy kilku luk.

Jeśli nie posiadasz licencji dla Kaspersky Security Center Linux z funkcją Zarządzanie lukami i poprawkami możesz użyć zadania *Napraw luki*. Korzystając z tego zadania, możesz wyeliminować luki poprzez zainstalowanie zalecanych poprawek dla oprogramowania firmy Microsoft oraz poprawek użytkownika dla innych programów innych firm.

Ze względów bezpieczeństwa wszelkie aktualizacje oprogramowania innych firm, które instalujesz za pomocą funkcji Zarządzanie lukami i poprawkami, są automatycznie skanowane w poszukiwaniu szkodliwego oprogramowania przez technologie firmy Kaspersky. Technologie te są używane do automatycznego sprawdzania plików i obejmują skanowanie antywirusowe, analizę statyczną, analizę dynamiczną, analizę zachowania w środowisku sandbox i uczenie maszynowe.

Eksperci firmy Kaspersky nie przeprowadzają ręcznej analizy aktualizacji oprogramowania innych firm, które są instalowane przez funkcję Zarządzanie lukami i poprawkami. Ponadto eksperci z firmy Kaspersky nie wyszukują luk (znanych lub nieznanych) ani nieudokumentowanych funkcji w takich aktualizacjach, a także nie przeprowadzają innych rodzajów analizy aktualizacji innych, niż określone w powyższym akapicie.

Interakcja użytkownika może być wymagana podczas aktualizacji aplikacji innej firmy lub naprawy luki w aplikacji innej firmy na zarządzanym urządzeniu. Na przykład, użytkownik może zostać poproszony o zamknięcie aplikacji innej firmy, jeśli jest ona aktualnie otwarta.

Aby naprawić niektóre luki w oprogramowaniu, należy zaakceptować Umowę licencyjną użytkownika końcowego (EULA) dla instalowanego oprogramowania, jeśli wymagane jest zaakceptowanie Umowy licencyjnej. Jeśli odrzucisz Umowę licencyjną użytkownika końcowego, luka w oprogramowaniu nie zostanie wyeliminowana.

Scenariusz: Wyszukiwanie i usuwanie luk w oprogramowaniu firm trzecich

Ta sekcja zawiera scenariusz wyszukiwania i naprawiania luk na zarządzanych urządzeniach działających pod kontrolą systemu Windows. Możesz znaleźć i naprawić luki w oprogramowaniu w systemie operacyjnym oraz w oprogramowaniu firm trzecich, w tym w oprogramowaniu firmy Microsoft.

Wymagania wstępne

- Kaspersky Security Center Linux zostanie wdrożony w Twojej organizacji.
- W Twojej organizacji znajdują się zarządzane urządzenia działające pod kontrolą systemu Windows.
- Połączenie internetowe w przypadku Serwera administracyjnego jest wymagane, aby można było wykonywać następujące zadania:
  - Sporządzanie listy zalecanych poprawek dla luk w oprogramowaniu firmy Microsoft. Lista jest tworzona i regularnie aktualizowana przez specjalistów z Kaspersky.
  - Naprawianie luk w oprogramowaniu firm trzecich innym niż oprogramowanie firmy Microsoft.

Etapy

Wyszukiwanie i naprawianie luk w oprogramowaniu odbywa się w następujących krokach:

1. **Skanowanie luk w oprogramowaniu zainstalowanym na zarządzanych urządzeniach**

   Aby odszukać luki w oprogramowaniu zainstalowanym na zarządzanych urządzeniach, uruchom zadanie *Wyszukiwanie luk i wymaganych aktualizacji*. Jeśli to zadanie zostanie zakończone, Kaspersky Security Center Linux pobierze listę wykrytych luk i żądanych aktualizacji dla oprogramowania firm trzecich zainstalowanego na urządzeniach, które określiłeś we właściwościach zadania.

   Zadanie *Wyszukiwanie luk i wymaganych aktualizacji* jest tworzone automatycznie przez Kreator wstępnej konfiguracji Kaspersky Security Center Linux. Jeśli nie uruchamiałeś kreatora, uruchom go teraz lub utwórz zadanie ręcznie.

   > Zadanie *Wyszukiwanie luk i wymaganych aktualizacji* możesz utworzyć tylko dla urządzeń z systemem Windows. Nie można utworzyć tego zadania dla urządzeń działających na innych systemach operacyjnych.

2. **Przeglądanie listy wykrytych luk w oprogramowaniu**

   Przejrzyj listę **Luki w oprogramowaniu** i zdecyduj, które luki mają zostać naprawione. Aby przejrzeć szczegółowe informacje o każdej luce, kliknij nazwę luki na liście. Dla każdej luki na liście możesz także przejrzeć statystyki dotyczące luki na zarządzanych urządzeniach.

3 Konfigurowanie naprawy luk

Jeśli luki w oprogramowaniu zostaną wykryte, możesz naprawić je na zarządzanych urządzeniach, korzystając z zadania *Zainstaluj wymagane aktualizacje i napraw luki* lub zadania *Napraw luki*.

Zadanie *Zainstaluj wymagane aktualizacje i napraw luki* jest używane do aktualizacji i naprawy luk w oprogramowaniu firm trzecich, w tym w oprogramowaniu firmy Microsoft, zainstalowanym na zarządzanych urządzeniach. To zadanie umożliwia zainstalowanie kilku aktualizacji i naprawę kilku luk zgodnie z pewnymi regułami. Pamiętaj, że to zadanie może zostać utworzone tylko wtedy, gdy masz licencję dla funkcji Zarządzanie lukami i poprawkami. Aby naprawić luki w oprogramowaniu, zadanie *Zainstaluj wymagane aktualizacje i napraw luki* używa zalecanych aktualizacji oprogramowania.

Zadanie *Napraw luki* nie wymaga opcji licencjonowania dla funkcji Zarządzanie lukami i poprawkami. Aby użyć tego zadania, należy ręcznie określić poprawki użytkownika dla luk w programach innych firm, wymienionych w ustawieniach zadania. Zadanie *Napraw luki* używa zalecanych poprawek dla oprogramowania firmy Microsoft oraz poprawek użytkownika dla programów innych firm.

> Możesz utworzyć zadania *Zainstaluj wymagane aktualizacje i napraw luki* oraz *Napraw luki* tylko dla urządzeń z systemem Windows. Nie można utworzyć tych zadań dla urządzeń działających na innych systemach operacyjnych.

Możesz uruchomić Kreator naprawiania luk, który tworzy jedno z tych zadań automatycznie, lub możesz utworzyć jedno z tych zadań ręcznie.

Jeśli utworzyłeś i skonfigurowałeś zadanie *Zainstaluj wymagane aktualizacje i napraw luki*, luki zostają naprawione na zarządzanych urządzeniach automatycznie. Jeśli utworzone zadanie zostaje uruchomione, zestawia listę dostępnych aktualizacji oprogramowania z regułami określonymi w ustawieniach zadania. Wszystkie aktualizacje oprogramowania, które spełniają kryteria w określonych regułach, zostaną pobrane do repozytorium Serwera administracyjnego i zostaną zainstalowane w celu naprawy luk w oprogramowaniu.

Jeśli utworzono zadanie *Napraw luki*, naprawione zostaną tylko luki w oprogramowaniu firmy Microsoft.

4 Konfigurowanie terminarza zadań

Zaplanuj okresowe automatyczne uruchamianie zadania *Wyszukiwanie luk i wymaganych aktualizacji*, aby lista luk była aktualna. Zalecana częstotliwość to raz na tydzień.

Jeśli utworzyłeś zadanie *Zainstaluj wymagane aktualizacje i napraw luki*, możesz skonfigurować terminarz tak, aby zadanie było uruchamiane z tą samą częstotliwością co zadanie *Wyszukiwanie luk i wymaganych aktualizacji* lub rzadziej. Podczas ustawiania terminarza zadania *Napraw luki* należy pamiętać, żeby wybrać poprawki dla oprogramowania Microsoft lub określić poprawki użytkownika dla oprogramowania innych firm za każdym razem przed rozpoczęciem zadania.

Jeśli konfigurujesz terminarz uruchamiania zadania, upewnij się, że utworzone zadanie napraw luk zostanie uruchomione po zakończeniu zadania *Wyszukiwanie luk i wymaganych aktualizacji*.

5 Ignorowanie luk w oprogramowaniu (opcjonalne)

Możesz zignorować niektóre luki w oprogramowaniu na wszystkich zarządzanych urządzeniach lub tylko na wybranych zarządzanych urządzeniach.

6 Uruchamianie zadania naprawy luk

Uruchom zadanie *Zainstaluj wymagane aktualizacje i napraw luki* lub zadanie *Napraw luki*. Gdy zadanie zostało zakończone, upewnij się, że na liście zadań posiada stan *Pomyślnie zakończone*.

7 Tworzenie raportu dotyczącego wyników naprawy luk w oprogramowaniu (opcja)

Aby wyświetlić szczegółowe statystyki dotyczące naprawy luk, wygeneruj Raport o lukach. Ten raport wyświetla informacje o lukach w oprogramowaniu, które nie zostały naprawione. Umożliwia identyfikację i usuwanie luk w oprogramowaniu innych firm, w tym w oprogramowaniu firmy Microsoft, używanym w Twojej organizacji.

8 Sprawdzanie konfiguracji wyszukiwania i naprawy luk w programach innych firm

Upewnij się, że wykonano następujące czynności:

- Uzyskałeś i przejrzałeś listę luk w oprogramowaniu na zarządzanych urządzeniach.
- W razie potrzeby zignorowano pewne luki w oprogramowaniu.
- Skonfigurowałeś zadanie naprawy luk.
- Skonfigurowano terminarz zadań wyszukiwania i naprawy luk w oprogramowaniu, dzięki czemu są uruchamianie po kolei.
- Sprawdzono, czy zadanie naprawy luk w oprogramowaniu zostało uruchomione.

Eliminowanie luk w oprogramowaniu innych firm

Aby znaleźć luki w oprogramowaniu innych firm, możesz utworzyć i uruchomić zadanie *Wyszukiwanie luk i wymaganych aktualizacji*, aby otrzymać listę luk w zabezpieczeniach oprogramowania. Po uzyskaniu listy luk zabezpieczeń w oprogramowaniu możliwe jest wyeliminowanie luk na zarządzanych urządzeniach działających pod kontrolą systemu Windows.

Luki w oprogramowaniu w systemie operacyjnym i oprogramowaniu innych firm, w tym w oprogramowaniu firmy Microsoft, można naprawić, tworząc i uruchamiając zadanie Napraw luki lub zadanie Zainstaluj wymagane aktualizacje i napraw luki.

> Interakcja użytkownika może być wymagana podczas aktualizacji aplikacji innej firmy lub naprawy luki w aplikacji innej firmy na zarządzanym urządzeniu. Na przykład, użytkownik może zostać poproszony o zamknięcie aplikacji innej firmy, jeśli jest ona aktualnie otwarta.

Opcjonalnie możesz utworzyć zadanie naprawiania luk w oprogramowaniu w następujący sposób:

- Otwierając listę luk i określając, które luki należy naprawić.

  W rezultacie powstaje nowe zadanie naprawy luk w oprogramowaniu. Istnieje możliwość dodania wybranych luk do istniejącego zadania.

- Uruchamiając Kreator naprawiania luk.

  > Funkcje kreatora naprawiania luk są dostępne tylko dla licencji Zarządzanie lukami i poprawkami.

  Kreator upraszcza tworzenie i konfigurację zadania naprawy luki w zabezpieczeniach i pozwala wyeliminować tworzenie zbędnych zadań.

Naprawianie luk w oprogramowaniu przy użyciu listy luk w zabezpieczeniach

Naprawianie luk w zabezpieczeniach oprogramowania przy użyciu listy luk:

1. Otwórz listę luk, wykonując jedną z następujących czynności:

   - W menu głównym przejdź do **Zarządzanie oprogramowaniem** → **Zarządzanie poprawkami** → **Luki w oprogramowaniu**.

   - W menu głównym przejdź do **Zarządzanie zasobami** → **Zasoby (urządzenia)** → <nazwa urządzenia> → **Zaawansowane** → **Luki w oprogramowaniu**.

   - W menu głównym przejdź do **Zarządzanie oprogramowaniem** → **Aplikacje innych firm** → **Rejestr aplikacji** → <application name> → **Luki**.

   Zostanie wyświetlona tabela z listą luk w oprogramowaniu innych firm, zainstalowanym na zarządzanych urządzeniach.

2. Na liście luk zaznacz pola wyboru obok luk, które chcesz naprawić, a następnie kliknij przycisk **Napraw lukę**.

   Jeśli brakuje zalecanej aktualizacji oprogramowania do naprawy jednej z wybranych luk, zostanie wyświetlony odpowiedni komunikat.

   Aby naprawić niektóre luki w oprogramowaniu, należy zaakceptować Umowę licencyjną użytkownika końcowego (EULA), dla instalowanego oprogramowania jeśli wymagane jest zaakceptowanie Umowy licencyjnej. Jeśli odrzucisz Umowę licencyjną użytkownika końcowego, luka w oprogramowaniu nie zostanie wyeliminowana.

3. Wybierz jedną z następujących opcji:

   - **Nowe zadanie**

     Zostanie uruchomiony Kreator tworzenia nowego zadania. Jeśli masz licencję Zarządzania lukami i poprawkami, domyślnie wybrany jest typ zadania Zainstaluj wymagane aktualizacje i napraw luki. Jeśli nie masz licencji, domyślnie wybrany jest typ zadania Napraw luki. Aby zakończyć tworzenie zadania, postępuj zgodnie z instrukcjami kreatora.

   - **Napraw lukę (dodaj regułę do określonego zadania)**

     Wybierz zadanie, do którego chcesz dodać wybrane luki. Jeśli masz licencję Zarządzania lukami i poprawkami, wybierz zadanie Zainstaluj wymagane aktualizacje i napraw luki. Nowa reguła eliminacji wybranych luk zostanie automatycznie dodania do wybranego zadania. Jeśli nie masz licencji, wybierz zadanie Napraw luki. Wybrane luki zostają dodane do właściwości zadania.

     Zostanie otwarte okno właściwości zadania. Kliknij przycisk **Zapisz**, aby zapisać zmiany.

   Jeśli wybrałeś utworzenie zadania, zadanie zostanie utworzone i wyświetlone na liście zadań, w sekcji **Zadania**. Jeśli wybrałeś dodanie luk do istniejącego zadania, luki zostaną zapisane we właściwościach zadania.

Aby wyeliminować luki w oprogramowaniu firm trzecich, uruchom zadanie Zainstaluj wymagane aktualizacje i napraw luki lub zadanie Napraw luki. Jeśli utworzyłeś zadanie Napraw luki w zabezpieczeniach, powinieneś ręcznie określić aktualizacje oprogramowania wymienione w ustawieniach zadania.

Naprawianie luk w oprogramowaniu przy użyciu kreatora naprawiania luk

Funkcje kreatora naprawiania luk są dostępne tylko dla licencji Zarządzanie lukami i poprawkami.

Aby naprawić luki w oprogramowaniu przy użyciu kreatora naprawiania luk:

1. W menu głównym przejdź do **Zarządzanie oprogramowaniem** → **Zarządzanie poprawkami** → **Luki w oprogramowaniu**.

   Zostanie wyświetlona tabela z listą luk w oprogramowaniu innych firm, zainstalowanym na zarządzanych urządzeniach.

2. Zaznacz pole obok luki, który chcesz wyeliminować.

3. Kliknij przycisk **Uruchom kreatora naprawiania luk**.

   Przycisk jest wyłączony, jeśli wybierzesz więcej niż jedną lukę.

   Zostanie uruchomiony Kreator naprawiania luk. Zostanie wyświetlona lista istniejących zadań. Ta lista może zawierać następujące typy zadań:

   - Zainstaluj wymagane aktualizacje i napraw luki
   - Napraw luki

   Nie możesz modyfikować zadania Napraw luki w celu zainstalowania nowych aktualizacji. Aby zainstalować nowe aktualizacje, możesz użyć tylko zadania Zainstaluj wymagane aktualizacje i napraw luki.

4. Jeśli chcesz, aby kreator wyświetlał tylko te zadania, które usuwają wybraną lukę, włącz opcję **Pokaż tylko zadania naprawiające tę lukę**.

5. Wykonaj jedną z poniższych czynności:

   - Aby rozpocząć zadanie, zaznacz pole wyboru obok nazwy zadania, a następnie kliknij przycisk **Uruchom**.

     Dalsze działania nie są wymagane. Możesz zamknąć kreator. Zadanie zakończy się w tle.

   - Dodaj regułę instalacji aktualizacji do istniejącego zadania Zainstaluj wymagane aktualizacje i napraw luki:

     a. Zaznacz pole obok nazwy zadania i kliknij przycisk **Dodaj regułę**.

     Jeśli wybierzesz więcej niż jedno zadanie, przycisk **Dodaj regułę** jest nieaktywny.

     Nie można dodać reguły do zadania Napraw luki. Jeśli wybierzesz zadanie Napraw luki wyświetli się następujące powiadomienie: „Aby zainstalować aktualizacje, użyj zadania „Zainstaluj wymagane aktualizacje i napraw luki"".

     b. Na wyświetlonej stronie skonfiguruj nową regułę:

     - **Reguła dla naprawiania luk tego priorytetu**

Czasami aktualizacje oprogramowania mogą wpłynąć ujemnie na doświadczenie użytkownika z oprogramowaniem. W takich przypadkach możesz zdecydować się na zainstalowanie tylko tych aktualizacji, które są krytyczne dla działania oprogramowania, a na pominięcie innych aktualizacji.

Jeśli ta opcja jest włączona, aktualizacje eliminują tylko te luki, dla których priorytet określony przez Kaspersky jest równy lub wyższy niż priorytet wybranej aktualizacji (**Średni**, **Wysoki** lub **Krytyczny**). Luki z priorytetem niższym niż wybrana wartość nie zostają wyeliminowane.

Jeśli ta opcja jest wyłączona, aktualizacje eliminują wszystkie luki niezależnie od ich priorytetu.

Domyślnie opcja ta jest wyłączona.

- **Reguła naprawiania luk za pomocą aktualizacji tego samego typu, co aktualizacja zdefiniowana jako zalecana dla wybranej luki**

  Ta reguła jest wyświetlana tylko w przypadku luk w oprogramowaniu Microsoft.

- **Reguła naprawiania luk w aplikacjach według wybranego dostawcy**

  Ta reguła jest wyświetlana tylko w przypadku luk w oprogramowaniu innych firm.

- **Reguła naprawiania luk we wszystkich wersjach wybranej aplikacji**

  Ta reguła jest wyświetlana tylko w przypadku luk w oprogramowaniu innych firm.

- **Reguła naprawiania wybranej luki**

- **Akceptuj aktualizacje, które naprawiają tę lukę**

  Instalacja wybranej aktualizacji zostanie zatwierdzona. Włącz tę opcję, jeśli niektóre stosowane reguły instalacji aktualizacji zezwalają tylko na instalację zaakceptowanych aktualizacji.

  Domyślnie opcja ta jest wyłączona.

c. Kliknij przycisk **Dodaj**.

Zostanie otwarte okno właściwości zadania. Nowa reguła została już dodana do właściwości zadania. Możesz przejrzeć lub zmodyfikować regułę lub ustawienia innego zadania. Kliknij przycisk **Zapisz**, aby zapisać zmiany.

- W celu utworzenia zadania:

a. Kliknij przycisk **Nowe zadanie**.

b. Na wyświetlonej stronie skonfiguruj nową regułę:

- **Reguła dla naprawiania luk tego priorytetu**

  Czasami aktualizacje oprogramowania mogą wpłynąć ujemnie na doświadczenie użytkownika z oprogramowaniem. W takich przypadkach możesz zdecydować się na zainstalowanie tylko tych aktualizacji, które są krytyczne dla działania oprogramowania, a na pominięcie innych aktualizacji.

  Jeśli ta opcja jest włączona, aktualizacje eliminują tylko te luki, dla których priorytet określony przez Kaspersky jest równy lub wyższy niż priorytet wybranej aktualizacji (**Średni**, **Wysoki** lub **Krytyczny**). Luki z priorytetem niższym niż wybrana wartość nie zostają wyeliminowane.

  Jeśli ta opcja jest wyłączona, aktualizacje eliminują wszystkie luki niezależnie od ich priorytetu.

  Domyślnie opcja ta jest wyłączona.

- **Reguła naprawiania luk za pomocą aktualizacji tego samego typu, co aktualizacja zdefiniowana jako zalecana dla wybranej luki**

  Ta reguła jest wyświetlana tylko w przypadku luk w oprogramowaniu Microsoft.

- **Reguła naprawiania luk w aplikacjach według wybranego dostawcy**

  Ta reguła jest wyświetlana tylko w przypadku luk w oprogramowaniu innych firm.

- **Reguła naprawiania luk we wszystkich wersjach wybranej aplikacji**

  Ta reguła jest wyświetlana tylko w przypadku luk w oprogramowaniu innych firm.

- **Reguła naprawiania wybranej luki**

- **Akceptuj aktualizacje, które naprawiają tę lukę**

  Instalacja wybranej aktualizacji zostanie zatwierdzona. Włącz tę opcję, jeśli niektóre stosowane reguły instalacji aktualizacji zezwalają tylko na instalację zaakceptowanych aktualizacji.

  Domyślnie opcja ta jest wyłączona.

c. Kliknij przycisk **Dodaj**.

d. Kontynuuj tworzenie zadania w Kreator tworzenia nowego zadania.

Nowa reguła dodana w Kreatorze naprawy luk zostanie wyświetlona w kroku **Określ reguły instalacji aktualizacji** kreatora nowego zadania. Po zakończeniu pracy kreatora, do listy zadań zostanie dodane zadanie Zainstaluj wymagane aktualizacje i napraw luki.

Tworzenie zadania Napraw luki

Zadanie *Napraw luki* pozwala naprawić luki w oprogramowaniu na zarządzanych urządzeniach. Możesz naprawić luki w oprogramowaniu firm trzecich, w tym w oprogramowaniu firmy Microsoft.

Zadanie *Napraw luki* możesz utworzyć tylko dla urządzeń z systemem Windows. Nie można utworzyć tego zadania dla urządzeń działających na innych systemach operacyjnych.

Możesz tworzyć nowe zadania *Napraw luki* tylko wtedy, gdy posiadasz Licencję na zarządzanie lukami i poprawkami.

Aby naprawić nowe luki, możesz dodać je do istniejącego zadania *Napraw luki*. Zalecamy użycie zadania *Zainstaluj wymagane aktualizacje i napraw luki* zamiast zadania *Napraw luki*. Zadanie *Zainstaluj wymagane aktualizacje i napraw luki* umożliwia automatyczne instalowanie wielu aktualizacji i naprawianie wielu luk w zabezpieczeniach, zgodnie z określonymi przez Ciebie regułami.

Interakcja użytkownika może być wymagana podczas aktualizacji aplikacji innej firmy lub naprawy luki w aplikacji innej firmy na zarządzanym urządzeniu. Na przykład, użytkownik może zostać poproszony o zamknięcie aplikacji innej firmy, jeśli jest ona aktualnie otwarta.

W celu utworzenia zadania Napraw luki:

1. W menu głównym przejdź do **Zadania**.

   Alternatywnie możesz utworzyć to zadanie w oknie właściwości urządzenia, na zakładce **Zadania**.

2. Kliknij **Dodaj**.

   Zostanie uruchomiony Kreator tworzenia nowego zadania. Przejdź przez kroki kreatora, korzystając z przycisku **Dalej**.

3. Z listy rozwijanej **Aplikacja** wybierz Kaspersky Security Center.

4. Z listy **Typ zadania** wybierz typ zadania **Napraw luki**.

5. W polu **Nazwa zadania** podaj nazwę nowego zadania.

   Nazwa zadania nie może zawierać więcej niż 100 znaków oraz nie może zawierać żadnych znaków specjalnych ("* <>?\:|).

6. Wybierz urządzenia, do których zadanie zostanie przypisane.

   Przejdź do następnego kroku kreatora.

7. Kliknij przycisk **Dodaj**.

   Zostanie otwarta lista luk.

8. Na liście luk zaznacz pola wyboru obok luk, które chcesz naprawić, a następnie kliknij przycisk **OK**.

   Luki w oprogramowaniu firmy Microsoft zwykle zawierają zalecane poprawki. Nie są wymagane żadne dodatkowe czynności.

   W przypadku luk w zabezpieczeniach oprogramowania innych producentów należy najpierw określić poprawkę użytkownika dla każdej luki, którą chcesz naprawić. Następnie będzie można dodać te luki do zadania *Napraw luki*.

   Przejdź do następnego kroku kreatora.

9. Określ ustawienia ponownego uruchamiania systemu operacyjnego:

   - **Nie uruchamiaj ponownie urządzenia**

     Urządzenia klienckie nie są automatycznie uruchamiane ponownie po działaniu. Aby zakończyć działanie, należy uruchomić urządzenie ponownie (na przykład ręcznie lub przy użyciu zadania zarządzania urządzeniem). Informacje o wymaganym ponownym uruchomieniu zostaną zapisane w wynikach zadania oraz w statusie urządzenia. Opcja ta jest odpowiednia dla zadań na serwerach i innych urządzeniach, na których działanie ciągłe jest krytyczne.

   - **Uruchom urządzenie ponownie**

     Urządzenia klienckie są zawsze automatycznie uruchamiane ponownie, jeśli jest to wymagane do zakończenia działania. Opcja jest przydatna, gdy zadania są uruchamiane na urządzeniach, na których możliwe są regularne przerwy w działaniu (wyłączenie lub ponowne uruchomienie).

   - **Pytaj użytkownika o akcję**

     Na urządzeniu klienckim wyświetlane jest przypomnienie o ręcznym ponownym uruchomieniu urządzenia. Dla tej opcji można zdefiniować pewne ustawienia zaawansowane: treść wyświetlanego komunikatu, częstotliwość wyświetlania wiadomości oraz przedział czasu, po upływie którego ponowne uruchomienie zostanie wymuszone (bez potwierdzenia ze strony użytkownika). Ta opcja jest najodpowiedniejsza dla stacji roboczych, na których użytkownicy muszą mieć możliwość wyboru odpowiedniej godziny ponownego uruchomienia.

     Domyślnie opcja ta jest zaznaczona.

- **Ponawiaj pytanie co (min)**

  Jeśli ta opcja jest włączona, aplikacja wyświetli pytanie o ponowne uruchomienie systemu operacyjnego z określoną częstotliwością.

  Domyślnie opcja ta jest włączona. Domyślnie przedział czasu wynosi 5 minut. Dostępne wartości znajdują się w zakresie od 1 do 1440 minut.

  Jeśli ta opcja jest wyłączona, monit zostaje wyświetlony tylko raz.

- **Uruchom ponownie po (min)**

  Po wyświetleniu monitu, aplikacja wymusza ponowne uruchomienie systemu operacyjnego po minięciu określonego przedziału czasu.

  Domyślnie opcja ta jest włączona. Domyślne opóźnienie wynosi 30 minut. Dostępne wartości znajdują się w zakresie od 1 do 1440 minut.

- **Wymuś zamknięcie aplikacji dla zablokowanych sesji**

  Uruchomione aplikacje mogą uniemożliwić ponowne uruchomienie urządzenia klienckiego. Na przykład, jeśli dokument jest edytowany w edytorze tekstu i nie zostanie zapisany, aplikacja nie zezwoli na ponowne uruchomienie urządzenia.

  Jeśli ta opcja jest włączona, zostaje wymuszone zamknięcie takich aplikacji na zablokowanym urządzeniu przed jego ponownym uruchomieniem. W wyniku tego działania użytkownicy mogą utracić niezapisane zmiany.

  Jeśli ta opcja jest wyłączona, zablokowane urządzenie nie zostanie uruchomione ponownie. Stan zadania na tym urządzeniu informuje, że wymagane jest ponowne uruchomienie urządzenia. Użytkownicy muszą ręcznie zamknąć wszystkie aplikacje uruchomione na zablokowanych urządzeniach i uruchomić ponownie te urządzenia.

  Domyślnie opcja ta jest wyłączona.

Przejdź do następnego kroku kreatora.

10. Określ ustawienia konta:

    - **Konto domyślne**

      Zadanie zostanie uruchomione z poziomu tego samego konta co aplikacja, która wykonuje to zadanie.

      Domyślnie opcja ta jest zaznaczona.

    - **Określ konto**

      Uzupełnij pola **Konto** i **Hasło**, aby określić szczegóły konta, z poziomu którego uruchamiane jest zadanie. Konto musi posiadać wystarczające uprawnienia dla tego zadania.

    - **Konto**

      Konto, z poziomu którego zadanie jest uruchamiane.

    - **Hasło**

      Hasło do konta, z poziomu którego zadanie będzie uruchamiane.

11. W kroku **Zakończ tworzenie zadania** kreatora, włącz opcję **Otwórz szczegóły zadania po jego utworzeniu**, aby zmodyfikować domyślne ustawienia zadania.

    Jeśli nie włączysz tej opcji, zadanie zostanie utworzone z domyślnymi ustawieniami. Możesz zmodyfikować domyślne ustawienia później.

12. Kliknij przycisk **Zakończ**.

    Kreator tworzy zadanie. Jeśli włączyłeś opcję **Otwórz szczegóły zadania po jego utworzeniu**, automatycznie zostanie otwarte okno właściwości zadania. W tym oknie możesz określić ogólne ustawienia zadania oraz w razie potrzeby zmienić ustawienia określone podczas tworzenia zadania.

    > Możesz także otworzyć okno właściwości zadania, klikając nazwę utworzonego zadania na liście zadań.

    Zadanie zostanie utworzone, skonfigurowane i będzie wyświetlane na liście zadań w sekcji **Zadania**.

13. Aby uruchomić zadanie, na liście zadań wybierz zadanie i kliknij przycisk **Uruchom**.

    Możesz także ustawić harmonogram uruchamiania zadania na karcie **Terminarz** w oknie właściwości zadania.

    Szczegółowy opis ustawień zaplanowanego uruchomienia znajduje się w ogólnych ustawieniach zadania.

Po zakończeniu zadania wybrane luki zostaną naprawione.

Wybieranie poprawek użytkownika dla luk w programach innych firm

Aby użyć zadania *Napraw luki*, należy ręcznie określić aktualizacje oprogramowania do naprawy luk w programach innych firm, wymienionych w ustawieniach zadania. Zadanie *Napraw luki* używa zalecanych poprawek dla oprogramowania firmy Microsoft oraz poprawek użytkownika dla innych programów innych firm.

Poprawki użytkownika to aktualizacje oprogramowania, które administrator ręcznie określa do zainstalowania w celu naprawy luk w zabezpieczeniach.

W celu wybrania poprawek użytkownika dla luk w programach firm trzecich:

1. W menu głównym przejdź do **Zarządzanie oprogramowaniem** → **Zarządzanie poprawkami** → **Luki w oprogramowaniu**.

   Zostanie wyświetlona tabela z listą luk w oprogramowaniu innych firm, zainstalowanym na zarządzanych urządzeniach.

2. Na liście luk w oprogramowaniu kliknij odnośnik z nazwą luki w oprogramowaniu, dla której chcesz określić poprawkę użytkownika.

   Zostanie otwarte okno właściwości wybranej luki w zabezpieczeniach.

3. W lewej części okna wybierz sekcję **Poprawki użytkownika i inne poprawki**.

   Zostanie wyświetlona lista poprawek użytkownika dla wybranej luki w oprogramowaniu.

4. Kliknij przycisk **Dodaj**.

   Zostanie wyświetlona lista dostępnych pakietów instalacyjnych. Lista wyświetlonych pakietów instalacyjnych odpowiada liście **Zarządzanie oprogramowaniem** → **Pakiety instalacyjne**.

   Jeśli nie utworzono pakietu instalacyjnego zawierającego poprawkę użytkownika dla wybranej luki, możesz utworzyć pakiet teraz, klikając przycisk **Nowy**, a następnie korzystając kreator tworzenia nowego pakietu.

5. Wybierz pakiet (lub pakiety) instalacyjny zawierający poprawkę użytkownika (lub poprawki użytkownika) dla wybranek luki.

6. Kliknij przycisk **Zapisz**.

   Zostaną określone pakiety instalacyjne zawierające poprawki użytkownika dla luki w oprogramowaniu. Po uruchomieniu zadania *Napraw luki* pakiet instalacyjny zostaje zainstalowany, a luka w oprogramowaniu zostaje naprawiona.

Przeglądanie informacji o lukach w oprogramowaniu wykrytych na wszystkich zarządzanych urządzeniach

Po przeskanowaniu oprogramowaniu na zarządzanych urządzeniach w poszukiwaniu luk, możesz przejrzeć listę wykrytych luk w oprogramowaniu. Jeśli uruchomisz zadanie dla hierarchii Serwerów administracyjnych, możesz wyświetlić listę zarządzanych urządzeń z wykrytymi lukami tylko dla wybranego Serwera administracyjnego.

Możesz także wygenerować i przejrzeć Raport o lukach.

W celu przejrzenia listy luk w oprogramowaniu wykrytych na wszystkich zarządzanych urządzeniach:

W menu głównym przejdź do **Operacje** → **Zarządzanie poprawkami** → **Luki w oprogramowaniu**.

Zostanie wyświetlona lista luk w oprogramowaniu wykrytych na urządzeniach klienckich.

Aby dostosować listę luk w oprogramowaniu,

Kliknij ikonę **Filtr** ( ) w prawym górnym rogu listy luk w oprogramowaniu, a następnie wybierz potrzebne filtry. Możesz także wybrać jeden z predefiniowanych filtrów z listy rozwijalnej **Wstępnie ustawione filtry** nad listą luk w oprogramowaniu.

Możesz uzyskać szczegółowe informacje o dowolnej luce z listy.

W celu uzyskania informacji o luce w oprogramowaniu,

Na liście luk w oprogramowaniu kliknij odnośnik z nazwą luki.

Zostanie otwarte okno właściwości luki w oprogramowaniu.

Przeglądanie informacji o lukach w oprogramowaniu wykrytych na wybranym zarządzanym urządzeniu

Możesz przejrzeć informacje o lukach w oprogramowaniu, wykrytych na wybranym zarządzanym urządzeniu działającym pod kontrolą systemu Windows.

W celu wyeksportowania listy luk w oprogramowaniu, wykrytych na wybranym zarządzanym urządzeniu:

1. W menu głównym przejdź do **Zarządzanie zasobami** → **Zasoby (urządzenia)**.

   Zostanie wyświetlona lista zarządzanych urządzeń.

2. Na liście zarządzanych urządzeń kliknij odnośnik z nazwą urządzenia, dla którego chcesz przejrzeć wykryte luki w oprogramowaniu.

   Zostanie wyświetlone okno właściwości wybranego urządzenia.

3. W oknie właściwości wybranego urządzenia wybierz zakładkę **Zaawansowane**.

4. W lewej części okna wybierz sekcję **Luki w oprogramowaniu**.

Zostanie wyświetlona lista luk w oprogramowaniu, wykrytych na wybranym, zarządzanym urządzeniu.

W celu przejrzenia właściwości wybranej luki w oprogramowaniu:

Kliknij odnośnik z nazwą luki w oprogramowaniu na liście luk w oprogramowaniu.

Zostanie otwarte okno właściwości wybranej luki w oprogramowaniu.

Przeglądanie statystyk dotyczących luk na zarządzanych urządzeniach

Statystyki dla każdej luki w oprogramowaniu możesz przejrzeć na zarządzanych urządzeniach. Statystyki są przedstawiane w postaci wykresu. Wykres wyświetla liczbę urządzeń z następującymi stanami:

- *Zignorowano na: <liczba urządzeń>*. Stan jest przypisywany, jeśli we właściwościach luki ręcznie ustawiono opcję ignorowania luki.
- *Naprawiono na: <liczba urządzeń>*. Ten stan jest przypisywany, jeśli zadanie naprawy luki zostało zakończone pomyślnie.
- *Naprawa zaplanowana na: <liczba urządzeń>*. Stan jest przypisywany, jeśli utworzono zadanie naprawy luki, ale zadanie nie zostało jeszcze wykonane.
- *Zastosowano poprawkę na: <liczba urządzeń>*. Stan jest przypisywany, jeśli ręcznie wybrano aktualizację oprogramowania do naprawy luki, ale ta aktualizacja oprogramowania nie naprawiła luki.
- *Naprawa wymagana na: <liczba urządzeń>*. Ten stan jest przypisywany, jeśli luka została naprawiona tylko na niektórych zarządzanych urządzeniach i wymagana jest naprawa luki na większej liczbie zarządzanych urządzeń.

W celu sprawdzenia statystyk dotyczących luki na zarządzanych urządzeniach:

1. W menu głównym przejdź do **Operacje** → **Zarządzanie poprawkami** → **Luki w oprogramowaniu**.

   Strona wyświetla listę luk w aplikacjach wykrytych na zarządzanych urządzeniach.

2. Zaznacz pole wyboru obok danej luki.

3. Kliknij przycisk **Statystyki luk na urządzeniach**.

> Przycisk **Statystyki luk na urządzeniach** jest nieaktywny, jeśli wybierzesz więcej niż jedną lukę.

Zostanie wyświetlony wykres stanów luk. Kliknięcie stanu spowoduje otwarcie listy urządzeń, na których luka posiada wybrany stan.

Eksportowanie listy luk w oprogramowaniu do pliku

Wyświetloną listę luk możesz pobrać w pliku w formacie CSV lub TXT. Możesz przesłać te pliki swojemu menadżerowi bezpieczeństwa informacji lub przechowywać je dla celów statystycznych.

W celu wyeksportowania listy luk w oprogramowaniu wykrytych na wszystkich zarządzanych urządzeniach do pliku tekstowy:

1. W menu głównym przejdź do **Operacje** → **Zarządzanie poprawkami** → **Luki w oprogramowaniu**.

   Wyświetlana jest lista luk w oprogramowaniu wykrytych na zarządzanych urządzeniach.

   Domyślnie eksportowane są tylko luki wyświetlane na bieżącej stronie.

   Jeśli chcesz wyeksportować tylko określone luki, zaznacz pola wyboru obok tych luk.

2. W zależności od preferowanego formatu eksportowania, kliknij przycisk **Eksportuj do pliku TXT** lub przycisk **Eksportuj do pliku CSV**. Jeśli którykolwiek z tych przycisków nie jest widoczny, kliknij przycisk wielokropka, a następnie wybierz żądaną opcję z listy rozwijanej.

Na Twoje urządzenie zostanie pobrany plik zawierający listę luk w oprogramowaniu.

W celu wyeksportowania listy luk w oprogramowaniu, wykrytych na wybranym zarządzanym urządzeniu:

1. W menu głównym przejdź do **Zarządzanie zasobami** → **Zasoby (urządzenia)**.

   Zostanie wyświetlona lista zarządzanych urządzeń.

2. Na liście zarządzanych urządzeń kliknij odnośnik z nazwą urządzenia, dla którego chcesz przejrzeć wykryte luki w oprogramowaniu.

   Zostanie wyświetlone okno właściwości wybranego urządzenia.

3. W oknie właściwości wybranego urządzenia wybierz zakładkę **Zaawansowane**.

4. W lewej części okna wybierz sekcję **Luki w oprogramowaniu**.

Zostanie wyświetlona lista luk w oprogramowaniu, wykrytych na wybranym, zarządzanym urządzeniu.

Domyślnie eksportowane są tylko luki wyświetlane na bieżącej stronie.

Jeśli chcesz wyeksportować tylko określone luki, zaznacz pola wyboru obok tych luk.

1. W zależności od preferowanego formatu eksportowania, kliknij przycisk **Eksportuj do pliku TXT** lub przycisk **Eksportuj do pliku CSV**. Jeśli którykolwiek z tych przycisków nie jest widoczny, kliknij przycisk wielokropka, a następnie wybierz żądaną opcję z listy rozwijanej.

Na Twoje urządzenie zostanie pobrany plik zawierający listę luk w oprogramowaniu.

Ignorowanie luk w oprogramowaniu

Możesz zignorować luki w oprogramowaniu, które mają zostać naprawione. Przyczyny zignorowania luk w oprogramowaniu mogą być, na przykład, następujące:

- Nie uważasz luki w oprogramowaniu za krytyczną dla swojej organizacji.
- Rozumiesz, poprawka luki w oprogramowaniu może uszkodzić dane związane z oprogramowaniem, które wymagało naprawy luki.
- Jesteś pewien, że luka w oprogramowaniu nie jest niebezpieczna dla sieci w Twojej organizacji, ponieważ używasz innych środków ochrony swoich zarządzanych urządzeń.

Możesz zignorować lukę w oprogramowaniu na wszystkich zarządzanych urządzeniach lub tylko na wybranych zarządzanych urządzeniach.

W celu zignorowania luki w oprogramowaniu na wszystkich zarządzanych urządzeniach:

1. W menu głównym przejdź do **Operacje** → **Zarządzanie poprawkami** → **Luki w oprogramowaniu**.

   Wyświetlana jest lista luk w oprogramowaniu wykrytych na zarządzanych urządzeniach.

2. Na liście luk w oprogramowaniu kliknij odnośnik z nazwą luki w oprogramowaniu, którą chcesz zignorować.

   Zostanie otwarte okno właściwości luk w oprogramowaniu.

3. Na zakładce **Ogólne** włącz opcję **Ignoruj lukę**.

4. Kliknij przycisk **Zapisz**.

   Okno właściwości luk w oprogramowaniu zostanie zamknięte.

Luka w oprogramowaniu zostanie zignorowana na wszystkich zarządzanych urządzeniach.

W celu zignorowania luki w oprogramowaniu na wybranym zarządzanym urządzeniu:

1. W menu głównym przejdź do **Zarządzanie zasobami** → **Zasoby (urządzenia)**.

   Zostanie wyświetlona lista zarządzanych urządzeń.

2. Na liście zarządzanych urządzeń kliknij odnośnik z nazwą urządzenia, na którym chcesz zignorować lukę w oprogramowaniu.

   Zostanie otwarte okno właściwości urządzenia.

3. W oknie właściwości urządzenia wybierz zakładkę **Zaawansowane**.

4. W lewej części okna wybierz sekcję **Luki w oprogramowaniu**.

   Zostanie wyświetlona lista luk w oprogramowaniu wykrytych na urządzeniu.

5. Na liście luk w oprogramowaniu wybierz lukę, którą chcesz zignorować na wybranym urządzeniu.

   Zostanie otwarte okno właściwości luk w oprogramowaniu.

6. W oknie właściwości luki w oprogramowaniu, na zakładce **Ogólne** włącz opcję **Ignoruj lukę**.

7. Kliknij przycisk **Zapisz**.

   Okno właściwości luk w oprogramowaniu zostanie zamknięte.

8. Zamknij okno właściwości urządzenia.

Luka w oprogramowaniu zostanie zignorowana na wybranym urządzeniu.

Zignorowana luka w oprogramowaniu nie zostanie naprawiona po zakończeniu wykonywania zadania *Napraw luki* lub zadania *Zainstaluj wymagane aktualizacje i napraw luki*. Możesz wykluczyć zignorowane luki w oprogramowaniu z listy luk z użyciem filtra.

Tworzenie pakietu instalacyjnego aplikacji innej firmy z bazy danych Kaspersky

Kaspersky Security Center Web Console pozwala na zdalną instalację aplikacji firm trzecich przy użyciu pakietów instalacyjnych. Takie aplikacje innych firm są zawarte w dedykowanej bazie danych Kaspersky. Ta baza danych jest tworzona automatycznie, gdy uruchamiasz zadanie *Pobierz aktualizacje do repozytorium Serwera administracyjnego* po raz pierwszy.

> Możesz utworzyć pakiet instalacyjny aplikacji innej firmy z bazy danych Kaspersky tylko wtedy, gdy posiadasz licencję na zarządzanie lukami i poprawkami.

W celu utworzenia pakietu instalacyjnego aplikacji innej firmy z bazy danych Kaspersky:

1. W menu głównym przejdź do **Zarządzanie oprogramowaniem** → **Pakiety instalacyjne**.

2. Kliknij przycisk **Dodaj**.

   Zostanie uruchomiony Kreator tworzenia nowego pakietu. Przejdź przez kroki kreatora, korzystając z przycisku **Dalej**.

3. Wybierz opcję **Wybierz aplikację z bazy danych Kaspersky do utworzenia pakietu instalacyjnego**.

   > Ta opcja jest dostępna tylko w ramach licencji na Zarządzanie lukami i poprawkami.

   Przejdź do następnego kroku kreatora.

4. Wybierz aplikację, dla której chcesz utworzyć pakiet instalacyjny.

   Przejdź do następnego kroku kreatora.

5. Wybierz odpowiedni język lokalizacji z listy rozwijanej, a następnie kliknij Dalej.

   > Ten krok jest wyświetlany tylko wtedy, gdy aplikacja umożliwia wybór opcji językowych.

6. Jeśli zostanie wyświetlony monit o zaakceptowanie umowy licencyjnej dotyczącej instalacji, w kroku kreatora **Umowy licencyjne i Polityki prywatności** wykonaj następujące czynności:

   a. Kliknij łącze **Pokaż**, aby przeczytać Umowę licencyjną na stronie internetowej dostawcy lub wyświetlić aktualizacje licencji.

   b. Zaznacz pole wyboru **Potwierdzam, że w pełni przeczytałem(-am), rozumiem i akceptuję warunki niniejszej Umowy licencyjnej użytkownika końcowego**.

   c. Kliknij przycisk **Zaakceptuj wszystkie**, aby zaakceptować wszystkie umowy licencyjne i polityki prywatności wyświetlane na liście.

7. W kroku kreatora **Nazwa nowego pakietu instalacyjnego** w polu **Nazwa pakietu** wprowadź nazwę pakietu instalacyjnego, a następnie kliknij opcję **Dalej**.

   Nowo utworzony pakiet instalacyjny zostanie przesłany na Serwer administracyjny. Kreator tworzenia nowego pakietu wyświetla komunikat informujący, że pakiet instalacyjny został pomyślnie utworzony.

8. Kliknij przycisk **Zakończ**.

Nowo utworzony pakiet instalacyjny zostaje wyświetlony na liście pakietów instalacyjnych. Możesz wybrać ten pakiet podczas tworzenia lub ponownego konfigurowania zadania *Zdalna instalacja aplikacji*.

> Możesz utworzyć i ponownie skonfigurować zadanie *Zdalna instalacja aplikacji* przy użyciu pakietu instalacyjnego aplikacji innej firmy z bazy danych Kaspersky tylko wtedy, gdy posiadasz licencję na zarządzanie lukami i poprawkami.

Przeglądanie i modyfikowanie ustawienia pakietu instalacyjnego aplikacji innej firmy z bazy danych Kaspersky

Jeśli poprzednio utworzyłeś jakiekolwiek pakiety instalacyjne aplikacji innych firm znajdujące się w bazie danych Kaspersky, możesz przejrzeć i zmodyfikować ustawienia tych pakietów.

> Modyfikowanie ustawień pakietu instalacyjnego aplikacji innej firmy z bazy danych Kaspersky jest dostępne tylko w licencji Zarządzanie lukami i poprawkami.

W celu przejrzenia i zmodyfikowania ustawień pakietu instalacyjnego aplikacji innej firmy z bazy danych Kaspersky:

1. W menu głównym przejdź do **Zarządzanie oprogramowaniem** → **Pakiety instalacyjne**.

2. Na otwartej liście pakietów instalacyjnych kliknij nazwę odpowiedniego pakietu.

   Zostanie otwarte okno właściwości.

3. W razie potrzeby zmodyfikuj ustawienia.

4. Kliknij przycisk **Zapisz**.

Zmodyfikowane ustawienia zostaną zapisane.

Ustawienia pakietu instalacyjnego aplikacji innej firmy z bazy danych Kaspersky

Ustawienia pakietu instalacyjnego aplikacji innej firmy są pogrupowane na następujących zakładkach:

Nie wszystkie ustawienia wymienione poniżej są wyświetlane domyślnie. Możesz dodać potrzebne kolumny, klikając przycisk **Filtr**, a następnie wybierając odpowiednie nazwy kolumn z listy.

- Zakładka **Ogólne**:
  - Pole wprowadzania, które zawiera nazwę pakietu instalacyjnego i które może być edytowane ręcznie
  - **Aplikacja**

    Nazwa aplikacji innej firmy, dla której tworzony jest pakiet instalacyjny.
  - **Wersja**

    Numer wersji aplikacji innej firmy, dla której tworzony jest pakiet instalacyjny.
  - **Rozmiar**

    Rozmiar pakietu instalacyjnego innej firmy (w kilobajtach).
  - **Utworzono**

    Data i godzina utworzenia pakietu instalacyjnego innej firmy.
  - **Ścieżka dostępu**

    Ścieżka do folderu sieciowego, w którym przechowywany jest pakiet instalacyjny innej firmy.
- Zakładka **Procedura instalacji**:
  - **Zainstaluj wymagane ogólne składniki systemu**

    Jeśli ta opcja jest włączona, przed zainstalowaniem aktualizacji aplikacja automatycznie instaluje wszystkie ogólne składniki systemu (wymagania wstępne), które są niezbędne do zainstalowania aktualizacji. Na przykład, tymi wymaganiami wstępnymi mogą być aktualizacje systemu operacyjnego.

    Jeśli ta opcja jest wyłączona, konieczne może być ręczne zainstalowanie wymagań wstępnych.

    Domyślnie opcja ta jest wyłączona.
  - Tabela która wyświetla właściwości aktualizacji i zawiera następujące kolumny:
    - **Nazwa**

      Nazwa aktualizacji.
    - **Opis**

      Opis aktualizacji.

- **Źródło**

  Źródło aktualizacji, czyli czy została ona wydana przez firmę Microsoft, czy przez inną niezależną firmę.

- **Typ**

  Rodzaj aktualizacji, czyli czy jest przeznaczona dla sterownika czy aplikacji.

- **Kategoria**

  Kategoria Windows Server Update Services (WSUS) wyświetlana dla aktualizacji firmy Microsoft (aktualizacje krytyczne, aktualizacje definicji, sterowniki, pakiety funkcji, aktualizacje zabezpieczeń, dodatki Service Pack, narzędzia, pakiety zbiorcze aktualizacji, aktualizacje lub uaktualnienie).

- **Istotność zgodnie z MSRC**

  Istotność aktualizacji określona przez Microsoft Security Response Center (MSRC).

- **Istotność**

  Istotność aktualizacji określona przez Kaspersky.

- **Istotność poprawki**

  Istotność poprawki, jeśli jest ona przeznaczona dla aplikacji Kaspersky.

- **Artykuł**

  Identyfikator (ID) artykułu w bazie wiedzy opisującego aktualizację.

- **Biuletyn**

  Identyfikator biuletynu zabezpieczeń opisującego aktualizację.

- **Nieprzypisane do instalacji (nowa wersja)**

  Wyświetla, czy aktualizacja ma stan Nieprzypisane do instalacji.

- **Do zainstalowania**

  Wyświetla, czy aktualizacja ma stan Do zainstalowania.

- **Instalowanie**

  Wyświetla, czy aktualizacja ma stan Instalowanie.

- **Zainstalowano**

  Wyświetla, czy aktualizacja ma stan Zainstalowana.

- **Niepowodzenie**

  Wyświetla, czy aktualizacja ma stan Niepowodzenie.

- **Wymagane jest ponowne uruchomienie**

  Wyświetla, czy aktualizacja ma stan Wymagane ponowne uruchomienie.

- **Zarejestrowano**

  Wyświetla datę i godzinę rejestracji aktualizacji.

- **Zainstalowana w trybie interaktywnym**

  Wyświetla, czy aktualizacja wymaga interakcji z użytkownikiem podczas instalacji.

- **Stan zatwierdzenia aktualizacji**

  Wyświetla, czy aktualizacja została zatwierdzona do instalacji.

- **Zmiana**

  Wyświetla aktualny numer wersji aktualizacji.

- **ID aktualizacji**

  Wyświetla identyfikator aktualizacji.

- **Wersja aplikacji**

  Wyświetla numer wersji, do której ma zostać zaktualizowana aplikacja.

- **Zastąpiony**

  Wyświetla inne aktualizacje, które mogą zastąpić aktualizację.

- **Zastępowanie**

  Wyświetla inne aktualizacje, które mogą zostać zastąpione przez aktualizację.

- **Akceptacja warunków Umowy licencyjnej jest wymagana**

  Wyświetla, czy aktualizacja wymaga akceptacji warunków Umowy licencyjnej użytkownika końcowego (EULA).

- **Adres strony z opisem**

  Wyświetla nazwę producenta aktualizacji.

- **Rodzina aplikacji**

  Wyświetla nazwę rodziny aplikacji, do której należy aktualizacja.

- **Aplikacja**

  Wyświetla nazwę aplikacji, do której należy aktualizacja.

- **Wersja językowa**

  Wyświetla język aktualizacji.

- **Nieprzypisane do instalacji (nowa wersja)**

  Wyświetla, czy aktualizacja ma stan Nie przypisano do instalacji (nowa wersja).

- **Wymaga instalacji elementów należących do wymagań wstępnych**

  Wyświetla, czy aktualizacja ma stan Wymaga instalacji wymagań wstępnych.

- **Tryb pobierania**

  Wyświetla tryb pobierania aktualizacji.

- **Jest poprawką**

  Wyświetla, czy aktualizacja jest poprawką.

- **Nie zainstalowano**

  Wyświetla, czy aktualizacja ma stan Nie zainstalowano.

- **Utworzono**

- Tabela **Ustawienia**, która wyświetla ustawienia pakietu instalacyjnego — z ich nazwami, opisami i wartościami — użyte jako parametry wiersza poleceń podczas instalacji. Jeśli pakiet nie zawiera takich ustawień, wyświetlana jest odpowiednia wiadomość. Możesz zmodyfikować wartości tych ustawień.

- Zakładka **Historia rewizji** wyświetlająca rewizje pakietów instalacyjnych i zawierająca następujące kolumny:

  - **Zmiana** — wyświetla liczbę rewizji pakietów instalacyjnych.

  - **Czas** — data i godzina modyfikacji ustawień pakietu instalacyjnego.

  - **Użytkownik** — nazwa użytkownika, który zmodyfikował pakiet instalacyjny.

  - **Adres IP urządzenia użytkownika** — adres IP urządzenia, z którego obiekt został zmodyfikowany.

  - **Adres IP Web Console** — adres IP Kaspersky Security Center Web Console, za pomocą którego obiekt został zmodyfikowany.

  - **Akcja** — wyświetla działanie (działania) wykonane na pakiecie instalacyjnym w obrębie rewizji.

  - **Opis** — opis rewizji związanej ze zmianą wprowadzoną w ustawieniach pakietu instalacyjnego.

    Domyślnie, pole opisu rewizji jest puste. Aby dodać opis do rewizji, wybierz żądaną rewizję i kliknij przycisk **Edytuj opis**. W otwartym oknie wprowadź tekst opisu rewizji.

Naprawianie luk w odizolowanej sieci

W tej sekcji opisano kroki, które możesz podjąć, aby usunąć luki w zabezpieczeniach oprogramowania firm trzecich na zarządzanych urządzeniach podłączonych do serwerów administracyjnych bez dostępu do Internetu.

Scenariusz: Eliminowanie luk w oprogramowaniu innych firm w odizolowanej sieci

Możesz instalować aktualizacje i eliminować luki w oprogramowaniu innych firm zainstalowanym na zarządzanych urządzeniach w odizolowanej sieci. Takie sieci obejmują serwery administracyjne i podłączone do nich zarządzane urządzenia, które nie mają dostępu do Internetu. Aby naprawić luki w takiej sieci, potrzebujesz serwera administracyjnego połączonego z Internetem. Używając Serwera administracyjnego z dostępem do Internetu, będziesz mógł pobierać poprawki (wymagane aktualizacje), a następnie przesyłać je do izolowanych Serwerów administracyjnych.

Możesz pobrać aktualizacje oprogramowania innych firm wydane przez dostawców oprogramowania, ale nie możesz pobierać aktualizacji oprogramowania firmy Microsoft na odizolowanych serwerach administracyjnych przy użyciu Kaspersky Security Center.

Aby uzyskać szczegółowe informacje, jak działa proces naprawiania luk w odizolowanej sieci, zapoznaj się z opisem i schematem tego procesu.

Wymagania wstępne

Zanim zaczniesz, wykonaj następujące czynności:

1. Przydziel jedno urządzenie do łączenia się z internetem i pobierania poprawek. To urządzenie będzie uznawane za Serwer administracyjny z dostępem do internetu.
2. Zainstaluj Kaspersky Security Center Linux, w wersji nie wcześniejszej niż 15.1, na następujących urządzeniach:
   - Przydzielone urządzenie, które będzie pełnić rolę serwera administracyjnego z dostępem do Internetu
   - Izolowane urządzenia, które będą działać jako izolowane od Internetu serwery administracyjne (zwane dalej odizolowanymi serwerami administracyjnymi)
3. Upewnij się, że każdy Serwer administracyjny ma: wystarczająco dużo miejsca na dysku do pobierania i przechowywania aktualizacji i poprawek.

Etapy

Instalowanie aktualizacji i eliminowanie luk w zabezpieczeniach oprogramowania firm trzecich na zarządzanych urządzeniach izolowanych Serwerów administracyjnych obejmuje następujące etapy:

1. **Konfigurowanie serwera administracyjnego z dostępem do Internetu**

   Przygotuj swój Serwer administracyjny z dostępem do Internetu do obsługi żądań dotyczących wymaganych aktualizacji oprogramowania innych firm i pobierania poprawek.

2. **Konfigurowanie izolowanych Serwerów administracyjnych**

   Przygotuj odizolowane serwery administracyjne, dzięki czemu mogą tworzyć listy wymaganych aktualizacji i obsługiwać poprawki pobrane przez serwer administracyjny z dostępem do Internetu. Po skonfigurowaniu odizolowane serwery administracyjne nie próbują już pobierać poprawek z Internetu. Zamiast tego uzyskują aktualizacje przez poprawki.

3. **Przesyłanie poprawek i instalowanie aktualizacji na odizolowanych serwerach administracyjnych**

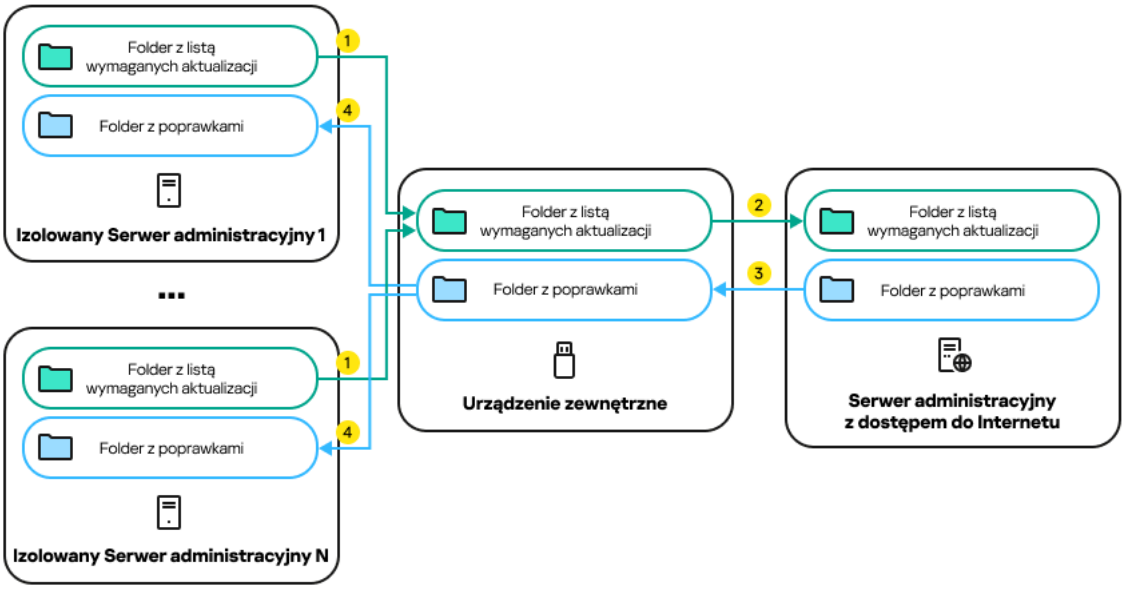
   Po zakończeniu konfigurowania Serwerów administracyjnych możesz: przesyłać wymagane listy aktualizacji i poprawek pomiędzy Serwerem administracyjnym z dostępem do internetu a odizolowanymi Serwerami administracyjnymi. Następnie aktualizacje z poprawek zostaną zainstalowane na zarządzanych urządzeniach przy użyciu zadania *Zainstaluj wymagane aktualizacje i napraw luki*.

Wyniki

W ten sposób aktualizacje oprogramowania firm trzecich są przesyłane do izolowanych Serwerów administracyjnych i instalowane na podłączonych zarządzanych urządzeniach za pomocą Kaspersky Security Center Linux. Wystarczy raz skonfigurować Serwery administracyjne, a potem możesz otrzymywać aktualizacje tak często, jak potrzebujesz, na przykład, raz lub kilka razy dziennie.

Eliminowanie luk w oprogramowaniu innych firm w odizolowanej sieci

Proces naprawiania luk w zabezpieczeniach oprogramowania firm trzecich w odizolowanej sieci jest przedstawiony na poniższym rysunku. Możesz okresowo powtarzać ten proces.



Proces przesyłania poprawek i lista wymaganych aktualizacji między serwerem administracyjnym z dostępem do Internetu a izolowanymi serwerami administracyjnymi

Każdy serwer administracyjny odizolowany od Internetu (zwany dalej izolowanym serwerem administracyjnym) generuje listę aktualizacji, które muszą zostać zainstalowanie na zarządzanych urządzeniach podłączonych do tego serwera administracyjnego. Ta lista aktualizacji jest przechowywana w określonym folderze jako zestaw plików binarnych, z których każdy ma nazwę zawierającą identyfikator poprawki zawierającej niezbędną aktualizację. Dlatego każdy plik na liście odpowiada określonej poprawce.

Lista wymaganych aktualizacji jest przesyłana z izolowanego Serwera administracyjnego do wyznaczonego Serwera administracyjnego z dostępem do Internetu za pomocą urządzenia zewnętrznego. Następnie wyznaczony Serwer administracyjny pobiera poprawki z Internetu i umieszcza je w wyznaczonym folderze.

Kiedy wszystkie poprawki zostaną pobrane i umieszczone w wyznaczonym folderze, zostaną one następnie przesłane z powrotem do każdego izolowanego Serwera administracyjnego, z którego uzyskano listę wymaganych aktualizacji. Poprawki są zapisywane w specjalnie dla nich utworzonym folderze na każdym izolowanym Serwerze administracyjnym.

W rezultacie zadanie *Zainstaluj wymagane aktualizacje i napraw luki* uruchamia poprawki i instaluje aktualizacje na zarządzanych urządzeniach izolowanych Serwerów administracyjnych.

Konfigurowanie serwera administracyjnego z dostępem do internetu w celu usunięcia luk w odizolowanej sieci

Aby przygotować się na naprawianie luk i przesyłanie poprawek w izolowanej sieci, najpierw skonfiguruj Serwer administracyjny z dostępem do Internetu, a następnie skonfiguruj odizolowane Serwery administracyjne.

W celu skonfigurowania serwera administracyjnego z dostępem do Internetu:

1. Utwórz dwa foldery na dysku, na którym zainstalowany jest serwer administracyjny:

   - Folder z listą wymaganych aktualizacji
   - Folder na poprawki

   Możesz nazwać te foldery według potrzeb.

2. Przyznaj prawa dostępu do **modyfikacji** do grupy KLAdmins w utworzonych folderach, korzystając ze standardowych narzędzi administracyjnych systemu operacyjnego.

3. Użyj narzędzia klscflag, aby określić ścieżki do folderów we właściwościach Serwera administracyjnego.

   Uruchom wiersz poleceń, a następnie zmień bieżący katalog na katalog z narzędziem klscflag. Narzędzie klscflag znajduje się w katalogu, w którym zainstalowany jest serwer administracyjny. Domyślna ścieżka instalacji to /opt/kaspersky/ksc64/sbin.

4. Uruchom następujące polecenie w wierszu poleceń:

   - W celu ustawienia ścieżki do folderu dla poprawek:
     ```
     klscflag -fset -pv klserver -n VAPM_DATA_EXPORT_PATH -t s -v "<ścieżka do folderu>"
     ```
   - W celu ustawienia ścieżki do folderu dla listy wymaganych aktualizacji:
     ```
     klscflag -fset -pv klserver -n VAPM_REQ_IMPORT_PATH -t s -v "<ścieżka do folderu>"
     ```

   Na przykład: `klscflag -fset -pv klserver -n VAPM_DATA_EXPORT_PATH -t s -v "/FolderForPatches"`

5. Jeśli to konieczne, użyj narzędzia klscflag, aby określić, jak często Serwer administracyjny powinien sprawdzać nowe żądania poprawek:
   ```
   klscflag -fset -pv klserver -n VAPM_DATA_EXPORT_PERIOD_SEC -t d -v <wartość w sekundach>
   ```

   Domyślna wartość to 120 sekund.

Na przykład: `klscflag -fset -pv klserver -n VAPM_DATA_EXPORT_PERIOD_SEC -t d -v 120`

6. Utwórz zadanie *Wyszukiwanie luk i wymaganych aktualizacji* aby uzyskać informacje o poprawkach oprogramowania innych firm zainstalowanych na zarządzanych urządzeniach, a następnie ustal harmonogram zadania.

7. Utwórz zadanie *Napraw luki* aby określić poprawki dla oprogramowania innych firm używane do naprawiania luk, a następnie ustaw harmonogram zadań.

   Uruchom zadanie ręcznie, jeśli chcesz, aby zostało uruchomione wcześniej niż jest to określone w harmonogramie zadań. Kolejność rozpoczynania zadań ma znaczenie. *Napraw luki* należy uruchomić po zakończeniu zadania *Wyszukiwanie luk i wymaganych aktualizacji*.

8. Uruchom ponownie usługę Serwera administracyjnego.

Serwer administracyjny z dostępem do Internetu jest gotowy do pobierania i przesyłania aktualizacji do izolowanych serwerów administracyjnych. Zanim zaczniesz naprawiać luki, skonfiguruj izolowane serwery administracyjne.

Konfigurowanie izolowanych Serwerów administracyjnych w celu usunięcia luk w odizolowanej sieci

Po skonfigurowaniu Serwera administracyjnego z dostępem do Internetu, przygotuj każdy odizolowany Serwer administracyjny w Twojej sieci, aby możliwe było naprawienie luk i zainstalowanie aktualizacji na zarządzanych urządzeniach podłączonych do izolowanych serwerów administracyjnych.

Aby skonfigurować izolowane Serwery administracyjne, wykonaj poniższe kroki dla każdego Serwera administracyjnego:

1. Aktywuj klucz licencyjny dla funkcji Zarządzanie lukami i poprawkami (VAPM).

2. Utwórz dwa foldery na dysku, na którym zainstalowany jest serwer administracyjny:

   - Folder z listą wymaganych aktualizacji

   - Folder na poprawki

   Możesz nazwać te foldery według potrzeb.

3. Przyznaj uprawnienia do **modyfikacji** do grupy KLAdmins w utworzonych folderach, korzystając ze standardowych narzędzi administracyjnych systemu operacyjnego.

4. Użyj narzędzia klscflag, aby określić ścieżki do folderów we właściwościach Serwera administracyjnego.

   Uruchom wiersz poleceń, a następnie zmień bieżący katalog na katalog z narzędziem klscflag. Narzędzie klscflag znajduje się w katalogu, w którym zainstalowany jest serwer administracyjny. Domyślna ścieżka instalacji to /opt/kaspersky/ksc64/sbin.

5. Uruchom następujące polecenie w wierszu poleceń:

   - W celu ustawienia ścieżki do folderu dla poprawek:
     `klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_PATH -t s -v "<ścieżka do folderu>"`

- W celu ustawienia ścieżki do folderu dla listy wymaganych aktualizacji:
  ```
  klscflag -fset -pv klserver -n VAPM_REQ_EXPORT_PATH -t s -v "<ścieżka do folderu>"
  ```

Na przykład: `klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_PATH -t s -v "/FolderForPatches"`

6. Jeśli to konieczne, użyj narzędzia klscflag, aby określić, jak często izolowany serwer administracyjny powinien sprawdzać dostępność nowych poprawek:
   ```
   klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_PERIOD_SEC -t d -v <wartość w sekundach>
   ```

   Domyślna wartość to 120 sekund.

   Na przykład: `klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_PERIOD_SEC -t d -v 120`

7. Jeśli to konieczne, użyj narzędzia klscflag, aby obliczyć skróty SHA256 poprawek:
   ```
   klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_VERIFY_HASH -t d -v 1
   ```

   Przez uruchomienie tego polecenia, możesz się upewnić, że poprawki nie zostały zmodyfikowane podczas przesyłania na izolowany Serwer administracyjny oraz że otrzymano prawidłowe poprawki zawierające wymagane aktualizacje.

   Domyślnie, Kaspersky Security Center Linux nie oblicza skrótów SHA256 poprawek. Jeśli włączysz tę opcję, po odebraniu przez izolowany serwer administracyjny poprawek, Kaspersky Security Center Linux oblicza ich skróty i porównuje uzyskane wartości ze skrótami przechowywanymi w bazie danych serwera administracyjnego. Jeśli obliczony skrót nie zgadza się ze skrótem w bazie danych, pojawia się błąd i trzeba zastąpić nieprawidłowe poprawki.

8. Utwórz zadanie *Wyszukiwanie luk i wymaganych aktualizacji* aby uzyskać informacje o poprawkach oprogramowania innych firm zainstalowanych na zarządzanych urządzeniach, a następnie ustal harmonogram zadania.

9. Utwórz zadanie *Napraw luki* aby określić poprawki dla oprogramowania innych firm używane do naprawiania luk, a następnie ustaw harmonogram zadań.

   Uruchom zadanie ręcznie, jeśli chcesz, aby zostało uruchomione wcześniej niż jest to określone w harmonogramie zadań. Kolejność rozpoczynania zadań ma znaczenie. *Napraw luki* należy uruchomić po zakończeniu zadania *Wyszukiwanie luk i wymaganych aktualizacji*.

10. Uruchom ponownie usługę Serwera administracyjnego.

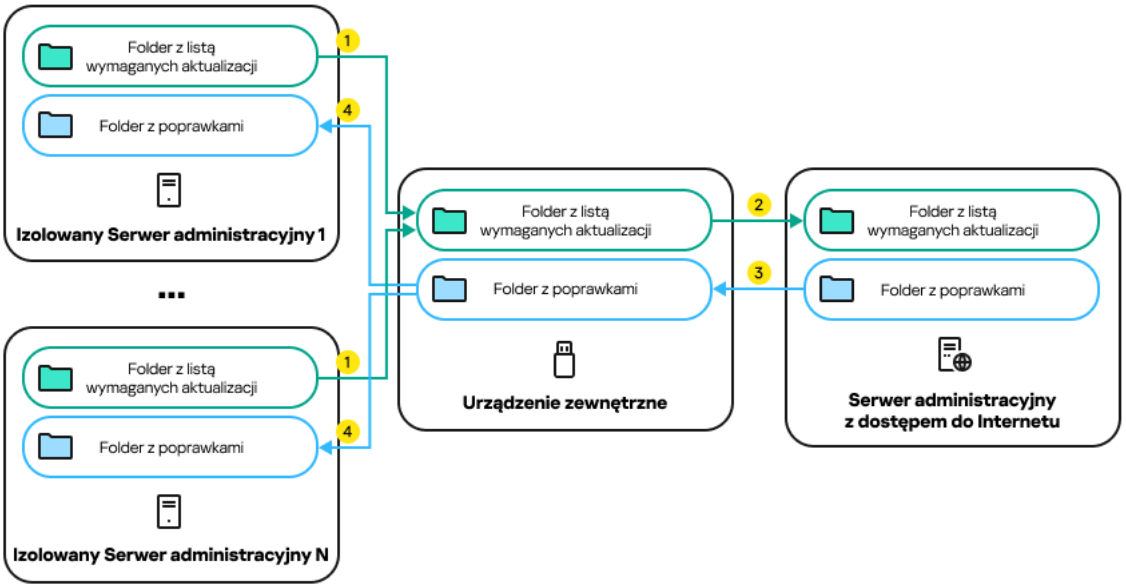
Po skonfigurowaniu wszystkich Serwerów administracyjnych możesz: przesyłać poprawki i listy wymaganych aktualizacji oraz eliminować luki w zabezpieczeniach oprogramowania firm trzecich na zarządzanych urządzeniach w odizolowanej sieci.

Przesyłanie poprawek i instalowanie aktualizacji w odizolowanej sieci

Po zakończeniu konfigurowania serwerów administracyjnych możesz przesyłać poprawki zawierające wymagane aktualizacje z serwera administracyjnego z dostępem do Internetu na izolowane serwery administracyjne. Możesz przesyłać i instalować aktualizacje tak często, jak potrzebujesz, na przykład, raz lub kilka razy dziennie.

Do przesyłania poprawek i listy wymaganych uaktualnień między Serwerami administracyjnymi potrzebny jest dysk zewnętrzny, taki jak dysk wymienny. Dlatego upewnij się, że na dysku zewnętrznym jest wystarczająco dużo miejsca do pobierania i przechowywania poprawek.

Proces przesyłania poprawek oraz lista wymaganych aktualizacji są wyświetlane na poniższym rysunku:



Proces przesyłania poprawek i lista wymaganych aktualizacji między serwerem administracyjnym z dostępem do Internetu a izolowanymi serwerami administracyjnymi

W celu zainstalowania aktualizacji i usunięcia luk na zarządzanych urządzeniach podłączonych do izolowanych Serwerów administracyjnych:

1. Uruchom zadanie *Zainstaluj wymagane aktualizacje i napraw luki*, jeśli nie zostało jeszcze uruchomione.

2. Podłącz dysk zewnętrzny do dowolnego izolowanego Serwera administracyjnego.

3. Utwórz dwa foldery na dysku zewnętrznym: jeden na listę wymaganych aktualizacji, a drugi na poprawki. Możesz nadać tym folderom dowolną nazwę.

   Jeśli wcześniej utworzono foldery, wyczyść je.

4. Skopiuj listę wymaganych aktualizacji z każdego izolowanego Serwera administracyjnego i wklej tę listę do folderu z listą wymaganych aktualizacji na dysku zewnętrznym.

   W rezultacie wszystkie listy uzyskane ze wszystkich izolowanych serwerów administracyjnych łączysz w jeden folder. Folder ten powinien zawierać pliki binarne z identyfikatorami poprawek wymaganych dla wszystkich izolowanych serwerów administracyjnych.

5. Podłącz dysk zewnętrzny do Serwera administracyjnego z dostępem do Internetu.

6. Skopiuj listę wymaganych aktualizacji z dysku zewnętrznego i wklej tę listę do folderu listy wymaganych aktualizacji na Serwerze administracyjnym z dostępem do Internetu.

   Wszystkie wymagane poprawki są automatycznie pobierane z Internetu do folderu łatek na Serwerze administracyjnym. To może potrwać kilka godzin.

7. Upewnij się, że wszystkie wymagane poprawki zostały pobrane. W tym celu możesz wykonać jedną z następujących czynności:

   - Sprawdź folder w poszukiwaniu poprawek na Serwerze administracyjnym z dostępem do internetu. Wszystkie poprawki, które zostały określone na liście wymaganych aktualizacji, należy pobrać do odpowiedniego folderu. Jest to wygodniejsze, jeśli wymagana jest niewielka liczba poprawek.

   - Przygotuj specjalny skrypt, na przykład, skrypt powłoki. Jeśli otrzymasz dużą liczbę poprawek, trudno będzie samodzielnie sprawdzić, czy wszystkie poprawki zostały pobrane. W takich przypadkach lepiej zautomatyzować sprawdzanie.

8. Skopiuj poprawki z Serwera administracyjnego z dostępem do Internetu i wklej je do odpowiedniego folderu na dysku zewnętrznym.

9. Prześlij poprawki do każdego izolowanego Serwera administracyjnego. Umieść poprawki w specjalnym folderze.

   W rezultacie każdy izolowany serwer administracyjny tworzy aktualną listę aktualizacji i poprawek wymaganych dla zarządzanych urządzeń podłączonych do bieżącego serwera administracyjnego. Po otrzymaniu przez serwer administracyjny z dostępem do Internetu listy wymaganych aktualizacji, serwer administracyjny pobiera poprawki z aktualizacjami z Internetu. Gdy te poprawki pojawią się na odizolowanych serwerach administracyjnych, zadanie *Zainstaluj wymagane aktualizacje i napraw luki* obsługuje poprawki. Aktualizacje są instalowane na zarządzanych urządzeniach, a luki w zabezpieczeniach oprogramowania innych firm są naprawiane.

Gdy uruchomione jest zadanie *Zainstaluj wymagane aktualizacje i napraw luki*, nie uruchamiaj ponownie urządzenia serwera administracyjnego ani nie uruchamiaj zadania *Kopia zapasowa danych Serwera administracyjnego* (spowoduje to również ponowne uruchomienie). W rezultacie zadanie *Zainstaluj wymagane aktualizacje i napraw luki* zostanie przerwane, a aktualizacje nie zostaną zainstalowane. W takim przypadku musisz zrestartować to zadanie ręcznie lub poczekać na uruchomienie zadania zgodnie ze skonfigurowanym harmonogramem.

Wyłączenie przesyłania poprawek i instalacji aktualizacji w sieci izolowanej

Można wyłączyć przesyłanie poprawek do izolowanych Serwerów administracyjnych, na przykład, jeśli zdecydowano się usunąć jeden lub więcej serwerów z odizolowanej sieci. W ten sposób możesz zmniejszyć liczbę poprawek i czas ich pobierania.

Aby wyłączyć przesyłanie poprawek do izolowanych Serwerów administracyjnych:

1. Jeśli chcesz wyłączyć wszystkie Serwery administracyjne z izolacji, we właściwościach Serwera administracyjnego z dostępem do Internetu usuń ścieżki do folderów z poprawkami oraz listę wymaganych aktualizacji. Jeśli chcesz, aby niektóre Serwery administracyjne znajdowały się w odizolowanej sieci, pomiń ten krok.

   Uruchom wiersz poleceń, a następnie zmień bieżący katalog na katalog z narzędziem klscflag. Narzędzie klscflag znajduje się w katalogu, w którym zainstalowany jest serwer administracyjny. Domyślna ścieżka instalacji to /opt/kaspersky/ksc64/sbin.

   Uruchom następujące polecenie w wierszu poleceń:

   - W celu usunięcia ścieżki do folderu dla poprawek:
     ```
     klscflag -fset -pv klserver -n VAPM_DATA_EXPORT_PATH -t s -v ""
     ```
   - W celu usunięcia ścieżki do folderu dla listy wymaganych aktualizacji:
     ```
     klscflag -fset -pv klserver -n VAPM_REQ_IMPORT_PATH -t s -v ""
     ```

2. Uruchom ponownie usługę na Serwerze administracyjnym z dostępem do Internetu, jeśli usunąłeś ścieżki do folderów.

3. We właściwościach każdego odizolowanego Serwera administracyjnego, który chcesz wyłączyć z izolacji, usuń ścieżki do folderów z poprawkami oraz listę wymaganych aktualizacji.

Uruchom następujące polecenia w wierszu poleceń na koncie z uprawnieniami roota:

- W celu usunięcia ścieżki do folderu dla poprawek:
  ```
  klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_PATH -t s -v ""
  ```
- W celu usunięcia ścieżki do folderu dla listy wymaganych aktualizacji:
  ```
  klscflag -fset -pv klserver -n VAPM_REQ_EXPORT_PATH -t s -v ""
  ```

4. Uruchom ponownie każdy Serwer administracyjny, z którego usunięto ścieżki do folderów.

Jeśli ponownie skonfigurowałeś Serwer administracyjny z dostępem do Internetu, poprawki nie będą już przesyłane przez Kaspersky Security Center Linux.

Jeśli ponownie skonfigurowano tylko określone Serwery administracyjne i usunięto je z izolowanej sieci, nie będą one już otrzymywać poprawek za pośrednictwem Kaspersky Security Center Linux. Tylko te Serwery administracyjne, które pozostają w izolowanej sieci, będą nadal otrzymywać poprawki.

Jeśli chcesz w przyszłości rozpocząć eliminowanie luk w zabezpieczeniach na wyłączonych izolowanych serwerach administracyjnych, musisz skonfigurować te serwery i serwer z dostępem do Internetu jeszcze raz.

Dokumentacja API

Ta Dokumentacja OpenAPI Kaspersky Security Center ma na celu pomóc w następujących zadaniach:

- Automatyzacja i personalizacja. Możesz zautomatyzować zadania, których możesz nie chcieć obsługiwać ręcznie. Na przykład, jako administrator możesz użyć Kaspersky Security Center OpenAPI do tworzenia i uruchamiania skryptów, które ułatwią tworzenie struktury grup administracyjnych i jej aktualizowanie.
- Niestandardowy rozwój. Korzystając z OpenAPI, możesz stworzyć aplikację kliencką.

Możesz użyć pola wyszukiwania w prawej części ekranu, aby znaleźć potrzebne informacje w Dokumentacji OpenAPI.

PRZEWODNIK PO OPENAPI

Próbki skryptów

Dokumentacja OpenAPI zawiera przykłady skryptów Pythona wymienionych w poniższej tabeli. Przykłady pokazują, w jaki sposób można wywoływać metody OpenAPI i automatycznie wykonywać różne zadania w celu ochrony sieci, na przykład utworzyć hierarchię „podstawowa/dodatkowa", uruchamiać zadania w Kaspersky Security Center Linux lub przypisywać punkty dystrybucji. Możesz uruchamiać próbki bez zmian lub tworzyć własne skrypty na ich podstawie.

Wywoływanie metody OpenAPI i uruchamianie skryptów,

Zainstaluj pakiet KlakOAPI z archiwum KlAkOAPI.tar.gz na urządzeniu, na którym zainstalowany jest Serwer administracyjny.

Pakiet KlAkOAPI zawiera zestaw próbek wykonujących typowe operacje. Możesz wywoływać metody OpenAPI, wykonywać próbki i własne skrypty tylko na urządzeniach, na których zainstalowano Serwer administracyjny i pakiet KlAkOAPI. Archiwum KlAkOAPI.tar.gz zawierające ten pakiet znajduje się w folderze instalacyjnym Kaspersky Security Center Linux.

Dopasowywanie scenariuszy użytkowników i próbek metod Kaspersky Security Center OpenAPI

Próbka	Cel próbki	Scenariusz
Zarejestruj KlAkParams	Możesz wyodrębniać i przetwarzać dane za pomocą struktury danych `KlAkParams`. Przykład pokazuje, jak pracować z tą strukturą danych. Przykładowe dane wyjściowe mogą być prezentowane na różne sposoby. Możesz uzyskać dane, aby wysłać metodę HTTP lub użyć ich w swoim kodzie.	Monitorowanie i raportowanie
Utwórz i usuń hierarchię „główny/podrzędny"	Możesz dodać podrzędny Serwer administracyjny i utworzyć hierarchię „główny/podrzędny". Alternatywnie, możesz odłączyć podrzędny Serwer administracyjny od hierarchii.	Tworzenie hierarchii Serwerów administracyjnych, dodawanie podrzędnego Serwera administracyjnego i usuwanie hierarchii Serwerów administracyjnych
Pobierz pliki listy sieci przez bramę połączenia do określonego hosta	Możesz nawiązać połączenie z Agentem sieciowym na żądanym urządzeniu za pomocą bramy połączenia, a następnie pobrać plik z listą sieci na swoje urządzenie.	Dostosowanie punktów dystrybucji i bram połączenia

Próbka	Cel próbki	Scenariusz
Zainstaluj klucz licencyjny przechowywany w głównym repozytorium Serwera administracyjnego na podrzędnych Serwerach administracyjnych	Możesz połączyć się z głównym Serwerem administracyjnym, pobrać z niego wymagany klucz licencyjny i przesłać go do wszystkich pomocniczych Serwerów administracyjnych znajdujących się w hierarchii.	Licencjonowanie zarządzanych aplikacji
Utwórz raport obowiązujących uprawnień użytkownika	Możesz utworzyć różne raporty. Na przykład, korzystając z tego przykładu, można wygenerować raport o obowiązujących uprawnieniach użytkownika. Ten raport opisuje uprawnienia, jakie użytkownik posiada, w zależności od jego grupy i roli. Raport można pobrać w formacie HTML, PDF lub Excel.	Generowanie i przeglądanie raportu
Uruchom zadanie urządzenia	Możesz nawiązać połączenie z Agentem sieciowym na żądanym urządzeniu za pomocą bramy połączenia, a następnie pobrać żądane zadanie.	Ręczne uruchamianie zadania
Zarejestruj punkty dystrybucji dla urządzeń w grupie	Zarządzane urządzenia można przypisać jako punkty dystrybucji (wcześniej nazywane agentami aktualizacji).	Aktualizowanie baz danych i aplikacji Kaspersky
Wylicz wszystkie grupy	Na grupach administracyjnych możesz wykonać różne akcje. Przykład pokazuje, jak wykonać następujące czynności: • Uzyskaj identyfikator grupy głównej „Zarządzane urządzenia” • Poruszaj się po hierarchii grupy • Pobierz pełną, rozszerzoną hierarchię grup wraz z ich nazwami i zagnieżdżeniem	Konfigurowanie Serwera administracyjnego
Wylicz zadania, przeszukaj statystyki zadań i uruchom zadanie	Możesz znaleźć następujące informacje: • Historia postępu zadania • Aktualny stan zadania • Liczba zadań z różnymi stanami Możesz także uruchomić zadanie. Domyślnie próbka uruchamia zadanie po wygenerowaniu statystyk.	Zarządzanie zadaniami
Utwórz i uruchom zadanie	Możesz utworzyć zadanie. W przykładzie określ następujące parametry zadania: • Typ • Metoda uruchamiania • Nazwa • Grupa urządzeń, dla której będzie używane zadanie Domyślnie, przykład tworzy zadanie typu „Pokaż wiadomość”. Możesz uruchomić to zadanie dla wszystkich zarządzanych urządzeń Serwera administracyjnego. W razie potrzeby możesz określić własne parametry zadania.	Tworzenie zadania
Wylicz klucze licencyjne	Możesz uzyskać listę wszystkich aktywnych kluczy licencyjnych dla aplikacji Kaspersky zainstalowanych na zarządzanych urządzeniach Serwera administracyjnego. Lista zawiera szczegółowe dane o każdym kluczu licencyjnym, takim jak nazwa, typ lub data wygaśnięcia.	Wyświetlanie informacji o używanych kluczach licencyjnych
Utwórz i znajdź użytkownika wewnętrznego	Możesz utworzyć konto do dalszej pracy.	Dodawanie konta użytkownika wewnętrznego
Utwórz kategorię niestandardową	Możesz utworzyć kategorię aplikacji z potrzebnymi parametrami.	Tworzenie kategorii aplikacji z zawartością dodaną ręcznie
Wylicz użytkowników przy użyciu SrvView	Możesz użyć klasy SrvView, aby zażądać szczegółowych informacji z serwera administracyjnego. Na przykład, możesz uzyskać listę użytkowników, korzystając z tego przykładu.	Zarządzanie użytkownikami i rolami użytkowników
Utwórz użytkowników wewnętrznych, utwórz i wyślij e-mailem pakiet instalacyjny Androida	Możesz tworzyć użytkowników wewnętrznych, korzystając z klasy SecurityPolicy, utwórz pakiet instalacyjny Androida i wyślij go do użytkowników pocztą elektroniczną.	Dodawanie konta użytkownika wewnętrznego

Aplikacje współpracujące z Kaspersky Security Center Linux poprzez interfejs OpenAPI

Niektóre aplikacje współpracują z Kaspersky Security Center Linux poprzez interfejs OpenAPI. Do takich aplikacji należą na przykład Kaspersky Anti Targeted Attack Platform lub Kaspersky Security for Virtualization. Może to być również niestandardowa aplikacja kliencka utworzona przez Ciebie w oparciu o OpenAPI.

Aplikacje współpracujące z Kaspersky Security Center Linux poprzez interfejs OpenAPI łączą się z serwerem administracyjnym. Jeżeli skonfigurowano listę zezwolonych adresów IP do łączenia się z serwerem administracyjnym, dodaj adresy IP urządzeń, na których zainstalowane są aplikacje korzystające z Kaspersky Security Center Linux OpenAPI. Aby dowiedzieć się, czy aplikacja, z której korzystasz, działa z interfejsem OpenAPI, zapoznaj się z sekcją pomocy dla tej aplikacji.

Praktyczne zastosowanie aplikacji dla dostawców usługi

Niniejsza sekcja zawiera informacje dotyczące konfiguracji i korzystania z Kaspersky Security Center Linux.

Ta sekcja zawiera zalecenia dotyczące instalacji, konfiguracji i korzystania z aplikacji, a także opisuje sposoby rozwiązywania typowych problemów występujących podczas działania aplikacji.

Planowanie wdrożenia Kaspersky Security Center Linux

Podczas planowania instalacji komponentów Kaspersky Security Center Linux w sieci organizacji należy uwzględnić rozmiar i obszar projektu, a zwłaszcza poniższe czynniki:

- Całkowitą liczbę urządzeń
- Liczbę klientów MSP

Jeden Serwer administracyjny może obsługiwać maksymalnie 50 000 urządzeń. Jeśli całkowita liczba urządzeń w sieci organizacji przekroczy 50 000, wówczas po stronie dostawcy usługi należy zainstalować kilka Serwerów administracyjnych i połączyć je w hierarchię w celu uproszczenia scentralizowanego zarządzania.

Na jednym Serwerze administracyjnym można utworzyć do 500 serwerów wirtualnych, czyli dla każdej grupy 500 klientów MSP potrzebny jest jeden Serwer administracyjny.

Na etapie planowania wdrożenia należy rozważyć przydzielenie do Serwera administracyjnego specjalnego certyfikatu X.509. Przydzielenie certyfikatu X.509 do Serwera administracyjnego może być przydatne między innymi do:

- Sprawdzania ruchu SSL poprzez kończenie żądań SSL na serwerze proxy
- Określenia wymaganych wartości w polach certyfikatu
- Zapewnienia wymaganej siły szyfrowania certyfikatu

Umożliwianie uzyskania dostępu do Serwera administracyjnego przez Internet

Aby zezwolić urządzeniom w sieci klienckiej na dostęp do Serwera administracyjnego poprzez internet, należy udostępnić następujące porty Serwera administracyjnego:

- 13000 TCP — port TLS Serwera administracyjnego do podłączania Agentów sieciowych zainstalowanych w sieci klienckiej
- 8061 TCP — port HTTPS do publikowania pakietów autonomicznych przy użyciu narzędzi Kaspersky Security Center Web Console

- 8060 TCP — port HTTP do publikowania pakietów autonomicznych przy użyciu narzędzi Kaspersky Security Center Web Console
- 13292 TCP — port TLS wymagany tylko tam, gdzie konieczne jest zarządzanie urządzeniami mobilnymi
- 8080 TCP — port HTTPS dla Kaspersky Security Center Web Console

Standardowa konfiguracja Kaspersky Security Center Linux

Jeden lub kilka Serwerów administracyjnych jest instalowanych na serwerach MSP. Liczba Serwerów administracyjnych może zostać wybrana w oparciu o dostępny sprzęt, całkowitą liczbę obsługiwanych klientów MSP lub całkowitą liczbę zarządzanych urządzeń.

Jeden Serwer administracyjny może obsługiwać maksymalnie 50 000 urządzeń. Należy rozważyć możliwość zwiększenia liczby zarządzanych urządzeń w najbliższej przyszłości: wygodniejsze może być podłączenie do jednego Serwera administracyjnego mniejszej liczby urządzeń.

Na jednym Serwerze administracyjnym można utworzyć do 500 serwerów wirtualnych, czyli dla każdej grupy 500 klientów MSP potrzebny jest jeden Serwer administracyjny.

Jeśli jest używanych kilka Serwerów, zalecane jest połączenie ich w hierarchię. Korzystanie z hierarchii Serwerów administracyjnych pozwala uniknąć mieszania zasad i zadań, zarządzać całym zbiorem zarządzanych urządzeń tak, jak by były zarządzane przez jeden Serwer administracyjny, czyli wyszukiwać urządzenia, tworzyć wybory urządzeń oraz generować raporty.

Na każdym serwerze wirtualnym, który odpowiada klientowi MSP, należy wskazać jeden lub kilka punktów dystrybucji. Jeśli klienci MSP i Serwer administracyjny są połączone przez Internet, przydatne może być utworzenie zadania *Pobierz uaktualnienia do repozytoriów punktów dystrybucji* dla punktów dystrybucji, aby mogły one pobierać uaktualnienia bezpośrednio z serwerów Kaspersky, a nie z Serwera administracyjnego.

Jeśli niektóre urządzenia w sieci klienckiej MSP nie mają bezpośredniego dostępu do Internetu, należy przełączyć punkty dystrybucji do trybu bramy połączenia. W tym przypadku Agenty sieciowe na urządzeniach w sieci klienckiej MSP zostaną połączone, w celu dalszej synchronizacji, z Serwerem administracyjnym, ale poprzez bramę, a nie bezpośrednio.

Ponieważ Serwer administracyjny najprawdopodobniej nie będzie mógł przeszukać sieci klienckiej MSP, zalecane jest przekazanie tej funkcji punktowi dystrybucji.

Serwer administracyjny nie będzie mógł wysyłać powiadomień poprzez port UDP o numerze 15000 na zarządzane urządzenia znajdujące się poza NAT w sieci klienckiej MSP. Aby rozwiązać ten problem, we właściwościach urządzeń pełniących rolę punktów dystrybucji i działających w trybie bramy połączenia może być pomocne włączenie trybu stałego połączenia z Serwerem administracyjnym (opcja **Nie odłączaj od Serwera administracyjnego**). Tryb stałego połączenia jest dostępny, jeśli całkowita liczba punktów dystrybucji nie przekracza 300.

Klient MSP może chcieć zarządzać urządzeniami z systemem Android i iOS pracowników. Serwer administracyjny zarządza urządzeniami mobilnymi przez TLS, port TCP 13292.

Informacje o punktach dystrybucji

Urządzenie z zainstalowanym Agentem sieciowym mogą być używane jako punkt dystrybucji. W tym trybie Agent sieciowy może wykonywać następujące funkcje:

- Przesyłać pliki na urządzenia klienckie, w tym:
  - Aktualizacje baz danych i modułów oprogramowania Kaspersky

    Uaktualnienia mogą być pobierane z Serwera administracyjnego lub z serwerów Kaspersky. W drugim przypadku należy utworzyć zadanie *Pobierz uaktualnienia do repozytoriów punktów dystrybucji* dla urządzenia pełniącego rolę punktu dystrybucji.
  - Instalowanie aktualizacji oprogramowania firm trzecich
  - Pakiety instalacyjne
- Instalować oprogramowanie (włączając w to wstępną instalację Agentów sieciowych) na pozostałych urządzeniach.
- Przeszukiwać sieć w celu odnalezienia nowych urządzeń i zaktualizowania informacji o tych istniejących. Punkt dystrybucji może stosować te same metody wykrywania urządzeń co Serwer administracyjny.

Instalacja punktów dystrybucji w sieci organizacji realizuje następujące cele:

- Zmniejsza obciążenie na Serwerze administracyjnym, jeśli działa jako źródło uaktualnień.
- Optymalizuje ruch internetowy, ponieważ, w tym przypadku, każde urządzenie w sieci klienckiej MSP nie musi uzyskać dostępu do serwerów Kaspersky lub Serwera administracyjnego w celu pobrania uaktualnień.
- Zapewnia Serwerowi administracyjnemu dostęp do urządzeń poza NAT (względem Serwera administracyjnego) sieci klienckiej MSP, co umożliwia Serwerowi administracyjnemu wykonanie następujących działań:
  - Wysyłanie powiadomień do urządzeń przez UDP w sieci IPv4 lub IPv6
  - Przeszukiwanie sieci IPv4 lub IPv6
  - Przeprowadzanie wstępnego wdrożenia
  - Pełnienie funkcji serwera push

Punkt dystrybucji jest przydzielony do grupy administracyjnej. W tym przypadku zakres działania punktu dystrybucji obejmuje wszystkie urządzenia w grupie administracyjnej i jej podgrupach. Jednakże urządzenie pełniące funkcję punktu dystrybucji nie musi znajdować się w grupie administracyjnej, do której zostało przydzielone.

Możesz sprawić, że punkt dystrybucji będzie działał jako brama połączenia. W tym przypadku urządzenia objęte zakresem działania tego punktu dystrybucji będą łączyły się z Serwerem administracyjnym poprzez bramę, a nie bezpośrednio. Możesz użyć tego trybu w scenariuszach, które nie zezwalają na nawiązywanie bezpośredniego połączenia między urządzeniami a Agentem sieciowym i Serwerem administracyjnym.

Urządzenia pełniące rolę punktów dystrybucji muszą być chronione, włączając w to ochronę fizyczną, przed wszelkim nieautoryzowanym dostępem.

Hierarchia Serwerów administracyjnych

Niektóre firmy klienckie, na przykład MSP, mogą uruchamiać wiele Serwerów administracyjnych. Niewygodne może być zarządzanie kilkoma oddzielnymi Serwerami administracyjnymi, dlatego dobrym wyjściem jest utworzenie hierarchii. W hierarchii serwer administracyjny oparty na systemie Linux może działać zarówno jako serwer podstawowy, jak i serwer pomocniczy. Podstawowy serwer oparty na systemie Linux może zarządzać serwerami pomocniczymi opartymi na systemie Linux i Windows. Podstawowy serwer oparty na systemie Windows może zarządzać dodatkowym serwerem opartym na systemie Linux.

Zastosowanie konfiguracji „główny/podrzędny" dla dwóch Serwerów administracyjnych oferuje następujące możliwości:

- Podrzędny Serwer administracyjny dziedziczy zasady, zadania, role użytkowników i pakiety instalacyjne z głównego Serwera administracyjnego, zapobiegając w ten sposób powielaniu ustawień.
- Wybory urządzeń na głównym Serwerze administracyjnym mogą zawierać urządzenia z podrzędnych Serwerów administracyjnych.
- Raporty na głównym Serwerze administracyjnym mogą zawierać dane (w tym szczegółowe informacje) z podrzędnych Serwerów administracyjnych.
- Główny Serwer administracyjny może być używany jako źródło aktualizacji dla podrzędnego Serwera administracyjnego.

W zakresie wyżej wymienionych opcji główny Serwer administracyjny odbiera dane tylko z niewirtualnych podrzędnych Serwerów administracyjnych. To ograniczenie nie dotyczy wirtualnych Serwerów administracyjnych, które współdzielą bazę danych ze swoim głównym Serwerem administracyjnym.

Hierarchia Serwerów administracyjnych zapewnia obsługę trybu wielodostępu. Tryb ten umożliwia głównemu administratorowi centralne zarządzanie wieloma klientami niezależnie. Każda organizacja lub biuro będące klientem jest odizolowane od pozostałych i nazywane jest dzierżawcą. Można przydzielić dzierżawcy wiele zarządzanych urządzeń wraz z powiązanymi danymi, ustawieniami, zasadami i zadaniami, a także skonfigurować uprawnienia użytkowników dla poszczególnych dzierżawców.

Główny Serwer administracyjny, zainstalowany w głównej infrastrukturze organizacji, pełni rolę głównego dzierżawcy. Główny Serwer administracyjny umożliwia podrzędnym lub wirtualnym Serwerom administracyjnym — jego odizolowanym dzierżawcom — niezależne odbieranie i przetwarzanie własnych zdarzeń oraz pracę z własnymi zasobami, usługami i konfiguracjami.

Dostawca usług, który ma klientów z wielu organizacji klienta, może udostępnić funkcjonalność Kaspersky Security Center Linux, w tym agregację alertów i działania reagowania, każdej organizacji klienta niezależnie. Aby to osiągnąć, dostawca usług łączy podrzędne lub wirtualne Serwery administracyjne jako dzierżawców dla każdej organizacji klienta. Dostawca usług świadczy usługi przy użyciu własnego personelu i zasobów.

Wirtualne Serwery administracyjne

W oparciu o fizyczny Serwer administracyjny można utworzyć kilka wirtualnych Serwerów administracyjnych, które będą podobne do podrzędnych Serwerów administracyjnych. W przeciwieństwie do trybu poufnego dostępu, który jest oparty na listach kontroli dostępu (ACL), tryb wirtualnego Serwera administracyjnego jest bardziej funkcjonalny i zapewnia większy stopień izolacji. Jako dodatek do dedykowanej struktury grup administracyjnych dla przypisanych urządzeń z zasadami i zadaniami, każdy wirtualny Serwer administracyjny zawiera swoją grupę nieprzypisanych urządzeń, własne zestawy raportów, wybranych urządzeń i zdarzeń, pakietów instalacyjnych, reguł przenoszenia itd. Dla maksymalnej wspólnej izolacji klientów MSP zalecane jest wybranie wirtualnych Serwerów administracyjnych jako funkcjonalności, która ma zostać użyta. Dodatkowo, utworzenie wirtualnego Serwera administracyjnego dla każdego klienta MSP umożliwia zapewnienie klientom podstawowych opcji zarządzania siecią za pośrednictwem Kaspersky Security Center Web Console.

Wirtualne Serwery administracyjne są bardzo podobne do podrzędnych Serwerów administracyjnych, jednakże posiadają pewne różnice:

- Wirtualny Serwer administracyjny nie posiada większości ustawień globalnych i swoich własnych portów TCP.
- Wirtualny Serwer administracyjny nie posiada podrzędnych Serwerów administracyjnych.
- Wirtualny Serwer administracyjny nie posiada innych wirtualnych Serwerów administracyjnych.
- Fizyczny Serwer administracyjny wyświetla urządzenia, grupy, zdarzenia i obiekty na zarządzanych urządzeniach (elementy w Kwarantannie, rejestrze aplikacji itd.) ze wszystkich swoich wirtualnych Serwerów administracyjnych.
- Wirtualny Serwer administracyjny może skanować sieć wyłącznie przy podłączonych punktach dystrybucji.

Instalacja i wstępna konfiguracja

Kaspersky Security Center Linux jest aplikacją oferującą wiele funkcji. Kaspersky Security Center Linux zawiera następujące komponenty:

- Serwer administracyjny—główny komponent, zaprojektowany do zarządzania urządzeniami w organizacji i przechowywania danych w DBMS.
- Kaspersky Security Center Web Console to interfejs sieciowy dla Serwera administracyjnego, zaprojektowany do wykonywania podstawowych działań. Możesz zainstalować ten komponent na dowolnym urządzeniu, które spełnia wymagania sprzętowe i programowe.
- Agent sieciowy — zaprojektowany do zarządzania aplikacją zabezpieczającą, zainstalowaną na urządzeniu, a także do zbierania informacji o tym urządzeniu. Agenty sieciowe są instalowane na urządzeniach w organizacji.

Wdrożenie Kaspersky Security Center Linux w sieci organizacji odbywa się w następujący sposób:

- Instalacja Serwera administracyjnego
- Instalacja Kaspersky Security Center Web Console
- Instalacja Agenta sieciowego i aplikacji zabezpieczającej na urządzeniach w firmie

Zalecenia dotyczące instalacji Serwera administracyjnego

Ta sekcja zawiera zalecenia dotyczące instalacji Serwera administracyjnego. Opisane są tu także scenariusze korzystania z folderu współdzielonego na urządzeniu z Serwerem administracyjnym w celu zainstalowania Agenta sieciowego na urządzeniach klienckich.

Tworzenie kont dla usług Serwera administracyjnego na klastrze typu failover

Przed rozpoczęciem wdrażania Kaspersky Security Center Linux w klastrze trybu failover należy utworzyć konta dla usług Kaspersky Security Center Linux.

W tym celu wykonaj następujące czynności na węźle aktywnym, węźle pasywnym i serwerze plików:

1. Utwórz grupę o nazwie „kladmins" i przypisz ten sam GID wszystkim trzem grupom.
2. Utwórz konto użytkownika o nazwie „ksc" i przypisz ten sam identyfikator UID do wszystkich trzech kont użytkowników. Ustaw grupę podstawową na „kladmins" dla utworzonych kont.
3. Utwórz konto użytkownika o nazwie „rightless" i przypisz ten sam identyfikator UID do wszystkich trzech kont użytkowników. Ustaw grupę podstawową na „kladmins" dla utworzonych kont.

Wybieranie systemu zarządzania bazą danych

Poniższa tabela zawiera listę prawidłowych opcji DBMS, a także zalecenia i ograniczenia dotyczące ich używania.

Zalecenia i ograniczenia dotyczące DBMS

DBMS	Zalecenia i ograniczenia
MySQL (zobacz obsługiwane wersje)	Użyj tego DBMS, jeśli zamierzasz uruchomić pojedynczy Serwer administracyjny dla mniej niż 20 000 urządzeń.
MariaDB (zobacz obsługiwane wersje)	Użyj tego DBMS, jeśli zamierzasz uruchomić pojedynczy Serwer administracyjny dla mniej niż 20 000 urządzeń.
PostgreSQL, Postgres Pro (zobacz obsługiwane wersje)	Użyj tego DBMS, jeśli zamierzasz uruchomić pojedynczy Serwer administracyjny dla mniej niż 50 000 urządzeń.
Tantor (zobacz obsługiwane wersje)	Użyj tego DBMS, jeśli zamierzasz uruchomić pojedynczy Serwer administracyjny dla mniej niż 50 000 urządzeń. System DBMS Tantor jest obsługiwany tylko w Astra Linux Special Edition RUSB.10015-01 (aktualizacja operacyjna 1.8).

Informacje o sposobie zainstalowania wybranego systemu DBMS znajdziesz w tym dokumencie.

Zaleca się wyłączenie zadania Inwentaryzacja oprogramowania i wyłączenie (w ustawieniach zasad Kaspersky Endpoint Security) powiadomień Serwera administracyjnego o uruchomionych aplikacjach.

> Jeśli zdecydujesz się zainstalować PostgreSQL lub Postgres Pro DBMS, upewnij się, że określone zostało hasło superużytkownika. Jeśli hasło nie zostanie określone, Serwer administracyjny może nie być w stanie połączyć się z bazą danych.

Jeśli instalujesz MySQL, MariaDB, PostgreSQL lub Postgres Pro, użyj zalecanych ustawień, aby zapewnić prawidłowe działanie DBMS.

Jeśli używasz systemu PostgreSQL, MariaDB lub MySQL DBMS, karta **Zdarzenia** może wyświetlać niekompletną listę zdarzeń dla wybranego urządzenia klienckiego. Dzieje się tak, gdy system DBMS przechowuje bardzo dużą liczbę zdarzeń. Liczbę wyświetlanych zdarzeń można zwiększyć, wykonując jedną z następujących czynności:

- Usuwanie niepotrzebnych zdarzeń.
- Skrócenie okresu przechowywania niepotrzebnych zdarzeń.

Aby zobaczyć pełną listę zdarzeń zarejestrowanych na Serwerze administracyjnym dla danego urządzenia, należy użyć opcji Raporty.

Określanie adresu Serwera administracyjnego

Podczas instalacji Serwera administracyjnego należy określić nazwę DNS lub statyczny adres IP Serwera administracyjnego. Podczas tworzenia pakietów instalacyjnych Agenta sieciowego ten adres będzie używany jako domyślny. Wówczas możliwa będzie zmiana adresu komputera z Serwerem administracyjnym przy użyciu narzędzi Kaspersky Security Center Web Console; adres nie zostanie zmieniony automatycznie w już utworzonych pakietach instalacyjnych Agenta sieciowego.

Utrzymywanie bezczynnych połączeń

Zalecamy skonfigurowanie następujących parametrów keepalive na urządzeniach bramy połączenia w celu poprawy stabilności połączenia:

- `net.ipv4.tcp_keepalive_intvl` określa, jak często wysyłać wiadomości keepalive po pierwszej. Ustaw ten parametr na `1`.
- `net.ipv4.tcp_keepalive_probes` określa, ile wiadomości keepalive może zostać wysłanych bez odpowiedzi, zanim połączenie zostanie uznane za martwe. Ustaw ten parametr na `10`.
- Parametr `net.ipv4.tcp_keepalive_time` określa czas oczekiwania po ostatnim pakiecie danych przed wysłaniem pierwszej wiadomości keepalive. Ustaw ten parametr na `900`.

Aby skonfigurować parametry keepalive:

1. Otwórz plik /etc/sysctl.conf.

2. Dodaj następujące wartości parametrów:

```
net.ipv4.tcp_keepalive_intvl = 1
net.ipv4.tcp_keepalive_probes = 10
net.ipv4.tcp_keepalive_time = 900
```

3. Uruchom następujące polecenie, aby zaktualizować parametry keepalive:

```
sudo sysctl -p /etc/sysctl.conf
```

4. Uruchom następujące polecenia, aby upewnić się, że wartości parametrów zostały zastosowane:

```
sudo sysctl net.ipv4.tcp_keepalive_intvl
sudo sysctl net.ipv4.tcp_keepalive_probes
sudo sysctl net.ipv4.tcp_keepalive_time
```

Wdrażanie Agenta sieciowego i aplikacji zabezpieczających

Aby zarządzać urządzeniami w organizacji i chronić je przed zagrożeniami bezpieczeństwa, należy zainstalować na każdym z nich Agenta sieciowego i aplikację zabezpieczającą Kaspersky.

Informacje na temat wdrażania ochrony można znaleźć w sekcji Wdrażanie Agenta sieciowego i aplikacji zabezpieczających.

Informacje na temat ochrony urządzeń mobilnych można znaleźć w sekcji Zarządzanie urządzeniami mobilnymi.

W systemie Microsoft Windows XP Agent sieciowy może nie wykonać poprawnie następujących działań: pobranie uaktualnień bezpośrednio z serwerów Kaspersky (jako punkt dystrybucji) i działanie jako serwer proxy KSN (jako punkt dystrybucji); oraz wykrywanie luk firm trzecich (jeśli używane jest Zarządzanie lukami i poprawkami).

Konfigurowanie ochrony w sieci organizacji klienta

Po zakończeniu instalacji Serwera administracyjnego, zostaje uruchomiona Kaspersky Security Center Web Console, która oferuje przeprowadzenie wstępnej konfiguracji przy użyciu odpowiedniego kreatora. Jeśli kreator wstępnej konfiguracji jest uruchomiony, w głównej grupie administracyjnej tworzone są następujące zasady i zadania:

- Zasada Kaspersky Endpoint Security
- Grupowe zadanie aktualizacji Kaspersky Endpoint Security
- Grupowe zadanie skanowania urządzenia z zainstalowanym programem Kaspersky Endpoint Security

- Zasada Agenta sieciowego
- Zadanie wykrywania luk (zadanie Agenta sieciowego)
- Zadanie instalacji uaktualnień i naprawy luk (zadanie Agenta sieciowego)

Zasady i zadania są tworzone z domyślnymi ustawieniami, które mogą okazać się nieoptymalne lub nawet niedopuszczalne dla organizacji. Dlatego też należy sprawdzić właściwości utworzonych obiektów i zmodyfikować je ręcznie (jeśli zajdzie taka konieczność).

Ta sekcja zawiera informacje dotyczące ręcznej konfiguracji zasad, zadań i innych ustawień Serwera administracyjnego, a także informacje o punkcie dystrybucji, tworzeniu struktury grup administracyjnych i hierarchii zadań oraz innych ustawień.

Ręczna konfiguracja zasady Kaspersky Endpoint Security

W tej sekcji można znaleźć zalecenia dotyczące konfiguracji zasady Kaspersky Endpoint Security, który jest tworzony przez Kreator wstępnej konfiguracji. Możesz przeprowadzić konfigurację w oknie właściwości zasady.

Edytując ustawienie, pamiętaj, że możesz je zablokować lub odblokować, aby uniemożliwić lub zezwolić na edycję jego wartości na stacji roboczej.

Konfigurowanie zasady w sekcji Zaawansowana ochrona przed zagrożeniami

Pełny opis ustawień w tej sekcji można znaleźć w dokumentacji do Kaspersky Endpoint Security for Windows.

W sekcji **Zaawansowana ochrona przed zagrożeniami** możesz skonfigurować używanie Kaspersky Security Network dla Kaspersky Endpoint Security for Windows. Możesz także skonfigurować moduły Kaspersky Endpoint Security for Windows, takie jak Wykrywanie zachowań, Ochrona przed exploitami, Ochrona przed włamaniami oraz Silnik korygujący.

W podsekcji **Kaspersky Security Network** zalecane jest włączenie opcji **Kaspersky Security Network**. Użyj tej opcji do redystrybucji i optymalizacji ruchu w sieci. Jeśli opcja **Kaspersky Security Network** jest wyłączona, możesz włączyć bezpośrednie korzystanie z serwerów KSN.

Konfigurowanie zasady w sekcji Podstawowa ochrona przed zagrożeniami

Pełny opis ustawień w tej sekcji można znaleźć w dokumentacji do Kaspersky Endpoint Security for Windows.

W sekcji **Essential Threat Protection** okna właściwości zasad, zalecamy określenie dodatkowych ustawień w podsekcjach **Firewall** i **Ochrona plików**.

Podsekcja **Firewall** zawiera ustawienia, które pozwalają kontrolować aktywność sieciową aplikacji na urządzeniach klienckich. Urządzenie klienckie korzysta z sieci, do której przypisany jest jeden z następujących statusów: publiczny, lokalny lub zaufany. W zależności od stanu sieci, Kaspersky Endpoint Security może zezwolić na aktywność sieciową na urządzeniu lub jej zabronić. Gdy dodajesz nową sieć do swojej organizacji, musisz przypisać jej odpowiedni status sieci. Na przykład, jeśli urządzeniem klienckim jest laptop, zalecamy, aby to urządzenie korzystało z sieci publicznej lub zaufanej, ponieważ laptop nie zawsze jest podłączony do sieci lokalnej. W podsekcji **Firewall** możesz sprawdzić, czy prawidłowo przypisano stany do sieci używanych w Twojej organizacji.

W celu sprawdzenia listy sieci:

1. We właściwościach zasady przejdź do **Essential Threat Protection** → **Firewall**.
2. W sekcji **Available networks** kliknij przycisk **Settings**.
3. W **Firewall**, które zostanie otwarte, przejdź do zakładki **Sieci**, aby wyświetlić listę sieci.

W podsekcji **Ochrona plików** możesz wyłączyć skanowanie dysków sieciowych. Skanowanie dysków sieciowych może spowodować znaczne obciążenie dysków sieciowych. Praktyczniejsze jest wykonywanie bezpośredniego skanowania na serwerach plików.

W celu wyłączenia skanowania dysków sieciowych:

1. We właściwościach zasady przejdź do **Essential Threat Protection** → **Ochrona plików**.
2. W sekcji **Security level** kliknij przycisk **Settings**.
3. W otwartym oknie **Ochrona plików**, na zakładce **General** odznacz pole **All network drives**.

Konfigurowanie zasady w sekcji Ustawienia ogólne

Pełny opis ustawień w tej sekcji można znaleźć w dokumentacji do Kaspersky Endpoint Security.

Poniżej opisano zaawansowane działania, które zalecamy wykonać w oknie właściwości zasady programu Kaspersky Endpoint Security w sekcji **Ustawienia ogólne**.

Sekcja Ustawienia ogólne, podsekcja Raporty i pliki danych

W sekcji **Transfer danych do Serwera administracyjnego** zaznacz pole **Informacje o uruchomionych aplikacjach**. Jeśli to pole jest zaznaczone, bazy danych Serwera administracyjnego zapisują informacje o wszystkich wersjach wszystkich modułów oprogramowania na urządzeniach w sieci. Informacje mogą wymagać znaczącej ilości miejsca na dysku dla bazy danych Kaspersky Security Center Linux (kilkadziesiąt gigabajtów). Dlatego, jeśli pole **Informacje o uruchomionych aplikacjach** jest cały czas zaznaczone w zasadzie o najwyższym poziomie, musi ono zostać odznaczone.

Sekcja Ustawienia ogólne, podsekcja Interfejs

Jeśli ochrona antywirusowa w sieci organizacji musi być zarządzana w sposób scentralizowany poprzez Kaspersky Security Center Web Console, musisz wyłączyć wyświetlanie interfejsu Kaspersky Endpoint Security na stacjach roboczych (odznaczając pole **Wyświetl interfejs aplikacji** w sekcji **Interakcja z użytkownikiem**) oraz włączyć na nich ochronę hasłem (zaznaczając pole **Włącz ochronę hasłem** w sekcji **Ochrona hasłem**).

Konfigurowanie zasad w sekcji Konfiguracja zdarzenia

W sekcji **Konfiguracja zdarzenia** należy wyłączyć zapisywanie wszystkich zdarzeń na Serwerze administracyjnym, za wyjątkiem następujących:

- Na zakładce **Krytyczny**:
  - *Application autorun is disabled*
  - *Access denied*
  - *Application startup prohibited*
  - *Disinfection impossible*
  - *End User License Agreement violated*
  - *Could not load encryption module*
  - *Cannot start two tasks at the same time*
  - *Active threat detected. Advanced Disinfection should be started*
  - *Network attack detected*
  - *Not all components were updated*
  - *Activation error*
  - *Error enabling portable mode*
  - *Error in interaction with Kaspersky Security Center*
  - *Error disabling portable mode*
  - *Error changing application components*
  - *Error applying file encryption / decryption rules*
  - *Policy cannot be applied*
  - *Process terminated*
  - *Network activity blocked*
- Na zakładce **Błąd funkcjonalny**: *Invalid task settings. Settings not applied*

- Na karcie **Ostrzeżenie**:
  - *Self-Defense is disabled*
  - *Incorrect reserve key*
  - *User has opted out of the encryption policy*
- Na karcie **Informacja**: *Zabroniono uruchomienia aplikacji w trybie testowym*

Ręczna konfiguracja grupowego zadania aktualizacji dla Kaspersky Endpoint Security

Jeśli Serwer administracyjny pełni rolę źródła uaktualnień, optymalną i zalecaną opcją terminarza dla Kaspersky Endpoint Security jest **Po pobraniu nowych uaktualnień do repozytorium**, gdy zaznaczone jest pole **Używaj automatycznie losowego opóźnienia dla uruchamiania zadań**.

Jeśli lokalne zadanie pobierania uaktualnień z serwerów Kaspersky do repozytorium jest tworzone na każdym punkcie dystrybucji, okresowe planowanie będzie optymalne i zalecane dla grupowego zadania aktualizacji Kaspersky Endpoint Security. W tym przypadku, dla przedziału randomizacji należy wybrać wartość - 1 godzina.

Ręczna konfiguracja grupowego zadania skanowania urządzeń z zainstalowanym programem Kaspersky Endpoint Security

Kreator wstępnej konfiguracji tworzy grupowe zadanie skanowania urządzeń. Jeżeli automatycznie określony harmonogram zadania skanowania grupowego nie jest odpowiedni dla Twojej organizacji, musisz ręcznie ustawić najdogodniejszy harmonogram tego zadania na podstawie zasad przyjętych w organizacji.

Domyślnie skonfigurowano terminarz **uruchamiania zadania we wtorki o godzinie 19:00** z automatyczną randomizacją i zaznaczonym polem **Uruchom pominięte zadania**. Oznacza to, że jeśli urządzenia w organizacji są wyłączone w piątki, na przykład o godzinie 18:30, zadanie skanowania urządzeń nigdy nie zostanie uruchomione. W takim przypadku musisz ręcznie skonfigurować zadanie skanowania grupowego.

Konfigurowanie terminarza zadania Wyszukiwanie luk i wymaganych aktualizacji

Kreator wstępnej konfiguracji tworzy dla Agenta sieciowego zadanie *Wyszukiwanie luk i wymaganych aktualizacji.* Domyślnie skonfigurowano terminarz **uruchamiania zadania we wtorki o godzinie 19:00** z automatyczną randomizacją i zaznaczonym polem **Uruchom pominięte zadania**.

Jeśli zasady obowiązujące w organizacji nakazują wyłączenie wszystkich urządzeń w tym czasie, zadanie *Wyszukiwanie luk i wymaganych aktualizacji* zostanie uruchomione, gdy urządzenia znowu zostaną włączone, czyli w środę rano. Takie działanie nie jest wskazane, ponieważ wykrywanie luk może zwiększać zużycie procesora i obciążenie podsystemów dysku. Terminarz dla tego zadania należy skonfigurować w oparciu o zasady obowiązujące w organizacji.

Ręczna konfiguracja grupowego zadania instalacji uaktualnień i naprawy luk

Kreator wstępnej konfiguracji tworzy dla Agenta sieciowego grupowe zadanie instalacji uaktualnień i naprawy luk. Domyślnie skonfigurowano terminarz uruchamiania zadania codziennie o godzinie 01:00 z automatyczną randomizacją i wyłączoną opcją **Uruchom pominięte zadania**.

Jeśli reguły obowiązujące w organizacji nakazują wyłączanie urządzeń na noc, zadanie instalacji uaktualnień nigdy nie zostanie uruchomione. Terminarz dla zadania wykrywania luk należy skonfigurować w oparciu o zasady obowiązujące w organizacji. Należy pamiętać, że zadanie instalacji uaktualnień może wymagać ponownego uruchomienia urządzenia.

Tworzenie struktury grup administracyjnych i przydzielanie punktów dystrybucji

Struktura grup administracyjnych w Kaspersky Security Center Linux pełni następujące funkcje:

- Tworzy zakres zasad.

  Istnieje alternatywny sposób stosowania odpowiednich ustawień na urządzeniach przy użyciu profili zasad. W takim przypadku, zakres zasad jest ustawiany, na przykład za pomocą znaczników urządzeń lub ról użytkownika.

- Tworzy zakres zadań grupowych.

  Istnieje sposób określania zakresu zadań grupowych, który nie jest oparty na hierarchii grup administracyjnych: korzystanie z zadań dla wyboru urządzeń oraz z zadań dla określonych urządzeń.

- Nadaje urządzeniom, wirtualnym Serwerom administracyjnym oraz podrzędnym Serwerom administracyjnym prawa dostępu.

- Przypisuje punkty dystrybucji.

Podczas tworzenia struktury grup administracyjnych należy wziąć pod uwagę topologię sieci organizacji dla optymalnego przydzielenia punktów dystrybucji. Optymalne przydzielenie punktów dystrybucji pozwala na zmniejszenie ruchu w sieci organizacji.

W zależności od schematu organizacyjnego oraz topologii sieci zaadaptowanej przez klienta MSP, w strukturze grup administracyjnych można zastosować następujące standardowe konfiguracje:

- Jedno biuro

- Wiele małych, oddzielonych od siebie biur

Standardowa konfiguracja klienta MSP: Jedno biuro

W standardowej konfiguracji „jedno biuro” wszystkie urządzenia znajdują się w obrębie sieci organizacji i są dla siebie widoczne. Sieć organizacji może zawierać kilka oddzielnych części (sieci lub fragmentów sieci) połączonych ze sobą wąskimi kanałami.

Dostępne są następujące metody tworzenia struktury grup administracyjnych:

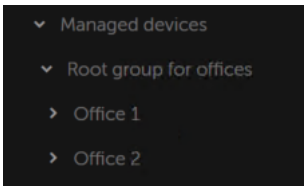
- Tworzenie struktury grup administracyjnych z uwzględnieniem topologii sieci. Struktura grup administracyjnych nie musi odzwierciedlać topologii sieci z absolutną dokładnością. Wystarczy dopasowanie oddzielnych części sieci i pewnych grup administracyjnych. Możesz skorzystać z automatycznego przydzielenia punktów dystrybucji lub zrobić to ręcznie.

- Tworzenie struktury grup administracyjnych bez uwzględnienia topologii sieci. W tym przypadku należy wyłączyć automatyczne przydzielanie punktów dystrybucji, a następnie wskazać jedno lub kilka urządzeń jako punkty dystrybucji dla głównej grupy administracyjnej w każdej z oddzielnych części sieci, na przykład dla grupy **Zarządzane urządzenia**. Wszystkie punkty dystrybucji będą na tym samym poziomie i będą obejmować ten sam obszar, uwzględniając wszystkie urządzenia w sieci organizacji. W takim przypadku każdy z Agentów sieciowych połączy się z punktem dystrybucji o najkrótszej trasie. Trasę do punktu dystrybucji można ustalić za pomocą narzędzia tracert lub traceroute.

Standardowa konfiguracja klienta MSP: Wiele małych, zdalnych biur

Ta standardowa konfiguracja została utworzona z myślą o małych zdalnych biurach, które mogą kontaktować się z główną siedzibą za pośrednictwem Internetu. Każde zdalne biuro znajduje się poza NAT, czyli połączenie jednego zdalnego biura z innym jest niemożliwe, gdyż biura są od siebie odizolowane.

Konfiguracja musi być odzwierciedlona w strukturze grup administracyjnych: dla każdego zdalnego biura musi zostać utworzona oddzielna grupa administracyjna (grupy **Office 1** i **Office 2** na rysunku poniżej).



Zdalne biura uwzględnione w strukturze grupy administracyjnej

Do każdej grupy administracyjnej odpowiadającej biuru należy przydzielić jeden lub kilka punktów dystrybucji. Punktami dystrybucji muszą być urządzenia w zdalnym biurze, które posiadają wystarczającą ilość wolnego miejsca na dysku. Urządzenia z grupy **Office 1** będą, na przykład, łączyć się z punktami dystrybucji przydzielonymi do grupy administracyjnej **Office 1**.

Jeśli niektórzy użytkownicy poruszają się między biurami ze swoimi laptopami, w każdym zdalnym biurze, dla grupy administracyjnej najwyższego poziomu (**Główna grupa dla biur** na poniższym rysunku) należy wskazać dwa lub więcej urządzeń jako punkty dystrybucji (oprócz już istniejących punktów dystrybucji).

Na przykład: Laptop znajduje się w grupie administracyjnej **Office 1**, a następnie zostaje fizycznie przeniesiony do biura, które odpowiada grupie administracyjnej **Office 2**. Po przeniesieniu laptopa, Agent sieciowy spróbuje połączyć się z punktami dystrybucji przypisanymi do grupy **Office 1**, ale te punkty dystrybucji są niedostępne. Następnie Agent sieciowy próbuje połączyć się z punktami dystrybucji, które zostały przypisane do **Głównej grupy dla biur**. Ponieważ zdalne biura są odizolowane od siebie, próby nawiązania połączenia z punktami dystrybucji przypisanymi do grupy administracyjnej **Główna grupa dla biur** zakończą się pomyślnie tylko wtedy, gdy Agent sieciowy spróbuje połączyć się z punktami dystrybucji w grupie **Office 2**. Oznacza to, że laptop pozostanie w grupie administracyjnej, która odpowiada pierwszemu biuru, ale będzie korzystał z punktu dystrybucji biura, w którym aktualnie się znajduje.

Hierarchia zasad i korzystanie z zasad

W tej sekcji można znaleźć informacje dotyczące stosowania zasad do urządzeń w grupach administracyjnych. Ta sekcja zawiera również informacje o profilach zasad.

Hierarchia zasad

W Kaspersky Security Center Linux zasad są używane do określenia jednego zestawu ustawień dla kilku urządzeń. Na przykład, obszar zasady aplikacji P zdefiniowanej dla grupy administracyjnej G zawiera zarządzane urządzenia z zainstalowaną aplikacją P, które zostały dodane do grupy G i wszystkich jej podgrup, za wyjątkiem podgrup, we właściwościach których odznaczono opcję **Dziedzicz z grupy nadrzędnej**.

Zasadę można odróżnić od lokalnego ustawienia po ikonach kłódki (🔒) obok jej ustawień. Jeśli ustawienie (lub grupa ustawień) jest zablokowane we właściwościach zasady, w pierwszej kolejności należy użyć tego ustawienia (lub grupy ustawień) podczas tworzenia obowiązującego ustawienia, a następnie należy zapisać ustawienie (lub grupę ustawień) do zasady podrzędnej.

Tworzenie obowiązujących ustawień można opisać w następujący sposób: wartości wszystkich ustawień, które nie zostały zablokowane, są kopiowane z zasady, a następnie są nadpisywane przez wartości ustawień lokalnych, a w kolejnym etapie wartości wynikowe są nadpisywane przez zablokowane ustawienia pobrane z zasady.

Zasady tej samej aplikacji oddziałują na siebie poprzez hierarchię grup administracyjnych: Zablokowane ustawienia z zasady nadrzędnej nadpisują te same ustawienia z zasady podrzędnej.

Dla użytkowników mobilnych istnieje specjalna zasada. Ta zasada jest aktywowana na urządzeniu, gdy to przełącza się do trybu użytkownika mobilnego. Zasady użytkowników mobilnych nie oddziałują na inne zasady poprzez hierarchię grup administracyjnych.

Profile zasad

Stosowanie zasad na urządzeniach tylko poprzez hierarchię grup administracyjnych może być niewygodne tylko w kilku przypadkach. Konieczne może być utworzenie kilku instancji jednej zasady, które różnią się jednym lub dwoma ustawieniami dla różnych grup administracyjnych, oraz zsynchronizowanie zawartości tych zasad w przyszłości.

Aby pomóc Ci uniknąć takich problemów, Kaspersky Security Center Linux obsługuje *profile zasad*. Profil zasad jest to inaczej podzbiór ustawień zasady. Ten podzbiór jest stosowany na urządzeniach docelowych wraz z zasadą i uzupełnia go zgodnie z określonym warunkiem zwanym *warunkiem aktywacji profilu*. Profile mogą zawierać tylko ustawienia różniące się od „podstawowej" zasady, która jest aktywna na urządzeniu klienckim (komputerze lub urządzeniu mobilnym). Aktywacja profilu zmodyfikuje ustawienia zasad, które były aktywne na urządzeniu przed aktywacją profilu. Te ustawienia przyjmują wartości określone w profilu.

Aktualnie na profile zasad nałożone są następujące ograniczenia:

- Zasada może zawierać maksymalnie 100 profili.
- Profil zasad nie może zawierać innych profili.
- Profil zasad nie może zawierać ustawień powiadamiania.

Zawartość profilu

Profil zasad zawiera następujące elementy:

- Nazwa. Profile z takimi samymi nazwami wpływają na siebie poprzez hierarchię grup administracyjnych ze wspólnymi regułami.
- Podzbiór ustawień zasady. Profil zawiera tylko aktualnie wymagane ustawienia (ustawienia zablokowane).
- Warunek aktywacji to wyrażenie logiczne z właściwościami urządzenia. Profil jest aktywny (uzupełnia zasadę) tylko wtedy, gdy warunek aktywacji profilu jest prawdziwy. We wszystkich pozostałych przypadkach profil jest nieaktywny i jest ignorowany. W wyrażeniu logicznym mogą być uwzględnione następujące właściwości urządzenia:
  - Stan trybu użytkownika mobilnego.
  - Właściwości środowiska sieciowego — nazwa aktywnej reguły dla połączenia z Agentem sieciowym.
  - Obecność lub brak określonych znaczników na urządzeniu.
  - Lokalizacja urządzenia w jednostce Active Directory: jawna (urządzenie znajduje się w określonej jednostce OU) lub niejawna (urządzenie jest w jednostce OU, która znajduje się w określonej jednostce OU na dowolnym poziomie zagnieżdżenia).
  - Członkostwo urządzenia w grupie zabezpieczeń Active Directory (jawne lub niejawne).
  - Członkostwo właściciela urządzenia w grupie zabezpieczeń Active Directory (jawne lub niejawne).
- Pole wyłączające profil. Wyłączone profile są zawsze ignorowane, a ich odpowiednie warunki aktywacji nie są sprawdzane.
- Priorytet profilu. Warunki aktywacji różnych profili są niezależne, a więc można aktywować kilka profili jednocześnie. Jeśli aktywne profile zawierają nienakładające się na siebie zbiory ustawień, nie pojawi się żaden problem. Jednakże dwa aktywne profile zawierające różne wartości tego samego ustawienia spowodują niejednoznaczność. Tę niejednoznaczność można wyeliminować poprzez priorytety profilu: Wartość niejednoznacznej zmiennej zostanie pobrana z profilu, który ma wyższy priorytet (ten, który znajduje się wyżej na liście profili).

Zachowanie profili, gdy zasady oddziałują na siebie poprzez hierarchię

Profile o tych samych nazwach zostają scalone zgodnie z regułami scalania zasad. Profile zasady nadrzędnej mają wyższy priorytet niż zasady podrzędnej. Jeśli modyfikowanie ustawień jest zabronione w zasadzie nadrzędnej (są zablokowane), zasada podrzędna używa warunków aktywacji profilu z zasady nadrzędnej. Jeśli modyfikowanie ustawień jest dozwolone w zasadzie nadrzędnej, używane są warunki aktywacji profilu z zasady podrzędnej.

Ponieważ w swoim warunku aktywacji profil zasad może zawierać opcję **Urządzenie jest w trybie offline**, profile całkowicie zastępują funkcję zasad dla użytkowników mobilnych, które nie będą już obsługiwane.

Zasada dla użytkowników mobilnych może zawierać profile, ale te profile mogą zostać aktywowane dopiero po przełączeniu urządzenia w tryb użytkownika mobilnego.

Zadania

Kaspersky Security Center Linux zarządza aplikacjami zabezpieczającymi Kaspersky, zainstalowanymi na urządzeniach poprzez tworzenie i uruchamianie *zadań*. Zadania są potrzebne do instalowania, uruchamiania i zatrzymywania działania aplikacji, skanowania plików, aktualizowania baz danych i modułów aplikacji, a także wykonywania innych działań na aplikacjach.

Zadania dla określonej aplikacji mogą być tworzone tylko wtedy, gdy zainstalowana jest wtyczka zarządzająca dla tej aplikacji.

Zadania mogą być wykonywane na Serwerze administracyjnym i na urządzeniach.

Na Serwerze administracyjnym wykonywane są następujące zadania:

- Automatyczne rozsyłanie raportów
- Pobieranie uaktualnień do repozytorium Serwera administracyjnego
- Tworzenie kopii zapasowych danych Serwera administracyjnego
- Obsługa baz danych

Na urządzeniach wykonywane są następujące typy zadań:

- *Zadania lokalne*—zadania wykonywane na określonym urządzeniu

  Zadania lokalne mogą zostać zmodyfikowane zarówno przez administratora przy użyciu narzędzi Kaspersky Security Center Web Console lub przez użytkownika zdalnego urządzenia (na przykład z poziomu interfejsu aplikacji zabezpieczającej). Jeśli zadanie lokalne zostało zmodyfikowane jednocześnie przez administratora i użytkownika zarządzanego urządzenia, zostaną zastosowane zmiany wprowadzone przez administratora, ponieważ mają wyższy priorytet.

- *Zadania grupowe*—zadania wykonywane na wszystkich urządzeniach określonej grupy

  Dopóki nie określono inaczej we właściwościach zadania, zadanie grupowe także wpływa na wszystkie podgrupy wybranej grupy. Zadanie grupowe także może wpływać (opcjonalnie) na urządzenia, które zostały podłączone do podrzędnych i wirtualnych Serwerów administracyjnych zainstalowanych w grupie lub w jej dowolnej podgrupie.

- *Zadania globalne*—zadania wykonywane na zbiorze urządzeń, niezależnie od tego, czy znajdują się w jakiejkolwiek grupie

Dla każdej aplikacji można utworzyć dowolną liczbę zadań grupowych, zadań globalnych lub zadań lokalnych.

Możesz wprowadzać zmiany w ustawieniach zadań, przeglądać postęp ich wykonywania, a także kopiować, eksportować, importować i usuwać zadania.

Zadanie jest uruchamiane na urządzeniu tylko wtedy, gdy uruchomiona jest aplikacja, dla której utworzono zadanie.

Wyniki zadań są zapisywane w dzienniku zdarzeń Syslog oraz w dzienniku zdarzeń Kaspersky Security Center Linux zarówno centralnie na Serwerze administracyjnym i lokalnie na każdym urządzeniu.

Nie używaj prywatnych danych w ustawieniach zadania. Na przykład, unikaj określania hasła administratora domeny.

Reguły przenoszenia urządzeń

Zalecane jest automatyczne przydzielanie urządzeń do grup administracyjnych za pośrednictwem *reguł przenoszenia urządzeń*. Reguła przenoszenia urządzeń składa się z trzech głównych części: nazwy, warunku wykonania (wyrażenie logiczne z atrybutami urządzenia) oraz docelowej grupy administracyjnej. Reguła przenosi urządzenie do docelowej grupy administracyjnej, jeśli atrybuty urządzenia spełniają warunek wykonania reguły.

Wszystkie reguły przenoszenia urządzeń posiadają priorytety. Serwer administracyjny sprawdza, czy atrybuty urządzenia spełniają warunek wykonania każdej reguły, w rosnącej kolejności priorytetów. Jeśli atrybuty urządzenia spełniają warunek wykonania reguły, urządzenie zostaje przeniesione do grupy docelowej, a przetwarzanie reguły zostanie zakończone dla tego urządzenia. Jeśli atrybuty urządzenia spełniają warunki kilku reguł, urządzenie zostanie przeniesione do grupy docelowej reguły z najwyższym priorytetem (czyli tej, która znajduje się najwyżej na liście).

Reguły przenoszenia urządzeń mogą być tworzone pośrednio. Na przykład, we właściwościach pakietu instalacyjnego lub zadania zdalnej instalacji możesz określić grupę administracyjną, do której urządzenie musi zostać przeniesione po zainstalowaniu na nim Agenta sieciowego. Również reguły przenoszenia urządzeń mogą być tworzone także bezpośrednio przez administratora Kaspersky Security Center Linux w sekcji **Zarządzanie zasobami** → **Reguły przenoszenia**.

Domyślnie reguła przenoszenia urządzeń jest przeznaczona do jednorazowego, wstępnego przydzielenia urządzeń do grup administracyjnych. Reguła przenosi urządzenia z grupy Urządzenia nieprzypisane tylko raz. Jeśli urządzenie było już raz przeniesione przy użyciu tej reguły, reguła ta nie przeniesie go już nawet wtedy, gdy ręcznie przeniesiesz urządzenie z powrotem do grupy Urządzenia nieprzypisane. Jest to zalecany sposób stosowania reguł przenoszenia.

Możesz przenieść urządzenia, które już zostały przydzielone do niektórych grup administracyjnych. Aby to zrobić, we właściwościach reguły odznacz pole **Przenoś tylko urządzenia, które nie są przypisane do grup administracyjnych**.

Stosowanie reguł przenoszenia do urządzeń, które już zostały przydzielone do niektórych grup administracyjnych, znacząco zwiększa obciążenie na Serwerze administracyjnym.

Pole wyboru **Przenoś tylko urządzenia, które nie są przypisane do grup administracyjnych** jest zablokowane we właściwościach automatycznie tworzonych reguł przenoszenia. Takie reguły są tworzone podczas dodawania zadania *Zdalna instalacja aplikacji* lub tworzenia autonomicznego pakietu instalacyjnego.

Możesz utworzyć regułę przenoszenia, która będzie nieprzerwanie oddziaływać na jedno urządzenie.

Szczególnie zalecane jest unikanie ciągłego przenoszenia jednego urządzenia z jednej grupy do drugiej (na przykład, w celu zastosowania specjalnej zasady do tego urządzenia, uruchomienia specjalnego zadania grupowego lub zaktualizowania urządzenia poprzez punkt dystrybucji).

Takie scenariusze nie są obsługiwane, ponieważ w bardzo dużym stopniu zwiększają obciążenie na Serwerze administracyjnym oraz ruch sieciowy. Te scenariusze doprowadzają też do konfliktu z zasadami działania Kaspersky Security Center Linux (szczególnie w obszarze uprawnień dostępu, zdarzeń i raportów). Należy znaleźć inne rozwiązanie, na przykład, poprzez użycie profili zasad, zadań dla wyborów urządzeń, przydzielania Agentów sieciowych zgodnie ze standardowym scenariuszem.

Kategoryzacja oprogramowania

Głównym narzędziem do monitorowania uruchomień aplikacji są *kategorie Kaspersky* (zwane dalej *Kategorie KL*). Kategorie KL umożliwiają administratorom Kaspersky Security Center Linux uproszczenie obsługi kategoryzacji oprogramowania i zminimalizowanie ruchu sieciowego skierowanego do zarządzanych urządzeń.

Kategorie użytkownika powinny być tworzone tylko dla aplikacji, których nie można zaklasyfikować do żadnej z istniejących kategorii KL (na przykład, dla oprogramowania wykonanego na zamówienie użytkownika). Kategorie użytkownika są tworzone na podstawie pakietu instalacyjnego aplikacji (MSI) lub folderu z pakietami instalacyjnymi.

Jeśli dostępna jest duża ilość programów, które nie zostały skategoryzowane poprzez kategorie KL, można utworzyć automatycznie aktualizowaną kategorię. Sumy kontrolne plików wykonywalnych będą automatycznie dodawane do tej kategorii po każdej modyfikacji folderu zawierającego pakiety dystrybucyjne.

Tworzenie kopii zapasowej i przywracanie ustawień Serwera administracyjnego

Tworzenie kopii zapasowej ustawień Serwera administracyjnego i jego baz danych odbywa się przy użyciu zadania tworzenia kopii zapasowej oraz narzędzia klbackup. Kopia zapasowa zawiera wszystkie główne ustawienia i obiekty dotyczące Serwera administracyjnego, takie jak certyfikaty, klucze główne do szyfrowania dysków na zarządzanych urządzeniach, klucze dla różnych licencji, strukturę grup administracyjnych z całą ich zawartością, zadaniami, zasadami itd. Przy pomocy kopii zapasowej można przywrócić działanie Serwera administracyjnego tak szybko, jak to możliwe, poświęcając na to od kilkunastu minut do kilku godzin.

Jeśli nie ma dostępnej kopii zapasowej, błąd może doprowadzić do bezpowrotnej utraty certyfikatów i wszystkich ustawień Serwera administracyjnego. Będzie to wymagało przeprowadzenia konfiguracji Kaspersky Security Center Linux od początku oraz ponownego zainstalowania Agenta sieciowego w sieci organizacji. Wszystkie klucze główne do szyfrowania dysków na zarządzanych urządzeniach zostaną utracone, co spowoduje ryzyko utraty zaszyfrowanych danych na urządzeniach z zainstalowanym programem Kaspersky Endpoint Security. Dlatego też nigdy nie rezygnuj z regularnego wykonywania kopii zapasowej Serwera administracyjnego przy użyciu standardowego zadania tworzenia kopii zapasowej.

Kreator wstępnej konfiguracji tworzy zadanie wykonywania kopii zapasowej dla ustawień Serwera administracyjnego i ustawia jego codzienne wykonywanie na godzinę 4:00. Kopie zapasowe są domyślnie zapisywane w folderze /var/opt/kaspersky/KSC_Backups*.

Ponieważ kopia zapasowa zawiera ważne dane, zadanie tworzenia kopii zapasowej oraz narzędzie klbackup oferują ochronę kopii zapasowej przy użyciu hasła. Domyślnie zadanie tworzenia kopii zapasowej wykonuje kopię zapasową z pustym hasłem. Hasło należy ustawić we właściwościach zadania tworzenia kopii zapasowej. Pominięcie tego wymagania doprowadza do sytuacji, w której wszystkie klucze certyfikatów Serwera administracyjnego, klucze dla licencji oraz klucze główne dla szyfrowania dysków na zarządzanych urządzeniach pozostaną niezaszyfrowane.

Oprócz regularnych kopii zapasowych, kopie zapasowe należy tworzyć także przed każdą znaczącą zmianą, w tym instalacją aktualizacji i łat Serwera administracyjnego.

> Przywracanie kopii zapasowej odbywa się przy użyciu narzędzia klbackup na działającej instancji Serwera administracyjnego, który został właśnie zainstalowany i posiada tę samą wersję (lub nowszą), dla której kopia zapasowa została utworzona.

Instancja Serwera administracyjnego, na którym kopia zapasowa ma zostać przywrócona, musi korzystać z systemu DBMS tego samego typu i tej samej lub nowszej wersji. Wersja Serwera administracyjnego może być taka sama (z tą samą lub późniejszą łatą) lub nowsza.

Sekcja opisuje standardowe scenariusze przywracania ustawień i obiektów Serwera administracyjnego.

Urządzenie z zainstalowanym Serwerem administracyjnym nie działa

Jeśli urządzenie, na którym jest zainstalowany Serwer administracyjny, nie działa z powodu błędu, zalecane jest wykonanie następujących działań:

- Nowy Serwer administracyjny musi mieć przypisaną taką samą nazwę DNS.

  Jeśli w pakiecie instalacyjnym Agenta sieciowego podczas wdrażania Agentów sieciowych ustawiono statyczny adres IP, należy również przypisać ten sam adres IP do nowego Serwera administracyjnego. Alternatywnie można użyć adresu połączenia, który określa Serwer administracyjny, z którym łączy się Agent sieciowy (możesz uzyskać ten adres na zarządzanych urządzeniach korzystając z narzędzia klnagchk).

- W pliku konfiguracyjnym IAM `var/opt/kaspersky/klnagent_srv/iam/iam_config.yaml`, należy ustawić parametr `server_iam.ksc_address` na dokładnie taki sam adres Serwera administracyjnego, jaki określono w polu Alternatywna nazwa podmiotu (SAN) poprzednio używanego certyfikatu Serwera administracyjnego. Szczegółowe informacje można znaleźć w następującym artykule: Dodawanie adresu Serwera administracyjnego do konfiguracji Serwera IAM.

- Zainstaluj Serwer administracyjny, używając systemu DBMS tego samego typu i w tej samej wersji. Możesz zainstalować tę samą wersję Serwera z tą samą (lub późniejszą) łatą lub nowszą wersję Serwera. Po instalacji nie przeprowadzaj wstępnej konfiguracji przy użyciu kreatora.

- Uruchom narzędzie klbackup i wykonaj przywracanie. Po pomyślnym przywróceniu zainstaluj ponownie Web Console.

Ustawienia Serwera administracyjnego lub bazy danych są uszkodzone

Jeżeli Serwer administracyjny nie działa ze względu na uszkodzone ustawienia lub bazę danych (na przykład, w wyniku przepięcia), zalecane jest użycie następujących scenariuszy:

1. Przeskanuj system plików na uszkodzonym urządzeniu.

2. Odinstaluj niedziałającą wersję Systemu operacyjnego.

3. Zainstaluj ponownie Serwer administracyjny, używając systemu DBMS tego samego typu i w tej samej (lub nowszej) wersji. Możesz zainstalować tę samą wersję Serwera z tą samą (lub późniejszą) łatą lub nowszą wersję Serwera. Po instalacji nie przeprowadzaj wstępnej konfiguracji przy użyciu kreatora.

4. Uruchom narzędzie klbackup i wykonaj przywracanie.

Zabronione jest przywracanie Serwera administracyjnego w sposób inny niż przy użyciu narzędzia klbackup.

Wszelkie próby przywrócenia Serwera administracyjnego przy użyciu oprogramowania firm trzecich doprowadzą do desynchronizacji danych na węzłach aplikacji Kaspersky Security Center Linux i w konsekwencji - do niepoprawnego działania aplikacji.

Informacje o profilach połączenia dla użytkowników mobilnych

Mobilni użytkownicy laptopów (zwanych dalej również "urządzeniami") mogą potrzebować zmiany metody łączenia się z Serwerem administracyjnym lub przełączania pomiędzy Serwerami administracyjnymi w zależności od aktualnej lokalizacji urządzenia w sieci firmowej.

Używanie różnych adresów jednego Serwera administracyjnego

Urządzenia z zainstalowanym Agentem sieciowym mogą łączyć się z Serwerem administracyjnym z poziomu wewnętrznej sieci organizacji lub internetu. W tej sytuacji wymagane może być, aby Agent sieciowy używał innych adresów do łączenia się z Serwerem administracyjnym: zewnętrznego adresu Serwera administracyjnego dla połączenia internetowego oraz wewnętrznego adresu Serwera administracyjnego dla wewnętrznego połączenia sieciowego.

W tym celu musisz dodać profil (dla połączenia z Serwerem administracyjnym z poziomu internetu) do zasady Agenta sieciowego. Dodaj profil we właściwościach zasady (sekcja **Łączność**, podsekcja **Profile połączenia**). W oknie tworzenia profilu należy wyłączyć opcję **Użyj tylko do pobierania uaktualnień** oraz wybrać opcję **Synchronizuj ustawienia połączenia z ustawieniami Serwera administracyjnego określonymi w tym profilu**. Jeśli do łączenia się z Serwerem administracyjnym używasz bramy połączenia (na przykład, w konfiguracji Kaspersky Security Center Linux, opisanej w sekcji Dostęp do internetu: Agent sieciowy jako brama połączenia w strefie zdemilitaryzowanej), w odpowiednim polu profilu połączenia musisz określić adres bramy połączenia.

Przełączanie pomiędzy Serwerami administracyjnymi w zależności od aktualnej sieci

Jeśli organizacja posiada kilka biur z różnymi Serwerami administracyjnymi, a niektóre urządzenia z zainstalowanym Agentem sieciowym są przenoszone pomiędzy nimi, Agent sieciowy musi łączyć się z Serwerem administracyjnym sieci lokalnej w biurze, w którym znajduje się urządzenie.

W tej sytuacji konieczne jest utworzenie profilu dla połączenia z Serwerem administracyjnym we właściwościach zasady Agenta sieciowego dla każdego z biur, za wyjątkiem głównego biura, w którym znajduje się oryginalny macierzysty Serwer administracyjny. W profilach połączenia należy określić adresy Serwerów administracyjnych i włączyć lub wyłączyć opcję **Użyj tylko do pobierania uaktualnień**:

- Wybierz tę opcję, jeśli chcesz, aby Agent sieciowy zsynchronizował się z macierzystym Serwerem administracyjnym, a Serwer lokalny był używany tylko do pobierania uaktualnień.
- Wyłącz tę opcję, jeśli Agent sieciowy ma być całkowicie zarządzany przez lokalny Serwer administracyjny.

Następnie powinieneś ustalić warunki przełączania do nowo utworzonych profili: przynajmniej jeden warunek dla każdego z biur, za wyjątkiem głównego biura. Celem każdego warunku jest wykrycie elementów, które są specyficzne dla środowiska sieciowego w biurze. Jeśli warunek jest prawdziwy, odpowiedni profil zostaje aktywowany. Jeśli żaden z warunków nie jest prawdziwy, Agent sieciowy przełączy się do macierzystego Serwera administracyjnego.

Informacje o przełączaniu Agenta sieciowego na inne Serwery administracyjne

Kaspersky Security Center Linux oferuje opcję przełączania Agenta sieciowego na urządzeniu klienckim na inne Serwery administracyjne, jeśli następujące ustawienia sieci zostały zmienione:

- **Warunek dla adresu serwera DHCP** — zmiana adresu IP serwera sieciowego (DHCP).

  Ustawienie **Warunek dla adresu serwera DHCP** jest obecnie niedostępny.

- **Warunek dla adresu domyślnej bramy połączenia** — zmiana adresu głównej bramy sieci.
- **Warunek dla domeny DNS** — zmiana sufiksu DNS podsieci.
- **Warunek dla adresu serwera DNS** — zmiana adresu IP serwera sieciowego DNS.
- **Warunek dla adresu serwera WINS** — zmiana adresu IP sewera sieciowego WINS. To ustawienie jest dostępne tylko dla urządzeń z systemem Windows.
- **Warunek dla rozwiązania nazw** — zmiana nazwy DNS lub NetBIOS urządzenia klienckiego.
- **Warunek dla podsieci** — zmiana adresu i maski podsieci.
- **Warunek dla dostępności domeny Windows** — zmiana stanu domeny systemu Windows, do której podłączone jest urządzenie klienckie. To ustawienie jest dostępne tylko dla urządzeń z systemem Windows.
- **Warunek dla dostępności adresu połączenia SSL** — urządzenie klienckie może lub nie może (w zależności od wybranej opcji) nawiązać połączenie SSL z określonym serwerem (nazwa:port). Musisz użyć dedykowanego serwera z oprogramowaniem zdolnym do obsługi dużego obciążenia i częstych żądań połączenia od Agenta sieciowego. Nie podawaj portu Serwera administracyjnego. Dla każdego serwera możesz dodatkowo określić certyfikat SSL. W takim przypadku Agent sieciowy weryfikuje certyfikat serwera, oprócz sprawdzenia możliwości połączenia SSL. Jeśli certyfikat nie pasuje, połączenie nie powiedzie się.

Początkowe ustawienia połączenia Agenta sieciowego z Serwerem administracyjnym są definiowane podczas instalacji Agenta sieciowego. Następnie, jeśli reguły przełączania Agenta sieciowego na inne Serwery administracyjne zostały zmienione, Agent sieciowy odpowiada na zmiany w ustawieniach sieci w następujący sposób:

- Jeśli ustawienia sieci pokrywają się z ustawieniami jednej z utworzonych reguł, Agent sieciowy nawiąże połączenie z Serwerem administracyjnym określonym w tej regule. Aplikacje zainstalowane na urządzeniach klienckich przełączają się do zasady użytkownika mobilnego pod warunkiem, że takie zachowanie jest dozwolone przez regułę.

- Jeśli nie jest stosowana żadna z reguł, Agent sieciowy przywróci ustawienia domyślne połączenia z Serwerem administracyjnym określone podczas instalacji. Aplikacje zainstalowane na urządzeniach klienckich przywracają aktywne zasady.

- Jeśli Serwer administracyjny jest niedostępny, Agent sieciowy używa zasad użytkownika mobilnego.

Agent sieciowy przełącza się do zasady użytkownika mobilnego tylko wtedy, gdy opcja **Włącz tryb użytkownika mobilnego, gdy Serwer administracyjny nie jest dostępny** jest włączona w ustawieniach zasady Agenta sieciowego.

Ustawienia połączenia Agenta sieciowego z Serwerem administracyjnym są zapisywane w profilu połączenia. W profilu połączenia możesz utworzyć reguły przełączania urządzeń klienckich do zasad użytkownika mobilnego, a także skonfigurować profil tak, aby mógł być używany tylko do pobierania uaktualnień.

Tworzenie profilu połączenia dla użytkowników mobilnych

W celu utworzenia profilu połączenia Agenta sieciowego z Serwerem administracyjnym dla użytkowników mobilnych:

1. Jeżeli chcesz utworzyć profil połączenia dla grupy zarządzanych urządzeń, otwórz zasadę agenta sieciowego tej grupy. W tym celu wykonaj następujące czynności:

   a. W menu głównym przejdź do **Zarządzanie zasobami** → **Zasady**.

   b. Wybierz grupę administracyjną dla której chcesz utworzyć profil połączenia:

      - W przypadku grupy głównej możesz przejść do następnego kroku.

      - Aby dodać podgrupę, kliknij przycisk **Pokaż hierarchię** u góry strony, a następnie w oknie, które zostanie otwarte, kliknij nazwę żądanej podgrupy.

      Ścieżka do wybranej grupy jest wyświetlana na górze strony. W razie potrzeby możesz kliknąć odnośnik z nazwą grupy administracyjnej, aby do niej przejść. Domyślnie ostatni odnośnik na ścieżce jest nieaktywny. Można również zamknąć okno hierarchii, klikając przycisk **Ukryj hierarchię**.

   c. Dodaj zasadę agenta sieciowego dla grupy zarządzanych urządzeń. Jeśli już ją utworzono, kliknij nazwę zasady agenta sieciowego, aby otworzyć właściwości zasady.

2. Jeśli chcesz utworzyć profil połączenia dla konkretnego zarządzanego urządzenia, wykonaj następujące czynności:

   a. W menu głównym przejdź do **Zarządzanie zasobami** → **Zasoby (urządzenia)**.

   b. Kliknij nazwę zarządzanego urządzenia.

   c. W otwartym oknie właściwości zarządzanego urządzenia kliknij zakładkę **Aplikacje**.

   d. Kliknij nazwę zasady agenta sieciowego, której dotyczy tylko wybrane zarządzane urządzenie.

3. W otwartym oknie właściwości przejdź do **Ustawienia aplikacji** → **Łączność** → **Profile połączenia.**

4. W grupie ustawień **Profile połączeń Serwera administracyjnego** kliknij przycisk **Dodaj**.

   Domyślnie, lista profili połączeń zawiera profile <Tryb offline> i <Macierzysty serwer administracyjny>. Profili nie można modyfikować ani usunąć.

   Profil <Tryb offline> nie określa żadnego Serwera do nawiązania połączenia. Dlatego też, Agent sieciowy, gdy zostaje przełączony do tego profilu, nie próbuje nawiązać połączenia z żadnym Serwerem administracyjnym, gdy aplikacje zainstalowane na urządzeniach klienckich działają pod kontrolą zasad użytkownika mobilnego. Profil <Tryb offline> może być używany, jeśli urządzenia są odłączone od sieci.

   Profil <Macierzysty serwer administracyjny> określa połączenie z serwerem administracyjnym, który został wybrany podczas instalacji agenta sieciowego. Profil <Macierzysty serwer administracyjny> jest stosowany, gdy urządzenie jest ponownie podłączane do macierzystego Serwera administracyjnego po tym, jak przez jakiś czas działało w sieci zewnętrznej.

5. W otwartym oknie **Konfiguruj profil** skonfiguruj profil połączenia:

   - **Nazwa profilu**

     W tym polu możesz przejrzeć lub zmienić nazwę profilu połączenia.

   - **Adres Serwera administracyjnego**

     Adres Serwera administracyjnego, z którym urządzenie klienckie musi łączyć się podczas aktywacji profilu.

   - **Numer portu**

     Numer portu używanego do nawiązywania połączenia.

   - **Port SSL**

     Numer portu połączenia podczas używania portu SSL.

   - **Użyj połączenia SSL**

     Jeśli ta opcja jest włączona, połączenie jest nawiązywane poprzez bezpieczny port przy użyciu protokołu SSL.

     Domyślnie opcja ta jest włączona. Zalecamy, aby nie wyłączać tej opcji, aby Twoje połączenie pozostało bezpieczne.

- Wybierz opcję **Użyj serwera proxy**, jeśli podczas łączenia z internetem chcesz korzystać z serwera proxy. Jeśli ta opcja jest wybrana, dostępne staną się pola do wprowadzenia ustawień. Dla połączenia z serwerem proxy określ następujące ustawienia:

  - **Adres**

    Adres serwera proxy używanego do łączenia Kaspersky Security Center Linux z Internetem.

  - **Numer portu**

    Numer portu, poprzez który zostanie nawiązane połączenie proxy Kaspersky Security Center Linux.

  - **Uwierzytelnianie na serwerze proxy**

    Jeśli to pole jest zaznaczone, w polach wejściowych możesz określić dane uwierzytelniające do autoryzacji na serwerze proxy.

  - **Nazwa użytkownika**

    Konto użytkownika, z poziomu którego nawiązywane jest połączenie z serwerem proxy (to pole jest dostępne, jeśli pole **Uwierzytelnianie na serwerze proxy** jest wybrane).

  - **Hasło**

    Hasło ustawione przez użytkownika, którego konto jest używane do nawiązywania połączenia z serwerem proxy (to pole jest dostępne, jeśli pole **Uwierzytelnianie na serwerze proxy** jest zaznaczone).

    Aby zobaczyć wprowadzone hasło, trzymaj kliknięty przycisk **Pokaż** tak długo, jak potrzebujesz.

- **Adres bramy połączenia**

  Adres bramy, poprzez którą urządzenia klienckie łączą się z Serwerem administracyjnym.

- **Włącz tryb użytkownika mobilnego, gdy Serwer administracyjny nie jest dostępny**

  Zaznacz to pole, aby zezwolić aplikacjom zainstalowanym na urządzeniu klienckim na korzystanie z profili zasad dla urządzeń w trybie użytkownika mobilnego, a także zasad użytkownika mobilnego, za każdym razem, gdy serwer administracyjny nie jest dostępny. Jeżeli dla aplikacji nie określono zasady użytkownika mobilnego, zostanie użyta zasada aktywna.

  Jeżeli ta opcja jest wyłączona, aplikacje będą używać zasad aktywnych.

  Domyślnie pole to nie jest zaznaczone.

- **Użyj tylko do pobierania uaktualnień**

  Jeżeli ta opcja jest włączona, profil będzie używany tylko do pobierania aktualizacji przez aplikacje zainstalowane na urządzeniu klienckim. Dla innych działań połączenie z Serwerem administracyjnym będzie nawiązywane z użyciem wstępnych ustawień określonych podczas instalacji Agenta sieciowego.

  Domyślnie opcja ta jest włączona.

- **Synchronizuj ustawienia połączenia z ustawieniami Serwera administracyjnego określonymi w tym profilu**

  Jeśli ta opcja jest włączona, Agent sieciowy nawiąże połączenie z Serwerem administracyjnym przy użyciu ustawień określonych we właściwościach profilu.

  Jeśli ta opcja jest wyłączona, Agent sieciowy nawiąże połączenie z Serwerem administracyjnym przy użyciu oryginalnych ustawień określonych podczas instalacji.

  Ta opcja jest dostępna, jeśli opcja **Użyj tylko do pobierania uaktualnień** jest wyłączona.

Domyślnie opcja ta jest wyłączona.

Profil połączenia Agenta sieciowego z Serwerem administracyjnym zostanie utworzony dla użytkowników mobilnych. Jeśli agent sieciowy łączy się z serwerem administracyjnym przy użyciu tego profilu, aplikacje zainstalowane na urządzeniu klienckim będą używać zasad dla urządzeń w trybie użytkownika mobilnego lub zasad użytkownika mobilnego.

Zdalny dostęp do zarządzanych urządzeń

Ta sekcja zawiera informacje o zdalnym dostępie do zarządzanych urządzeń.

Korzystanie z opcji „Nie odłączaj od Serwera administracyjnego" w celu zapewnienia ciągłej łączności między zarządzanym urządzeniem a Serwerem administracyjnym

Jeśli nie używasz serwerów push, Kaspersky Security Center Linux nie zapewnia ciągłej łączności między zarządzanymi urządzeniami a Serwerem administracyjnym. Agenty sieciowe na zarządzanych urządzeniach okresowo nawiązują połączenie i synchronizują się z Serwerem administracyjnym. Przerwa między tymi synchronizacjami jest definiowana w zasadzie Agenta sieciowego. Jeśli wymagana jest wczesna synchronizacja, Serwer administracyjny (lub punkt dystrybucji, jeśli jest w użyciu) wysyła podpisany pakiet sieciowy poprzez sieć IPv4 lub IPv6 do portu UDP Agenta sieciowego. Domyślnym numerem portu jest 15000. Jeśli nie jest możliwe nawiązanie połączenia między Serwerem administracyjnym a zarządzanym urządzeniem przy użyciu UDP, synchronizacja zostanie uruchomiona przy następnym regularnym połączeniu Agenta sieciowego z Serwerem administracyjnym w trakcie okresu synchronizacji.

Niektórych operacji nie można wykonać bez wcześniejszego nawiązania połączenia między Agentem sieciowym a Serwerem administracyjnym, takich jak uruchamianie i zatrzymywanie zadań lokalnych lub odbieranie statystyk dla zarządzanej aplikacji. Aby rozwiązać ten problem, jeśli nie korzystasz z serwerów push, możesz użyć opcji **Nie odłączaj od Serwera administracyjnego**, aby upewnić się, że istnieje ciągła łączność między zarządzanym urządzeniem a serwerem administracyjnym.

W celu zapewnienia ciągłego połączenia między zarządzanym urządzeniem a Serwerem administracyjnym:

1. W menu głównym przejdź do **Zarządzanie zasobami** → **Zasoby (urządzenia)**.

   Zostanie wyświetlona lista zarządzanych urządzeń.

2. Na liście zarządzanych urządzeń, kliknij odnośnik z nazwą żądanego urządzenia.

3. W oknie właściwości urządzenia, w sekcji **Ogólne**, włącz opcję **Nie odłączaj od Serwera administracyjnego**.

   Trwałe połączenie jest nawiązywane między zarządzanym urządzeniem a Serwerem administracyjnym.

Maksymalna całkowita liczba urządzeń z wybraną opcją **Nie odłączaj od Serwera administracyjnego** to 300.

Informacje o sprawdzaniu czasu połączenia pomiędzy urządzeniem a Serwerem administracyjnym

Po wyłączeniu urządzenia, Agent sieciowy powiadamia Serwer administracyjny o tym zdarzeniu. W Kaspersky Security Center Web Console urządzenie to jest wyświetlane jako wyłączone. Jednakże Agent sieciowy nie może powiadamiać Serwera administracyjnego o wszystkich tego typu zdarzeniach. Dlatego też Serwer administracyjny okresowo analizuje atrybut **Połączono z Serwerem administracyjnym** (wartość tego atrybutu jest wyświetlana w Kaspersky Security Center Web Console, we właściwościach urządzenia, w sekcji **Ogólne**) dla każdego urządzenia i porównuje go z interwałem synchronizacji z aktualnych ustawień Agenta sieciowego. Jeśli urządzenie nie odpowiedziało w ponad trzech pomyślnych interwałach synchronizacji, to urządzenie zostanie oznaczone jako wyłączone.

Informacje o wymuszonej synchronizacji

Chociaż Kaspersky Security Center Linux automatycznie synchronizuje stan, ustawienia, zadania i zasady dla zarządzanych urządzeń, to w niektórych przypadkach administrator musi dokładnie wiedzieć, czy dla określonego urządzenia w danym momencie została już przeprowadzona synchronizacja.

Okno właściwości zarządzanego urządzenia zawiera przycisk **Wymuś synchronizację**. Jeśli Kaspersky Security Center Linux wykona to polecenie, Serwer administracyjny podejmie próbę nawiązania połączenia z urządzeniem. Jeśli ta próba zakończy się pomyślnie, zostanie wykonana wymuszona synchronizacja. W innym przypadku synchronizacja zostanie wymuszona dopiero po kolejnym zaplanowanym połączeniu nawiązanym pomiędzy Agentem sieciowym a Serwerem administracyjnym.

Poradnik dotyczący rozmiarów

Ta sekcja zawiera informacje na temat szacowania rozmiaru dla komponentów Kaspersky Security Center Linux.

Informacje o podręczniku

Poradnik dotyczący rozmiarów dla Kaspersky Security Center Linux (zwany również Kaspersky Security Center) jest przeznaczony dla profesjonalistów, którzy instalują i zarządzają Kaspersky Security Center, a także dla tych, którzy zapewniają wsparcie techniczne organizacjom korzystającym z programu Kaspersky Security Center.

Wszystkie zalecenia i obliczenia zostały podane dla sieci, w których Kaspersky Security Center zarządza ochroną urządzeń z zainstalowanymi programami firmy Kaspersky.

Aby uzyskać i utrzymać optymalną wydajność w różnych warunkach pracy, należy wziąć pod uwagę liczbę urządzeń w sieci, topologię sieci oraz zestaw funkcji Kaspersky Security Center, jakich potrzebujesz.

Podręcznik zawiera następujące informacje:

- Ograniczenia Kaspersky Security Center
- Wyliczenia dla kluczowych węzłów Kaspersky Security Center (Serwerów administracyjnych i punktów dystrybucji):
  - Wymagania sprzętowe dla Serwerów administracyjnych i punktów dystrybucji
  - Obliczenie liczby i hierarchia Serwerów administracyjnych
  - Obliczenie liczby i konfiguracja punktów dystrybucji
- Konfiguracja rejestrowania zdarzeń w bazie danych w zależności od liczby urządzeń w sieci
- Popularne najlepsze praktyki optymalizacji wydajności
- Konfiguracja określonych zadań mających na celu zapewnienie optymalnego działania Kaspersky Security Center
- Ilość ruchu sieciowego (obciążenie sieci) pomiędzy Serwerem administracyjnym Kaspersky Security Center a chronionym urządzeniem

Korzystanie z tego podręcznika jest zalecane w następujących przypadkach:

- Podczas rozplanowywania zasobów przed instalacją Kaspersky Security Center
- Podczas rozplanowywania istotnych zmian w sieci, w której wdrożony jest Kaspersky Security Center
- Jeśli przełączasz z używania Kaspersky Security Center w obrębie ograniczonego segmentu sieci (środowisko testowe) do wdrożenia Kaspersky Security Center na pełną skalę w sieci korporacyjnej
- Podczas wprowadzania zmian do zestawu używanych funkcji Kaspersky Security Center

Wyliczenia dla Serwerów administracyjnych

Ta sekcja zawiera wymagania programowe i sprzętowe dla urządzeń używanych jako Serwery administracyjne. Można tu znaleźć także zalecenia odnośnie wyliczania liczby i hierarchii Serwerów administracyjnych w zależności od konfiguracji sieci organizacji.

Zaleca się, aby po zainstalowaniu Serwera administracyjnego i systemu DBMS na urządzeniach zainstalować na nich Kaspersky Endpoint Security for Linux. Informacje o wymaganiach sprzętowych Kaspersky Endpoint Security można znaleźć w Pomocy Kaspersky Endpoint Security for Linux.

Obciążenie generowane przez Kaspersky Endpoint Security for Linux po zintegrowaniu z Managed Detection and Response oraz Kaspersky Endpoint Detection and Response Expert (lokalnie) nie jest uwzględniane w obliczeniach dotyczących instalacji jednoczesnej Kaspersky Security Center Linux i Kaspersky Endpoint Security for Linux.

Obliczanie zasobów sprzętowych dla Serwera administracyjnego

Ta sekcja zawiera obliczenia pomagające w rozplanowaniu zasobów sprzętowych dla Serwera administracyjnego.

Wymagania sprzętowe dla systemu zarządzania bazą danych i Serwera administracyjnego

W poniższej tabeli zostały uwzględnione zalecane minimalne wymagania sprzętowe dla DBMS i Serwera administracyjnego uzyskane w trakcie testów. Pełna lista obsługiwanych systemów operacyjnych i systemów DBMS znajduje się na liście wymagań sprzętowych i programowych.

Należy włączyć plik wymiany na urządzeniu z zainstalowanym Serwerem administracyjnym. Minimalny rozmiar pliku wymiany musi być 1,5 raza większy niż ilość pamięci RAM.

Zalecamy, aby po zainstalowaniu Serwera administracyjnego i systemu DBMS na urządzeniach zainstalować na nich Kaspersky Endpoint Security for Linux.
W przypadku instalacji jednoczesnej wymagane jest co najmniej 225 IOPS, a do wymagań Serwera administracyjnego z systemem DBMS należy dodać 1,5 GB pamięci RAM.
Wymagania sprzętowe Kaspersky Endpoint Security można znaleźć w Pomocy Kaspersky Endpoint Security for Linux.

Sieć zawiera 50,000 urządzeń

Konfiguracja urządzenia z zainstalowanym Serwerem administracyjnym

Sprzęt	Wartość
Procesor	8 rdzeni (zalecane 12 rdzeni), 2500 MHz
Pamięć RAM	16 GB
Przestrzeń dyskowa	300 GB, 150 IOPS lub więcej

Konfiguracja urządzenia z zainstalowanym DBMS PostgreSQL

Sprzęt	Wartość
Procesor	16 rdzenie, 2500 MHz
Pamięć RAM	32 GB
Przestrzeń dyskowa	300 GB, 150 IOPS lub więcej

Konfiguracja węzłów dla klastra pracy awaryjnej

Sprzęt	Wartość
Procesor	16 rdzenie, 2500 MHz
Pamięć RAM	32 GB
Przestrzeń dyskowa	500 GB, 300 IOPS lub więcej
Kontroler interfejsu sieciowego	1 Gb/s

Konfiguracja urządzenia z zainstalowanym Serwerem administracyjnym i PostgreSQL DBMS

Sprzęt	Wartość
Procesor	24 rdzenie (zalecane 28 rdzeni), 2500 MHz
Pamięć RAM	48 GB
Przestrzeń dyskowa	600 GB, 300 IOPS lub więcej

Sieć zawiera 30,000 urządzeń

Konfiguracja urządzenia z zainstalowanym Serwerem administracyjnym

Sprzęt	Wartość
Procesor	6 rdzeni (zalecane 8 rdzeni), 2500 MHz
Pamięć RAM	12 GB
Przestrzeń dyskowa	200 GB, 150 IOPS lub więcej

Konfiguracja urządzenia z zainstalowanym DBMS PostgreSQL

Sprzęt	Wartość
Procesor	12 rdzeni, 2500 MHz
Pamięć RAM	22 GB
Przestrzeń dyskowa	250 GB, 150 IOPS lub więcej

Konfiguracja węzłów dla klastra pracy awaryjnej

Sprzęt	Wartość
Procesor	16 rdzeni, 2500 MHz
Pamięć RAM	32 GB
Przestrzeń dyskowa	500 GB, 300 IOPS lub więcej
Kontroler interfejsu sieciowego	1 Gb/s

Konfiguracja urządzenia z zainstalowanym Serwerem administracyjnym i PostgreSQL DBMS

Sprzęt	Wartość
Procesor	16 rdzeni (zalecane 20 rdzeni), 2500 MHz
Pamięć RAM	34 GB
Przestrzeń dyskowa	450 GB, 300 IOPS lub więcej

Sieć zawiera 10,000 urządzeń

Konfiguracja urządzenia z zainstalowanym Serwerem administracyjnym

Sprzęt	Wartość
Procesor	4 rdzenie (zalecane 6 rdzeni), 2500 MHz
Pamięć RAM	8 GB
Przestrzeń dyskowa	100 GB, 150 IOPS lub więcej

Konfiguracja urządzenia z zainstalowanym DBMS PostgreSQL

Sprzęt	Wartość
Procesor	6 rdzeni, 2500 MHz
Pamięć RAM	10 GB
Przestrzeń dyskowa	200 GB, 150 IOPS lub więcej

Konfiguracja węzłów dla klastra pracy awaryjnej

Sprzęt	Wartość
Procesor	16 rdzeni, 2500 MHz
Pamięć RAM	32 GB
Przestrzeń dyskowa	500 GB, 300 IOPS lub więcej
Kontroler interfejsu sieciowego	1 Gb/s

Konfiguracja urządzenia z zainstalowanym Serwerem administracyjnym i PostgreSQL DBMS

Sprzęt	Wartość
Procesor	8 rdzeni (zalecane 14 rdzeni), 2500 MHz
Pamięć RAM	18 GB
Przestrzeń dyskowa	300 GB, 300 IOPS lub więcej

Sieć zawiera 1000 urządzeń

Konfiguracja urządzenia z zainstalowanym Serwerem administracyjnym

Sprzęt	Wartość
Procesor	2 rdzenie, 2500 MHz
Pamięć RAM	6 GB
Przestrzeń dyskowa	10 GB, 150 IOPS lub więcej

Konfiguracja urządzenia z zainstalowanym DBMS PostgreSQL

Sprzęt	Wartość
Procesor	2 rdzenie, 2500 MHz
Pamięć RAM	4 GB
Przestrzeń dyskowa	20 GB, 150 IOPS lub więcej

Konfiguracja węzłów dla klastra pracy awaryjnej

Sprzęt	Wartość
Procesor	16 rdzeni, 2500 MHz
Pamięć RAM	32 GB

Sprzęt	Wartość
Przestrzeń dyskowa	500 GB, 300 IOPS lub więcej
Kontroler interfejsu sieciowego	1 Gb/s

Konfiguracja urządzenia z zainstalowanym Serwerem administracyjnym i PostgreSQL DBMS

Sprzęt	Wartość
Procesor	4 rdzenie, 2500 MHz
Pamięć RAM	10 GB
Przestrzeń dyskowa	30 GB, 300 IOPS lub więcej

Testy zostały przeprowadzone z użyciem następujących ustawień:

- Automatyczne przydzielanie punktów dystrybucji jest włączone na Serwerze administracyjnym lub punkty dystrybucji są przydzielane ręcznie według zalecanej tabeli.
- DBMS PostgreSQL nie zawiera żadnych rozszerzeń innych niż plpgsql.

Na urządzeniu z zainstalowanym systemem DBMS baza danych zajmuje około 100 GB miejsca na dysku, a dziennik transakcji zajmuje około 200 GB miejsca na dysku.

Obliczanie pojemności bazy danych

Przybliżoną ilość miejsca, jaką powinna zajmować baza danych, można obliczyć, korzystając z następującego wzoru:

(600 * C + 2.3 * E + 2.5 * A + 1.2 * N * F), KB

gdzie:

- C to liczba urządzeń.

  > Jeśli wśród zarządzanych urządzeń znajdują się dynamiczne maszyny wirtualne, C jest sumą liczby niedynamicznych zarządzanych urządzeń oraz liczby dynamicznych maszyn wirtualnych, na których Agent sieciowy został utworzony między dwoma kolejnymi uruchomieniami zadania **Konserwacja Serwera administracyjnego**.

- E to liczba przechowywanych zdarzeń.
- A to całkowita liczba obiektów Active Directory:
  - Konta urządzeń
  - Konta użytkowników
  - Konta grup bezpieczeństwa
  - Jednostki organizacyjne Active Directory

  Jeśli skanowanie Active Directory jest wyłączone, zmienna A będzie równa zero.

- N to średnia liczba zinwentaryzowanych plików wykonywalnych na urządzeniu końcowym.
- F to liczba urządzeń końcowych, na których zinwentaryzowano pliki wykonywalne.

Jeśli planujesz włączyć w ustawieniach zasady Kaspersky Endpoint Security powiadamianie Serwera administracyjnego o aplikacjach, które uruchamiasz, będziesz potrzebował dodatkowej ilości (0,03 * C) gigabajtów do przechowywania w bazie danych informacji o aplikacjach, które uruchamiasz.

Podczas działania, w bazie danych zawsze znajduje się część *nieprzydzielonego obszaru*. Dlatego też rzeczywisty rozmiar pliku bazy danych często okazuje się około dwukrotnie większy od ilości miejsca zajmowanego w bazie danych.

Nie jest zalecane wyraźne ograniczenie rozmiaru dziennika transakcji. Zalecane jest pozostawienie domyślnej wartości parametru MAXSIZE.

Obliczanie miejsca na dysku

Przestrzeń dyskowa na Serwerze administracyjnym, wymagana dla folderu /var/opt/kaspersky/klnagent_srv/, może zostać oszacowana w przybliżeniu przy użyciu wzoru:

(724 * C + 0,15 * E + 0,17 * A), KB

gdzie:

- C to liczba urządzeń.

  Jeśli wśród zarządzanych urządzeń znajdują się dynamiczne maszyny wirtualne, C jest sumą liczby niedynamicznych zarządzanych urządzeń oraz liczby dynamicznych maszyn wirtualnych, na których Agent sieciowy został utworzony między dwoma kolejnymi uruchomieniami zadania **Konserwacja Serwera administracyjnego**.

- E to liczba przechowywanych zdarzeń.
- A to całkowita liczba obiektów Active Directory:
  - Konta urządzeń
  - Konta użytkowników
  - Konta grup bezpieczeństwa
  - Jednostki organizacyjne Active Directory

Jeśli skanowanie Active Directory jest wyłączone, zmienna A będzie równa zero.

Obliczanie liczby i konfigurowanie Serwerów administracyjnych

Aby zmniejszyć obciążenie na głównym Serwerze administracyjnym, do każdej grupy administracyjnej możesz przypisać oddzielny Serwer administracyjny. Liczba podrzędnych Serwerów administracyjnych nie może przekraczać 500 dla jednego głównego Serwera administracyjnego.

Zalecane jest utworzenie konfiguracji Serwerów administracyjnych w odniesieniu do konfiguracji sieci organizacji.

Zalecenia dotyczące łączenia dynamicznych maszyn wirtualnych z Kaspersky Security Center

Dynamiczne maszyny wirtualne (nazywane również dynamicznymi maszynami wirtualnymi) zużywają więcej zasobów niż statyczne maszyny wirtualne.

Aby uzyskać więcej informacji na temat dynamicznych maszyn wirtualnych, zobacz Obsługa dynamicznych maszyn wirtualnych.

Po podłączeniu nowej dynamicznej maszyny wirtualnej Kaspersky Security Center Linux tworzy wpis dla tej dynamicznej maszyny wirtualnej w konsoli Kaspersky Security Center Web Console i przenosi dynamiczną maszynę wirtualną do grupy administracyjnej. Następnie dynamiczna maszyna wirtualna jest dodawana do bazy danych Serwera administracyjnego. Serwer administracyjny jest w pełni zsynchronizowany z Agentem sieciowym zainstalowanym na tej dynamicznej maszynie wirtualnej.

W sieci organizacji Agent sieciowy tworzy następujące listy sieci dla każdej dynamicznej maszyny wirtualnej:

- Sprzęt
- Zainstalowane oprogramowanie
- Wykryte luki w zabezpieczeniach
- Zdarzenia i listy plików wykonywalnych komponentu Kontrola aplikacji

Agent sieciowy przesyła te listy sieciowe do Serwera administracyjnego. Rozmiar list sieciowych zależy od komponentów zainstalowanych na dynamicznej maszynie wirtualnej i może wpływać na wydajność Kaspersky Security Center Linux i systemu zarządzania bazami danych (DBMS). Należy zauważyć, że obciążenie może rosnąć nieliniowo.

Po zakończeniu pracy z dynamiczną maszyną wirtualną przez użytkownika i wyłączeniu jej, maszyna ta jest następnie usuwana z infrastruktury wirtualnej, a wpisy dotyczące tej maszyny są usuwane z bazy danych Serwera administracyjnego.

Wszystkie te działania zużywają dużo zasobów bazy danych Kaspersky Security Center Linux i Serwera administracyjnego i mogą zmniejszyć wydajność Kaspersky Security Center Linux i DBMS. Zalecamy podłączenie do 20 000 dynamicznych maszyn wirtualnych do Kaspersky Security Center Linux.

Możesz podłączyć ponad 20 000 dynamicznych maszyn wirtualnych do Kaspersky Security Center Linux, jeśli połączone dynamiczne maszyny wirtualne wykonują standardowe operacje (na przykład aktualizacje baz danych) i zużywają nie więcej niż 80 procent pamięci i 75–80 procent dostępnych rdzeni.

Zmiana ustawień zasad, oprogramowania lub systemu operacyjnego na dynamicznej maszynie wirtualnej może zmniejszyć lub zwiększyć zużycie zasobów. Za optymalne uważa się zużycie 80–95 procent zasobów.

Wyliczenia dla punktów dystrybucji i bram połączenia

Ta sekcja zawiera wymagania sprzętowe dla urządzeń używanych jako punkty dystrybucji wraz z zaleceniami dotyczącymi obliczenia liczby punktów dystrybucji i bram połączenia w zależności od konfiguracji sieci firmowej.

Wymagania wobec punktu dystrybucji

W tym artykule opisano wymagania sprzętowe i programowe dla punktów dystrybucji opartych na systemach Windows i Linux.

Jeśli jakiekolwiek zadanie zdalnej instalacji jest oczekujące na Serwerze administracyjnym, urządzenie z zainstalowanym punktem dystrybucji będzie także wymagało wolnej przestrzeni na dysku równej całkowitemu rozmiarowi pakietów instalacyjnych przeznaczonych do zainstalowania.

Jeśli na Serwerze administracyjnym jest oczekujące jedno lub kilka zadań instalacji aktualizacji (poprawek) i naprawy luk, urządzenie z zainstalowanym punktem dystrybucji będzie także wymagało dodatkowej wolnej przestrzeni na dysku równej podwojonej wartości całkowitego rozmiaru wszystkich poprawek przeznaczonych do zainstalowania.

Jeśli używasz schematu, gdy punkty dystrybucji otrzymują aktualizacje baz danych i modułów aplikacji bezpośrednio z serwerów aktualizacji Kaspersky, punkty dystrybucji muszą być podłączone do Internetu.

> Nie zaleca się wyznaczania Serwera administracyjnego jako punktu dystrybucji, ponieważ zwiększy to obciążenie Serwera administracyjnego.

Wymagania sprzętowe dla punktów dystrybucji opartych na systemie Windows

Minimalne wymagania sprzętowe dla punktów dystrybucji opartych na systemie Windows

Liczba urządzeń klienckich	Procesor	Pamięć RAM	Pamięć RAM z włączoną funkcją zarządzania poprawkami	Przestrzeń dyskowa
10 000	4 rdzenie, 2500 MHz	8 GB	8 GB	120 GB
5000	4 rdzenie, 2500 MHz	6 GB	8 GB	120 GB
1000	2 rdzenie, 2500 MHz	4 GB	8 GB	120 GB

Wymagania sprzętowe dla punktów dystrybucji opartych na systemie Linux

Minimalne wymagania sprzętowe dla punktów dystrybucji opartych na systemie Linux

Liczba urządzeń klienckich	Procesor	Pamięć RAM	Przestrzeń dyskowa
10 000	4 rdzenie, 2500 MHz	10 GB	120 GB

5000	4 rdzenie, 2500 MHz	8 GB	120 GB
1000	2 rdzenie, 2500 MHz	6 GB	120 GB

Obliczanie liczby i konfigurowanie punktów dystrybucji

Im więcej urządzeń klienckich zawiera sieć, tym więcej punktów dystrybucji wymaga. Nie jest zalecane wyłączanie automatycznego przypisywania punktów dystrybucji. Jeśli automatyczne przypisywanie punktów dystrybucji jest włączone, Serwer administracyjny przypisuje punkty dystrybucji, gdy liczba urządzeń klienckich jest dosyć duża, oraz definiuje ich konfigurację.

Używanie specjalnie przypisanych punktów dystrybucji

Jeśli planujesz używać określonych urządzeń jako punktów dystrybucji (na przykład, specjalnie wybranych serwerów), możesz zrezygnować z automatycznego przypisywania punktów dystrybucji. W tym przypadku upewnij się, że na urządzeniach, które mają pełnić rolę punktów dystrybucji, jest wystarczająca ilość wolnego miejsca, nie są regularnie wyłączane, a tryb uśpienia jest na nich wyłączony.

Liczba specjalnie przypisanych punktów dystrybucji w sieci, która zawiera pojedynczy segment sieci w oparciu o liczbę urządzeń w sieci

Liczba urządzeń klienckich w segmencie sieci	Liczba punktów dystrybucji
Mniej niż 300	0 (nie przypisuj punktów dystrybucji)
Więcej niż 300	Dopuszczalne: (N/10 000 + 1), zalecane: (N/5000 + 2), gdzie N to liczba urządzeń w sieci

Liczba specjalnie przypisanych punktów dystrybucji w sieci, która zawiera kilka segmentów sieci w oparciu o liczbę urządzeń w sieci

Liczba urządzeń klienckich na segment sieci	Liczba punktów dystrybucji
Mniej niż 10	0 (nie przypisuj punktów dystrybucji)
10–100	1
Więcej niż 100	Dopuszczalne: (N/10 000 + 1), zalecane: (N/5000 + 2), gdzie N to liczba urządzeń w sieci

Korzystanie ze standardowych urządzeń klienckich (stacji roboczych) jako punktów dystrybucji

Jeśli planujesz używać standardowych urządzeń klienckich (czyli stacji roboczych) jako punktów dystrybucji, zalecane jest przypisanie punktów dystrybucji w sposób pokazany w tabelach poniżej, aby uniknąć nadmiernego obciążenia kanałów komunikacji i Serwera administracyjnego:

Liczba stacji roboczych działających jako punkty dystrybucji w sieci, która zawiera pojedynczy segment sieci w oparciu o liczbę urządzeń w sieci

Liczba urządzeń klienckich w segmencie sieci	Liczba punktów dystrybucji
Mniej niż 300	0 (nie przypisuj punktów dystrybucji)
Więcej niż 300	(N/300 + 1), gdzie N oznacza liczbę urządzeń w sieci; muszą być przynajmniej 3 punkty dystrybucji

Liczba stacji roboczych działających jako punkty dystrybucji w sieci, która zawiera kilka segmentów sieci w oparciu o liczbę urządzeń w sieci

Liczba urządzeń klienckich na segment sieci	Liczba punktów dystrybucji
Mniej niż 10	0 (nie przypisuj punktów dystrybucji)
10–30	1

Liczba urządzeń klienckich na segment sieci	Liczba punktów dystrybucji
31–300	2
Więcej niż 300	(N/300 + 1), gdzie N oznacza liczbę urządzeń w sieci; muszą być przynajmniej 3 punkty dystrybucji

Jeśli punkt dystrybucji jest wyłączony (lub z jakiegoś powodu niedostępny), zarządzane urządzenia w tym obszarze mogą uzyskać dostęp do Serwera administracyjnego w celu pobrania uaktualnień.

Obliczanie liczby bram połączenia

Jeśli planujesz używać bramy połączenia, zalecane jest wskazanie specjalnego urządzenia do pełnienia tej funkcji.

Brama połączenia może obejmować maksymalnie 10 000 zarządzanych urządzeń.

Zapisywanie informacji o zdarzeniach dla zadań i zasad

Ta sekcja zawiera wyliczenia związane z przechowywaniem zdarzeń w bazie danych Serwera administracyjnego i oferuje zalecenia dotyczące zminimalizowania liczby zdarzeń, co pozwala zmniejszyć obciążenie na Serwerze administracyjnym.

Domyślnie, właściwości każdego zadania i zasady zapewniają przechowywanie wszystkich zdarzeń związanych z wykonywaniem zadań i wymuszeniem zasady.

Jednakże, jeśli zadanie jest uruchamiane dość często (na przykład, więcej niż raz w tygodniu) i na całkiem dużej liczbie urządzeń (na przykład, więcej niż 10 000), liczba zdarzeń może okazać się zbyt duża i zdarzenia mogą wypełnić bazę danych. W tym przypadku zalecane jest wybranie jednej z dwóch opcji w ustawieniach zadania:

- **Zapisz zdarzenia dotyczące postępu zadania**. W tym przypadku baza danych pobiera tylko informacje o uruchomieniu zadania, postępie i zakończeniu (pomyślnie, z ostrzeżeniem lub błędem) z każdego urządzenia, na którym zadanie jest uruchomione.

- **Zapisz jedynie wyniki wykonywania zadania**. W tym przypadku baza danych pobiera tylko informacje o zakończeniu zadania (pomyślnie, z ostrzeżeniem lub błędem) z każdego urządzenia, na którym zadanie jest uruchomione.

Jeśli zasada została zdefiniowana dla całkiem dużej liczby urządzeń (na przykład, więcej niż 10 000), liczba zdarzeń może okazać się zbyt duża i zdarzenia mogą wypełnić bazę danych. W tym przypadku zalecane jest wybranie tylko najbardziej krytycznych zdarzeń w ustawieniach zasady i włączenie ich zapisywania. Zalecane jest wyłączenie zapisywania wszystkich pozostałych zdarzeń.

Postępując w ten sposób, zmniejszysz liczbę zdarzeń w bazie danych, zwiększysz prędkość wykonywania scenariuszy skojarzonych z analizą tabeli zdarzeń w bazie danych, a także zmniejszysz ryzyko nadpisania krytycznych zdarzeń przez dużą liczbę zdarzeń.

Możesz także skrócić okres przechowywania zdarzeń skojarzonych z zadaniem lub zasadą. Domyślny okres wynosi 7 dni dla zdarzeń związanych z zadaniem oraz 30 dni dla zdarzeń związanych z zasadą. Podczas zmiany okresu przechowywania zdarzeń należy uwzględnić procedury obowiązujące w organizacji oraz czas, jaki administrator systemu może poświęcić na przeanalizowanie każdego zdarzenia.

Zmodyfikowanie ustawień przechowywania zdarzeń jest zalecane w następujących przypadkach:

- Zdarzenia dotyczące zmian w stanach pośrednich zadań grupowych oraz zdarzenia dotyczące stosowania zasad zajmują dużą część wszystkich zdarzeń w bazie danych Kaspersky Security Center Linux.
- Dziennik systemu operacyjnego zaczyna wyświetlać wpisy o automatycznym usuwaniu zdarzeń, gdy przekroczony zostanie ustawiony limit całkowitej liczby zdarzeń przechowywanych w bazie danych.

Wybierz opcje zapisywania zdarzeń w oparciu o założenie, że optymalna liczba zdarzeń pochodzących z jednego urządzenia w ciągu dnia nie może przekraczać 20. Jeśli to konieczne, możesz delikatnie zwiększyć ten limit, ale tylko wtedy, gdy liczba urządzeń w sieci jest relatywnie mała (mniej niż 10 000).

Najlepsze praktyki dla Serwera administracyjnego zarządzającego dużą liczbą urządzeń

Najlepsze praktyki korzystania z DBMS

Skonfiguruj zadanie **Konserwacja Serwera administracyjnego**, aby było uruchamiane regularnie, zwłaszcza jeśli używasz systemu DBMS PostgreSQL.

Wyklucz folder DBMS ze skanowania IoC.

Najlepsze praktyki dotyczące zasad i profili

Zmniejsz liczbę aktywnych zasad dla komponentu (np. Kaspersky Endpoint Security for Windows). Możesz zastąpić zasady profilami zasad.

Najlepsze praktyki dla Serwera administracyjnego zarządzającego dużą liczbą urządzeń

Zmniejsz liczbę jednocześnie wykonywanych zadań, zwłaszcza zdalnej instalacji i zarządzania poprawkami.

Zmniejsz liczbę i zoptymalizuj harmonogram zadań, które wymagają wyboru urządzeń.

W sekcji **Konfiguracja zdarzenia** w ustawieniach zasad zminimalizuj liczbę zapisywanych typów zdarzeń.

Najlepsze praktyki dot. przechowywania zdarzeń

Zmniejsz częstotliwość zdarzeń pojedynczego typu ze składnika Kontrola aplikacji. Aby uzyskać szczegółowe informacje, zapoznaj się z poniższym artykułem: Informacje o blokowaniu często występujących zdarzeń.

Zmniejsz okres przechowywania zdarzeń z komponentów (takich jak Kaspersky Endpoint Security for Windows) i zdarzeń informacyjnych o naprawionych lukach.

Włącz opcję **Zapisz zdarzenia dotyczące postępu zadania** w ustawieniach zadania dla typowych zadań, takich jak zadania aktualizacji. Aby uzyskać szczegółowe informacje, zapoznaj się z poniższym artykułem: Rejestrowanie informacji o zdarzeniach dotyczących zadań i zasad.

Zoptymalizuj ustawienia zadania inwentaryzacji. Aby uzyskać szczegółowe informacje, zapoznaj się z poniższym tematem: Zadanie inwentaryzacji.

Szczególne względy i optymalne ustawienia określonych zadań

Niektóre zadania podlegają szczególnym zasadom dotyczącym liczby urządzeń w sieci. Ta sekcja oferuje zalecenia odnośnie optymalnej konfiguracji ustawień takich zadań.

Wyszukiwanie urządzeń, zadanie tworzenia kopii zapasowej danych, zadanie konserwacji baz danych oraz grupowe zadania aktualizacji Kaspersky Endpoint Security są częścią podstawowej funkcjonalności Kaspersky Security Center Linux.

Zadanie inwentaryzacji jest częścią funkcji Zarządzanie lukami i poprawkami i jest niedostępne, jeśli ta funkcja nie została aktywowana.

Częstotliwość wykrywania urządzeń

Nie jest zalecane zwiększanie domyślnej częstotliwości wyszukiwania urządzeń, gdyż może to spowodować znaczne obciążenie kontrolerów domeny. Natomiast zalecane jest skonfigurowanie terminarza przeszukiwania z minimalną możliwą częstotliwością dozwoloną przez potrzeby organizacji. Zalecenia dotyczące obliczenia optymalnego terminarza znajdują się w tabeli poniżej.

Terminarz wyszukiwania urządzeń

Liczba urządzeń w sieci	Zalecana częstotliwość wyszukiwania urządzeń
Mniej niż 10 000	Domyślna częstotliwość lub mniejsza
10 000 lub większa	Raz dziennie lub rzadziej

Zadanie tworzenia kopii zapasowej danych Serwera administracyjnego i zadanie konserwacji baz danych

Serwer administracyjny przestaje działać podczas wykonywania następujących zadań:

- Tworzenie kopii zapasowych danych Serwera administracyjnego
- Konserwacja Serwera administracyjnego

Podczas wykonywania tych zadań baza danych nie może pobierać żadnych danych.

Konieczna może okazać się zmiana terminarza uruchamiania tych zadań, aby nie były uruchamiane w tym samym czasie co inne zadania Serwera administracyjnego.

Grupowe zadania aktualizacji Kaspersky Endpoint Security

Jeśli Serwer administracyjny pełni rolę źródła uaktualnień, zalecana opcja terminarza dla grupowych zadań aktualizacji Kaspersky Endpoint Security 10 i nowszych wersji to **Po pobraniu nowych uaktualnień do repozytorium** z zaznaczonym polem wyboru **Używaj automatycznie losowego opóźnienia dla uruchamiania zadań**.

Jeśli lokalne zadanie pobierania uaktualnień z serwerów Kaspersky do repozytorium jest tworzone na każdym punkcie dystrybucji, okresowe planowanie jest zalecane dla grupowego zadania aktualizacji Kaspersky Endpoint Security. W tym przypadku okres randomizacji musi wynosić jedną godzinę.

Zadanie inwentaryzacji

Możesz zmniejszyć obciążenie bazy danych, jednocześnie uzyskując informacje o plikach wykonywalnych. W tym celu zalecamy uruchomienie zadania inwentaryzacji dla Kaspersky Endpoint Security na odpowiednich urządzeniach, na których jest zainstalowany standardowy zestaw oprogramowania.

Liczba plików wykonywalnych pobranych przez Serwer administracyjny z jednego urządzenia nie może przekraczać 150 000. Jeśli Kaspersky Security Center Linux osiągnie ten limit, nie będzie mógł otrzymywać nowych plików.

Zazwyczaj liczba plików na standardowym urządzeniu klienckim nie przekracza 60 000. Liczba plików wykonywalnych na serwerze plików może być większa, a nawet przekraczać wartość progową wynoszącą 150 000.

Szczegóły dotyczące obciążenia sieci pomiędzy Serwerem administracyjnym a chronionymi urządzeniami

Ta sekcja zawiera wyniki pomiarów testowych ruchu sieciowego wraz z opisem warunków, w jakich te pomiary były robione. Możesz użyć tych informacji podczas planowania infrastruktury sieci i przepustowości sieci w organizacji (lub pomiędzy Serwerem administracyjnym a inną organizacją z urządzeniami, które mają być chronione). Znając przepustowość sieci, możesz w przybliżeniu oszacować czas potrzebny na przesłanie różnych danych.

Zużycie ruchu sieciowego w różnych scenariuszach

Poniższa tabela przedstawia wyniki testów pomiarowych ruchu sieciowego pomiędzy Serwerem administracyjnym a zarządzanym urządzeniem w różnych scenariuszach.

Domyślnie, urządzenia są synchronizowane z Serwerem administracyjnym co 15 minut lub w dłuższych odstępach czasu. Jednakże, jeśli zmodyfikujesz ustawienia zasady lub zadania na Serwerze administracyjnym, wczesna synchronizacja będzie miała miejsce na urządzeniach, do których zasada (lub zadanie) ma zastosowanie, aby nowe ustawienia zostały przesłane na te urządzenia.

Ilość ruchu sieciowego między Serwerem administracyjnym a zarządzanym urządzeniem

Scenariusz	Ruch sieciowy z Serwera administracyjnego do każdego zarządzanego urządzenia	Ruch sieciowy z każdego zarządzanego urządzenia do Serwera administracyjnego
Instalowanie Kaspersky Endpoint Security for Linux z zaktualizowanymi bazami danych	390 MB	3.3 MB
Instalacja Agenta sieciowego	75 MB	397 KB
Instalacja jednoczesna Agenta sieciowego i Kaspersky Endpoint Security for Linux	459 MB	3.6 MB
Wstępna aktualizacja antywirusowych baz danych bez aktualizowania baz danych w pakiecie (jeśli uczestnictwo w Kaspersky Security Network zostało wyłączone)	113 MB	1,8 MB
Codzienna aktualizacja antywirusowych baz danych (jeśli uczestnictwo w Kaspersky Security Network zostało włączone)	22 MB	373 MB
Wstępna synchronizacja przed zaktualizowaniem baz danych na urządzeniu (przesłanie zasad i zadań)	382 KB	446 KB
Wstępna synchronizacja po aktualizacji baz danych na urządzeniu	20 KB	157 KB
Synchronizacja bez zmian na Serwerze administracyjnym (zgodnie z terminarzem)	18 KB	23 KB
Synchronizacja po zmianie jednego ustawienia w zasadzie grupy (natychmiast po zmianie ustawienia)	19 KB	20 KB
Synchronizacja po zmianie jednego ustawienia w zadaniu grupowym (natychmiast po zmianie ustawienia)	14 KB	11 KB
Wymuszona synchronizacja	110 KB	109 KB
Zdarzenie **Wykryto wirusa** (1 wirus)	44 KB	50 KB
Zdarzenie **Wykryto wirusa** (10 wirusów)	58 KB	77 KB
Jednorazowy ruch po włączeniu listy Rejestr aplikacji	do 10 KB	do 12 KB
Codzienny ruch, gdy lista Rejestr aplikacji jest włączona	do 840 KB	do 1 MB

Przeciętne zużycie ruchu sieciowego w ciągu 24 godzin

Średnie 24-godzinne zużycie ruchu sieciowego między Serwerem administracyjnym a zarządzanym urządzeniem jest następujące:

- Ruch sieciowy z Serwera administracyjnego na zarządzane urządzenie wynosi 840 KB.
- Ruch sieciowy z zarządzanego urządzenia do Serwera administracyjnego wynosi 1 MB.

Ruch sieciowy mierzono w następujących warunkach:

- Na zarządzanym urządzeniu zainstalowano Agenta sieciowego i Kaspersky Endpoint Security for Linux.
- Urządzenie nie zostało wskazane jako punkt dystrybucji.
- Funkcja Zarządzanie lukami i poprawkami nie została włączona.
- Częstotliwość synchronizacji z Serwerem administracyjnym wynosiło 15 minut.

Znane problemy

Kaspersky Security Center Linux ma następujące ograniczenia, które nie są krytyczne dla działania aplikacji:

- 10373324: Jeśli na żadnym z węzłów nie zainstalowano Agenta sieciowego, podczas obliczania stanu wskaźnika uwzględniany jest tylko aktualnie aktywny węzeł. Jeśli Agent sieciowy jest zainstalowany na jednym z węzłów, węzeł ten zostanie uwzględniony dopiero, gdy stanie się aktywny. Aby zatem wszystkie węzły były uwzględniane podczas obliczania stanu wskaźnika, należy zainstalować Agenta sieciowego na każdym węźle, a każdy węzeł musi być aktywny co najmniej raz.

- 8994760: Jeśli masz prawa dostępu do wirtualnych Serwerów administracyjnych, ale nie masz praw dostępu do głównego Serwera administracyjnego i próbujesz zalogować się do Kaspersky Security Center Linux, występuje błąd, a komunikat o błędzie **Twoje żądanie nie może być obecnie przetwarzane. Prosimy odczekać i spróbować ponownie później** jest nieprawidłowy. Tekst błędu musi być następujący: **Sprawdź swoje uprawnienia dostępu. Musisz posiadać uprawnienia dostępu na serwerze głównym lub tylko na jednym z serwerów wirtualnych. Skontaktuj się z głównym administratorem, a następnie spróbuj ponownie**

- 10085767: Podczas migracji do Kaspersky Security Center Linux zakres raportu może być wyświetlany nieprawidłowo.

- 10292104: Jeśli w Kaspersky Security Center Web Console w wersji 15.1 lub 15.2 zaktualizujesz wtyczkę Kaspersky Endpoint Detection and Response Optimum do wersji 16.3, sekcja **Alerty** może nie wyświetlać alertów.

- 10308380: Po utworzeniu kategorii aplikacji, jeśli spróbujesz otworzyć jej właściwości z poziomu okna dialogowego potwierdzenia, klikając przycisk **OK**, okno właściwości nie zostanie otwarte.

- 10253149: W przypadku zasad aplikacji, jeśli na karcie **Konfiguracja zdarzenia** wybierzesz zdarzenie masowe, rozwijany blok **Pokaż więcej** z ostrzeżeniem o wpływie takich zdarzeń na wydajność Serwera administracyjnego lub systemu DBMS nie jest wyświetlany.

- 10127434: Jeśli po zalogowaniu się do Kaspersky Security Center Web Console na głównym Serwerze administracyjnym otworzysz sekcję **Zadania**, a następnie otworzysz okno hierarchii, serwer wirtualny jest wyświetlany jako serwer główny.

- 9302142: Opcja **Użyj Agenta sieciowego jako bramy połączenia w DMZ** nie jest obsługiwana w systemie Microsoft Windows opartym na architekturze ARM.

- 9065814: Podczas próby uwierzytelnienia domeny z urządzenia z systemem Windows w domenie Samba 4 może wystąpić błąd.

- 9335676: Po przełączeniu węzła głównego w klastrze DBMS o wysokiej dostępności, dostęp do Kaspersky Security Center Web Console może być niemożliwy lub znacznie opóźniony. Jeśli Kaspersky Security Center Web Console pozostaje niedostępna przez ponad 10 minut, uruchom ponownie usługę IAM za pomocą następującego polecenia:

  ```
  systemctl restart kliam_srv.service
  ```

- 9157005, 9157085: Podczas uruchamiania zadania *Zainstaluj wymagane aktualizacje i napraw luki* na urządzeniu zarządzanym z systemem Windows z włączoną opcją **Uruchom instalację podczas ponownego uruchamiania lub wyłączania urządzenia** zadanie może zakończyć się niepowodzeniem z błędem. Ten problem może wystąpić, gdy zaplanowano instalację dużej liczby aktualizacji. Aby rozwiązać ten problem, uruchom zadanie bez włączania opcji **Uruchom instalację podczas ponownego uruchamiania lub wyłączania urządzenia**.

- 9272534: Jeśli tabela użytkowników zawiera ponad 50 000 użytkowników, wyświetlanych jest tylko pierwszych 50 000 użytkowników, a pozostali użytkownicy nie są widoczni.

- 9291235: Po przywróceniu kopii zapasowej na Serwerze administracyjnym w wersji 16.1, Kaspersky Security Center Web Console wyświetla stronę logowania. Po pomyślnym uwierzytelnieniu wyświetlany jest monit o podanie jednorazowego kodu zabezpieczającego do uwierzytelniania dwuskładnikowego. Po wprowadzeniu prawidłowego jednorazowego kodu zabezpieczającego wyświetlany jest komunikat o błędzie informujący o niepoprawnym kodzie zabezpieczającym. W takim przypadku należy odczekać kilka minut, a następnie ręcznie odświeżyć stronę, aby ponowić próbę zalogowania się do Kaspersky Security Center Web Console. Po pełnym zakończeniu procesu przywracania kopii zapasowej, przy kolejnej próbie uwierzytelnianie zakończy się pomyślnie.

- 7939561: Próba modyfikacji chronionego konta użytkownika po kliknięciu przycisku **Anuluj** w oknie wprowadzania danych uwierzytelniających **Ochrona konta** powoduje wystąpienie błędu.

- 8562938: Otwarcie portu dla urządzeń mobilnych we właściwościach zasad Serwera administracyjnego nie powoduje włączenia funkcji Zarządzanie urządzeniami mobilnymi i nie wyzwala generowania certyfikatu mobilnego. Aby włączyć funkcję Zarządzanie urządzeniami mobilnymi, należy otworzyć port dla urządzeń mobilnych we właściwościach Serwera administracyjnego.

- 8732282: W przypadku użytkownika, który we właściwościach konta w usłudze Active Directory ma włączoną opcję **Użytkownik nie może zmienić hasła**, działanie reagowania **Resetuj hasło** w usłudze Active Directory nie zostanie wykonana. Administrator kontrolera domeny musi wyłączyć opcję **Użytkownik nie może zmienić hasła** dla tego użytkownika lub ręcznie zresetować hasło. Problem ten występuje, jeśli masz licencjonowanie Kaspersky Next XDR Optimum, włączona jest integracja z usługą Active Directory, a użytkownik jest uwzględniony w grupie zabezpieczeń usługi Active Directory.

- 8688182: Jeśli użytkownik ma włączoną opcję **Hasło nigdy nie wygasa** we właściwościach konta w usłudze Active Directory, po wykonaniu działania reagowania **Resetuj hasło**, opcja **Hasło nigdy nie wygasa** zostanie wyłączona, a użytkownik będzie musiał zmienić hasło domeny przy następnym logowaniu. Problem ten występuje, jeśli masz licencjonowanie Kaspersky Next XDR Optimum, włączona jest integracja z usługą Active Directory, a użytkownik jest uwzględniony w grupie zabezpieczeń usługi Active Directory.

- 8703857: Połączenie z serwerem proxy dla Kaspersky Security Center Web Console i webowych wtyczek administracyjnych jest nawiązywane tylko wtedy, gdy serwer proxy obsługuje podstawowe uwierzytelnianie.

- 7911778: Po uruchomieniu zadania **Zdalna dezinstalacja aplikacji** w celu odinstalowania Agenta sieciowego z urządzenia, na którym działa system operacyjny z architekturą Arm i które ma również niezsynchronizowany czas z Serwerem administracyjnym, status zadania nie zmienia się z **Uruchomione** na **Zakończone** nawet po pomyślnym odinstalowaniu Agenta sieciowego z urządzenia. Aby rozwiązać ten problem, przed **Zdalna dezinstalacja aplikacji** należy zsynchronizować czas na urządzeniu z zainstalowanym Agentem sieciowym oraz czas na urządzeniu z Serwerem administracyjnym.

- 6896585: Zarządzane urządzenie nie może połączyć się z KSN poprzez usługę KSN Proxy, jeśli Kaspersky Security Center Linux jest zainstalowany na urządzeniu, które ma w nazwie symbole cyrylicy.

- 7523299: Agent sieciowy nie uruchamia się ponownie po zakończeniu procesu na zarządzanym urządzeniu z systemem CentOS 6.6.

- Jeśli utworzysz zadanie z ustawieniami terminarza **Co N dni** i **Według dni tygodnia** w Kaspersky Security Center Web Console w wersji 15.2 lub nowszej, a następnie otworzysz zadanie w starszych wersjach Kaspersky Security Center Web Console lub Konsoli administracyjnej (na przykład, gdy zadanie jest również stosowane na podrzędnych Serwerach administracyjnych, które mogą być zarówno oparte na systemie Linux, jak i Windows), ustawienia terminarza mogą być wyświetlane nieprawidłowo lub może wystąpić błąd.

- 7208621: W przypadku importowania zadania *Pobierz uaktualnienia do repozytoriów punktów dystrybucji* lub zadania *Weryfikacja uaktualnień*, włączona jest opcja **Wybierz urządzenia, do których zadanie zostanie przypisane**. Zadań tych nie można przypisać do wyboru urządzenia ani do określonych urządzeń. W przypadku przypisania zadania *Pobierz uaktualnienia do repozytoriów punktów dystrybucji* lub zadania *Weryfikacja aktualizacji* do określonych urządzeń, zadanie zostanie zaimportowane niepoprawnie.

- 6511063: Jeśli aplikacja z sekcji **Rejestr aplikacji** została wykryta na urządzeniu z systemem Linux, właściwości aplikacji nie zawierają informacji o powiązanych plikach wykonywalnych.

- 5915107: W raportach o formacie literowym podział strony może przecinać linię tekstu w poziomie.

- 5556109: Zarządzane urządzenie, które ma więcej niż jedną kartę sieciową, wysyła do Serwera administracyjnego informacje o adresie MAC karty sieciowej, która nie jest używana do łączenia się z Serwerem administracyjnym.

- 9093038: Jeżeli Serwer administracyjny Kaspersky Security Center Linux nie uruchomi się po instalacji, a dziennik systemu operacyjnego zawiera błąd 213/SECUREBITS związany z usługą kladminserver_srv.service, wykonaj następujące polecenia jako superużytkownik:

  ```
  mkdir -p /etc/systemd/system/kladminserver_srv.service.d
  echo "[Service]" > /etc/systemd/system/kladminserver_srv.service.d/override.conf
  echo "AmbientCapabilities=CAP_IPC_LOCK" >> /etc/systemd/system/kladminserver_srv.service.d/override.conf
  mkdir -p /etc/systemd/system/klwebsrv_srv.service.d
  echo "[Service]" > /etc/systemd/system/klwebsrv_srv.service.d/override.conf
  echo "AmbientCapabilities=CAP_IPC_LOCK" >> /etc/systemd/system/klwebsrv_srv.service.d/override.conf
  ```

  Jeżeli Kaspersky Security Center Web Console nie uruchomi się po instalacji, a dziennik systemu operacyjnego zawiera błąd 213/SECUREBITS związany z KSCWebConsole.service, wykonaj następujące polecenia jako superużytkownik:

  ```
  mkdir -p /etc/systemd/system/KSCSvcWebConsole.service.d
  echo "[Service]" > /etc/systemd/system/KSCSvcWebConsole.service.d/override.conf
  echo "AmbientCapabilities=CAP_IPC_LOCK" >> /etc/systemd/system/KSCSvcWebConsole.service.d/override.conf
  mkdir -p /etc/systemd/system/KSCWebConsoleManagement.service.d
  echo "[Service]" > /etc/systemd/system/KSCWebConsoleManagement.service.d/override.conf
  echo "AmbientCapabilities=CAP_IPC_LOCK" >> /etc/systemd/system/KSCWebConsoleManagement.service.d/override.conf
  mkdir -p /etc/systemd/system/KSCWebConsoleNATS.service.d
  echo "[Service]" > /etc/systemd/system/KSCWebConsoleNATS.service.d/override.conf
  echo "AmbientCapabilities=CAP_IPC_LOCK" >> /etc/systemd/system/KSCWebConsoleNATS.service.d/override.conf
  mkdir -p /etc/systemd/system/KSCWebConsolePlugin.service.d
  echo "[Service]" > /etc/systemd/system/KSCWebConsolePlugin.service.d/override.conf
  echo "AmbientCapabilities=CAP_IPC_LOCK" >> /etc/systemd/system/KSCWebConsolePlugin.service.d/override.conf
  mkdir -p /etc/systemd/system/KSCWebConsole.service.d
  echo "[Service]" > /etc/systemd/system/KSCWebConsole.service.d/override.conf
  echo "AmbientCapabilities=CAP_IPC_LOCK" >> /etc/systemd/system/KSCWebConsole.service.d/override.conf
  ```

  Jeśli usługa kliam_srv nie uruchomi się po instalacji, a dziennik systemu operacyjnego zawiera błąd 213/SECUREBITS związany z usługą, wykonaj następujące polecenia jako superużytkownik:

  ```
  mkdir -p /etc/systemd/system/kliam_srv.service.d
  echo "[Service]" > /etc/systemd/system/kliam_srv.service.d/override.conf
  echo "AmbientCapabilities=CAP_IPC_LOCK" >> /etc/systemd/system/kliam_srv.service.d/override.conf
  ```

- 9165434: Uwierzytelnianie NTLM nie działa dla kont użytkowników należących do grupy Chronieni użytkownicy.

Kontakt z działem pomocy technicznej

Ta sekcja opisuje sposób uzyskania pomocy technicznej oraz warunki, na jakich jest ona dostępna.

Jak uzyskać pomoc techniczną

Jeśli nie znajdziesz rozwiązania swojego problemu w dokumentacji do Kaspersky Security Center Linux lub w jednym z dodatkowych źródeł informacji o Kaspersky Security Cente Linuxr, skontaktuj się z działem pomocy technicznej Kaspersky. Specjaliści z działu pomocy technicznej odpowiedzą na wszystkie pytania związane z instalacją i użytkowaniem Kaspersky Security Center Linux.

Kaspersky zapewnia wsparcie dla Kaspersky Security Center Linux w trakcie jej cyklu życia (zobacz stronę zawierającą czas trwania wsparcia technicznego aplikacji). Przed skontaktowaniem się z działem pomocy technicznej przeczytaj zasady korzystania z pomocy technicznej.

Możesz skontaktować się z działem pomocy technicznej na jeden z następujących sposobów:

- Odwiedzając witrynę pomocy technicznej
- Wysyłając zgłoszenie do pomocy technicznej poprzez portal Kaspersky CompanyAccount

Pomoc techniczna poprzez Kaspersky CompanyAccount

Kaspersky CompanyAccount jest to portal dla firm korzystających z aplikacji firmy Kaspersky. Portal Kaspersky CompanyAccount został zaprojektowany w celu ułatwienia interakcji między użytkownikami a specjalistami z Kaspersky poprzez zgłoszenia online. Możesz używać Kaspersky CompanyAccount do śledzenia stanu zgłoszeń online, a także przechowywać ich historię.

Możliwe jest zarejestrowanie wszystkich pracowników firmy pod jednym kontem w serwisie Kaspersky CompanyAccount. Jedno konto umożliwia scentralizowane zarządzanie zgłoszeniami elektronicznymi zarejestrowanych pracowników oraz zarządzanie uprawnieniami tych pracowników poprzez Kaspersky CompanyAccount.

Portal Kaspersky CompanyAccount jest dostępny w następujących językach:

- angielskim
- hiszpańskim
- włoskim
- niemieckim
- polskim
- portugalskim

- rosyjskim
- francuskim
- japońskim

Więcej informacji o Kaspersky CompanyAccount można znaleźć na stronie pomocy technicznej.

Uzyskiwanie plików zrzutu Serwera administracyjnego

Pliki zrzutów Serwera administracyjnego zawierają wszystkie informacje o procesach Serwera administracyjnego w danym momencie. Pliki zrzutów Serwera administracyjnego są przechowywane w katalogu /var/lib/systemd/coredump. Pliki zrzutów są przechowywane tak długo, jak używany jest Kaspersky Security Center Linux, i w przypadku usunięcia są usuwane trwale. Pliki zrzutu nie są automatycznie wysyłane do Kaspersky.

Jeśli Serwer administracyjny ulegnie awarii, możesz skontaktować się z pomocą techniczną Kaspersky, specjalista pomocy technicznej może poprosić Cię o przesłanie plików zrzutów Serwera administracyjnego w celu dalszej analizy w Kaspersky.

Pliki zrzutów mogą zawierać dane osobowe. Zalecamy, aby przed wysłaniem informacji do Kaspersky zabezpieczyć je przed nieautoryzowanym dostępem.

Źródła informacji o aplikacji

Strona Kaspersky Security Center Linux w witrynie internetowej Kaspersky

Na stronie Kaspersky Security Center Linux w witrynie internetowej Kaspersky znajdziesz ogólne informacje o aplikacji, jej funkcjach i właściwościach.

Strona Kaspersky Security Center Linux w Bazie wiedzy

Baza wiedzy to sekcja na stronie działu pomocy technicznej Kaspersky.

Na stronie Kaspersky Security Center Linux w Bazie wiedzy możesz przeczytać artykuły zawierające przydatne informacje, zalecenia i odpowiedzi na najczęściej zadawane pytania dotyczące zakupu, instalacji i korzystania z aplikacji.

Artykuły w Bazie wiedzy mogą zawierać odpowiedzi na pytania dotyczące Kaspersky Security Center Linux, a także innych aplikacji firmy Kaspersky. Artykuły w Bazie wiedzy mogą zawierać także nowości z działu pomocy technicznej.

Społeczność użytkowników produktów firmy Kaspersky

Jeżeli zapytanie nie wymaga natychmiastowej odpowiedzi, możesz przedyskutować je ze specjalistami z firmy Kaspersky lub z innymi użytkownikami na naszym Forum.

Na Forum możesz przeglądać istniejące tematy, pozostawiać swoje komentarze i tworzyć nowe tematy.

> Do przeglądania zasobów internetowych wymagane jest połączenie z internetem.

Jeśli nie możesz znaleźć rozwiązania swojego problemu, skontaktuj się z działem pomocy technicznej.

Słownik

Administrator dostawcy usługi

Pracownik u dostawcy usługi ochrony antywirusowej. Administrator wdraża i obsługuje systemy ochrony antywirusowej oparte na produktach antywirusowych firmy Kaspersky oraz zapewnia klientom pomoc techniczną.

Administrator Kaspersky Security Center Linux

Osoba zarządzająca działaniami aplikacji poprzez system scentralizowanej zdalnej administracji Kaspersky Security Center Linux.

Administrator klienta

Pracownik firmy klienta, który jest odpowiedzialny za stan ochrony antywirusowej i monitorowanie.

Agent autoryzacji

Interfejs umożliwiający przeprowadzenie procesu autoryzacji w celu uzyskania dostępu do zaszyfrowanych dysków twardych i załadowania systemu operacyjnego po zaszyfrowaniu dysku twardego.

Agent sieciowy

Składnik Kaspersky Security Center Linux umożliwiający interakcję Serwera administracyjnego z aplikacjami firmy Kaspersky zainstalowanymi na określonym węźle sieciowym (stacji roboczej lub serwerze). Ten moduł jest wspólny dla wszystkich produktów Kaspersky dla Microsoft® Windows®. Oddzielne wersje Agenta sieciowego dostępne są dla aplikacji Kaspersky przeznaczonych dla systemów Unix i macOS.

Aktualizacja

Procedura zastępowania lub dodawania nowych plików (baz danych lub modułów aplikacji) pobieranych z serwerów aktualizacji firmy Kaspersky.

Aktywny klucz

Klucz, który jest aktualnie używany przez aplikację.

Antywirusowe bazy danych

Bazy danych zawierają opisy zagrożeń ochrony komputera znane specjalistom z Kaspersky w momencie opublikowania antywirusowych baz danych. Wpisy w antywirusowych bazach danych pozwalają na wykrywanie szkodliwego kodu w skanowanych obiektach. Antywirusowe bazy danych są tworzone przez specjalistów z Kaspersky i aktualizowane co godzinę.

Atak wirusa

Seria celowych prób zainfekowania urządzenia wirusem.

Bezpośrednie zarządzanie aplikacjami

Zarządzanie aplikacją poprzez interfejs lokalny.

Brama połączenia

Brama połączenia to Agent sieciowy działający w trybie specjalnym. Brama połączenia akceptuje połączenia z innych Agentów sieciowych i tuneluje je przez Serwer administracyjny poprzez własne połączenie z serwerem. W przeciwieństwie do zwykłego Agenta sieciowego brama połączenia oczekuje na połączenia z Serwerem administracyjnym bardziej niż nawiązuje te połączenia z Serwerem administracyjnym.

Certyfikat współdzielony

Certyfikat, który jest przeznaczony do identyfikacji urządzenia mobilnego użytkownika.

Certyfikatu Serwera administracyjnego

Certyfikat używany przez Serwer administracyjny do następujących celów:

- Uwierzytelnianie Serwera administracyjnego podczas łączenia się z Kaspersky Security Center Web Console
- Bezpieczna interakcja pomiędzy Serwerem administracyjnym a Agentami sieciowymi na zarządzanych urządzeniach
- Uwierzytelnianie Serwerów administracyjnych podczas łączenia głównego Serwera administracyjnego z podrzędnym Serwerem administracyjnym

Certyfikat jest tworzony automatycznie podczas instalacji Serwera administracyjnego, a następnie jest przechowywany na Serwerze administracyjnym.

Cloud Discovery

Cloud Discovery zarządza dostępem użytkowników do usług w chmurze. Do usług w chmurze zalicza się np. Microsoft Teams, Salesforce, Microsoft Office 365. Usługi w chmurze są pogrupowane w kategorie, na przykład *Udostępnianie plików*, *Komunikatory*, *Poczta e-mail*.

Dodatkowy (lub rezerwowy) klucz licencyjny

Klucz, który daje prawo do korzystania z aplikacji, chociaż nie jest on aktualnie w użyciu.

Domena rozgłoszeniowa

Logiczny obszar sieci, w której wszystkie węzły mogą wymieniać dane przy użyciu kanału informacyjnego na poziomie modelu OSI (Open Systems Interconnection Basic Reference Model).

Dostawca usługi ochrony antywirusowej

Firma, która oferuje organizacji klienta usługę ochrony antywirusowej opartą na rozwiązaniach firmy Kaspersky.

Dostępne aktualizacje

Zestaw uaktualnień dla modułów aplikacji firmy Kaspersky, w tym krytycznych aktualizacji zebranych przez pewien okres czasu oraz zmiany w architekturze aplikacji.

FileTransferBridge

Wewnętrzny komponent Kaspersky Security Center Linux zapewniający lokalne dostarczanie aktualizacji aplikacji firmy Kaspersky. FileTransferBridge jest zintegrowany z Agentem sieciowym (klnagent) i działa lokalnie na każdym zarządzanym urządzeniu.

Gdy aplikacje firmy Kaspersky otrzymują aktualizacje z Kaspersky Security Center Linux, Agent sieciowy pobiera pliki aktualizacji z Serwera administracyjnego lub punktu dystrybucji. FileTransferBridge przekazuje następnie pliki lokalnie do zainstalowanych aplikacji firmy Kaspersky, zapewniając niezawodne dostarczanie aktualizacji baz danych i poprawek oprogramowania.

FileTransferBridge używa portów TCP 30522 i 30523. Porty nasłuchują wyłącznie na interfejsie localhost (127.0.0.1) i nie akceptują połączeń przychodzących z sieci zewnętrznych.

Folder Kopia zapasowa

Specjalny folder do przechowywania kopii danych Serwera administracyjnego utworzonych przy użyciu narzędzia kopii zapasowej.

Funkcja rozpoznawania lokalizacji w sieci (NLA)

Usługa systemu Windows, która pomaga systemowi operacyjnemu zidentyfikować bieżącą sieć. NLA wykrywa zmiany w sieci i dostosowuje konfigurację zabezpieczeń urządzenia.

Grupa administracyjna

Zestaw urządzeń pogrupowanych według funkcji i zainstalowanych aplikacji firmy Kaspersky. Urządzenia są pogrupowane dla ułatwienia zarządzania nimi jako pojedynczą jednostką. Grupa może zawierać w sobie inne grupy. Zasady grupy i zadania grupy mogą być tworzone dla każdej zainstalowanej aplikacji w grupie.

Grupa ról

Grupa użytkowników urządzeń mobilnych z Exchange ActiveSync, którzy uzyskali podobne uprawnienia administracyjne.

HTTPS

Bezpieczny protokół używający szyfrowania do przesyłania danych między przeglądarką internetową a serwerem sieciowym. HTTPS jest używany w celu uzyskania dostępu do poufnych informacji, takich jak dane firmowe i finansowe.

Instalacja lokalna

Instalacja aplikacji zabezpieczającej na urządzeniu w sieci firmowej, która zakłada ręczne uruchomienie procesu instalacji z pakietu dystrybucyjnego aplikacji antywirusowej lub ręczne uruchomienie opublikowanego pakietu instalacyjnego, który wcześniej został pobrany na urządzenie.

Instalacja ręczna

Instalacja aplikacji zabezpieczającej na urządzeniu w sieci firmowej z pakietu dystrybucyjnego. Ręczna instalacja musi odbywać się z udziałem administratora lub innego specjalisty ds. IT. Zazwyczaj ręczna instalacja jest wykonywana wtedy, gdy zdalna instalacja zakończyła się błędem.

Instalacja zdalna

Instalacja aplikacji firmy Kaspersky przy użyciu usług oferowanych przez Kaspersky Security Center Linux.

Istotność poprawki

Atrybut poprawki. Dla poprawek firmy Microsoft i poprawek firm trzecich istnieje pięć poziomów istotności:

- Krytyczny
- Wysoki
- Średni
- Niski
- Nieznany

Istotność poprawki firmy trzeciej lub firmy Microsoft jest determinowana przez najmniej preferowane priorytety wśród luk, które poprawka powinna wyeliminować.

JavaScript

Język programowania rozszerzający działanie stron internetowych. Strony internetowe utworzone przy użyciu JavaScript mogą wykonywać funkcje (na przykład zmieniać widok elementów interfejsu lub otwierać dodatkowe okna) bez konieczności odświeżania strony internetowej z nowymi danymi z serwera sieciowego. Aby przeglądać strony utworzone przy użyciu JavaScript, włącz obsługę JavaScript w ustawieniach swojej przeglądarki internetowej.

Kaspersky Private Security Network (KPSN)

Sieć Kaspersky Private Security Network to rozwiązanie, które daje użytkownikom urządzeń z zainstalowanymi aplikacjami firmy Kaspersky możliwość dostępu do baz danych reputacji Kaspersky Security Network i innych danych statystycznych bez wysyłania danych z ich urządzeń do Kaspersky Security Network. Sieć Kaspersky Private Security Network została zaprojektowana dla klientów korporacyjnych, którzy nie mogą uczestniczyć w Kaspersky Security Network z jednego z następujących powodów:

- Urządzenia nie są podłączone do Internetu.
- Przesyłanie jakichkolwiek danych poza kraj lub firmową sieć LAN jest zabronione przez prawo lub politykę bezpieczeństwa firmy.

Kaspersky Security Center Linux Web Server

Składnik Kaspersky Security Center Linux, który jest instalowany razem z Serwerem administracyjnym. Serwer WWW został zaprojektowany do przesyłania za pośrednictwem sieci autonomicznych pakietów instalacyjnych, profili iOS MDM oraz plików z folderu współdzielonego.

Kaspersky Security Center System Health Validator (SHV)

Składnik aplikacji Kaspersky Security Center Linux, zaprojektowany do sprawdzania działania systemu operacyjnego w przypadku równoczesnego działania Kaspersky Security Center Linux i Microsoft NAP.

Klient Serwera administracyjnego (urządzenie klienckie)

Urządzenie, serwer lub stacja robocza, na której zainstalowany jest Agent sieciowy i zarządzane aplikacje Kaspersky.

Konsola administracyjna

Składnik Kaspersky Security Center oparty na systemie Windows (zwany również Konsolą administracyjną opartą na MMC). Ten składnik zapewnia interfejs użytkownika dla usług administracyjnych Serwera administracyjnego i Agenta sieciowego. Konsola administracyjna jest odpowiednikiem Kaspersky Security Center Web Console.

Kopia zapasowa danych Serwera administracyjnego

Kopiowanie przy użyciu narzędzia kopii zapasowej danych Serwera administracyjnego do miejsca przechowywania oraz ich późniejsze przywracanie. Narzędzie to umożliwia zapisanie:

- Bazy danych Serwera administracyjnego (zasady, zadania, ustawienia aplikacji, zdarzenia zapisane na Serwerze administracyjnym)
- Informacji o konfiguracji struktury grup administracyjnych i urządzeń klienckich
- Miejsc przechowywania plików instalacyjnych przeznaczonych do zdalnej instalacji aplikacji (zawartość folderów: Pakiety, Dezinstalacja uaktualnień)
- Certyfikatu Serwera administracyjnego

Lightweight Nagent (LWNGT)

Protokół interakcji z Kaspersky Endpoint Security na urządzeniach mobilnych. Protokół LWNGT (zwany również protokołem mobilnym) funkcjonuje jako Agent sieciowy bez konieczności faktycznej instalacji Agenta sieciowego na urządzeniach mobilnych.

Luka

Jest to słaby punkt systemu operacyjnego lub aplikacji, który może zostać wykorzystany przez twórców szkodliwego oprogramowania w celu przeniknięcia do systemu operacyjnego lub aplikacji i naruszenia jego/jej integralności. Duża liczba luk w systemie operacyjnym świadczy o jego zawodności, gdyż wirusy, które przeniknęły do systemu, mogą powodować błędy w działaniu systemu i zainstalowanych aplikacjach.

Macierzysty Serwer administracyjny

Macierzysty Serwer administracyjny jest to Serwer administracyjny, który został określony podczas instalacji Agenta sieciowego. Macierzysty Serwer administracyjny może zostać użyty w ustawieniach profili połączenia Agenta sieciowego.

Menedżer tożsamości i dostępu (IAM)

Komponent Serwera administracyjnego, który umożliwia korzystanie z uwierzytelniania domeny (pojedynczego logowania). Funkcja pojedynczego logowania umożliwia użytkownikowi włączenie bezpiecznego uwierzytelniania w konsoli Kaspersky Security Center Web Console bez konieczności ponownego wprowadzania hasła w sieci firmowej.

Niekompatybilna aplikacja

Aplikacja antywirusowa innego producenta lub aplikacja firmy Kaspersky, która nie obsługuje opcji zarządzania poprzez Kaspersky Security Center Linux.

Ochrona antywirusowa sieci

Zestaw działań technicznych i firmowych, które zmniejszają prawdopodobieństwo przeniknięcia wirusów i spamu do sieci organizacji, a także blokują ataki sieciowe, phishing i inne zagrożenia. Ochrona sieci wzrasta, gdy używasz usług i aplikacji zabezpieczających i gdy stosujesz zasady ochrony danych firmowych.

Okres licencji

Przedział czasu, w którym masz dostęp do funkcji aplikacji i posiadasz uprawnienia do korzystania z dodatkowych usług. Zakres usług zależy od typu licencji.

Operator Kaspersky Security Center

Użytkownik monitorujący stan i działanie systemu ochrony zarządzanego poprzez Kaspersky Security Center.

Pakiet instalacyjny

Zestaw plików utworzonych dla zdalnej instalacji aplikacji Kaspersky przy pomocy systemu zdalnego zarządzania Kaspersky Security Center. Pakiet instalacyjny zawiera zakres ustawień potrzebnych do zainstalowania aplikacji i uruchomienia jej natychmiast po zainstalowaniu. Ustawienia odpowiadają domyślnym ustawieniom aplikacji. Pakiet instalacyjny jest tworzony przy użyciu plików z rozszerzeniami .kpd i .kud zawartych w pakiecie dystrybucyjnym aplikacji.

Plik klucza

Plik w formacie xxxxxxxx.key pozwala na korzystanie z aplikacji firmy Kaspersky na warunkach licencji testowej lub komercyjnej.

Priorytet zdarzenia

Cecha zdarzenia, które wystąpiło podczas działania aplikacji firmy Kaspersky. Dostępne są następujące priorytety:

- Zdarzenie krytyczne
- Błąd funkcjonalny
- Ostrzeżenie
- Informacja

Zdarzenia tego samego typu mogą posiadać różne poziomy priorytetu, w zależności od sytuacji, w której wystąpiły.

Profil

Zbiór ustawień urządzeń mobilnych Exchange określających ich zachowanie po podłączeniu do serwera Microsoft Exchange Server.

Profil informacyjny

Zbiór ustawień dotyczących działania aplikacji na urządzeniach mobilnych iOS. Profil informacyjny zawiera informacje o licencji; jest związany z określoną aplikacją.

Profil konfiguracyjny

Zasada zawierająca zbiór ustawień i ograniczeń dla urządzenia mobilnego iOS MDM.

Przywracanie

Przeniesienie oryginalnego obiektu z kwarantanny lub folderu kopii zapasowej do folderu, w którym się znajdował przed umieszczeniem go w kwarantannie, wyleczeniem czy usunięciem, lub do folderu wskazanego przez użytkownika.

Przywrócenie danych Serwera administracyjnego

Przywrócenie danych Serwera administracyjnego z informacji zapisanej w kopii zapasowej przy pomocy narzędzia kopii zapasowej. Narzędzie to umożliwia przywrócenie:

- Bazy danych Serwera administracyjnego (zasady, zadania, ustawienia aplikacji, zdarzenia zapisane na Serwerze administracyjnym)
- Informacji o konfiguracji struktury grup administracyjnych i urządzeń klienckich
- Miejsc przechowywania plików instalacyjnych przeznaczonych do zdalnej instalacji aplikacji (zawartość folderów: Pakiety, Dezinstalacja uaktualnień)
- Certyfikatu Serwera administracyjnego

Punkt dystrybucji

Komputer, na którym został zainstalowany Agent sieciowy i który jest używany do rozsyłania uaktualnień, zdalnej instalacji aplikacji, uzyskiwania informacji o komputerach w grupie administracyjnej i/lub domenie rozgłoszeniowej. Punkty dystrybucji zostały utworzone w celu zmniejszenia obciążenia na Serwerze administracyjnym podczas dystrybucji aktualizacji i zoptymalizowania ruchu sieciowego. Punkty dystrybucji mogą być wskazywane automatycznie, przez Serwer administracyjny, lub ręcznie, przez administratora. Punkt dystrybucji był wcześniej znany jako agent aktualizacji.

Repozytorium zdarzeń

Część bazy danych Serwera administracyjnego przeznaczonej do przechowywania informacji o zdarzeniach, które występują w Kaspersky Security Center Linux.

Scentralizowane zarządzanie aplikacjami

Zdalne zarządzanie aplikacją przy pomocy usług administracyjnych zawartych w Kaspersky Security Center.

Serwer administracyjny

Moduł aplikacji Kaspersky Security Center Linux realizujący funkcje scentralizowanego przechowywania informacji na temat wszystkich aplikacji firmy Kaspersky zainstalowanych w sieci korporacyjnej. Może być używany do zarządzania tymi aplikacjami.

Serwer iOS MDM

Składnik Kaspersky Security Center zainstalowany na urządzeniu klienckim pozwalający na połączenie urządzeń mobilnych iOS z Serwerem administracyjnym za pośrednictwem usługi Apple Push Notifications (APN).

Serwery aktualizacji Kaspersky

Serwery HTTP(S) firmy Kaspersky, z których aplikacje Kaspersky pobierają uaktualnienia baz danych i modułów aplikacji.

Sklep aplikacji

Składnik Kaspersky Security Center Linux. Sklep aplikacji jest używany do zainstalowania aplikacji na urządzeniach z systemem Android, należących do użytkownika. Sklep aplikacji umożliwia opublikowanie plików APK aplikacji oraz odnośników do aplikacji w Google Play.

SSL

Protokół szyfrowania danych używany w internecie i sieciach lokalnych. Protokół Secure Sockets Layer (SSL) jest używany w aplikacjach internetowych do tworzenia bezpiecznego połączenia między klientem a serwerem.

Stacja robocza administratora

Urządzenie, z którego otwierasz Kaspersky Security Center Web Console. Ten składnik zapewnia interfejs zarządzania Kaspersky Security Center Linux.

Stacja robocza administratora służy do konfigurowania i zarządzania częścią serwerową Kaspersky Security Center Linux. Korzystając ze stacji roboczej administratora, administrator tworzy i zarządza scentralizowanym systemem ochrony antywirusowej dla korporacyjnych sieci LAN opartych o aplikacje Kaspersky.

Stan ochrony

Bieżący stan ochrony, który odzwierciedla poziom ochrony komputera.

Stan ochrony sieci

Bieżący stan ochrony, który definiuje bezpieczeństwo urządzeń w sieci firmowej. Stan ochrony sieci uwzględnia takie czynniki, jak zainstalowane aplikacje zabezpieczające, użycie kluczy licencyjnych oraz liczba i typy wykrytych zagrożeń.

Strefa zdemilitaryzowana (DMZ)

Strefa zdemilitaryzowana jest segmentem sieci lokalnej zawierającej serwery, które odpowiadają na zapytania z sieci globalnej. Aby zapewnić bezpieczeństwo firmowej sieci lokalnej, dostęp do sieci LAN z poziomu strefy zdemilitaryzowanej jest chroniony przez zaporę sieciową.

Uprawnienia administracyjne

Poziom uprawnień użytkownika wymaganych do zarządzania obiektami Exchange w obrębie organizacji Exchange.

Urządzenie iOS MDM

Urządzenie mobilne, które jest podłączone do serwera iOS MDM poprzez protokół iOS MDM. Urządzenia działające pod kontrolą systemu operacyjnego iOS mogą być podłączane i zarządzane poprzez protokół iOS MDM.

Ustawienia programu

Ustawienia aplikacji, które są wspólne dla wszystkich typów zadań i zarządzają ogólnym działaniem aplikacji, na przykład, ustawienia działania aplikacji, ustawienia raportowania i ustawienia tworzenia kopii zapasowej.

Ustawienia zadania

Ustawienia aplikacji, które są specyficzne dla każdego typu zadania.

Użytkownicy wewnętrzni

Konta użytkowników wewnętrznych są używane do pracy z wirtualnymi Serwerami administracyjnymi. Kaspersky Security Center Linux nadaje wewnętrznym użytkownikom aplikacji uprawnienia rzeczywistych użytkowników.

Konta wewnętrznych użytkowników są tworzone i używane tylko w obrębie Kaspersky Security Center Linux. Do systemu operacyjnego nie są przesyłane żadne dane dotyczące wewnętrznych użytkowników. Kaspersky Security Center Linux uwierzytelnia wewnętrznych użytkowników.

Wirtualny Serwer administracyjny

Składnik Kaspersky Security Center Linux zaprojektowany do zarządzania systemem ochrony sieci organizacji klienta.

Wirtualny Serwer administracyjny jest szczególnym przypadkiem podrzędnego Serwera administracyjnego i ma następujące ograniczenia w porównaniu z fizycznym Serwerem administracyjnym:

- Wirtualny Serwer administracyjny można utworzyć tylko na głównym Serwerze administracyjnym.
- Podczas działania wirtualny Serwer administracyjny używa bazy danych głównego Serwera administracyjnego. Zadania tworzenia kopii zapasowych i przywracania danych, a także zadania pobierania i skanowania aktualizacji nie są obsługiwane na wirtualnym Serwerze administracyjnym.
- Serwer wirtualny nie obsługuje tworzenia podrzędnych Serwerów administracyjnych (łącznie z Serwerami wirtualnymi).

Właściciel urządzenia

Właściciel urządzenia to użytkownik, z którym administrator może skontaktować się, gdy zajdzie potrzeba wykonania określonych działań na urządzeniu.

Zadanie

Funkcje wykonywane przez aplikacje Kaspersky są zaimplementowane w postaci zadań, na przykład: Ochrona plików w czasie rzeczywistym, Pełne skanowanie komputera, Aktualizacja baz danych.

Zadanie dla określonych urządzeń

Zadanie przypisane do zbioru urządzeń klienckich z dowolnej grupy administracyjnej, wykonywane na tych urządzeniach.

Zadanie grupowe

Zadanie zdefiniowane dla grupy administracyjnej i wykonywane na wszystkich urządzeniach klienckich należących do tej grupy administracyjnej.

Zadanie lokalne

Zadanie utworzone i uruchomione na pojedynczym komputerze klienckim.

Zarządzane urządzenia

Urządzenia z sieci firmowej, które znajdują się w grupie administracyjnej.

Zasada

Zasada określa ustawienia aplikacji i zarządza możliwością konfigurowania tą aplikacją na komputerach w grupie administracyjnej. Dla każdej aplikacji należy utworzyć jedną zasadę. Możliwe jest utworzenie kilku zasad dla aplikacji zainstalowanych na komputerach w każdej grupie administracyjnej, ale tylko jedna zasada może być stosowana do każdej aplikacji w obrębie grupy administracyjnej w danym czasie.

Informacje o kodzie firm trzecich

Informacje o kodzie firm trzecich znajdują się w pliku legal_notices.txt w katalogu instalacyjnym aplikacji.

Informacje o znakach towarowych

Zastrzeżone znaki towarowe i usługowe stanowią odpowiednio własność ich właścicieli.

Adobe, Acrobat, Flash, PostScript i Shockwave są zastrzeżonymi znakami towarowymi lub znakami towarowymi firmy Adobe w Stanach Zjednoczonych i/lub innych krajach.

AMD, AMD64 są znakami towarowymi lub zastrzeżonymi znakami towarowymi firmy Advanced Micro Devices, Inc.

Amazon, Amazon Web Services, AWS, Amazon EC2, AWS Marketplace są znakami towarowymi firmy Amazon.com, Inc. lub jej podmiotów stowarzyszonych.

Apache jest zastrzeżonym znakiem towarowym lub znakiem towarowym firmy Apache Software Foundation w Stanach Zjednoczonych i/lub innych krajach.

Apple, AirPlay, AirDrop, AirPrint, App Store, Apple Configurator, AppleScript, FaceTime, FileVault, iBook, iBooks, iCloud, iPad, iPhone, iTunes, Leopard, macOS, Mac, Mac OS, OS X, Safari, Snow Leopard, Tiger, QuickTime i Touch ID są zastrzeżonymi znakami towarowymi firmy Apple Inc.

Arm jest zastrzeżonym znakiem towarowym firmy Arm Limited (lub jej spółek zależnych) w Stanach Zjednoczonych i/lub innych krajach.

Logo, marka i słowo Bluetooth należą do firmy Bluetooth SIG, Inc.

Ubuntu, LTS są zastrzeżonymi znakami towarowymi firmy Canonical Ltd.

Cisco, Cisco Jabber, Cisco Systems, IOS są zastrzeżonymi znakami towarowymi lub znakami towarowymi firmy Cisco Systems, Inc. i/lub jej oddziałów w Stanach Zjednoczonych i innych krajach.

Citrix, XenServer są zarejestrowanymi znakami towarowymi lub znakami towarowymi firmy Cloud Software Group, Inc. i/lub jej spółek zależnych w Stanach Zjednoczonych i/lub innych krajach.

Corel jest zastrzeżonym znakiem towarowym bądź znakiem towarowym firmy Corel Corporation i/lub jej oddziałów w Kanadzie, Stanach Zjednoczonych i/lub innych krajach.

Cloudflare, logo Cloudflare i Cloudflare Workers są znakami towarowymi i/lub zastrzeżonymi znakami towarowymi firmy Cloudflare, Inc. w Stanach Zjednoczonych i innych jurysdykcjach.

Dropbox jest zastrzeżonym znakiem towarowym firmy Dropbox, Inc.

Radmin jest zastrzeżonym znakiem towarowym firmy Famatech.

Firebird jest zastrzeżonym znakiem towarowym firmy Firebird Foundation.

Foxit jest zastrzeżonym znakiem towarowym firmy Foxit Corporation.

FreeBSD jest zastrzeżonym znakiem towarowym firmy The FreeBSD Foundation.

Google, Android, Chrome, Chromium, Dalvik, Firebase, Google Chrome, Google Earth, Google Play, Google Maps, Google Public DNS, Hangouts i YouTube są zastrzeżonymi znakami towarowymi firmy Google, Inc.

EulerOS, FusionCompute, FusionSphere są znakami towarowymi firmy Huawei Technologies Co., Ltd.

Intel, Core, Xeon są znakami towarowymi firmy Intel Corporation lub jej spółek zależnych.

IBM, QRadar są znakami towarowymi firmy International Business Machines Corporation, zarejestrowanymi w wielu jurysdykcjach na świecie.

Node.js jest zastrzeżonym znakiem towarowym firmy Joyent, Inc.

Linux jest zastrzeżonym znakiem towarowym Linus Torvalds w Stanach Zjednoczonych i innych krajach.

Logitech jest zastrzeżonym znakiem towarowym lub znakiem towarowym firmy Logitech w Stanach Zjednoczonych i/lub innych krajach.

Microsoft, Active Directory, ActiveSync, BitLocker, Excel, Forefront, Internet Explorer, InfoPath, Hyper-V, Microsoft Edge, MultiPoint, MS-DOS, PowerShell, PowerPoint, SharePoint, SQL Server, Office 365, OneNote, Outlook, Skype, Tahoma, Visio, Win32, Windows, Windows PowerShell, Windows Media, Windows Server, Windows Phone, Windows Vista, oraz Windows Azure są znakami towarowymi grupy firm Microsoft.

Mozilla, Firefox, Thunderbird są znakami towarowymi Mozilla Foundation w Stanach Zjednoczonych i innych krajach.

Novell jest zastrzeżonym znakiem towarowym firmy Novell Enterprises Inc. w Stanach Zjednoczonych i innych krajach.

OpenSSL jest znakiem towarowym będącym własnością OpenSSL Software Foundation.

OpenVPN jest zarejestrowanym znakiem towarowym OpenVPN, Inc.

Oracle, Java, JavaScript i TouchDown są zastrzeżonymi znakami towarowymi firmy Oracle i/lub jej oddziałów.

Parallels, logo Parallels i Coherence są znakami towarowymi lub zastrzeżonymi znakami towarowymi firmy Parallels International GmbH.

Chef jest znakiem towarowym lub zastrzeżonym znakiem towarowym firmy Progress Software Corporation i/lub jednym z jej oddziałów lub podmiotów, zarejestrowanym w Stanach Zjednoczonych i/lub innych krajach.

Puppet jest znakiem towarowym lub zastrzeżonym znakiem towarowym firmy Puppet, Inc.

Python jest znakiem towarowym lub zastrzeżonym znakiem towarowym Python Software Foundation.

Red Hat, Fedora i Red Hat Enterprise Linux są znakami towarowymi lub zastrzeżonymi znakami towarowymi firmy Red Hat, Inc. lub jej oddziałów, zarejestrowanymi w Stanach Zjednoczonych i innych krajach.

Ansible jest zastrzeżonym znakiem towarowym firmy Red Hat, Inc. w Stanach Zjednoczonych i innych krajach.

CentOS jest znakiem towarowym lub zarejestrowanym znakiem towarowym firmy Red Hat, Inc. lub jej spółek zależnych w Stanach Zjednoczonych i innych krajach.

BlackBerry jest zastrzeżonym znakiem towarowym firmy Research In Motion Limited zarejestrowanym na terenie Stanów Zjednoczonych i jest w trakcie rejestrowania lub już jest zarejestrowany na terenie innych krajów.

Rocky Linux jest znakiem towarowym The Rocky Enterprise Software Foundation.

Samsung jest znakiem towarowym firmy SAMSUNG w Stanach Zjednoczonych i innych krajach.

Debian jest zastrzeżonym znakiem towarowym firmy Software in the Public Interest, Inc.

Splunk, SPL są zastrzeżonymi znakami towarowymi lub znakami towarowymi firmy Splunk Inc., zarejestrowanymi w Stanach Zjednoczonych i innych krajach.

SUSE jest zastrzeżonym znakiem towarowym firmy SUSE LLC, zarejestrowanym w Stanach Zjednoczonych i innych krajach.

Symbian jest znakiem towarowym firmy Symbian Foundation Ltd.

OpenAPI to znak towarowy firmy The Linux Foundation.

UNIX jest zastrzeżonym znakiem towarowym w Stanach Zjednoczonych i innych krajach, używanym na wyłącznej licencji firmy X/Open Company Limited.

Zabbix jest zastrzeżonym znakiem towarowym firmy Zabbix SIA.