kaspersky

Kaspersky Security Center 15 Linux

© 2024 AO Kaspersky Lab

Spis treści

System pomocy Kaspersky Security Center Linux

Nowości

Informacje o Kaspersky Security Center Linux

- Wymagania sprzętowe i programowe
  - Wymagania Serwera administracyjnego
  - Wymagania Web Console
  - Wymagania Agenta sieciowego
- Kompatybilne aplikacje i rozwiązania Kaspersky
- Nieobsługiwane systemy operacyjne i platformy
  - Nieobsługiwane systemy operacyjne i platformy. Serwer administracyjny
  - Nieobsługiwane systemy operacyjne i platformy. Kaspersky Security Center Web Console Server
  - Nieobsługiwane systemy operacyjne i platformy. Agent sieciowy
- Pakiet dystrybucyjny
- Informacje o kompatybilności Serwera administracyjnego i Kaspersky Security Center Web Console
- Porównanie Kaspersky Security Center: opartego na systemie Windows i opartego na systemie Linux
- Informacje o Kaspersky Security Center Cloud Console

Architektura i podstawowe pojęcia

- Architektura
- Diagram zdalnej instalacji 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
  - Agent sieciowy
  - Grupy administracyjne
  - Zarządzane urządzenie
  - Urządzenie nieprzypisane
  - Stacja robocza administratora
  - Sieciowa wtyczka administracyjna
  - Zasady
  - Profile zasad
  - Zadania
  - Obszar zadania
  - Jak ustawienia lokalne aplikacji mają się do zasad
  - Punkt dystrybucji
  - Brama połączenia

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, zapora 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
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
Scenariusz: uwierzytelnianie serwera PostgreSQL
Scenariusz: uwierzytelnianie serwera MySQL
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 Web Console połączonej z Serwerem administracyjnym zainstalowanym na węzłach klastra przełączania awaryjnego Kaspersky Security Center Linux
Wdrażanie klastra trybu failover Kaspersky Security Center Linux
Scenariusz: Wdrażanie klastra trybu failover Kaspersky Security Center Linux
Informacje o klastrze trybu failover Kaspersky Security Center Linux
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
Konta do pracy z DBMS
Konfiguracja konta DBMS do pracy z MySQL i MariaDB
Konfiguracja konta DBMS do pracy z PostgreSQL i Postgres Pro
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
Określanie folderu współdzielonego
Logowanie do Kaspersky Security Center Web Console i wylogowywanie
Zmiana języka interfejsu oprogramowania Kaspersky Security Center Web Console
Konfigurowanie serwera MySQL x64 do pracy z Kaspersky Security Center Linux
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. Tworzenie podstawowej konfiguracji ochrony sieci
Krok 10. Konfigurowanie powiadomień e-mail
Krok 11. Zamykanie kreatora wstępnej konfiguracji
Kreator wdrażania ochrony
Uruchamianie kreatora wdrażania ochrony
Krok 1. Wybieranie pakietu instalacyjnego
Krok 2. Wybieranie metody rozsyłania pliku klucza lub kodu aktywacyjnego
Krok 3. Wybieranie wersji Agenta sieciowego
Krok 4. Wybór urządzeń
Krok 5. Określanie ustawień zadania zdalnej instalacji
Krok 6. Usuwanie niekompatybilnych aplikacji przed instalacją
Krok 7. Przenoszenie urządzeń do grupy Zarządzane urządzenia
Krok 8. Wybieranie konta w celu uzyskania dostępu do urządzeń
Krok 9. Uruchamianie instalacji
Aktualizacja Kaspersky Security Center Linux
Aktualizacja Kaspersky Security Center Linux przy użyciu pliku instalacyjnego
Aktualizacja Kaspersky Security Center Linux poprzez kopię zapasową
Aktualizowanie Kaspersky Security Center Linux na węzłach klastra trybu failover Kaspersky Security Center Linux
Migracja do Kaspersky Security Center Linux
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 połączenia Kaspersky Security Center Web Console z Serwerem administracyjnym
Konfigurowanie listy dozwolonych adresów IP do logowania się do 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
Przeglądanie raportów połączeń z Serwerem administracyjnym
Określanie maksymalnej liczby zdarzeń w repozytorium zdarzeń
Przenoszenie Serwera administracyjnego na inne urządzenie
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
Konserwacja Serwera administracyjnego
Usuwanie hierarchii Serwerów administracyjnych
Dostęp do publicznych serwerów DNS
Konfigurowanie interfejsu
Szyfrowanie komunikacji z TLS
Wykrywanie urządzeń w sieci
Scenariusz: Wykrywanie urządzeń w sieci
Przeszukiwanie zakresu IP
Dodawanie i modyfikowanie zakresu IP
Przeszukiwanie Zeroconf
Przeszukiwanie kontrolera domeny
Konfigurowanie kontrolera domeny Samba
Używanie dynamicznego trybu VDI na urządzeniach klienckich
Włączanie dynamicznego trybu VDI we właściwościach pakietu instalacyjnego Agenta sieciowego
Przenoszenie urządzeń z VDI do grupy administracyjnej
Wdrażanie praktycznego zastosowania aplikacji
Przewodnik zwiększania bezpieczeństwa
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
Przygotowanie do zdalnej instalacji
Planowanie instalacji Kaspersky Security Center Linux
Typowe schematy wdrażania systemu ochrony
Informacje dotyczące planowania instalacji Kaspersky Security Center Linux w sieci organizacji
Wybieranie struktury ochrony firmy
Standardowa konfiguracja Kaspersky Security Center Linux
Standardowa konfiguracja: Jedno biuro
Standardowa konfiguracja: Duże oddziały posiadające swoich administratorów
Standardowa konfiguracja: Małe zdalne biura
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
Dostęp do internetu: Agent sieciowy jako brama połączenia w strefie zdemilitaryzowanej
Informacje o punktach dystrybucji
Obliczanie liczby i konfigurowanie punktów dystrybucji
Wirtualne Serwery administracyjne
Ustawienia sieciowe dotyczące interakcji z usługami zewnętrznymi
Instalowanie Agenta sieciowego i aplikacji zabezpieczającej
Wstępna zdalna instalacja
Konfigurowanie instalatorów

Pakiety instalacyjne
Informacje o zadaniach zdalnej instalacji w Kaspersky Security Center Linux
Instalacja poprzez przechwycenie i skopiowanie obrazu urządzenia
Tryb klonowania dysku Agenta sieciowego
Wymuszona zdalna instalacja przy użyciu zadania zdalnej instalacji z Kaspersky Security Center Linux
Uruchamianie pakietów autonomicznych utworzonych przez Kaspersky Security Center Linux
Zdalna instalacja aplikacji na urządzeniach z zainstalowanym Agentem sieciowym
Zarządzanie ponownym uruchamianiem urządzeń w zadaniu zdalnej instalacji
Aktualizowanie baz danych w pakiecie instalacyjnym aplikacji zabezpieczającej
Monitorowanie zdalnej instalacji
Konfigurowanie instalatorów
Informacje ogólne
Instalacja w trybie cichym (z plikiem odpowiedzi)
Częściowa konfiguracja instalacji poprzez setup.exe
Parametry instalacji Serwera administracyjnego
Parametry instalacji Agenta sieciowego
Infrastruktura wirtualna
Wskazówki dotyczące zmniejszenia obciążenia na maszynach wirtualnych
Obsługa dynamicznych maszyn wirtualnych
Obsługa kopiowania maszyn wirtualnych
Obsługa przywracania systemu plików dla urządzeń z zainstalowanym Agentem sieciowym
Lokalna instalacja aplikacji
Lokalna instalacja Agenta sieciowego
Instalowanie Agenta sieciowego w trybie cichym
Lokalna instalacja wtyczki zarządzającej aplikacją
Instalowanie aplikacji w trybie cichym
Instalowanie aplikacji przy pomocy pakietów autonomicznych
Ustawienia pakietu instalacyjnego Agenta sieciowego
Ręczna konfiguracja grupowego zadania skanowania urządzeń z zainstalowanym programem Kaspersky Endpoint Security
Zarządzanie urządzeniami klienckimi
Ustawienia zarządzanego urządzenia
Tworzenie grup administracyjnych
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
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
Modyfikowanie listy punktów dystrybucji dla grupy administracyjnej
Włączanie serwera push

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
Informacje o znacznikach 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
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
Zmienianie Serwera administracyjnego dla urządzeń klienckich
Przeglądanie i konfigurowanie działań, gdy urządzenia wykazują brak aktywności
Wysyłanie wiadomości na urządzenia użytkowników
Zdalne włączanie, wyłączanie i ponowne uruchamianie urządzeń klienckich
Wdrażanie aplikacji Kaspersky
Scenariusz: Wdrażanie aplikacji Kaspersky
Dodawanie wtyczek administracyjnych dla aplikacji Kaspersky
Pobieranie i tworzenie pakietów instalacyjnych dla aplikacji Kaspersky
Tworzenie pakietów instalacyjnych z pliku
Tworzenie autonomicznych pakietów instalacyjnych
Zmienianie ograniczenia rozmiaru danych niestandardowego pakietu instalacyjnego
Instalowanie Agenta sieciowego dla systemu Linux w trybie cichym (z plikiem odpowiedzi)
Przygotowanie urządzenia z systemem Astra Linux w trybie zamkniętego środowiska oprogramowania do instalacji Agenta sieciowego
Przeglądanie listy autonomicznych pakietów instalacyjnych
Rozsyłanie pakietów instalacyjnych na podrzędne Serwery administracyjne
Przygotowanie urządzenia z systemem Linux i zdalna instalacja Agenta sieciowego na urządzeniu z systemem Linux
Instalowanie aplikacji przy pomocy zadania zdalnej instalacji
Zdalna instalacja aplikacji
Instalowanie aplikacji na podrzędnych Serwerach administracyjnych
Określanie ustawień zdalnej instalacji na urządzeniach z systemem Unix

Zastępowanie aplikacji zabezpieczających firm trzecich
Zdalne usuwanie aplikacji lub aktualizacji oprogramowania
Przygotowanie urządzenia z systemem SUSE Linux Enterprise Server 15 do instalacji Agenta sieciowego
Przygotowanie urządzenia z systemem Windows do zdalnej instalacji. Narzędzie Riprep
Przygotowanie urządzenia z systemem Windows do zdalnej instalacji w trybie interaktywnym
Przygotowanie urządzenia z systemem Windows do zdalnej instalacji w trybie cichym
Licencjonowanie
Informacje dotyczące licencjonowania oprogramowania Kaspersky Security Center Linux
Informacje o Umowie licencyjnej
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 ograniczeń licencyjnych
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 profili: Metoda skoncentrowana na urządzeniu
Konfiguracja i przydzielanie profili: Metoda skoncentrowana na użytkowniku
Profile i profile zasad
Informacje o zasadach i profilach zasad
Informacje o blokadzie i zablokowanych ustawieniach
Dziedziczenie zasad i profili zasad
Hierarchia profili
Profile zasad w hierarchii zasad
Implementacja ustawień na zarządzanym urządzeniu
Zarządzanie profilami
Przeglądanie listy zasad
Tworzenie zasady
Ogólne ustawienia zasady
Modyfikowanie zasady
Włączanie i wyłączanie opcji dziedziczenia zasady
Kopiowanie zasady

Przenoszenie zasady
Eksportowanie profilu
Importowanie profilu
Wymuszona synchronizacja
Przeglądanie wykresu stanu dystrybucji zasad
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
Ustawienia zasady Agenta sieciowego
Korzystanie z Agenta sieciowego dla systemu Windows, Linux i macOS: porównanie
Porównanie ustawień Agenta sieciowego według systemów operacyjnych
Ręczna konfiguracja zasady Kaspersky Endpoint Security
Konfigurowanie Kaspersky Security Network
Sprawdzanie listy sieci chronionych przez Zaporę sieciową
Wyłączanie skanowania urządzeń sieciowych
Wykluczanie szczegółów oprogramowania z pamięci Serwera administracyjnego
Konfigurowanie dostępu do interfejsu Kaspersky Endpoint Security for Windows na stacjach roboczych
Zapisywanie ważnych zdarzeń dot. zasad w bazie danych Serwera administracyjnego
Ręczna konfiguracja grupowego zadania aktualizacji dla Kaspersky Endpoint Security
Kaspersky Security Network (KSN)
Informacje o KSN
Konfigurowanie dostępu do KSN
Włączanie i wyłączanie KSN
Przeglądanie zaakceptowanego Oświadczenia KSN
Akceptowanie zaktualizowanego Oświadczenia KSN
Sprawdzanie, czy punkt dystrybucji działa jako serwer proxy KSN
Zarządzanie zadaniami
Informacje o zadaniach
Informacje o obszarze zadania
Tworzenie zadania
Ręczne uruchamianie zadania
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
Informacje o znacznikach aplikacji
Tworzenie znacznika aplikacji

Zmienianie nazwy znacznika aplikacji
Przydzielanie znaczników do aplikacji
Usuwanie przydzielonych znaczników z aplikacji
Usuwanie znacznika aplikacji
Udzielanie dostępu offline urządzeniu zewnętrznemu, zablokowanemu przez Kontrolę urządzeń
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 uprawnień dostępu użytkownikom i grupom
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
Włączanie ochrony konta przed nieautoryzowaną modyfikacją
Weryfikacja dwuetapowa
Scenariusz: konfigurowanie weryfikacji dwuetapowej dla wszystkich użytkowników
Informacje o dwuetapowej weryfikacji konta
Włączanie weryfikacji dwuetapowej dla własnego konta
Włączanie weryfikacji dwuetapowej dla wszystkich użytkowników
Wyłączanie weryfikacji dwuetapowej dla konta użytkownika
Wyłączanie weryfikacji dwuetapowej dla wszystkich użytkowników
Wykluczanie kont z weryfikacji dwuetapowej
Konfigurowanie weryfikacji dwuetapowej dla własnego konta
Uniemożliwienie nowym użytkownikom konfigurowania dla siebie weryfikacji dwuetapowej
Generowanie nowego tajnego klucza
Edytowanie nazwy wystawcy kodu zabezpieczającego
Zmienianie liczby dozwolonych prób wprowadzenia hasła
Usuwanie użytkownika lub grupy bezpieczeństwa
Tworzenie roli użytkownika
Edytowanie roli użytkownika
Edytowanie obszaru roli użytkownika
Usuwanie roli użytkownika
Kojarzenie profili zasad z rolami
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 uaktualnień do repozytoriów punktów dystrybucji
Dodawanie źródeł uaktualnień dla zadania Pobierz uaktualnienia do repozytorium Serwera administracyjnego
Informacje o używaniu plików diff do aktualizowania baz danych i modułów aplikacji Kaspersky
Włączania funkcji Pobierz pliki diff: scenariusz
Pobieranie uaktualnień przez punkty dystrybucji
Aktualizowanie baz danych i modułów Kaspersky na urządzeniach offline
Tworzenie kopii zapasowych i przywracanie wtyczek webowych
Monitorowanie, raportowanie i audyt
Scenariusz: Monitorowanie i raportowanie
Informacje o typach monitorowania i raportowania
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 samego pulpitu
Konfigurowanie trybu samego pulpitu
Raporty
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
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 funkcyjnego Serwera administracyjnego
Zdarzenia ostrzegające Serwera administracyjnego
Zdarzenia informacyjne Serwera administracyjnego
Zdarzenia 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
Eksportowanie zdarzeń do systemów SIEM
Scenariusz: 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
Oznaczenie zdarzeń do wyeksportowania do systemów SIEM w formacie Syslog
Informacje dotyczące oznaczania zdarzeń do wyeksportowania do systemu 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
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
Informacje o rewizjach obiektów
Przywracanie poprzedniej wersji obiektu
Usuwanie obiektów
Pobieranie i usuwanie plików z Kwarantanny i Kopii zapasowej
Pobieranie plików z Kwarantanny i Kopii zapasowej
Informacje o usuwaniu obiektów z repozytoriów Kwarantanny, Kopii zapasowej lub Aktywnych zagrożeń
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
Generowania pliku zrzutu dla aplikacji
Uruchamianie zdalnej diagnostyki na urządzeniu klienckim z systemem Linux
Zarządzanie aplikacjami firm trzecich na urządzeniach klienckich
Scenariusz: Zarządzanie aplikacjami
Informacje o Kontroli aplikacji
Uzyskiwanie i przeglądanie listy aplikacji zainstalowanych na urządzeniach klienckich
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
Konfigurowanie Kontroli aplikacji w zasadzie Kaspersky Endpoint Security for Windows
Dodawanie plików wykonywalnych dotyczących zdarzeń do kategorii aplikacji
Przewodnik po API
Podręcznik szacowania rozmiaru
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 profili
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 Inwentaryzacja oprogramowania
Szczegóły dotyczące obciążenia sieci pomiędzy Serwerem administracyjnym a chronionymi urządzeniami
Zużycie ruchu sieciowego w różnych scenariuszach
Przeciętne zużycie ruchu sieciowego w ciągu 24 godzin
Kontakt z działem pomocy technicznej
Jak uzyskać pomoc techniczną
Pomoc techniczna poprzez Kaspersky CompanyAccount
Źródła informacji o aplikacji
Znane problemy
Słownik

Administrator dostawcy usługi
Administrator Kaspersky Security Center Linux
Administrator klienta
Agent autoryzacji
Agent sieciowy
Aktualizacja
Aktywny klucz
Antywirusowe bazy danych
Bezpośrednie zarządzanie aplikacjami
Brama połączenia
Certyfikat współdzielony
Certyfikatu Serwera administracyjnego
Dodatkowy klucz subskrypcyjny
Domena rozgłoszeniowa
Dostawca usługi ochrony antywirusowej
Dostępne aktualizacje
Folder Kopia zapasowa
Grupa administracyjna
Grupa licencjonowanych aplikacji
Grupa ról
HTTPS
Instalacja lokalna
Instalacja ręczna
Instalacja zdalna
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
Macierzysty Serwer administracyjny
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

Serwery aktualizacji Kaspersky
Sklep aplikacji
SSL
Stacja robocza administratora
Stan ochrony
Stan ochrony sieci
Strefa zdemilitaryzowana (DMZ)
Uprawnienia administracyjne
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

	Nowości Zapoznaj się z nowościami w najnowszym wydaniu produktu.		**Aplikacje Kaspersky. Licencjonowanie i aktywacja** Aktywuj aplikacje Kaspersky w kilku krokach.
	Zastępowanie aplikacji zabezpieczających firm trzecich Poznaj metody odinstalowywania niekompatybilnych aplikacji.		**Podręcznik szacowania rozmiaru (tylko pomoc online)** Aby zapewnić optymalną wydajność w różnych warunkach pracy, należy wziąć pod uwagę liczbę urządzeń w sieci, topologię sieci oraz zestaw funkcji Kaspersky Security Center Linux, jakich potrzebujesz.
	Wymagania sprzętowe i programowe Sprawdź, które systemy operacyjne i wersje aplikacji są obsługiwane.		**Konfigurowanie ochrony sieci** Zarządzaj bezpieczeństwem organizacji.
	Instalacja Zainstaluj Serwer administracyjny i Kaspersky Security Center Web Console.		**Aplikacje Kaspersky. Aktualizowanie baz danych i modułów aplikacji** Zachowaj niezawodność systemu ochrony.
	Wykrywanie urządzeń w sieci Wyszukuj istniejące i nowe urządzenia w sieci organizacji.		**Monitorowanie i raportowanie** Sprawdź swoją infrastrukturę, stany ochrony i statystyki.
	Aplikacje Kaspersky. Zdalna instalacja Rozplanuj korzystanie z zasobów, instalację Serwera administracyjnego, instalację Agenta sieciowego i aplikacji zabezpieczających na urządzeniach klienckich.		**Dostosowanie punktów dystrybucji i/lub bram połączenia** Konfiguruj punkty dystrybucji.
	Eksportowanie zdarzeń do systemów SIEM Skonfiguruj eksportowanie zdarzeń do systemów SIEM w celu przeprowadzenia analizy.		

Nowości

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, profili 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 **Zarządzane 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.

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 zarządzających wtyczek sieciowych 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, dodatkowymi 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.

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 politykami bezpieczeństwa 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 rozsyłanie 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.

Wymagania sprzętowe i programowe

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

Wymagania Serwera administracyjnego

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: 4 GB.
- Dostępne miejsce na dysku: 10 GB.

Obsługiwane są następujące systemy operacyjne:

- Debian GNU/Linux 10.x (Buster) 64-bitowy
- Debian GNU/Linux 11.x (Bullseye) 64-bitowy
- Debian GNU/Linux 12 (Bookworm) 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
- CentOS 7.x 64-bitowy
- CentOS Stream 9 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
- 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-bit

- Astra Linux Common Edition (aktualizacja operacyjna 2.12) 64-bitowy
- ALT SP Server 10 64-bitowy
- ALT Server 10 64-bitowy
- ALT Server 9.2 64-bitowy
- ALT 8 SP Server (LKNV.11100-01) 64-bitowy
- ALT 8 SP Server (LKNV.11100-02) 64-bitowy
- ALT 8 SP Server (LKNV.11100-03) 64-bitowy
- Oracle Linux 7 64-bitowy
- Oracle Linux 8 64-bitowy
- Oracle Linux 9 64-bitowy
- RED OS 7.3 Server 64-bitowy
- RED OS 7.3 Certified Edition 64-bitowy
- ROSA COBALT 7.9 64-bitowy

Obsługiwane są następujące platformy wirtualizacji:

- VMware vSphere 6.7
- VMware vSphere 7.0
- VMware vSphere 8.0
- VMware Workstation 16 Pro
- VMware Workstation 17 Pro
- Microsoft Hyper-V Server 2012 64-bitowy
- Microsoft Hyper-V Server 2012 R2 64-bitowy
- Microsoft Hyper-V Server 2016 64-bitowy
- Microsoft Hyper-V Server 2019 64-bitowy
- Microsoft Hyper-V Server 2022 64-bitowy
- Citrix XenServer 7.1 LTSR
- Citrix XenServer 8.x
- Parallels Desktop 17
- Oracle VM VirtualBox 6.x

- Oracle VM VirtualBox 7.x
- Maszyna wirtualna oparta na jądrze (wszystkie systemy operacyjne Linux obsługiwane przez Serwer administracyjny)

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

- MySQL 5.7 Community 32-bitowy/64-bitowy
- MySQL 8.0 32-bitowy/64-bitowy
- MariaDB 10.1 (kompilacja 10.1.30 i nowsze) 32-bitowe/64-bitowe
- MariaDB 10.3 (kompilacja 10.3.22 i nowsze) 32-bitowe/64-bitowe
- MariaDB 10.4 (kompilacja 10.4.26 i nowsze) 32-bitowe/64-bitowe
- MariaDB 10.5 (kompilacja 10.5.17 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
- Postgres Pro 13.x 64-bitowy (wszystkie wersje)
- Postgres Pro 14.x 64-bitowy (wszystkie wersje)
- Postgres Pro 15.x 64-bitowy (wszystkie wersje)
- Platforma V Pangolin 5.4.0 64-bitowa

Wymagania Web Console

Kaspersky Security Center Web Console Server

Minimalne wymagania sprzętowe:

- Procesor: 4 rdzenie, częstotliwość taktowania wynosząca 2,5 GHz.
- Pamięć RAM: 8 GB.
- Dostępne miejsce na dysku: 40 GB.

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

- Debian GNU/Linux 10.x (Buster)
- Debian GNU/Linux 11.x (Bullseye)

- Debian GNU/Linux 12 (Bookworm)
- Ubuntu Server 18.04 LTS (Bionic Beaver)
- Ubuntu Server 20.04 LTS (Focal Fossa)
- Ubuntu Server 22.04 LTS (Jammy Jellyfish)
- CentOS Stream 9
- Red Hat Enterprise Linux Server 7.x
- Red Hat Enterprise Linux Server 8.x
- Red Hat Enterprise Linux Server 9.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.10015-01 (aktualizacja operacyjna 1.7)
- Astra Linux Common Edition (aktualizacja operacyjna 2.12)
- ALT SP Server 10
- ALT Server 10
- ALT Server 9.2
- ALT 8 SP Server (LKNV.11100-01)
- ALT 8 SP Server (LKNV.11100-02)
- ALT 8 SP Server (LKNV.11100-03)
- Oracle Linux 7
- Oracle Linux 8
- Oracle Linux 9
- RED OS 7.3 Server
- RED OS 7.3 Certified Edition
- ROSA COBALT 7.9
- Maszyna wirtualna oparta na jądrze (wszystkie systemy operacyjne Linux obsługiwane przez serwer Kaspersky Security Center Web Console)

Urządzenia klienckie

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

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 100.0.4896.88 lub nowszej (wersja oficjalna)
- Microsoft Edge w wersji 100 lub nowszej
- Safari 15 dla systemu macOS
- Przeglądarka „Yandex" 23.5.0.2271 lub nowsza
- Wydłużone wsparcie techniczne Mozilla Firefox w wersji 102.0 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.

Obsługiwane są następujące systemy operacyjne:

- 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 version 1703 32-bitowy/64-bitowy
- Microsoft Windows 10 IoT Enterprise version 1709 32-bitowy/64-bitowy

- Microsoft Windows 10 IoT Enterprise version 1803 32-bitowy/64-bitowy
- Microsoft Windows 10 IoT Enterprise version 1809 32-bitowy/64-bitowy
- Microsoft Windows 10 20H2 IoT Enterprise 32-bitowy/64-bitowy
- Microsoft Windows 10 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 Home RS3 (Fall Creators Update, v1709) 32-bitowy/64-bitowy
- Microsoft Windows 10 Pro RS3 (Fall Creators Update, v1709) 32-bitowy/64-bitowy
- Microsoft Windows 10 Pro for Workstations RS3 (Fall Creators Update, v1709) 32-bitowy/64-bitowy
- Microsoft Windows 10 Enterprise RS3 (Fall Creators Update, v1709) 32-bitowy/64-bitowy
- Microsoft Windows 10 Education RS3 (Fall Creators Update, v1709) 32-bitowy/64-bitowy
- Microsoft Windows 10 Home RS4 (April 2018 Update, 17134) 32-bitowy/64-bitowy
- Microsoft Windows 10 Pro RS4 (April 2018 Update, 17134) 32-bitowy/64-bitowy
- Microsoft Windows 10 Pro for Workstations RS4 (April 2018 Update, 17134) 32-bitowy/64-bitowy
- Microsoft Windows 10 Enterprise RS4 (April 2018 Update, 17134) 32-bitowy/64-bitowy
- Microsoft Windows 10 Education RS4 (April 2018 Update, 17134) 32-bitowy/64-bitowy
- Microsoft Windows 10 Home RS5 (październik 2018 r.) 32-bitowy/64-bitowy
- Microsoft Windows 10 Pro RS5 (październik 2018 r.) 32-bitowy/64-bitowy
- Microsoft Windows 10 Pro for Workstations RS5 (październik 2018 r.) 32-bitowy/64-bitowy
- Microsoft Windows 10 Enterprise RS5 (październik 2018 r.) 32-bitowy/64-bitowy
- Microsoft Windows 10 Education RS5 (październik 2018 r.) 32-bitowy/64-bitowy
- Microsoft Windows 10 Home 19H1 32-bitowy/64-bitowy
- Microsoft Windows 10 Pro 19H1 32-bitowy/64-bitowy
- Microsoft Windows 10 Pro for Workstations 19H1 32-bitowy/64-bitowy
- Microsoft Windows 10 Enterprise 19H1 32-bitowy/64-bitowy
- Microsoft Windows 10 Education 19H1 32-bitowy/64-bitowy

- Microsoft Windows 10 Home 19H2 32-bitowy/64-bitowy
- Microsoft Windows 10 Pro 19H2 32-bitowy/64-bitowy
- Microsoft Windows 10 Pro for Workstations 19H2 32-bitowy/64-bitowy
- Microsoft Windows 10 Enterprise 19H2 32-bitowy/64-bitowy
- Microsoft Windows 10 Education 19H2 32-bitowy/64-bitowy
- Microsoft Windows 10 Home 20H1 (May 2020 Update) 32-bitowy/64-bitowy
- Microsoft Windows 10 Pro 20H1 (May 2020 Update) 32-bitowy/64-bitowy
- Microsoft Windows 10 Enterprise 20H1 (May 2020 Update) 32-bitowy/64-bitowy
- Microsoft Windows 10 Education 20H1 (May 2020 Update) 32-bitowy/64-bitowy
- Microsoft Windows 10 Home 20H2 (October 2020 Update) 32-bitowy/64-bitowy
- Microsoft Windows 10 Pro 20H2 (October 2020 Update) 32-bitowy/64-bitowy
- Microsoft Windows 10 Enterprise 20H2 (October 2020 Update) 32-bitowy/64-bitowy
- Microsoft Windows 10 Education 20H2 (October 2020 Update) 32-bitowy/64-bitowy
- Microsoft Windows 10 Home 21H1 (May 2021 Update) 32-bitowy/64-bitowy
- Microsoft Windows 10 Pro 21H1 (May 2021 Update) 32-bitowy/64-bitowy
- Microsoft Windows 10 Enterprise 21H1 (May 2021 Update) 32-bitowy/64-bitowy
- Microsoft Windows 10 Education 21H1 (May 2021 Update) 32-bitowy/64-bitowy
- Microsoft Windows 10 Home 21H2 (October 2021 Update) 32-bitowy/64-bitowy
- Microsoft Windows 10 Pro 21H2 (October 2021 Update) 32-bitowy/64-bitowy
- Microsoft Windows 10 Enterprise 21H2 (October 2021 Update) 32-bitowy/64-bitowy
- Microsoft Windows 10 Education 21H2 (October 2021 Update) 32-bitowy/64-bitowy
- Microsoft Windows 10 Home 22H2 (October 2023 Update) 32-bitowy/64-bitowy
- Microsoft Windows 10 Pro 22H2 (aktualizacja z października 2023 r.) 32-bitowy/64-bitowy
- Microsoft Windows 10 Enterprise 22H2 (aktualizacja z października 2023 r.) 32-bitowy/64-bitowy
- Microsoft Windows 10 Education 22H2 (aktualizacja z października 2023 r.) 32-bitowy/64-bitowy
- Microsoft Windows 11 Home 64-bitowy
- Microsoft Windows 11 Pro 64-bitowy
- Microsoft Windows 11 Enterprise 64-bitowy

- Microsoft Windows 11 Education 64-bitowy
- Microsoft Windows 11 22H2
- Microsoft Windows 8.1 Pro 32-bitowy/64-bitowy
- Microsoft Windows 8.1 Enterprise 32-bitowy/64-bitowy
- Microsoft Windows 8 Pro 32-bitowy/64-bitowy
- Microsoft Windows 8 Enterprise 32-bitowy/64-bitowy
- Microsoft Windows 7 Professional z pakietem Service Pack 1 i nowszy, 32-bitowy/64-bitowy
- Microsoft Windows 7 Enterprise/Ultimate z pakietem Service Pack 1 i nowszy, 32-bitowy/64-bitowy
- Microsoft Windows 7 Home Basic/Premium z pakietem Service Pack 1 lub 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)
- Microsoft Windows XP Professional dla systemów wbudowanych z dodatkiem Service Pack 3 32-bit (obsługiwany przez Agenta sieciowego w wersji 14.0.0.20023)
- Windows MultiPoint Server 2011 Standard/Premium 64-bitowy
- Windows Server 2008 Foundation z dodatkiem Service Pack 2 32-bitowy/64-bitowy
- Windows Server 2008 z dodatkiem Service Pack 2 (wszystkie wersje) 32-bitowy/64-bitowy
- Windows Server 2008 R2 Datacenter z pakietem Service Pack 1 i nowszym 64-bitowym
- Windows Server 2008 R2 Enterprise z pakietem Service Pack 1 i nowszym 64-bitowym
- Windows Server 2008 R2 Foundation z pakietem Service Pack 1 i nowszym 64-bitowym
- Windows Server 2008 R2 Core Mode z pakietem Service Pack 1 i nowszym 64-bitowym
- Windows Server 2008 R2 Standard z pakietem Service Pack 1 i nowszym 64-bitowym
- Windows Server 2008 R2 z pakietem Service Pack 1 (wszystkie wersje) 64-bitowy
- Windows Server 2012 Server Core 64-bitowy
- Windows Server 2012 Datacenter 64-bitowy
- Windows Server 2012 Essentials 64-bitowy
- Windows Server 2012 Foundation 64-bitowy
- Windows Server 2012 Standard 64-bitowy
- Windows Server 2012 R2 Server Core 64-bitowy

- Windows Server 2012 R2 Datacenter 64-bitowy
- Windows Server 2012 R2 Essentials 64-bitowy
- Windows Server 2012 R2 Foundation 64-bitowy
- Windows Server 2012 R2 Standard 64-bitowy
- Windows Server 2016 Datacenter (LTSB) 64-bitowy
- Windows Server 2016 Standard (LTSB) 64-bitowy
- Windows Server 2016 Server Core (Opcja instalacji) (LTSB) 64-bitowy
- Windows Server 2019 Standard 64-bitowy
- Windows Server 2019 Datacenter 64-bitowy
- Windows Server 2019 Core 64-bitowy
- Windows Server 2022 Standard 64-bitowy
- Windows Server 2022 Datacenter 64-bitowy
- Windows Server 2022 Core 64-bitowy
- 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
- Ubuntu Server 18.04 LTS (Bionic Beaver) 32-bitowy/64-bitowy
- Ubuntu Server 20.04 LTS (Focal Fossa) 32-bitowy/64-bitowy
- Ubuntu Server 22.04 LTS (Jammy Jellyfish) 64-bitowy
- CentOS 7.x 64-bitowy
- CentOS Stream 9 64-bitowy
- Red Hat Enterprise Linux Server 6.x 32-bitowy/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
- SUSE Linux Enterprise Server 12 (wszystkie pakiety Service Pack) 64-bitowy
- SUSE Linux Enterprise Server 15 (wszystkie pakiety Service Pack) 64-bitowy
- SUSE Linux Enterprise Desktop 15 z Service Pack 3 ARM 64-bitowy

- openSUSE 15 64-bitowy
- EulerOS 2.0 SP8 ARM
- 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-bit
- Astra Linux Common Edition (aktualizacja operacyjna 2.12) 64-bitowy
- Astra Linux Special Edition RUSB.10152-02 (aktualizacja operacyjna 4.7) ARM 64-bitowy
- ALT SP Server 10 64-bitowy
- ALT SP Workstation 10 64-bitowy
- ALT Server 10 64-bitowy
- ALT Server 9.2 64-bitowy
- ALT Workstation 9.2 32-bitowy/64-bitowy
- ALT Workstation 10 32-bitowy/64-bitowy
- ALT 8 SP Server (LKNV.11100-01) 64-bitowy
- ALT 8 SP Server (LKNV.11100-02) 64-bitowy
- ALT 8 SP Server (LKNV.11100-03) 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
- Mageia 4 32-bitowy
- Oracle Linux 7 64-bitowy
- Oracle Linux 8 64-bitowy
- Oracle Linux 9 64-bitowy
- Linux Mint 20.x 64-bitowy
- AlterOS 7.5 i nowsze wersje, 64-bitowe
- GosLinux IC6 64-bitowy
- RED OS 7.3 64-bitowy
- RED OS 7.3 Server 64-bitowy
- RED OS 7.3 Certified Edition 64-bitowy

- ROSA COBALT 7.9 64-bitowy
- ROSA CHROME 12 64-bitowy
- macOS Big Sur (11.x)
- macOS Monterey (12.x)
- macOS Ventura (13.x)

  Dla Agenta sieciowego architektura Apple Silicon (M1) jest także obsługiwana (tak jak Intel).

Obsługiwane są następujące platformy wirtualizacji:

- VMware vSphere 6.7
- VMware vSphere 7.0
- VMware vSphere 8.0
- VMware Workstation 16 Pro
- VMware Workstation 17 Pro
- Microsoft Hyper-V Server 2012 64-bitowy
- Microsoft Hyper-V Server 2012 R2 64-bitowy
- Microsoft Hyper-V Server 2016 64-bitowy
- Microsoft Hyper-V Server 2019 64-bitowy
- Microsoft Hyper-V Server 2022 64-bitowy
- Citrix XenServer 7.1 LTSR
- Citrix XenServer 8.x
- Parallels Desktop 17
- Oracle VM VirtualBox 6.x
- Oracle VM VirtualBox 7.x
- Maszyna wirtualna oparta na jądrze (wszystkie systemy operacyjne Linux obsługiwane przez Agenta sieciowego)

Na urządzeniach działających pod kontrolą systemu 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 lub Windows MultiPoint Server 2011 upewnij się, że zainstalowano aktualizację zabezpieczeń systemu Windows 7 (KB3063858).

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

Możesz zainstalować lub zaktualizować Network Agent for 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.

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 następującymi aplikacjami Kaspersky:

- Kaspersky Endpoint Security for Windows 12.0 lub nowszy (obsługuje serwery plików)
- Kaspersky Endpoint Security for Linux 11.2 lub nowszy (obsługuje serwery plików)
- Kaspersky Endpoint Security for Linux Elbrus Edition 10 lub nowszy
- Kaspersky Endpoint Security for Linux ARM Edition 11.2 lub nowszy
- Kaspersky Endpoint Security for Mac 11.3 lub nowszy
- Kaspersky Industrial CyberSecurity for Linux Nodes 1.3 lub nowszy
- Kaspersky Industrial CyberSecurity for Nodes 3.2 lub nowszy
- Kaspersky Industrial CyberSecurity for Networks 3.2 lub nowszy
- Kaspersky Endpoint Agent 3.15 lub nowszy
- Kaspersky Embedded Systems Security for Windows 3.2 lub nowszy
- Kaspersky Embedded Systems Security for Linux 3.3 lub nowszy
- Kaspersky Security for Virtualization Light Agent 5.2 lub nowszy

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

Znane problemy

Kaspersky Security Center Linux obsługuje zarządzanie Kaspersky Endpoint Security for Windows z następującymi ograniczeniami:

- Komponent Adaptacyjna kontrola anomalii nie jest obsługiwany. Kaspersky Security Center Linux nie obsługuje reguł Adaptacyjnej kontroli anomalii.
- Komponenty Kaspersky Sandbox nie są obsługiwane.
- Funkcja Aktualizacje oprogramowania Kaspersky jest niedostępna.

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

Nieobsługiwane systemy operacyjne i platformy

- Nieobsługiwane systemy operacyjne i platformy. Serwer administracyjny
- Nieobsługiwane systemy operacyjne i platformy. Kaspersky Security Center Web Console Server
- Nieobsługiwane systemy operacyjne i platformy. Agent sieciowy

Nieobsługiwane systemy operacyjne i platformy. Serwer administracyjny

Serwer administracyjny nie jest kompatybilny z następującymi systemami operacyjnymi:

- Debian GNU/Linux 7.x (do 7.8) 32-bitowy/64-bitowy
- Debian GNU/Linux 8.x (Jessie) 32-bitowy/64-bitowy
- Debian GNU/Linux 9.x (Stretch) 32-bitowy/64-bitowy
- Ubuntu Server 14.04 LTS (Trusty Tahr) 32-bitowy/64-bitowy
- Ubuntu Server 16.04 LTS (Xenial Xerus) 32-bitowy/64-bitowy
- Ubuntu Server 18.04 LTS (Bionic Beaver) 32-bitowy
- Ubuntu Server 20.04.04 LTS (Focal Fossa) ARM 64-bitowy
- Ubuntu Server 20.04 LTS (Focal Fossa) 32-bitowy
- Ubuntu Desktop 14.04 LTS (Trusty Tahr) 32-bitowy/64-bitowy
- Ubuntu Desktop 16.04 LTS (Xenial Xerus) 32-bitowy/64-bitowy
- Ubuntu Desktop 18.04 LTS (Bionic Beaver) 32-bitowy/64-bitowy
- Ubuntu Desktop 20.04 LTS (Focal Fossa) 32-bitowy/64-bitowy
- CentOS 6.x (do 6.6) 64-bitowy
- CentOS 7.x ARM 64-bitowy

- CentOS 8.x 64-bitowy
- Red Hat Enterprise Linux Server 6.x 32-bitowy/64-bitowy
- SUSE Linux Enterprise Desktop 12 (wszystkie pakiety Service Pack) 64-bitowy
- SUSE Linux Enterprise Desktop 15 (wszystkie pakiety Service Pack) 64-bitowy
- SUSE Linux Enterprise Desktop 15 z Service Pack 3 ARM 64-bitowy
- openSUSE 15 64-bitowy
- EulerOS 2.0 SP8 ARM
- Pardus OS 19.1 64-bitowy
- Astra Linux Special Edition 1.5 64-bitowy
- Astra Linux Special Edition RUSB.10152-02 (aktualizacja operacyjna 4.7) ARM 64-bit
- ALT Workstation 9.2 32-bitowy/64-bitowy
- ALT Workstation 10 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
- Mageia 4 32-bitowy
- Linux Mint 19.x 32-bitowy
- Linux Mint 20.x 64-bitowy
- AlterOS 7.5 i nowszy 64-bitowy
- RED OS 7.3 64-bitowy
- GosLinux IC6 64-bitowy
- ROSA Enterprise Linux Server 7.3 64-bitowy
- ROSA Enterprise Linux Desktop 7.3 64-bitowy
- ROSA COBALT Workstation 7.3 64-bitowy
- ROSA COBALT Server 7.3 64-bitowy
- ROSA CHROME 12 64-bitowy
- Lotos (rdzeń Linux w wersji 4.19.50, DE: MATE) 64-bitowy

Serwer bazy danych:

- PostgreSQL Pangolin 64-bitowy
- Microsoft SQL Server 2005 Express 32-bitowy
- Microsoft SQL Server 2005 (wszystkie wersje) 32-bitowy/64-bitowy
- Microsoft SQL Server 2008 Express 32-bitowy
- Microsoft SQL Server 2008 (wszystkie wersje) 32-bitowy/64-bitowy
- Microsoft SQL Server 2008 R2 (wszystkie wersje) 64-bitowy
- Microsoft SQL Server 2008 R2 z Service Pack 2 (wszystkie wersje) 64-bitowy
- Microsoft SQL Server 2012 (wszystkie wersje) 64-bitowy
- MySQL 5.0 32-bitowy/64-bitowy
- MySQL Enterprise 5.0 32-bitowy/64-bitowy
- MySQL Standard Edition 5.5 32-bitowy/64-bitowy
- MySQL Enterprise Edition 5.5 32-bitowy/64-bitowy
- MySQL Standard Edition 5.6 32-bitowy/64-bitowy
- MySQL Enterprise Edition 5.6 32-bitowy/64-bitowy
- MySQL Standard Edition 5.7 32-bitowy/64-bitowy
- MySQL Enterprise Edition 5.7 32-bitowy/64-bitowy
- MySQL 5.6 Community 32-bitowy/64-bitowy
- MariaDB Galera Cluster 10.4 32-bitowy/64-bitowy

Obsługiwane są następujące platformy wirtualizacji:

- VMware vSphere 4.1
- VMware vSphere 5.0
- VMware vSphere 5.1
- VMware vSphere 5.5
- VMware vSphere 6
- VMware vSphere 6.5
- VMware Workstation 9.x
- VMware Workstation 10.x
- VMware Workstation 11.x

- VMware Workstation 12.x Pro
- VMware Workstation Pro 14
- VMware Workstation Pro 15
- Microsoft Hyper-V Server 2008 64-bitowy
- Microsoft Hyper-V Server 2008 R2 64-bitowy
- Microsoft Hyper-V Server 2008 R2 z Service Pack 1 i nowszy 64-bitowy
- Microsoft Virtual PC 2007 (6.0.156.0) 32-bitowy/64-bitowy
- Citrix XenServer 5.6
- Citrix XenServer 6.0
- Citrix XenServer 6.1
- Citrix XenServer 6.2
- Citrix XenServer 6.5
- Citrix XenServer 7
- Parallels Desktop 7
- Parallels Desktop 11
- Parallels Desktop 14
- Parallels Desktop 16
- Oracle VM VirtualBox 4.0.4-70112
- Oracle VM VirtualBox 5.x

Nieobsługiwane systemy operacyjne i platformy. Kaspersky Security Center Web Console Server

Kaspersky Security Center Web Console Server nie jest kompatybilny z systemami operacyjnymi:

- Debian GNU/Linux 7.x (do 7.8) 32-bitowy/64-bitowy
- Debian GNU/Linux 8.x (Jessie) 32-bitowy/64-bitowy
- Debian GNU/Linux 9.x (Stretch) 32-bitowy/64-bitowy
- Ubuntu Server 14.04 LTS (Trusty Tahr) 32-bitowy/64-bitowy
- Ubuntu Server 16.04 LTS (Xenial Xerus) 32-bitowy/64-bitowy

- Ubuntu Server 20.04.04 LTS (Focal Fossa) ARM 64-bitowy
- Ubuntu Desktop 14.04 LTS (Trusty Tahr) 32-bitowy/64-bitowy
- Ubuntu Desktop 16.04 LTS (Xenial Xerus) 32-bitowy/64-bitowy
- Ubuntu Desktop 18.04 LTS (Bionic Beaver) 32-bitowy/64-bitowy
- Ubuntu Desktop 20.04 LTS (Focal Fossa) 32-bitowy/64-bitowy
- CentOS 6.x (do 6.6) 64-bitowy
- CentOS 7.x ARM 64-bitowy
- CentOS 7.x 64-bitowy
- CentOS 8.x 64-bitowy
- Red Hat Enterprise Linux Server 6.x 32-bitowy/64-bitowy
- SUSE Linux Enterprise Desktop 12 (wszystkie pakiety Service Pack) 64-bitowy
- SUSE Linux Enterprise Desktop 15 (wszystkie pakiety Service Pack) 64-bitowy
- SUSE Linux Enterprise Desktop 15 z Service Pack 3 ARM 64-bitowy
- openSUSE 15 64-bitowy
- EulerOS 2.0 SP8 ARM
- Pardus OS 19.1 64-bitowy
- Astra Linux Special Edition 1.5 64-bitowy
- Astra Linux Special Edition RUSB.10152-02 (aktualizacja operacyjna 4.7) ARM 64-bit
- ALT Workstation 9.2 32-bitowy/64-bitowy
- ALT Workstation 10 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
- Mageia 4 32-bitowy
- Linux Mint 19.x 32-bitowy
- Linux Mint 20.x 64-bitowy
- AlterOS 7.5 i nowszy 64-bitowy
- RED OS 7.3 64-bitowy

- GosLinux IC6 64-bitowy
- ROSA Enterprise Linux Server 7.3 64-bitowy
- ROSA Enterprise Linux Desktop 7.3 64-bitowy
- ROSA COBALT Workstation 7.3 64-bitowy
- ROSA COBALT Server 7.3 64-bitowy
- ROSA CHROME 12 64-bitowy
- Lotos (rdzeń Linux w wersji 4.19.50, DE: MATE) 64-bitowy

Nieobsługiwane systemy operacyjne i platformy. Agent sieciowy

Następujące systemy operacyjne nie są obsługiwane:

- Microsoft Windows Embedded POSReady 7 32-/64-bitowy
- Microsoft Windows Embedded 8 Standard 32-bitowy/64-bitowy
- Microsoft Windows Embedded 8 Industry Pro 32-bitowy/64-bitowy
- Microsoft Windows Embedded 8 Industry Enterprise 32-bitowy/64-bitowy
- Microsoft Windows Embedded 8.1 Industry Enterprise 32-bitowy/64-bitowy
- Microsoft Windows Embedded 8.1 Industry Update 32-bitowy/64-bitowy
- Microsoft Windows 10 Home (Threshold 1, 1507) 32-bitowy/64-bitowy
- Microsoft Windows 10 Pro (Threshold 1, 1507) 32-bitowy/64-bitowy
- Microsoft Windows 10 Enterprise (Threshold 1, 1507) 32-bitowy/64-bitowy
- Microsoft Windows 10 Education (Threshold 1, 1507) 32-bitowy/64-bitowy
- Microsoft Windows 10 Mobile (Threshold 1, 1507) 32-bitowy
- Microsoft Windows 10 Mobile Enterprise (Threshold 1, 1507) 32-bitowy
- Microsoft Windows 10 Home Threshold 2 (aktualizacja z listopada 2015 r., 1511) 32-bitowy/64-bitowy
- Microsoft Windows 10 Pro Threshold 2 (aktualizacja z listopada 2015 r., 1511) 32-bitowy/64-bitowy
- Microsoft Windows 10 Enterprise Threshold 2 (aktualizacja z listopada 2015 r., 1511) 32-bitowy/64-bitowy
- Microsoft Windows 10 Education Threshold 2 (aktualizacja z listopada 2015 r., 1511) 32-bitowy/64-bitowy
- Microsoft Windows 10 Mobile Threshold 2 (aktualizacja z listopada 2015 r., 1511) 32-bitowy
- Microsoft Windows 10 Mobile Enterprise Threshold 2 (aktualizacja z listopada 2015 r., 1511) 32-bitowy

- Microsoft Windows 10 Home RS1 (aktualizacja rocznicowa, 1607) 32-bitowy/64-bitowy
- Microsoft Windows 10 Pro RS1 (aktualizacja rocznicowa, 1607) 32-bitowy/64-bitowy
- Microsoft Windows 10 Enterprise RS1 (aktualizacja rocznicowa, 1607) 32-bitowy/64-bitowy
- Microsoft Windows 10 Education RS1 (aktualizacja rocznicowa, 1607) 32-bitowy/64-bitowy
- Microsoft Windows 10 Mobile RS1 (aktualizacja rocznicowa, 1607) 32-bitowy
- Microsoft Windows 10 Mobile Enterprise RS1 (aktualizacja rocznicowa, 1607) 32-bitowy
- Microsoft Windows 10 Home RS2 (Creators Update, 1703) 32-bitowy/64-bitowy
- Microsoft Windows 10 Pro RS2 (Creators Update, 1703) 32-bitowy/64-bitowy
- Microsoft Windows 10 Enterprise RS2 (Creators Update, 1703) 32-bitowy/64-bitowy
- Microsoft Windows 10 Education RS2 (Creators Update, 1703) 32-bitowy/64-bitowy
- Microsoft Windows 10 Mobile RS2 (Creators Update, 1703) 32-bitowy
- Microsoft Windows 10 Mobile Enterprise RS2 (Creators Update, 1703) 32-bitowy
- Microsoft Windows 10 Mobile RS3 32-bitowy
- Microsoft Windows 10 Mobile Enterprise RS3 32-bitowy
- Microsoft Windows 10 Mobile RS4 32-bitowy
- Microsoft Windows 10 Mobile Enterprise RS4 32-bitowy
- Microsoft Windows 10 Mobile RS5 32-bitowy
- Microsoft Windows 10 Mobile Enterprise RS5 32-bitowy
- Microsoft Windows 8 (Core) 32-bitowy/64-bitowy
- Microsoft Windows 7 Professional 32-bitowy/64-bitowy
- Microsoft Windows 7 Enterprise/Ultimate 32-bitowy/64-bitowy
- Microsoft Windows 7 Home Basic/Premium 32-bitowy/64-bitowy
- Microsoft Windows Vista Business z Service Pack 1 32-bitowy/64-bitowy
- Microsoft Windows Vista Enterprise z Service Pack 1 32-bitowy/64-bitowy
- Microsoft Windows Vista Ultimate z Service Pack 1 32-bitowy/64-bitowy
- Microsoft Windows Vista Business z Service Pack 2 i nowszy 32-bitowy/64-bitowy
- Microsoft Windows Vista Enterprise z Service Pack 2 i nowszy 32-bitowy/64-bitowy
- Microsoft Windows Vista Ultimate z Service Pack 2 i nowszy 32-bitowy/64-bitowy

- Microsoft Windows XP Professional z dodatkiem Service Pack 2 32-bitowy/64-bitowy
- Microsoft Windows XP Home Service Pack 3 i wyższy 32-bitowy
- Windows Essential Business Server 2008 Standard 64-bitowy
- Windows Essential Business Server 2008 Premium 64-bitowy
- Windows Small Business Server 2003 Standard z Service Pack 1 32-bitowy
- Windows Small Business Server 2003 Premium z Service Pack 1 32-bitowy
- Windows Small Business Server 2003 R2 Standard 32-bitowy
- Windows Small Business Server 2003 R2 Premium 32-bitowy
- Windows Small Business Server 2008 Standard 64-bitowy
- Windows Small Business Server 2008 Premium 64-bitowy
- Windows Small Business Server 2011 Standard 64-bitowy
- Windows Small Business Server 2011 Premium Add-on 64-bitowy
- Windows Small Business Server 2011 Essentials 64-bitowy
- Windows Home Server 2011 64-bitowy
- Windows MultiPoint Server 2010 Standard 64-bitowy
- Windows MultiPoint Server 2010 Premium 64-bitowy
- Windows MultiPoint Server 2012 Standard/Premium 64-bitowy
- Microsoft Windows 2000 Server 32-bitowy
- Windows Server 2003 Enterprise z Service Pack 2 32-bitowy/64-bitowy
- Windows Server 2003 Standard z Service Pack 2 32-bitowy/64-bitowy
- Windows Server 2003 R2 Enterprise z Service Pack 2 32-bitowy/64-bitowy
- Windows Server 2003 R2 Standard z Service Pack 2 32-bitowy/64-bitowy
- Windows Server 2008 Datacenter z Service Pack 1 32-bitowy/64-bitowy
- Windows Server 2008 Enterprise z Service Pack 1 32-bitowy/64-bitowy
- Windows Server 2008 z Service Pack 1 Server Core 32-bitowy/64-bitowy
- Windows Server 2008 Standard z Service Pack 1 32-bitowy/64-bitowy
- Windows Server 2008 Standard 32-bitowy/64-bitowy
- Windows Server 2008 Enterprise 32-bitowy/64-bitowy

- Windows Server 2008 Datacenter 32-bitowy/64-bitowy
- Windows Server 2008 R2 Server Core 64-bitowy
- Windows Server 2008 R2 Datacenter 64-bitowy
- Windows Server 2008 R2 Enterprise 64-bitowy
- Windows Server 2008 R2 Foundation 64-bitowy
- Windows Server 2008 R2 Standard 64-bitowy
- Windows Server 2016 Nano (Opcja instalacji) (CBB)
- Windows Storage Server 2008 32-bitowy/64-bitowy
- Windows Storage Server 2008 z Service Pack 2 64-bitowy
- Windows Storage Server 2008 R2 64-bitowy
- Windows Storage Server 2012 64-bitowy
- Windows Storage Server 2012 R2 64-bitowy
- Windows Storage Server 2016 64-bitowy
- Windows Storage Server 2019 64-bitowy
- Debian GNU/Linux 9.x (Stretch) 32-bitowy/64-bitowy
- Debian GNU/Linux 7.x (do 7.8) 32-bitowy/64-bitowy
- Debian GNU/Linux 8.x (Jessie) 32-bitowy/64-bitowy
- Ubuntu Server 14.04 LTS (Trusty Tahr) 32-bitowy/64-bitowy
- Ubuntu Server 16.04 LTS (Xenial Xerus) 32-bitowy/64-bitowy
- Ubuntu Server 20.04.04 LTS (Focal Fossa) ARM 64-bitowy
- Ubuntu Desktop 14.04 LTS (Trusty Tahr) 32-bitowy/64-bitowy
- Ubuntu Desktop 16.04 LTS (Xenial Xerus) 32-bitowy/64-bitowy
- Ubuntu Desktop 18.04 LTS (Bionic Beaver) 32-bitowy/64-bitowy
- Ubuntu Desktop 20.04 LTS (Focal Fossa) 32-bitowy/64-bitowy
- CentOS 6.x (do 6.6) 64-bitowy
- CentOS 7.x ARM 64-bitowy
- CentOS 8.x 64-bitowy
- SUSE Linux Enterprise Desktop 12 (wszystkie SP) 64-bitowy

- SUSE Linux Enterprise Desktop 15 (wszystkie pakiety Service Pack) 64-bitowy
- Astra Linux Special Edition 1.5 64-bitowy
- Astra Linux Special Edition RUSB.10265-01 (aktualizacja operacyjna 8.1) Elbrus
- Astra Linux Special Edition RUSB.10015-16 (aktualizacja operacyjna 8.1) Elbrus
- Pardus OS 19.1 64-bitowy
- Linux Mint 19.x 32-bitowy
- Lotos (rdzeń Linux w wersji 4.19.50, DE: MATE) 64-bitowy
- ROSA Enterprise Linux Server 7.3 64-bitowy
- ROSA Enterprise Linux Desktop 7.3 64-bitowy
- ROSA COBALT Workstation 7.3 64-bitowy
- ROSA COBALT Server 7.3 64-bitowy

Następujące platformy wirtualizacji nie są obsługiwane:

- VMware vSphere 4.1
- VMware vSphere 5.0
- VMware vSphere 5.1
- VMware vSphere 5.5
- VMware vSphere 6
- VMware vSphere 6.5
- VMware Workstation 9.x
- VMware Workstation 10.x
- VMware Workstation 11.x
- VMware Workstation 12.x Pro
- VMware Workstation Pro 14
- VMware Workstation Pro 15
- Microsoft Hyper-V Server 2008 64-bitowy
- Microsoft Hyper-V Server 2008 R2 64-bitowy
- Microsoft Hyper-V Server 2008 R2 z Service Pack 1 i nowszy 64-bitowy
- Citrix XenServer 6.0

- Citrix XenServer 6.1
- Citrix XenServer 6.2
- Citrix XenServer 6.5
- Citrix XenServer 7

Pakiet dystrybucyjny

Aplikację można kupić w sklepie internetowym Kaspersky (na przykład, https://www.kaspersky.pl lub u partnerów firmy.

Jeśli zakupisz Kaspersky Security Center Linux w sklepie internetowym, pobierz aplikację ze strony internetowej sklepu. Informacje potrzebne do aktywacji aplikacji są przesyłane drogą elektroniczną po dokonaniu płatności.

Informacje o kompatybilności Serwera administracyjnego i Kaspersky Security Center Web Console

Zalecamy korzystanie z najnowszej wersji Serwera administracyjnego Kaspersky Security Center Linux i Kaspersky Security Center Web Console. W przeciwnym razie funkcjonalność Kaspersky Security Center Linux może być ograniczona.

Możesz niezależnie zainstalować i uaktualnić Serwer administracyjny Kaspersky Security Center Linux 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.

- Konsola internetowa Kaspersky Security Center Linux 15 obsługuje serwer administracyjny Kaspersky Security Center Linux w następujących wersjach: 15 i 14.2.
- Serwer administracyjny Kaspersky Security Center Linux 15 obsługuje Kaspersky Security Center Web Console w następujących wersjach: 15 i 14.2.

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 Linux. 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 14.2 Windows	Kaspersky Security Center 15 Linux
Lokalizacja Serwera administracyjnego	Lokalnie	Lokalnie
Lokalizacja systemu zarządzania bazą danych (DBMS)	Lokalnie	Lokalnie
System operacyjny do zainstalowania Serwera administracyjnego	Windows	Linux
Typ konsoli administracyjnej	Lokalne i internetowe	Internetowe
System operacyjny do zainstalowania internetowej konsoli administracyjnej	Windows lub Linux	Linux
Hierarchia Serwerów administracyjnych	✓	✓
Hierarchia Grupy administracyjnej	✓	✓
Przeszukiwanie sieci	✓	✓ (według zakresów adresów IP i kontrolerów domen, Samba 4 Active Directory, Microsoft Active Directory)
Maksymalna liczba zarządzanych urządzeń	100 000	50 000 (z PostgreSQL i Postgres Pro)
Ochrona urządzeń zarządzanych przez systemy Windows, macOS i Linux	✓	✓
Ochrona urządzeń mobilnych	✓	–
Ochrona maszyn wirtualnych	✓	✓
Ochrona infrastruktury chmury publicznej	✓	–
Zarządzanie bezpieczeństwem zorientowane na urządzenie	✓	✓
Zarządzanie bezpieczeństwem zorientowane na użytkownika	✓	✓
Zasady aplikacji	✓	✓
Zadania dla aplikacji Kaspersky	✓	✓
Kaspersky Security Network	✓	✓
KSN Proxy	✓	✓
Kaspersky Private Security Network	✓	✓
Scentralizowane wdrażanie kluczy licencyjnych dla aplikacji Kaspersky	✓	✓
Automatyczna aktualizacja antywirusowych baz danych	✓	✓
Obsługa wirtualnych Serwerów administracyjnych	✓	✓
Instalowanie aktualizacji oprogramowania firm trzecich i naprawianie luk w zabezpieczeniach oprogramowania firm trzecich	✓	– (tylko przy użyciu zadania zdalnej instalacji)
Powiadomienia o zdarzeniach, które miały	✓	✓

miejsce na zarządzanych urządzeniach		
Tworzenie i zarządzanie kontami użytkowników	✓	✓
Zaloguj się do konsoli przy użyciu uwierzytelniania domeny	✓	✓ (Pojedyncze logowanie nie jest obecnie obsługiwane)
Integracja z systemami SIEM	✓	✓ (tylko przy użyciu Syslog)
Monitorowanie statusu polityk i zadań	✓	✓
Wdrażanie klastra trybu failover Kaspersky Security Center	✓	✓
Instalowanie Serwera administracyjnego na klastrze trybu failover Windows Server	✓	–
Używanie SNMP do wysyłania statystyk Serwera administracyjnego do aplikacji innych firm	✓	–
Zdalna diagnostyka urządzeń klienckich	✓	✓
Zdalne połączenie z pulpitem urządzenia klienckiego	✓	–
Zarządzanie rewizjami obiektów	✓	–
Automatyczna aktualizacja aplikacji Kaspersky	✓	–
Instalacja systemów operacyjnych na urządzeniach klienckich	✓	–
Serwer WWW do publikowania pakietów instalacyjnych i innych plików	✓	–
Przeglądanie i praca z alertami wykrytymi przez Kaspersky Endpoint Detection and Response Optimum	✓	✓
Używanie Serwera administracyjnego jako serwera WSUS	✓	–
Integracja z Kaspersky Managed Detection and Response	✓	–
Obsługa Adaptacyjnej kontroli anomalii	✓	–
Obsługa klastrów i macierzy serwerowych w grupach administracyjnych	✓ (tylko w konsoli administracyjnej opartej na konsoli MMC)	✓
Zarządzanie licencjami stron trzecich	✓	–

Informacje o Kaspersky Security Center Cloud Console

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 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. Zarządzasz systemem ochrony sieci za pośrednictwem Konsoli administracyjnej opartej o chmurę o nazwie Kaspersky Security Center Cloud Console. Ta konsola posiada interfejs podobny do interfejsu Kaspersky Security Center Web Console.

Interfejs i dokumentacja Kaspersky Security Center Cloud Console są dostępne w następujących językach:

- angielskim
- francuskim
- niemieckim
- włoskim
- japońskim
- portugalskim (Brazylijski)
- rosyjskim
- hiszpańskim
- hiszpańskim (LATAM)

Więcej informacji o konsoli Kaspersky Security Center Cloud Console i jej funkcjach można znaleźć w dokumentacji do Kaspersky Security Center Cloud Console oraz w dokumentacji do 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.

Diagram zdalnej instalacji Serwera administracyjnego Kaspersky Security Center Linux i konsoli Kaspersky Security Center Web Console

Rysunek poniżej przedstawia diagram zdalnej instalacji Serwera administracyjnego Kaspersky Security Center Linux i konsoli Kaspersky Security Center Web Console.

Diagram zdalnej instalacji 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, serwer Kaspersky Security Center Web Console Server komunikuje się z serwerem administracyjnym Kaspersky Security Center Linux poprzez interfejs OpenAPI. Serwer 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

Poniżej znajduje się tabela zawierająca domyślne porty, które muszą być otwarte na Serwerze administracyjnym i urządzeniach klienckich. 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.
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 domyślny numer portu w ustawieniach profilu Agenta sieciowego.
13299	klserver	TCP (TLS)	Odbieranie połączeń od Kaspersky Security Center Web Console do Serwera administracyjnego; odbieranie połączeń do Serwera administracyjnego poprzez OpenAPI	Kaspersky Security Center Web Console, OpenAPI. Domyślny numer portu można zmienić w oknie właściwości Serwera administracyjnego (w podsekcji **Porty połączeń** w sekcji **Ogólne**) lub podczas tworzenia hierarchii Serwerów administracyjnych.
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.

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.
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**).
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 za pomocą narzędzia klscflag.

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 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 od 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 domyślny numer portu w ustawieniach profilu Agenta sieciowego.
15000	klnagent	Emisja protokołu 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 Serwera administracyjnego.

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.

Następująca 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	ksnproxy	TCP	Odbieranie żądań od	Serwer KSN proxy.

usługa KSN proxy jest uruchomiona na urządzeniu)			zarządzanych urządzeń do serwera 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.

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	Obs
2001	Wtyczka KSCWebConsolePlugin	HTTPS	Port API używany przez procesy wtyczki zarządzania do odbierania żądań z KSCWebConsoleManagementService	Uruchami procesów wtyczek zarządzar
1329, 2003	KSCWebConsoleManagementService	HTTPS	Porty API, które są używane do otrzymywania żądań z usługi KSCWebConsole działającej na tym samym urządzeniu	Aktualizo składnikó Kaspersk Security Web Cor
2005	KSCWebConsole	HTTPS	Port API, który jest używany do otrzymywania żądań z usługi KSCWebConsoleManagementService działającej na tym samym urządzeniu	Uruchami procesów Kaspersk Security Web Cor
8200	—	HTTP	Port API, który jest używany do generowania certyfikatów przy użyciu magazynu HashiCorp Vault (więcej informacji znajdziesz na stronie internetowej HashiCorp Vault)	Instalowa Kaspersk Security Web Cor aktualizo składnikó Kaspersk Security Web Cor
4150, 4151, 4152	KSCWebConsoleMessageQueue	HTTPS	Porty API brokera komunikatów, które są używane do komunikacji między procesami Kaspersky Security Center Web Console oraz wtyczek administracyjnych	Interakcja Kaspersk Security Web Cor wtyczek administr

Podstawowe pojęcia

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

Serwer administracyjny

Komponenty Kaspersky Security Center 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:

- Nosi nazwę „Serwer administracyjny Kaspersky Security Center"
- Ustawiony do automatycznego uruchamiania po załadowaniu systemu operacyjnego
- Posiada konto **SystemLokalny** lub konto użytkownika wybrane podczas instalacji Serwera administracyjnego

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 profilami i zadaniami na urządzeniach klienckich
- Przechowuje informacje o zdarzeniach, które wystąpiły na urządzeniach klienckich
- Generuje raporty z działania aplikacji Kaspersky
- Rozsyła klucze licencyjne do urządzeń klienckich 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 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.

- Korzystaj z Kaspersky Security Center przez dostawców usług. Dostawca usługi musi tylko zainstalować Kaspersky Security Center i Kaspersky Security Center Web Console. Aby zarządzać dużą liczbą urządzeń klienckich różnych organizacji, usługodawca 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://<nazwa serwera sieciowego>:<port HTTPS>/public/<obiekt>,
```

gdzie:

- `<nazwa serwera sieciowego>` to nazwa serwera sieciowego Kaspersky Security Center Web Server.
- `<port HTTPS>` 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.
- `<obiekt>` 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.

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.

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

- Nosi nazwę „Agent sieciowy Kaspersky Security Center”
- Ustawiony do automatycznego uruchamiania po załadowaniu systemu operacyjnego
- Korzysta z konta SystemLokalny

Urządzenie, na którym jest zainstalowany Agent sieciowy, nazywa się *zarządzane urządzenie* lub *urządzenie*. Możesz zainstalować Agenta sieciowego z jednego z następujących źródeł:

- Pakiet instalacyjny w magazynie Serwera administracyjnego (należy posiadać zainstalowany Serwer administracyjny)
- Pakiet instalacyjny znajduje się na serwerach sieciowych Kaspersky

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.

Nazwy procesu uruchamianego przez Agenta sieciowego są następujące:

- klnagent64.service (dla 64-bitowego systemu operacyjnego)
- klnagent.service (dla 32-bitowego systemu operacyjnego)

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 urządzenia klienckie w danej grupie administracyjnej są tak skonfigurowane, aby:

- Używać tych samych ustawień aplikacji (które można określić w profilach 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 komputer tego pracownika z grupy administracyjnej Księgowi do grupy administracyjnej Deweloperzy. Komputer automatycznie pobierze ustawienia aplikacji wymagane dla deweloperów.

Zarządzane urządzenie

Zarządzane urządzenie to komputer z systemem Linux i zainstalowanym Agentem sieciowym. Możesz zarządzać takimi urządzeniami poprzez utworzenie zadań i profili 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. Jeden Serwer administracyjny może obsługiwać maksymalnie 20 000 urządzeń.

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.

Sieciowa wtyczka administracyjna

Specjalny składnik — *sieciowa 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 profile dla aplikacji.

Wtyczki sieciowe do zarządzania można pobrać ze strony internetowej pomocy technicznej 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 zbiorów 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 jednego profilu dla różnych grup administracyjnych; możesz także zmodyfikować ustawienia tych profili w sposób scentralizowany. Te instancje mogą różnić się jednym lub dwoma ustawieniami. Na przykład, wszyscy księgowi w firmie pracują pod kontrolą tego samego profilu—ale starsi księgowi mogą korzystać z dysków flash, a młodsi księgowi nie mają takich uprawnień. W tym przypadku, zastosowanie profili 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 profili.

Profil zasad jest to inaczej podzbiór ustawień profilu. Ten podzbiór jest stosowany na urządzeniach docelowych wraz z profilem i uzupełnia go zgodnie z określonym warunkiem zwanym *warunkiem aktywacji profilu*. Profile mogą zawierać tylko ustawienia różniące się od „podstawowego" profilu, który jest aktywny na zarządzanym urządzeniu. Aktywacja profilu zmodyfikuje ustawienia „podstawowego" profilu, 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
- Tworzenie pakietów instalacyjnych w oparciu o obraz systemu operacyjnego odpowiedniego urządzenia

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.

- 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 profili możliwe jest ustawienie wspólnych wartości ustawień aplikacji dla wszystkich urządzeń należących do grupy.

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

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

- Jeśli modyfikacja ustawienia jest zablokowana, wówczas ta sama wartość (określona w profilu) używana jest na wszystkich urządzeniach klienckich.
- Jeśli modyfikacja ustawienia jest odblokowana, wówczas na każdym urządzeniu klienckim aplikacja używa wartości lokalnej zamiast wartości określonej w profilu. 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 profilu.
- W profilu grupy, jeżeli zablokowane jest modyfikowanie ustawienia.

Lokalne ustawienia aplikacji są zmieniane po pierwszym zastosowaniu profilu w zgodzie z jego 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. 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 eliminacji 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 we 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.

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 uaktualnień 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 SSL o numerze 13000.

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

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.

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 SSL o numerze 13000.

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

Serwer administracyjny w sieci LAN, zarządzane urządzenia w Internecie, zapora 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 używana jest wybrana przez Ciebie firmowa zapora sieciowa. Więcej informacji można znaleźć w dokumentacji aplikacji.

Serwer administracyjny w sieci lokalnej; zarządzane urządzenia nawiązują połączenie z Serwerem administracyjnym poprzez firmową zaporę sieciową

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 SSL o numerze 13000.

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

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 Microsoft Forefront Threat Management Gateway (TMG) lub firmowej zapory sieciowej.

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 TMG 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 SSL o numerze 13000.

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

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 SSL o numerze 13000.

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

4a. Brama połączenia w strefie DMZ odbiera również połączenie z Serwera administracyjnego przez port SSL 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 mobilne nawiązują także połączenie z bramą połączenia za pośrednictwem portu SSL 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 są przesyłane do serwera WWW, który znajduje się na tym samym urządzeniu co Serwer administracyjny.

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.

Oznaczenia stosowane w dokumencie

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 z Serwera administracyjnego zostają wprowadzone do bazy danych.

Serwer administracyjny i 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.

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	Nazwa procesu, który	Protokół	Przeznaczenie portu

	portu	otwiera port		
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	Nazwa procesu, który	Protokół	Przeznaczenie portu

	portu	otwiera port		
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 14 Web Console (ruch sieciowy)

Urządzenie	Numer portu	Nazwa procesu, który otwiera port	Protokół	Przeznaczenie portu

Serwer administracyjny	13299	klserver	TCP (TLS)	Odbieranie połączeń od Kaspersky Security Center Web Console do Serwera administracyjnego poprzez OpenAPI
Serwer Kaspersky Security Center Web Console lub Serwer administracyjny	8080	Node.js: Server-side JavaScript	TCP (TLS)	Odbieranie połączeń od Kaspersky Security Center Web Console

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 Buisness 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 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.

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 wtyczek zarządzających**

   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 wtyczkę internetową do zarządzania 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 profili 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 profili 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.

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

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=<wartość>
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
```

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.

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.

Konfigurowanie serwera PostgreSQL lub Postgres Pro do pracy z Kaspersky Security Center Linux

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

Zalecane parametry w przypadku PostgreSQL i Postgres Pro:

- `shared_buffers =` 25% wartości pamięci RAM urządzenia, na którym jest zainstalowany DBMS

  Jeśli pamięć RAM to mniej niż 1 GB, pozostaw wartość domyślną.

- `max_stack_depth =` maksymalny rozmiar stosu (wykonaj polecenie „ `ulimit -s` ", aby uzyskać tę wartość w KB) minus margines bezpieczeństwa 1 MB

- `temp_buffers = 24MB`

- `work_mem = 16MB`

- `max_connections = 151`

- `max_parallel_workers_per_gather = 0`

- `maintenance_work_mem = 128 MB`

Zrestartuj lub przeładuj serwer po zaktualizowaniu pliku postgresql.conf, aby zastosować zmiany. Więcej informacji można znaleźć w dokumentacji PostgreSQL .

Zapoznaj się z następującym tematem, aby uzyskać szczegółowe informacje na temat tworzenia i konfigurowania kont dla PostgreSQL i Postgres Pro: Konfigurowanie kont do pracy z PostgreSQL i Postgres Pro.

Aby uzyskać szczegółowe informacje na temat parametrów serwerów PostgreSQL i Postgres Pro oraz sposobu określania parametrów, zapoznaj się z odpowiednią dokumentacją DBMS.

Scenariusz: uwierzytelnianie serwera PostgreSQL

Zalecamy użycie certyfikatu TLS do uwierzytelnienia serwera PostgreSQL. Możesz użyć certyfikatu z zaufanego urzędu certyfikacji lub certyfikatu z podpisem własnym. Użyj certyfikatu z zaufanego urzędu certyfikacji, ponieważ certyfikat z podpisem własnym zapewnia tylko ograniczoną ochronę.

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

Wykonaj poniższe kroki, aby skonfigurować uwierzytelnianie SSL dla PostgreSQL:

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 all all 0.0.0.0/0 md5
```

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 ='*'
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 ='*'
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]

Przejdź do katalogu ServerFlags i utwórz plik odpowiadający fladze serwera KLSRV_POSTGRES_OPT_SSL_CA:

```
cd /etc/opt/kaspersky/klnagent_srv/1093/1.0.0.0/ServerFlags/
mkfile KLSRV_POSTGRES_OPT_SSL_CA
```

W utworzonym pliku określ ścieżkę do pliku psql.crt.

[Dwukierunkowe uwierzytelnianie SSL]

Przejdź do katalogu ServerFlags i utwórz pliki odpowiadające flagom serwera:

```
cd /etc/opt/kaspersky/klnagent_srv/1093/1.0.0.0/ServerFlags/
mkfile KLSRV_POSTGRES_OPT_SSL_CA
mkfile KLSRV_POSTGRES_OPT_SSL_CERT
mkfile KLSRV_POSTGRES_OPT_SSL_KEY
```

Edytuj utworzone pliki w następujący sposób:

- KLSRV_POSTGRES_OPT_SSL_CA: określ ścieżkę do pliku psql.crt.
- KLSRV_POSTGRES_OPT_SSL_CERT: określ ścieżkę do pliku postgres.crt.
- KLSRV_POSTGRES_OPT_SSL_KEY: określ ścieżkę do pliku postgres.key.

Jeśli plik postgres.key wymaga hasła, utwórz plik KLSRV_POSTGRES_OPT_TLS_PASPHRASE w folderze ServerFlags i podaj w nim hasło.

7. **Uruchom ponownie usługę Serwera administracyjnego.**

Scenariusz: uwierzytelnianie serwera MySQL

Zalecamy użycie certyfikatu TLS do uwierzytelnienia serwera MySQL. Możesz użyć certyfikatu z zaufanego urzędu certyfikacji lub certyfikatu z podpisem własnym. Użyj certyfikatu z zaufanego urzędu certyfikacji, ponieważ certyfikat z podpisem własnym zapewnia tylko ograniczoną ochronę.

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. Przejdź do katalogu ServerFlags i utwórz plik odpowiadający fladze serwera KLSRV_MYSQL_OPT_SSL_CA:

   ```
   cd /etc/opt/kaspersky/klnagent_srv/1093/1.0.0.0/ServerFlags/
   mkfile KLSRV_MYSQL_OPT_SSL_CA
   ```

2. W pliku KLSRV_MYSQL_OPT_SSL_CA określ ścieżkę do certyfikatu (plik ca-cert.pem).

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

   ```
   [mysqld]
   ssl-ca="C:/mysqlCerts/ca-cert.pem"
   ssl-cert="C:/mysqlCerts/server-cert.pem"
   ssl-key="C:/mysqlCerts/server-key.pem"
   ```

Włącz dwukierunkowe uwierzytelnianie SSL

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

1. Przejdź do katalogu ServerFlags i utwórz pliki odpowiadające flagom serwera:

```
cd /etc/opt/kaspersky/klnagent_srv/1093/1.0.0.0/ServerFlags/
mkfile KLSRV_MYSQL_OPT_SSL_CA
mkfile KLSRV_MYSQL_OPT_SSL_CERT
mkfile KLSRV_MYSQL_OPT_SSL_KEY
```

2. Edytuj utworzone pliki w następujący sposób:

   KLSRV_MYSQL_OPT_SSL_CA: określ ścieżkę do pliku ca-cert.pem.

   KLSRV_MYSQL_OPT_SSL_CERT: określ ścieżkę do pliku server-cert.pem.

   KLSRV_MYSQL_OPT_SSL_KEY: określ ścieżkę do pliku klucz-serwera.pem.

   Jeśli plik server-key.pem wymaga hasła, utwórz plik KLSRV_MARIADB_OPT_TLS_PASPHRASE w folderze ServerFlags i podaj w nim hasło.

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

```
[mysqld]
ssl-ca="C:/mysqlCerts/ca-cert.pem"
ssl-cert="C:/mysqlCerts/server-cert.pem"
ssl-key="C:/mysqlCerts/server-key.pem"
```

Instalowanie Kaspersky Security Center Linux

Ta procedura opisuje sposób instalacji Kaspersky Security Center Linux.

Przed instalacją:

- Zainstaluj system DBMS.
- Upewnij się, że na urządzeniu, na którym chcesz zainstalować Kaspersky Security Center Linux, działa jedna z obsługiwanych dystrybucji systemu Linux.

Użyj pliku instalacyjnego — ksc64_[version_number]_amd64.deb lub ksc64-[version_number].x86_64.rpm — który odpowiada dystrybucji Linux zainstalowanej na urządzeniu. Plik instalacyjny można pobrać ze strony internetowej Kaspersky.

W celu zainstalowania Kaspersky Security Center Linux:

1. W wierszu poleceń uruchom polecenia podane w tej instrukcji na koncie z uprawnieniami administratora.

2. Utwórz grupę „kladmins" i konto nieuprzywilejowane „ksc". 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
```

3. Uruchom instalację Kaspersky Security Center Linux. W zależności od dystrybucji Linux uruchom jedno z następujących poleceń:

   - `# apt install /<path>/ksc64_[ version_number ]_amd64.deb`

- `# yum install /<path>/ksc64-[version_number].x86_64.rpm -y`

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. Wpisz `n`, jeśli nie akceptujesz warunków umowy licencyjnej. Aby korzystać z Kaspersky Security Center Linux, musisz zaakceptować warunki umowy licencyjnej.

   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. Po wyświetleniu monitu wprowadź następujące ustawienia:

   a. Wprowadź nazwę DNS Serwera administracyjnego lub stały adres IP. `127.0.0.1` dla lokalnej instalacji bazy danych.

   b. Wprowadź numer portu SSL Serwera administracyjnego. Domyślnie wykorzystywany jest port 13000.

   c. Oceń przybliżoną liczbę urządzeń, którymi zamierzasz zarządzać:

      - Jeśli masz od 1 do 100 urządzeń sieciowych, wpisz 1.
      - Jeśli masz od 101 do 1000 urządzeń sieciowych, wpisz 2.
      - Jeśli masz więcej niż 1000 urządzeń sieciowych, wpisz 3.

   d. Wprowadź nazwę grupy zabezpieczeń dla usług. Domyślnie używana jest grupa `kladmins`.

   e. Wprowadź nazwę konta, aby uruchomić usługę Serwera administracyjnego. Konto musi należeć do wprowadzonej grupy zabezpieczeń. Domyślnie używane jest konto `ksc`.

   f. Wprowadź nazwę konta, aby uruchomić inne usługi. Konto musi należeć do wprowadzonej grupy zabezpieczeń. Domyślnie używane jest konto `ksc`.

   g. 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.

   h. Wprowadź nazwę DNS lub adres IP urządzenia, na którym zainstalowana jest baza danych. `127.0.0.1` dla lokalnej instalacji bazy danych.

   i. 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

j. Wprowadź nazwę bazy danych.

k. Wprowadź login konta głównego bazy danych, którego używasz do uzyskiwania dostępu do bazy danych.

l. Wprowadź hasło konta głównego bazy danych, którego używasz do uzyskiwania dostępu do bazy danych.

   Poczekaj, aż usługi zostaną dodane i uruchomione automatycznie:

   - `klnagent_srv`
   - `kladminserver_srv`
   - `klactprx_srv`
   - `klwebsrv_srv`

m. Utwórz konto, które będzie działać jako administrator Serwera administracyjnego. Wprowadź nazwę użytkownika i hasło. Możesz użyć następującego polecenia, aby utworzyć nowego użytkownika:
   `/opt/kaspersky/ksc64/sbin/kladduser -n ksc -p <hasło>`

   Hasło musi być zgodne z następującymi regułami:

   - Hasło użytkownika nie może mieć mniej niż 8 ani więcej niż 16 znaków.
   - Hasło musi zawierać znaki z przynajmniej trzech z poniższych grup:
     - Wielkie litery (A-Z)
     - Małe litery (a-z)
     - Cyfry (0-9)
     - Znaki specjalne (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)

Użytkownik zostanie dodany i zainstalowany Kaspersky Security Center Linux.

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`

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:

- Zainstaluj system zarządzania bazą danych (DBMS).
- Upewnij się, że na urządzeniu, na którym chcesz zainstalować Kaspersky Security Center Linux, działa jedna z obsługiwanych dystrybucji systemu Linux.

W celu zainstalowania Kaspersky Security Center Linux w trybie cichym:

1. Przeczytaj Umowę licencyjną. Wykonaj poniższe kroki tylko wtedy, gdy rozumiesz i akceptujesz warunki Umowy licencyjnej.
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
   ```
3. 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.
4. Ustaw wartość zmiennej środowiskowej `KLAUTOANSWERS` w środowisku root zawierającej pełną nazwę pliku odpowiedzi wraz ze ścieżką, na przykład za pomocą następującego polecenia:
   ```
   export KLAUTOANSWERS=/tmp/ksc_install/answers.txt
   ```
5. Uruchom instalację Kaspersky Security Center Linux w trybie cichym — w zależności od używanej dystrybucji Linuksa uruchom jedno z następujących poleceń:
   - `# apt install /<path>/ksc64_[ version_number ]_amd64.deb`
   - `# yum install /<path>/ksc64-[ version_number ].x86_64.rpm -y`
6. 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 ksc -p < hasło >`, gdzie hasło musi zawierać co najmniej 8 znaków.

Zmienne pliku odpowiedzi użyte jako parametry instalacji Kaspersky Security Center Linux w trybie cichym

Nazwa zmiennej	Wymagane	Opis	Możliwe
`EULA_ACCEPTED`	Tak	Ten parametr potwierdza, że w pełni przeczytano, zrozumiano i zaakceptowano warunki Umowy licencyjnej.	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
`KLSRV_UNATT_PORT_SRV`	Nie	Wprowadź numer portu Serwera administracyjnego. Domyślna wartość to 14000.	Numer port

`KLSRV_UNATT_PORT_SRV_SSL`	Nie	Wprowadź numer portu SSL Serwera administracyjnego. Domyślna wartość to 13000.	Numer port
`KLSRV_UNATT_PORT_KLOAPI`	Nie	Numer portu KLOAPI Serwera administracyjnego. Domyślna wartość to 13299.	Numer port
`KLSRV_UNATT_PORT_GUI`	Nie	Numer portu GUI Serwera administracyjnego. Opcja, domyślna wartość to 13291.	Numer port
`KLSRV_UNATT_NETRANGETYPE`	Nie	Oceń przybliżoną liczbę urządzeń, którymi zamierzasz zarządzać. Opcja, domyślna wartość to 1.	`1` dla 1 do 10 sieciowych. `2` dla 101 do urządzeń sie `3` dla ponad urządzeń sie
`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.	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.	`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_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 Linu odpowiedzi musi zawierać następujące dodatkowe zmienne:			
`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.	`VirtualAd`
			lub
			`ExternalL`

W przypadku, gdy zmienna `KLFOC_UNATT_CONN_MODE` ma wartość `VirtualAdapter`, plik odpowiedzi musi za następujące zmienne dodatkowe:			
`KLFOC_UNATT_CONN_MODE_VA_NAME`		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.
- Upewnij się, że na urządzeniu, na którym chcesz zainstalować Kaspersky Security Center Linux, działa jedna z obsługiwanych dystrybucji systemu Linux.
- Pobierz klucz aplikacji kaspersky_astra_pub_key.gpg.

Użyj pliku instalacyjnego ksc64_[version_number]_amd64.deb. Plik instalacyjny można pobrać ze strony internetowej Kaspersky.

W wierszu poleceń uruchom polecenia podane w tej instrukcji na koncie z uprawnieniami administratora.

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 dyski RAM:

```
update-initramfs -u -k all
```

Uruchom ponownie system.

6. Utwórz grupę „kladmins" i konto nieuprzywilejowane „ksc". 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
```

7. Uruchom instalację Kaspersky Security Center Linux:

```
# apt install /<path>/ksc64_[ version_number ]_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. Wpisz `n`, jeśli nie akceptujesz warunków umowy licencyjnej. Aby korzystać z Kaspersky Security Center Linux, musisz zaakceptować warunki umowy licencyjnej.

   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 urządzeń sieciowych, wpisz 1.
      - Jeśli masz od 101 do 1000 urządzeń sieciowych, wpisz 2.
      - Jeśli masz więcej niż 1000 urządzeń sieciowych, wpisz 3.

   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. Wprowadź adres IP urządzenia, na którym zainstalowana jest baza danych.

i. Wprowadź numer portu bazy danych. Ten port jest używany do komunikacji z Serwerem administracyjnym. Domyślnie wykorzystywany jest port 3306.

j. Wprowadź nazwę bazy danych.

k. Wprowadź login konta głównego bazy danych, którego używasz do uzyskiwania dostępu do bazy danych.

l. Wprowadź hasło konta głównego bazy danych, którego używasz do uzyskiwania dostępu do bazy danych.

   Poczekaj, aż usługi zostaną dodane i uruchomione automatycznie:

   - `klnagent_srv`
   - `kladminserver_srv`
   - `klactprx_srv`
   - `klwebsrv_srv`

m. 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 16 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`

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
- Dla ALT 8 SP – ksc-web-console-[build_number]-alt8p.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 (EULA). Jeśli pakiet dystrybucyjny Kaspersky Security Center Linux nie zawiera pliku TXT z treścią umowy EULA, 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. Nadaj plikowi nazwę ksc-web-console-setup.json i umieść go w następującym katalogu: /etc/ksc-web-console-setup.json.

   Przykład pliku odpowiedzi zawierającego minimalny zestaw parametrów oraz domyślny adres i port:

   ```
   {
    "address": "127.0.0.1",
    "port": 8080,
    "trusted":
   "127.0.0.1|13299|/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer|KSC
   Server",
    "acceptEula": true
   }
   ```

   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 dpkg -i ksc-web-console-[build_number].x86_64.deb
     ```
   - W celu zainstalowania Kaspersky Security Center Web Console z pliku .rpm uruchom jedno z następujących poleceń:
     ```
     $ sudo rpm -ivh --nodeps ksc-web-console-[build_number].x86_64.rpm
     ```
     lub
     ```
     $ sudo alien -i ksc-web-console-[build_number].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 rpm -Uvh --nodeps --force ksc-web-console-[build_number].x86_64.rpm
       ```
     - Dla urządzeń z systemem operacyjnym opartym na systemie Debian:
       ```
       $ sudo dpkg -i 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. 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.

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.

Poniżej znajduje się przykład pliku odpowiedzi zawierającego minimalny zestaw parametrów oraz domyślny adres i port:

```
{
 "address": "127.0.0.1",
 "port": 8080,
 "defaultLangId": 1049,
 "enableLog": false,
```

```
 "trusted": "127.0.0.1|13299|/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer|KSC
Server",
 "acceptEula": true,
 "certPath": "/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer",
 "webConsoleAccount": "Group1:User1",
 "managementServiceAccount": "Group1:User2",
 "serviceWebConsoleAccount": "Group1:User3",
 "pluginAccount": "Group1:User4",
 "messageQueueAccount": "Group1:User5"
}
```

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 war
`address`	Adres Kaspersky Security Center Web Console Server (wymagany).	Wartość wiersza.
`port`	Numer portu, którego Kaspersky Security Center Web Console Server użyje do nawiązywania połączenia z Serwerem administracyjnym (wymagany).	Wartość numeryczna.
`defaultLangId`	Język interfejsu użytkownika (domyślnie, `1033`).	Kod numeryczny języka: • Niemiecki: `1031` • Angielski: `1033` • Hiszpański: `3082` • Hiszpański (Meksyk): `2058` • Francuski: `1036` • Japoński: `1041` • Kazachstański: `1087` • Polski: `1045` • Portugalski (Brazylia): `1046` • Rosyjski: `1049` • Turecki: `1055` • Chiński uproszczony: `4` • Chiński tradycyjny: `31748`

		Jeśli nie określono wartości, używany jest
`enableLog`	Czy włączyć rejestrowania aktywności Kaspersky Security Center Web Console.	Wartość zerojedynkowa: • `true`—rejestrowanie jest włączone (w • `false`—rejestrowanie jest wyłączone

`trusted`	Lista zaufanych Serwerów administracyjnych upoważnionych do nawiązywania połączenia z Kaspersky Security Center Web Console. Każdy Serwer administracyjny musi być zdefiniowany z następującymi parametrami:
	• Adres Serwera administracyjnego
	• Port OpenAPI, który jest używany przez Kaspersky Security Center Web Console do nawiązywania połączenia z Serwerem administracyjnym (domyślnie jest to port 13299)
	• Ścieżka do certyfikatu Serwera administracyjnego
	• Nazwa Serwera administracyjnego, która jest wyświetlana w oknie logowania
	Parametry są oddzielane pionowymi słupkami. Jeśli określasz kilka Serwerów administracyjnych, oddziel je dwoma pionowymi słupkami.
		Wartość wiersza w następującym formac
		`" server address | port | certifica`
		Na przykład:
		`"X.X.X.X|13299|/cert/server-1.ce`
		`1 ||Y.Y.Y.Y|13299|/cert/server-2.`

`acceptEula`	Czy chcesz zaakceptować warunki Umowy licencyjnej (EULA). Plik zawierający warunki Umowy licencyjnej jest pobierany wraz z plikiem instalacyjnym.	Wartość zerojedynkowa: • `true`—W pełni przeczytałem, zrozumi Umowy licencyjnej. • `false`—Nie akceptuję postanowień i (wybrana domyślnie). Jeśli nie zostanie określona żadna wartoś Security Center Web Console wyświetli zgadzasz się zaakceptować warunki umo
`certDomain`	Jeśli chcesz wygenerować nowy certyfikat, użyj tego parametru do określenia nazwy domeny, dla której zostanie wygenerowany nowy certyfikat.	Wartość wiersza.
`certPath`	Jeśli chcesz użyć istniejącego certyfikatu, użyj tego parametru	Wartość wiersza.

	do określenia ścieżki do pliku certyfikatu.	Określ ścieżkę `"/var/opt/kaspersky/klnagent_srv` do korzystania z istniejącego certyfikatu. niestandardowego określ ścieżkę, w które certyfikat niestandardowy.
`keyPath`	Jeśli chcesz użyć istniejącego certyfikatu, użyj tego parametru do określenia ścieżki do pliku klucza.	Wartość wiersza.
`webConsoleAccount`	Nazwa konta, pod którym uruchomiona jest usługa KSCWebConsole .	Wartość wiersza w następującym formac `name "`. Przykład: `" Group1 : User1 "`. Jeśli nie określono żadnej wartości, instala Center Web Console utworzy nowe kont `user_management_%uid%`.
`managementServiceAccount`	Nazwa konta uprzywilejowanego, w ramach którego uruchomiona jest usługa KSCWebConsoleManagement.	Wartość wiersza w następującym formac `name "`. Przykład: `" Group1 : User1 "`. Jeśli nie określono żadnej wartości, instala Center Web Console utworzy nowe kont `user_nodejs_%uid%`.
`serviceWebConsoleAccount`	Nazwa konta, w ramach którego uruchomiona jest usługa KSCSvcWebConsole .	Wartość wiersza w następującym formac `name "`. Przykład: `" Group1 : User1 "`. Jeśli nie określono żadnej wartości, instala Center Web Console utworzy nowe kont `user_svc_nodejs_%uid%`.
`pluginAccount`	Nazwa konta, pod którym uruchomiona jest usługa KSCWebConsolePlugin.	Wartość wiersza w następującym formac `name "`. Przykład: `" Group1 : User1 "`. Jeśli nie określono żadnej wartości, instala Center Web Console utworzy nowe kont `user_web_plugin_%uid%`.
`messageQueueAccount`	Nazwa konta, pod którym uruchomiona jest usługa KSCWebConsoleMessageQueue.	Wartość wiersza w następującym formac `name "`. Przykład: `" Group1 : User1 "`. Jeśli nie określono żadnej wartości, instala Center Web Console utworzy nowe kont `user_message_queue_%uid%`.

Jeśli określisz parametry `webConsoleAccount`, `managementServiceAccount`, `serviceWebConsoleAccount`, `pluginAccount` lub `messageQueueAccount`, 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 bezpieczeństwa, a następnie utworzy w tej grupie konta użytkowników o domyślnych nazwach.

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 (EULA). Jeśli pakiet dystrybucyjny Kaspersky Security Center Linux nie zawiera pliku TXT z treścią umowy EULA, 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. Nadaj plikowi nazwę ksc-web-console-setup.json i umieść go w następującym katalogu: /etc/ksc-web-console-setup.json.

   Przykład pliku odpowiedzi zawierającego minimalny zestaw parametrów oraz domyślny adres i port:

   ```
   {
    "address": "127.0.0.1",
    "port": 8080,
    "trusted":
   "127.0.0.1|13299|/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer|KSC
   Server",
    "acceptEula": true
   }
   ```

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 dpkg -i ksc-web-console-[build_number].x86_64.deb
     ```
   - W celu przeprowadzenia aktualizacji z poprzedniej wersji Kaspersky Security Center Web Console, uruchom następujące polecenie:
     ```
     $ sudo dpkg -i 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.

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 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.

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 `zaufany` parametr instalacji, aby zezwolić klastrowi pracy awaryjnej Kaspersky Security Center Linux na połączenie z Kaspersky Security Center Web Console. Wartość ciągu tego parametru ma następujący format:
   ```
   "trusted": "server address|port|certificate path|server name"
   ```
   Określ składniki parametru `trusted` instalacji:

   - **Adres Serwera administracyjnego**. Jeśli utworzyłeś dodatkową kartę sieciową podczas przygotowywania węzłów klastra, użyj adresu IP karty jako adresu klastra pracy awaryjnej Kaspersky Security Center Linux. W przeciwnym razie określ adres IP modułu równoważenia obciążenia innej firmy, którego używasz.

   - **Port Serwera administracyjnego**. Port OpenAPI, którego Kaspersky Security Center Web Console używa do łączenia się z Serwerem administracyjnym (wartość domyślna to 13299).

   - **Certyfikatu Serwera administracyjnego**. Certyfikat Serwera administracyjnego znajduje się we współdzielonym magazynie danych klastra pracy awaryjnej 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.

- **Nazwa Serwera administracyjnego**. Nazwa klastra pracy awaryjnej Kaspersky Security Center Linux, która będzie wyświetlana w oknie logowania Kaspersky Security Center Web Console.

3. Kontynuuj standardową instalację Kaspersky Security Center Web Console.

Po zakończeniu instalacji, skrót pojawi się na Twoim pulpicie i będziesz mógł/mogła zalogować się do Kaspersky Security Center Web Console.

Możesz przejść do opcji **Wykrywanie i wdrażanie** → **Urządzenia nieprzypisane** aby wyświetlić informacje o węzłach klastra i serwerze plików.

Wdrażanie klastra trybu failover Kaspersky Security Center Linux

Ta sekcja zawiera zarówno ogólne informacje o klastrze trybu failover Kaspersky Security Center Linux, jak i instrukcje dotyczące przygotowania i instalacji 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.

Wymagania wstępne

Masz sprzęt spełniający wymagania dla klastra trybu failover.

Wdrożenie aplikacji firmy Kaspersky odbywa się w krokach:

1. **Tworzenie kont dla usług Kaspersky Security Center Linux**

   Wykonaj następujące czynności na węźle aktywnym, węźle pasywnym i serwerze plików:

   1. Utwórz grupę domeny 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.

2. **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

3. **Przygotowanie węzłów aktywnych i pasywnych**

   Przygotuj dwa komputery z identycznym sprzętem i oprogramowaniem do pracy jako węzły aktywne i pasywne.

   Instrukcje: Przygotowywanie węzłów dla klastra trybu failover Kaspersky Security Center Linux

4. **Instalacja systemu zarządzania bazą danych (DBMS)**

   Masz dwie opcje:

   - Jeśli chcesz korzystać z MariaBD Galera Cluster, nie potrzebujesz dedykowanego komputera dla DBMS. Zainstaluj klaster MariaDB Galera Cluster na każdym z węzłów.
   - Jeśli chcesz użyć innego obsługiwanego DBMS, zainstaluj wybrany DBMS na dedykowanym komputerze.

5. **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 aktywnym węźle, a następnie zainstalować go na węźle pasywnym.

   Dodatkowo, możesz zainstalować Kaspersky Security Center Web Console na oddzielnym urządzeniu, które nie jest węzłem klastra.

6. **Testowanie klastra trybu failover**

   Sprawdź, czy poprawnie skonfigurowano klaster trybu failover i czy działa poprawnie. Na przykład możesz zatrzymać jedną z usług Kaspersky Security Center Linux na aktywnym węźle: kladminserver, klnagent, ksnproxy, klactprx lub klwebsrv. Po zatrzymaniu usługi zarządzanie ochroną musi zostać automatycznie przełączone na węzeł pasywny.

Wyniki

Wdrożony zostaje klaster trybu failover Kaspersky Security Center Linux. Prosimy o zapoznanie się ze zdarzeniami, które prowadzą do przełączenia między aktywnym i pasywnym węzłem.

Informacje o klastrze 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.

> W klastrze pracy awaryjnej Kaspersky Security Center Linux, wszystkie usługi Kaspersky Security Center Linux są zarządzane automatycznie. Nie próbuj ponownie uruchamiać usług ręcznie.

Wymagania sprzętowe i programowe

W celu zainstalowania klastra trybu failover Kaspersky Security Center Linux musisz mieć następujący sprzęt:

- Dwa komputery z identycznym sprzętem i oprogramowaniem. Te komputery będą działać jako węzły aktywne i pasywne.

- Serwer plików z systemem Linux z systemem plików EXT4. Musisz zapewnić dedykowany komputer, który będzie działał jako serwer plików.

  Upewnij się, że zapewniłeś wysoką przepustowość sieci między serwerem plików a aktywnymi i pasywnymi węzłami.

- Komputer z systemem zarządzania bazami danych (DBMS). Jeśli używasz MariaBD Galera Cluster jako DBMS, dedykowany komputer do tego celu nie jest wymagany.

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 celowo zamknięta przez użytkownika. Usługi Kaspersky Security Center Linux są następujące: kladminserver, klnagent, klactprx i klwebsrv.
- Połączenie sieciowe między aktywnym węzłem a magazynem na serwerze plików zostało przerwane lub zakończone.

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
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.

Uruchom następujące polecenia:

```
sudo yum install nfs-utils
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 777 /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 cat /etc/exports
sudo exportfs -a
sudo systemctl start rpcbind
sudo service nfs start
```

Włącz autostart, uruchamiając następujące polecenie:

```
sudo systemctl enable rpcbind
```

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

Przygotuj dwa komputery do pracy jako węzły aktywne i pasywne dla klastra trybu failover Kaspersky Security Center Linux.

W celu przygotowania węzłów dla klastra trybu failover Kaspersky Security Center Linux:

1. Upewnij się, że masz dwa komputery, które spełniają wymagania sprzętowe i programowe. Te komputery będą działać jako aktywne i pasywne węzły klastra trybu failover.

2. Aby węzły działały jako klienci NFS, zainstaluj pakiet nfs-utils na każdym węźle.

   Uruchom następujące polecenie:

   ```
   sudo yum install nfs-utils
   ```

3. Utwórz punkty montowania, uruchamiając następujące polecenia:

   ```
   sudo mkdir -p /mnt/KlFocStateShare
   sudo mkdir -p /mnt/KlFocDataShare_klfoc
   ```

4. Sprawdź, czy współdzielone foldery mogą zostać pomyślnie zamontowane. [krok opcjonalny]

   Uruchom następujące polecenia:

   ```
   sudo mount -t nfs -o vers=4,nolock,local_lock=none,auto,user,rw {server}:{path to
   the KlFocStateShare folder} /mnt/KlFocStateShare
   sudo mount -t nfs -o vers=4,nolock,local_lock=none,noauto,user,rw {server}:{path to
   the KlFocDataShare_klfoc folder} /mnt/KlFocDataShare_klfoc
   ```

   Tutaj `{server}:{path to the KlFocStateShare folder}` oraz `{server}:{path to the KlFocDataShare_klfoc folder}` są ścieżkami sieciowymi do folderów współdzielonych na serwerze plików.

   Po pomyślnym zamontowaniu folderów współdzielonych odmontuj je, uruchamiając następujące polecenia:

```
sudo umount /mnt/KlFocStateShare
sudo umount /mnt/KlFocDataShare_klfoc
```

5. Dopasuj punkty montowania i foldery współdzielone:

```
sudo vi /etc/fstab
{server}:{path to the KlFocStateShare folder} /mnt/KlFocStateShare nfs
vers=4,nolock,local_lock=none,auto,user,rw 0 0
{server}:{path to the KlFocDataShare_klfoc folder} /mnt/KlFocDataShare_klfoc nfs
vers=4,nolock,local_lock=none,noauto,user,rw 0 0
```

Tutaj `{server}:{path to the KlFocStateShare folder}` oraz `{server}:{path to the KlFocDataShare_klfoc folder}` są ścieżkami sieciowymi do folderów współdzielonych na serwerze plików.

6. Zrestartuj oba węzły.

7. Zamontuj foldery współdzielone, uruchamiając następujące polecenia:

```
mount /mnt/KlFocStateShare
mount /mnt/KlFocDataShare_klfoc
```

8. Upewnij się, że uprawnienia dostępu do folderów udostępnionych należą do ksc:kladmins.

Uruchom następujące polecenie:

```
sudo ls -la /mnt/
```

9. W każdym z węzłów skonfiguruj dodatkową kartę sieciową.

Dodatkowa karta sieciowa może być fizyczna lub wirtualna. Jeśli chcesz użyć fizycznej karty sieciowej, podłącz ją i skonfiguruj za pomocą standardowych narzędzi systemu operacyjnego. Jeśli chcesz użyć wirtualnej karty sieciowej, utwórz ją za pomocą oprogramowania innej firmy.

Wykonaj jedną z poniższych czynności:

- Użyj wirtualnej karty sieciowej.

  a. Użyj następującego polecenia, aby sprawdzić, czy NetworkManager jest używany do zarządzania adapterem fizycznym:

  ```
  nmcli device status
  ```

  Jeśli w danych wyjściowych adapter fizyczny jest wyświetlany jako niezarządzany, skonfiguruj program NetworkManager do zarządzania adapterem fizycznym. Dokładne kroki konfiguracji zależą od Twojej dystrybucji.

  b. Użyj następującego polecenia, aby zidentyfikować interfejsy:

  ```
  ip a
  ```

  c. Utwórz nowy profil konfiguracji:

  ```
  nmcli connection add type macvlan dev <interfejs fizyczny> mode bridge
  ifname <interfejs wirtualny> ipv4.addresses <maska adresu> ipv4.method
  manual autoconnect no
  ```

- Użyj fizycznej karty sieciowej lub hipernadzorcy. W tym scenariuszu wyłącz oprogramowanie NetworkManager.

  a. Usuń połączenia NetworkManager dla interfejsu docelowego:

  ```
  nmcli con del <nazwa połączenia>
  ```

  Użyj następującego polecenia, aby sprawdzić, czy interfejs docelowy ma połączenia:

  ```
  nmcli con show
  ```

b. Edytuj plik NetworkManager.conf. Znajdź sekcję pliku klucza i przypisz interfejs docelowy do parametru unmanaged-devices.

```
[keyfile]
unmanaged-devices=interface-name:<nazwa interfejsu>
```

c. Uruchom ponownie Network Managera:

```
systemctl przeładuj NetworkManager
```

Użyj następującego polecenia, aby sprawdzić, czy interfejs docelowy nie jest zarządzany:

```
nmcli dev status
```

- Użyj modułu równoważenia obciążenia innej firmy. Na przykład, możesz użyć serwera nginx. W takim przypadku wykonaj następujące czynności:

  a. Zapewnij dedykowany komputer oparty o system Linux z zainstalowanym nginx.

  b. Skonfiguruj moduł równoważenia obciążenia. Ustaw węzeł aktywny jako serwer główny, a węzeł pasywny jako serwer zapasowy.

  c. Na serwerze nginx otwórz wszystkie porty Serwera administracyjnego: TCP 13000, UDP 13000, TCP 13291, TCP 13299 i TCP 17000.

Węzły są przygotowane. Aby zainstalować klaster trybu failover Kaspersky Security Center Linux, postępuj zgodnie z dalszymi instrukcjami scenariusza.

Instalowanie Kaspersky Security Center Linux na węzłach klastra trybu failover Kaspersky Security Center Linux

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.

Użyj pliku instalacyjnego — ksc64_[version_number]_amd64.deb lub ksc64-[version_number].x86_64.rpm — który odpowiada dystrybucji Linux zainstalowanej na urządzeniu. Plik instalacyjny można pobrać ze strony internetowej Kaspersky.

Tylko użytkownik z grupy domen KLAdmins może zainstalować Kaspersky Security Center Linux na każdym węźle.

Instalacja na węźle podstawowym (aktywnym)

W celu zainstalowania Kaspersky Security Center Linux na węźle podstawowym:

1. Upewnij się, że na urządzeniu, na którym chcesz zainstalować Kaspersky Security Center Linux, działa jedna z obsługiwanych dystrybucji systemu Linux.

2. W wierszu poleceń uruchom polecenia podane w tej instrukcji na koncie z uprawnieniami administratora.

3. Uruchom instalację Kaspersky Security Center Linux. W zależności od dystrybucji Linux uruchom jedno z następujących poleceń:

   - `sudo apt install /<path>/ksc64_[version_number]_amd64.deb`
   - `sudo yum install /<path>/ksc64-[version_number].x86_64.rpm -y`

4. Uruchom konfigurację Kaspersky Security Center Linux:

   ```
   sudo /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. Wpisz `n`, jeśli nie akceptujesz warunków umowy licencyjnej. Aby korzystać z Kaspersky Security Center Linux, musisz zaakceptować warunki umowy licencyjnej.

   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 wprowadź następujące ustawienia:

   a. Wprowadź ścieżkę lokalną do punktu podłączenia dzielenia stanu.

   b. Wprowadź ścieżkę lokalną do punktu podłączenia dzielenia danych.

   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. Gdy pojawi się monit o podanie nazwy DNS serwera administracyjnego lub statycznego adresu IP, wprowadź adres IP dodatkowej karty sieciowej lub adres 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 urządzeń sieciowych, wpisz 1.
      - Jeśli masz od 101 do 1000 urządzeń sieciowych, wpisz 2.
      - Jeśli masz więcej niż 1000 urządzeń sieciowych, wpisz 3.

   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 głównego bazy danych, którego używasz do uzyskiwania dostępu do bazy danych.

p. Wprowadź hasło konta głównego bazy danych, którego używasz do uzyskiwania dostępu do bazy danych.

Poczekaj, aż usługi zostaną dodane i uruchomione automatycznie:

- klnagent_srv
- kladminserver_srv
- klactprx_srv
- klwebsrv_srv

q. 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 16 znaków.

Użytkownik zostanie dodany, a Kaspersky Security Center Linux zostanie zainstalowany na węźle podstawowym.

Instalacja na węźle dodatkowym (pasywnym)

W celu zainstalowania Kaspersky Security Center 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. W wierszu poleceń uruchom polecenia podane w tej instrukcji na koncie z uprawnieniami administratora.
3. Uruchom instalację Kaspersky Security Center Linux. W zależności od dystrybucji Linux uruchom jedno z następujących poleceń:
   - `sudo apt install /<path>/ksc64_[version_number]_amd64.deb`
   - `sudo yum install /<path>/ksc64-[version_number].x86_64.rpm -y`
4. Uruchom konfigurację Kaspersky Security Center Linux:

   ```
   sudo /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. Wpisz `n`, jeśli nie akceptujesz warunków umowy licencyjnej. Aby korzystać z Kaspersky Security Center Linux, musisz zaakceptować warunki umowy licencyjnej.

   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 **Dodatkowy węzeł klastra** jako tryb instalacji Serwera administracyjnego.

7. Po wyświetleniu monitu wprowadź ścieżkę lokalną do punktu montowania dzielenia stanu.

Kaspersky Security Center Linux jest zainstalowany na aktywnym węźle.

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`

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:

1. W aktywnym węźle przejdź do /opt/kaspersky/ksc64/sbin.

2. Otwórz wiersz polecenia, a następnie uruchom jedno z następujących poleceń:

   - Aby zatrzymać klaster, uruchom: `klfoc -stopcluster --stp klfoc`
   - Aby uruchomić klaster, uruchom: `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`.

Węzeł jest utrzymywany i dołączany do klastra trybu failover.

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 (na przykład SQL Server Management Studio) 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.

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.

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.

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.

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 KSCAdmin i podaj hasło dla KSCAdmin */
   CREATE USER 'KSCAdmin' 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 'KSCAdmin'@'%' IDENTIFIED WITH mysql_native_password BY '<password>';
     ```

   - Aby zmienić uwierzytelnianie dla istniejącego konta DBMS, wykonaj następujące polecenie:

     ```
     ALTER USER 'KSCAdmin'@'%' IDENTIFIED WITH mysql_native_password BY '<password>';
     ```

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 przechowywana sys.table_exists: EXECUTE
   - Globalne uprawnienia dla wszystkich schematów: PROCESS, SUPER

   Aby nadać wymagane uprawnienia utworzonemu kontu DBMS, uruchom następujący skrypt:

   ```
   /* Przyznaj uprawnienia KSCAdmin */
   ```

```
GRANT USAGE ON *.* TO 'KSCAdmin';
GRANT ALL ON kav.* TO 'KSCAdmin';
GRANT SELECT, SHOW VIEW ON mysql.* TO 'KSCAdmin';
GRANT SELECT, SHOW VIEW ON sys.* TO 'KSCAdmin';
GRANT EXECUTE ON PROCEDURE sys.table_exists TO 'KSCAdmin';
GRANT PROCESS ON *.* TO 'KSCAdmin';
GRANT SUPER ON *.* TO 'KSCAdmin';
```

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 'KSCAdmin'.`

4. Aby wyświetlić listę uprawnień nadanych kontu DBMS, wykonaj następującą komendę:

```
SHOW grants for 'KSCAdmin';
```

5. Aby utworzyć bazę danych Serwera administracyjnego, uruchom następujący skrypt (w tym skrypcie nazwa bazy danych Serwera administracyjnego to *kav*):

```
CREATE DATABASE kav
DEFAULT CHARACTER SET utf8
DEFAULT COLLATE utf8_general_ci;
```

Użyj tej samej nazwy bazy danych co określona w skrypcie tworzącym konto DBMS.

6. 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.

Konfigurowanie konta DBMS do instalacji Serwera administracyjnego (automatyczne tworzenie bazy danych Serwera administracyjnego)

W celu skonfigurowania konta DBMS instalacji Serwera administracyjnego:

1. Uruchom środowisko do pracy z PostgreSQL i Postgres Pro.
2. Wybierz rolę Postgres, aby uzyskać dostęp do DBMS. Możesz wybrać jedną z następujących opcji:
   - Użytkownik *postgres* (domyślna rola Postgres).

Jeśli używasz użytkownika *postgres*, nie musisz nadawać mu dodatkowych uprawnień.

Domyślnie użytkownik *postgres* nie ma hasła. Jednak do zainstalowania Kaspersky Security Center Linux wymagane jest hasło. Aby ustawić hasło dla użytkownika *postgres*, uruchom następujący skrypt:

```
ALTER USER user_name WITH PASSWORD '<password>';
```

- Nowa rola Postgres.

  Jeśli chcesz użyć nowej roli Postgres, utwórz tę rolę, a następnie nadaj jej uprawnienie CREATEDB. W tym celu uruchom następujący skrypt (w tym skrypcie rolą jest *KCSAdmin*):

  ```
  CREATE USER "KSCAdmin" WITH PASSWORD '<password>' CREATEDB;
  ```

  Utworzona rola będzie używana jako właściciel bazy danych Serwera administracyjnego (zwanej dalej również Bazą danych Serwera).

3. Zainstaluj Serwera administracyjnego.

Po zakończeniu instalacji baza danych Serwera jest tworzona automatycznie i Serwer administracyjny jest gotowy do użycia.

Konfigurowanie konta DBMS do instalacji Serwera administracyjnego (ręczne tworzenie bazy danych Serwera administracyjnego)

W celu skonfigurowania konta DBMS instalacji Serwera administracyjnego:

1. Uruchom środowisko do pracy z Postgres.

2. Utwórz nową rolę Postgres i bazę danych Serwera administracyjnego. Następnie nadaj roli wszystkie uprawnienia w bazie danych Serwera administracyjnego. W tym celu zaloguj się jako użytkownik *postgres* w bazie danych *postgres* i uruchom następujący skrypt (w tym skrypcie rola to *KCSAdmin*, nazwa bazy danych Serwera administracyjnego to *KAV*):

   ```
   CREATE USER "KSCAdmin" WITH PASSWORD '<password>';
   CREATE DATABASE "KAV" ENCODING 'UTF8' OWNER "KSCAdmin";
   GRANT ALL PRIVILEGES ON DATABASE "KAV" TO "KSCAdmin";
   ```

   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 "KSCAdmin" TEMPLATE template0;`
   zamiast:
   `CREATE DATABASE "KAV" ENCODING 'UTF8' OWNER "KSCAdmin";`

3. Nadaj następujące uprawnienia utworzonej roli Postgres:

   - Uprawnienia do wszystkich tabel w schemacie publicznym: ALL
   - Uprawnienia do wszystkich sekwencji w schemacie publicznym: ALL

   W tym celu zaloguj się jako użytkownik *postgres* w bazie danych Serwera i uruchom następujący skrypt (w tym skrypcie rola to *KCSAdmin*):

   ```
   GRANT ALL PRIVILEGES ON ALL TABLES IN SCHEMA "public" TO "KSCAdmin";
   GRANT ALL PRIVILEGES ON ALL SEQUENCES IN SCHEMA "public" TO "KSCAdmin";
   ```

4. Zainstaluj Serwera administracyjnego.

Po zakończeniu instalacji Serwer administracyjny użyje utworzonej bazy danych do przechowywania danych Serwera administracyjnego. Serwer administracyjny jest gotowy do użycia.

Certyfikaty do pracy z Kaspersky Security Center Linux

Ta sekcja zawiera informacje o certyfikatach Kapsersky 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 serwera sieciowego
- Certyfikat Kaspersky Security Center Web Console

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. 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

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 podczas łączenia się z Kaspersky Security Center Web Console
- Bezpieczna interakcja pomiędzy Serwerem administracyjnym a Agentem sieciowym na zarządzanych urządzeniach
- Uwierzytelnianie, gdy główne Serwery administracyjne są połączone z dodatkowymi 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.

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.

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.

Certyfikat serwera sieciowego

Specjalny typ certyfikatu jest używany przez serwer sieciowy, komponent Serwer administracyjny Kaspersky Security Center. Ten certyfikat jest wymagany do publikowania pakietów instalacyjnych Agenta sieciowego, które są następnie pobierane na zarządzane urządzenia. W tym celu serwer sieciowy może użyć różnych certyfikatów.

Serwer sieci Web używa jednego z następujących certyfikatów, w kolejności priorytetu:

1. Niestandardowy certyfikat serwera sieciowego, który określono ręcznie za pomocą Kaspersky Security Center Web Console

2. 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.

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: • Urząd certyfikacji (CA): prawda • Ograniczenie długości ścieżki: brak Użycie klucza: • Podpis cyfrowy • Podpisywanie certyfikatów • Szyfrowanie kluczy • Podpisywanie CRL Rozszerzone użycie klucza (opcjonalnie): uwierzytelnianie serwera, uwierzytelnianie klienta.	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.	Nienadająca się do zastosowania.

	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	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. 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.

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. Utwórz nowy plik odpowiedzi wymagany do instalacji Kaspersky Security Center Web Console.
2. W tym pliku określ ścieżki do niestandardowego pliku certyfikatu i pliku kluczy, używając parametru `certPath` i parametru `keyPath`.
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 <filename.pfx> -clcerts -nokeys | sed -ne '/-BEGIN CERTIFICATE-/,/-END CERTIFICATE-/p' > server.crt
   ```

   ```
   openssl pkcs12 -in <filename.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

Nowy certyfikat musi być utworzony w formacie PKCS#12 (na przykład, za pomocą PKI organizacji) i musi być wystawiony przez zaufany urząd certyfikacji (CA). Ponadto nowy certyfikat musi zawierać cały łańcuch zaufania oraz klucz prywatny, który musi być przechowywany w pliku z rozszerzeniem pfx lub p12. W przypadku nowego certyfikatu należy spełnić wymagania wymienione poniżej.

Typ Certyfikatu: Certyfikat standardowy, standardowy certyfikat zapasowy („C", „CR")

Wymagania:

- Minimalna długość klucza: 2048.
- Podstawowe ograniczenia:
  - Urząd certyfikacji (CA): prawda
  - 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 kluczy
  - 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.

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.

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

W celu zastąpienia certyfikatu Serwera administracyjnego:

W wierszu polecenia uruchom następujące narzędzie:

```
klsetsrvcert [-t <typ> {-i <plikwejściowy> [-p <hasło>] [-o <chkopt>] | -g <nazwadns>}]
[-f <czas>][-r <calistfile>][-l <plikraportu>]
```

Nie ma konieczności pobierania narzędzia klsetsrvcert. To narzędzie znajduje się w pakiecie dystrybucyjnym Kaspersky Security Center Linux. Nie jest kompatybilne z poprzednimi wersjami Kaspersky Security Center Linux.

Opis parametrów narzędzia klsetsrvcert przedstawia poniższa tabela.

Wartości parametrów narzędzia klsetsrvcert

Parametr	Wartość
`-t <type>`	Typ zastępowanego certyfikatu. Możliwe wartości parametru `<type>` to: • `C` – zastępuje certyfikat standardowy dla portów 13000 i 13291. • `CR` – zastępuje zapasowy certyfikat standardowy dla portów 13000 i 13291.
`-f <time>`	Terminarz zmiany certyfikatu w formacie „DD-MM-RRRR gg:mm" (dla portów: 13000 i 13291). Użyj tego parametru, jeśli chcesz zastąpić standardowy lub standardowy certyfikat zapasowy przed jego wygaśnięciem. Określ czas, w którym zarządzane urządzenia muszą synchronizować się z Serwerem administracyjnym na nowym certyfikacie.

`-i <inputfile>`	Kontener z certyfikatem i kluczem prywatnym w formacie PKCS#12 (plik z rozszerzeniem .p12 lub .pfx).
`-p <password>`	Hasło używane do ochrony kontenera p12. Certyfikat i klucz prywatny są przechowywane w kontenerze, dlatego do odszyfrowania pliku z kontenerem wymagane jest hasło.
`-o <chkopt>`	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.
`-g <dnsname>`	Nowy certyfikat zostanie utworzony dla określonej nazwy DNS.
`-r <calistfile>`	Lista zaufanych urzędów certyfikacji w formacie PEM.
`-l <logfile>`	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 <plikwejściowy> -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:

```
klsetsrvcert -f "DD-MM-RRRR gg:mm" -t CR -i <plik wejściowy> -p <hasło> -o NoCA
```

gdzie „`DD-MM-RRRR gg:mm`” to data 3–4 tygodnie przed datą bieżącą. Przesunięcie czasowe zmiany certyfikatu na zapasowy pozwoli na rozesłanie nowego certyfikatu do wszystkich Agentów sieciowych.

Podłączanie Agentów sieciowych do Serwera administracyjnego przy użyciu narzędzia klmover

Po zastąpieniu certyfikatu Serwera administracyjnego za pomocą polecenia narzędzia klsetsrvcert, musisz nawiązać połączenie SSL między Agentami sieciowymi a Serwerem administracyjnym, ponieważ połączenie jest zerwane.

W celu określenia nowego certyfikatu Serwera administracyjnego i przywrócenia połączenia:

W wierszu polecenia uruchom następujące narzędzie:

```
klmover [-address <server address>] [-pn <port number>] [-ps <SSL port number>] [-
nossl] [-cert <path to certificate file>]
```

To narzędzie jest automatycznie kopiowane do folderu instalacyjnego Agenta sieciowego, gdy Agent sieciowy jest instalowany na urządzeniu klienckim.

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 profilu Agenta sieciowego.

Narzędzie klmover wymaga uprawnień administratora lokalnego. Zabezpieczenie hasłem do uruchomienia narzędzia klmover można pominąć w przypadku urządzeń obsługiwanych bez uprawnień administratora lokalnego.

Włączenie opcji **Użyj hasła dezinstalacyjnego** umożliwia również ochronę hasłem narzędzia do usuwania dla Kaspersky Security Center Web Console (cleaner.exe).

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 parametr 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.

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 instalacji 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.

W celu zalogowania się do Kaspersky Security Center Web Console:

1. W swojej przeglądarce przejdź do <Adres internetowy Serwera administracyjnego>:<Numer portu>.

   Zostanie wyświetlona strona logowania.

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 jest zablokowana.

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 opcję **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**.

Po zalogowaniu zostanie wyświetlony pulpit nawigacyjny zawierający język i motyw, których ostatnio używano. 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 menu głównym przejdź do ustawień konta, a następnie wybierz **Wyloguj się**.

Konsola Kaspersky Security Center Web Console zostanie zamknięta i zostanie wyświetlona strona logowania.

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.

Konfigurowanie serwera MySQL x64 do pracy z Kaspersky Security Center Linux

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.ini:
```
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= the real value must be no less than 80% of the expected KAV
database size
innodb_thread_concurrency=20
innodb_flush_log_at_trx_commit=0 ( in most cases, the server uses small transactions )
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.

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 (w celu zapewnienia poprawnego działania opcji dostarczania powiadomień, na Serwerze administracyjnym i wszystkich urządzeniach, na które mają być wysyłane powiadomienia, powinna być włączona usługa Posłaniec).
- Utworzyć zasadę ochrony dla stacji roboczych i serwerów, a także zadania skanowania w poszukiwaniu złośliwego oprogramowania, zadania pobierania uaktualnień i zadania tworzenia kopii zapasowej danych dla najwyższego poziomu hierarchii zarządzanych urządzeń.

  Kreator wstępnej konfiguracji tworzy zasady tylko dla tych aplikacji, dla których folder **Zarządzane 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 aplikacji kliknij ikonę ustawienia ( ) obok nazwy żądanego Serwera administracyjnego.

   Zostanie otwarte okno właściwości Serwera administracyjnego.

2. Na zakładce **Ogólne** wybierz sekcję **Ogólne**.
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:

- **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.

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. 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.

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. 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. Zapoznaj się z treścią wyświetlonej Umowy licencyjnej, zaznacz pole **Zgadzam się na korzystanie z Kaspersky Security Network** i kliknij przycisk **Zainstaluj**. Jeśli nie akceptujesz warunków Umowy licencyjnej, 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.

Aby zakończyć pobieranie niektórych pakietów dystrybucyjnych, należy zaakceptować Umowę licencyjną. Jeśli klikniesz przycisk **Zaakceptuj**, zostanie wyświetlona treść Umowy licencyjnej. Aby przejść do kolejnego kroku kreatora, należy zaakceptować warunki i postanowienia Umowy licencyjnej oraz warunki i postanowienia Polityki prywatności Kaspersky. Jeśli nie akceptujesz warunków i postanowień, pobieranie pakietu zostanie anulowane.

Po zaakceptowaniu warunków i postanowień Umowy licencyjnej 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. 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 Kaspersky**.

- **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 Kaspersky**.

- Odraczając aktywację 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. 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.

Krok 10. 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 profili aplikacji.

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 11. Zamykanie kreatora wstępnej konfiguracji

Aby zamknąć kreator, kliknij przycisk **Zakończ**.

Po zakończeniu działania kreatora szybkiego startu 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: **Wykrywanie i wdrażanie** → **Wdrażanie i przypisywanie** → **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.

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 1. 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.

Krok 2. 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.

Krok 3. Wybieranie wersji Agenta sieciowego

Jeśli wybrałeś pakiet instalacyjny aplikacji innej niż Agent sieciowy, musisz także zainstalować Agenta sieciowego, który łączy aplikację z Serwerem administracyjnym Kaspersky Security Center.

Wybierz najnowszą wersję Agenta sieciowego.

Krok 4. 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.

Krok 5. 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.

Krok 6. 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 7. 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.

Krok 8. Wybieranie konta 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, aby zainstalować aplikację.

Aby określić konto użytkownika, z poziomu którego zostanie uruchomiony instalator aplikacji, kliknij przycisk **Dodaj**, wybierz **Konto lokalne**, a następnie określ poświadczenia konta użytkownika.

Możesz określić kilka kont użytkowników, na przykład, jeśli żadne z nich nie ma wszystkich wymaganych uprawnień na wszystkich urządzeniach, dla których definiujesz zadanie. W tym przypadku wszystkie dodane konta są używane do uruchomienia zadania, zaczynając od góry.

Krok 9. 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 15 na urządzeniu, na którym jest zainstalowana wcześniejsza wersja Serwera administracyjnego (począwszy od wersji 13). Podczas aktualizowania do wersji 15 wszystkie dane i ustawienia z poprzedniej wersji Serwera administracyjnego zostają zachowane.

Podczas aktualizacji równoczesne korzystanie z DBMS przez Serwer administracyjny i inną aplikację jest surowo zabronione.

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

Jeżeli Twoja sieć zawiera kilka Serwerów administracyjnych, musisz zaktualizować każdy Serwer ręcznie. Kaspersky Security Center Linux nie obsługuje scentralizowanej aktualizacji.

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 przy użyciu pliku instalacyjnego

Aby zaktualizować Serwer administracyjny z poprzedniej wersji (począwszy od wersji 13) do wersji 15, możesz zainstalować nową wersję na wcześniejszej przy użyciu pliku instalacyjnego Kaspersky Security Center Linux.

W celu uaktualnienia wcześniejszej wersji Serwera administracyjnego do wersji 15 przy użyciu pliku instalacyjnego:

1. Pobierz plik instalacyjny Kaspersky Security Center Linux z pełnym pakietem dla wersji 15 ze strony internetowej Kaspersky:
   - Dla urządzeń z systemem operacyjnym opartym na RPM — ksc64-<numer wersji>-11247.x86_64.rpm
   - Dla urządzeń z systemem operacyjnym opartym na Debian — ksc64_<numer wersji>-11247_amd64.deb
2. Uaktualnij pakiet instalacyjny za pomocą menedżera pakietów, którego używasz na swoim Serwerze administracyjnym. Na przykład możesz użyć następujących poleceń w terminalu wiersza poleceń na koncie z uprawnieniami roota:
   - W przypadku urządzeń z systemem operacyjnym opartym na RPM:
     ```
     $ sudo rpm -Uvh --nodeps --force ksc64-<numer wersji>-11247.x86_64.rpm
     ```
   - Dla urządzeń z systemem operacyjnym opartym na systemie Debian:
     ```
     $ sudo dpkg -i ksc64_<numer wersji>-11247_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.

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 EULA.

   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 EULA 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. 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.

Aktualizacja Kaspersky Security Center Linux poprzez kopię zapasową

Aby zaktualizować Serwer administracyjny z poprzedniej wersji (począwszy od wersji 13) do wersji 15, możesz utworzyć kopię zapasową danych Serwera administracyjnego i przywrócić te dane po zainstalowaniu Kaspersky Security Center Linux nowej wersji. 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.

W celu zaktualizowania wcześniejszej wersji Serwera administracyjnego do wersji 15:

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 15 na poprzednim Serwerze administracyjnym.

4. Przywróć dane Serwera administracyjnego z kopii zapasowej utworzonej przed aktualizacją.

5. 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.

Aktualizowanie Kaspersky Security Center Linux na węzłach klastra trybu failover Kaspersky Security Center Linux

Możesz zainstalować Serwer administracyjny w wersji 15 na każdym węźle klastra typu failover Kaspersky Security Center Linux, na którym zainstalowany jest Serwer administracyjny we wcześniejszej wersji (począwszy od wersji 14). Podczas aktualizowania do wersji 15 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 na węzłach klastra trybu failover Kaspersky Security Center Linux:

1. Pobierz plik instalacyjny Kaspersky Security Center Linux z pełnym pakietem dla wersji 15 ze strony internetowej Kaspersky:

   - Dla urządzeń z systemem operacyjnym opartym na RPM — ksc64-<version number>-<build number>.x86_64.rpm

   - Dla urządzeń z systemem operacyjnym opartym na Debian — ksc64_<version number>-<build number>_amd64.deb

2. Zatrzymaj klaster.

3. Na aktywnym węźle klastra zaktualizuj pakiet instalacyjny przy użyciu menedżera pakietów używanego na serwerze administracyjnym.

   Na przykład możesz użyć następujących poleceń w terminalu wiersza poleceń na koncie z uprawnieniami roota:

   - W przypadku urządzeń z systemem operacyjnym opartym na RPM:
     ```
     $ sudo rpm -Uvh --nodeps --force ksc64-<version number>-<build number>.x86_64.rpm
     ```

   - Dla urządzeń z systemem operacyjnym opartym na systemie Debian:
     ```
     $ sudo dpkg -i 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.

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 EULA.

   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.

```
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 EULA 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.

   > Pamiętaj, że możesz uruchomić klaster na dowolnym węźle. Jeśli uruchomisz klaster w węźle pasywnym, stanie się on węzłem aktywnym.

   W rezultacie zainstalowałeś Serwer administracyjny najnowszej wersji na węzłach klastra typu failover Kaspersky Security Center Linux.

Migracja do Kaspersky Security Center Linux

Postępując zgodnie z tym scenariuszem, możesz przenieść strukturę grupy administracyjnej, dołączone zarządzane urządzenia i inne obiekty grupowe (profile, zadania, zadania globalne, znaczniki i wybór urządzeń) z Kaspersky Security Center Windows w ramach zarządzania Kaspersky Security Center Linux.

Ograniczenia:

- Migracja jest możliwa tylko z Kaspersky Security Center 14.2 Windows do Kaspersky Security Center 15.0 Linux.
- 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. **Eksportowanie danych z Kaspersky Security Center Windows**

   Otwórz Kaspersky Security Center Windows, a następnie uruchom Kreatora migracji.

3. **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.

4. **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
- Przypisz i skonfiguruj punkty dystrybucji
- Skonfiguruj reguły przenoszenia urządzeń
- Skonfiguruj reguły automatycznego znakowania urządzeń
- Utwórz kategorie aplikacji

5. **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. W aktualnej wersji Kaspersky Security Center Linux możesz to zrobić jedną z następujących metod:

   - Za pomocą narzędzia klmover

     Użyj narzędzia klmover i określ ustawienia połączenia dla nowego Serwera administracyjnego.

   - Poprzez instalację lub 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. Użyj pakietu instalacyjnego, aby zainstalować Agenta sieciowego na zaimportowanych zarządzanych urządzeniach poprzez zadanie zdalnej instalacji. Aby uzyskać więcej informacji, zobacz punkt Przełączanie zarządzanych urządzeń na zarządzane przez Kaspersky Security Center Linux.

     Można także utworzyć autonomiczny pakiet instalacyjny i używać go do lokalnej instalacji Agenta sieciowego.

6. **Zaktualizuj Agenta sieciowego do najnowszej wersji**

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

7. **Upewnij się, że zarządzane urządzenia są widoczne na nowym Serwerze administracyjnym**

   Na Serwerze administracyjnym Kaspersky Security Center Linux otwórz listę zarządzanych urządzeń (**Zasoby (urządzenia)** → **Zarządzane 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 profili i zadań:

- Wyeksportuj zadania z Kaspersky Security Center Windows, a następnie zaimportuj zadania do Kaspersky Security Center Linux.
- Wyeksportuj określone profile z Kaspersky Security Center Windows, a następnie zaimportuj profile do Kaspersky Security Center Linux. Powiązane profile zasad są eksportowane i importowane razem z wybranymi politykami.

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 for Linux lub platformy Kaspersky 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 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 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, profile, 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.

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 **Zasoby (urządzenia)** 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.

W aktualnej wersji Kaspersky Security Center Linux możesz przenieść zarządzane urządzenia do Kaspersky Security Center Linux przy użyciu narzędzia klmover lub instalując Agenta sieciowego na zarządzanych urządzeniach poprzez zadanie zdalnej instalacji.

W celu przełączenia zarządzanych urządzeń, aby były zarządzane przez Kaspersky Security Center Linux poprzez zainstalowanie Agenta sieciowego:

1. Przełącz się na Serwer administracyjny Kaspersky Security Center Windows.

2. Przejdź do opcji **Wykrywanie i wdrażanie** → **Wdrażanie i przypisywanie** → **Pakiety instalacyjne**, a następnie otwórz właściwości istniejącego pakietu instalacyjnego Agenta sieciowego.

   Jeżeli na liście pakietów nie ma pakietu instalacyjnego Agenta sieciowego, pobierz nowy.

3. Na karcie **Ustawienia** wybierz sekcję **Połączenie**. Określ ustawienia połączenia Serwera administracyjnego Kaspersky Security Center Linux.

4. 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**.

5. 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

Ta sekcja opisuje proces konfiguracji i właściwości Serwera administracyjnego Kaspersky Security Center.

Konfigurowanie połączenia Kaspersky Security Center Web Console z Serwerem administracyjnym

W celu określenia portów połączenia Serwera administracyjnego:

1. W menu aplikacji kliknij ikonę ustawienia ( ) obok nazwy żądanego Serwera administracyjnego.

   Zostanie otwarte okno właściwości Serwera administracyjnego.

2. Na zakładce **Ogólne** wybierz sekcję **Porty połączenia**.

Aplikacja wyświetli główne ustawienia połączenia wybranego serwera.

Konfigurowanie listy dozwolonych adresów IP do logowania się do Kaspersky Security Center Linux

Domyślnie użytkownicy mogą logować się do Kaspersky Security Center Linux na dowolnym urządzeniu, na którym można otworzyć Kaspersky Security Center Web Console. Możesz jednak skonfigurować serwer administracyjny tak, aby użytkownicy mogli łączyć się z nim tylko z urządzeń o dozwolonych adresach IP. W takim przypadku, nawet jeśli intruz ukradnie konto Kaspersky Security Center Linux, nie będzie mógł zalogować się do Kaspersky Security Center Linux, ponieważ adres IP urządzenia intruza nie znajduje się na liście zezwolonych.

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 urządzenie użytkownika próbuje nawiązać połączenie z Serwerem administracyjnym. Jeśli adresu IP urządzenia nie ma na liście dozwolonych, wystąpi błąd uwierzytelniania, a zdarzenie KLAUD_EV_SERVERCONNECT powiadamia, że połączenie z serwerem administracyjnym nie zostało nawiązane.

Wymagania dotyczące listy dozwolonych 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 serwer 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 serwer 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 dozwolonych adresów IP

Jeśli wcześniej nie ustawiono listy dozwolonych, postępuj zgodnie z poniższymi instrukcjami.

W celu ustanowienia listy dozwolonych 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 dozwolonych adresów IP w dzienniku zdarzeń Syslog na serwerze administracyjnym.

Jak zmienić listę dozwolonych adresów IP

Listę dozwolonych adresów można zmienić tak samo, jak podczas jej tworzenia. W tym celu uruchom to samo polecenie i określ nową listę dozwolonych 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 dozwolonych, przepisz je. Na przykład, lista dozwolonych 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 dozwolonych adresów IP

Aby zresetować już skonfigurowaną listę dozwolonych 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 aplikacji kliknij ikonę ustawień ( ) obok nazwy 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

     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 profile, zadania, role użytkowników i pakiety instalacyjne z podstawowego 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 dodatkowego 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.

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 do odbierania połączeń od podrzędnych Serwerów administracyjnych.

2. Na przyszłym głównym Serwerze administracyjnym kliknij ikonę ustawienia ( ).

3. W otwartym oknie właściwości przejdź na 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.

6. W pierwszym kroku kreatora 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.

   - **Port SSL Serwera administracyjnego**

     Określ numer portu SSL na głównym Serwerze administracyjnym. Domyślny numer portu to 13000.

   - **Port API Serwera administracyjnego**

     Określ numer portu na głównym Serwerze administracyjnym do odbierania połączeń poprzez OpenAPI. Domyślny numer portu to 13299.

   - **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, podstawowy Serwer administracyjny inicjuje połączenie z pomocniczym Serwerem administracyjnym. W przeciwnym razie pomocniczy Serwer administracyjny inicjuje połączenie z podstawowym 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**
- **Nazwa użytkownika**
- **Hasło**

7. Określ ustawienia połączenia:

   - Wprowadź adres przyszłego podstawowego Serwera administracyjnego.
   - Jeśli przyszły pomocniczy 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 pomocniczym Serwerze administracyjnym.

   Upewnij się, że weryfikacja dwuetapowa jest wyłączona dla określonego konta. Jeśli dla tego konta włączona jest weryfikacja dwuetapowa, możesz utworzyć hierarchię tylko z przyszłego serwera pomocniczego (zobacz instrukcje poniżej). To znany problem.

   Jeśli ustawienia połączenia są prawidłowe, nawiązywane jest połączenie z przyszłym serwerem pomocniczym i budowana jest hierarchia „primary/secondary". Jeśli połączenie nie powiodło się, sprawdź ustawienia połączenia lub ręcznie określ certyfikat przyszłego Serwera pomocniczego.

   Połączenie może się również nie powieść, ponieważ przyszły serwer pomocniczy jest uwierzytelniany za pomocą samopodpisanego certyfikatu, który został automatycznie wygenerowany przez Kaspersky Security Center Linux. W rezultacie przeglądarka może zablokować pobieranie automatycznie podpisanego certyfikatu. W takim przypadku 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.

   Po zakończeniu pracy kreatora zostanie utworzona hierarchia „główny/podrzędny". Połączenie między głównym i pomocniczym 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.

Dodawanie podrzędnego Serwera administracyjnego (wykonywane na przyszłym podrzędnym Serwerze administracyjnym)

Jeśli nie możesz połączyć się z przyszłym pomocniczym Serwerem administracyjnym (na przykład ponieważ był on tymczasowo odłączony lub niedostępny albo ponieważ plik certyfikatu dodatkowego Serwera administracyjnego jest samopodpisany), nadal możesz dodać dodatkowy 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 ikonę ustawienia ( ).

   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:

W oknie głównym aplikacji kliknij nazwę Serwera administracyjnego, która znajduje się obok ikony ustawienia ( ).

Zostanie wyświetlona lista rozwijana podrzędnych (w tym wirtualnych) Serwerów administracyjnych.

Możesz przejść do dowolnego z tych Serwerów administracyjnych, klikając jego nazwę.

Grupy administracyjne są także wyświetlane, ale są wyszarzone i nie są dostępne do zarządzania w tym menu.

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 dodatkowy 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.
  2. Uruchomi się Kreator konfiguracji.
  3. W pierwszym kroku kreatora wybierz opcję **Aktualizuj**.
  4. Na stronie **Typ modyfikacji** wybierz opcję **Edycja ustawień połączenia**.
  5. Na stronie **Zaufane serwery administracyjne** dodaj wymagany dodatkowy serwer administracyjny.
  6. W ostatnim kroku kreatora kliknij **Modyfikuj**, aby zastosować nowe ustawienia.
  7. 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.

W celu utworzenia i dodania wirtualnego Serwera administracyjnego:

1. W menu głównym kliknij ikonę ustawienia ( ) obok nazwy żądanego 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.

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 dodatkowy 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.

  2. Uruchomi się Kreator konfiguracji.

  3. W pierwszym kroku kreatora wybierz opcję **Aktualizuj**.

  4. Na stronie **Typ modyfikacji** wybierz opcję **Edycja ustawień połączenia**.

  5. Na stronie **Zaufane serwery administracyjne** dodaj wymagany dodatkowy serwer administracyjny.

  6. W ostatnim kroku kreatora kliknij **Modyfikuj**, aby zastosować nowe ustawienia.

  7. 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 aplikacji kliknij ikonę ustawienia ( ) obok nazwy żądanego 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 podstawowego 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 podstawowym 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. W menu głównym przejdź do wymaganego wirtualnego Serwera administracyjnego:

   a. Kliknij ikonę jodełki ( ) po prawej stronie bieżącej nazwy Serwera administracyjnego.

   b. Wybierz wymagany Serwer administracyjny.

2. W menu aplikacji kliknij ikonę ustawienia ( ) obok nazwy żądanego Serwera administracyjnego.

   Zostanie otwarte okno właściwości Serwera administracyjnego.

3. Na zakładce **Prawa dostępu** kliknij przycisk **Dodaj**.

   Zostanie otwarta ujednolicona lista użytkowników podstawowego 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.

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. W menu głównym przejdź do wymaganego wirtualnego Serwera administracyjnego:

   a. Kliknij ikonę jodełki ( ) po prawej stronie bieżącej nazwy Serwera administracyjnego.

b. Wybierz wymagany Serwer administracyjny.

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. Możesz przełączać zarządzanie urządzeniami pomiędzy następującymi Serwerami administracyjnymi:

- Główny Serwer administracyjny i jeden z jego wirtualnych Serwerów administracyjnych
- Dwa wirtualne Serwery administracyjne tego samego głównego Serwera administracyjnego

W celu zmiany Serwera administracyjnego zarządzającego urządzeniami klienckimi na inny Serwer:

1. W menu głównym przejdź do **Zasoby (urządzenia)** → **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 zadanie **Zmiana Serwera administracyjnego.**
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. Wybierz Serwer administracyjny, którego chcesz używać do zarządzania wybranymi urządzeniami.
7. 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 na stronie **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.

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.

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. W menu aplikacji kliknij ikonę ustawienia ( ) obok nazwy żądanego Serwera administracyjnego.

2. W otwartym oknie przejdź na zakładkę **Serwery administracyjne**.

3. Wybierz wirtualny Serwer administracyjny, który chcesz usunąć.

4. W wierszu menu kliknij **Usuń**.

Wirtualny Serwer administracyjny zostanie usunięty.

Przeglądanie raportów połączeń z Serwerem administracyjnym

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 ikonę ustawienia ( ) obok nazwy żądanego 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.

Aby ograniczyć liczbę zdarzeń, które mogą być przechowywane w repozytorium zdarzeń na Serwerze administracyjnym:

1. W menu aplikacji kliknij ikonę ustawienia ( ) obok nazwy żądanego 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**.

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.
- 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. 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.

3. Na nowym urządzeniu zainstaluj system DBMS, z którego będzie korzystał Serwer administracyjny.

   Kiedy wybierasz DBMS, weź pod uwagę liczbę urządzeń obsługiwanych przez Serwer administracyjny.

4. Zainstaluj Serwer administracyjny na wybranym urządzeniu.

   Zwróć uwagę, że jeśli przenosisz serwer bazy danych na nowe urządzenie, należy określić adres lokalny jako adres IP urządzenia, na którym zainstalowana jest baza danych (element „h" w instrukcji Instalowanie Kaspersky Security Center). Jeśli chcesz zachować serwer bazy danych na poprzednim urządzeniu, wprowadź adres IP poprzedniego urządzenia w pozycji „h" instrukcji Instalowanie Kaspersky Security Center Linux.

5. Po zakończeniu instalacji odzyskaj dane Serwera administracyjnego na nowym urządzeniu za pomocą narzędzia klbackup.

   > Jeśli używasz programu SQL Server jako DBMS na poprzednich i nowych urządzeniach, pamiętaj, że wersja programu SQL Server zainstalowana na nowym urządzeniu musi być taka sama lub nowsza niż wersja programu SQL Server zainstalowana na poprzednim urządzeniu. W przeciwnym razie nie będzie możliwe odzyskanie danych Serwera administracyjnego na nowym urządzeniu.

6. Otwórz Kaspersky Security Center Web Console i połącz się z Serwerem administracyjnym.

7. Sprawdź, czy wszystkie urządzenia klienckie są połączone z Serwerem administracyjnym.

8. Odinstaluj Serwer administracyjny i serwer bazy danych z poprzedniego urządzenia.

Zmiana poświadczeń DBMS

Czasami może zajść potrzeba zmiany poświadczeń DBMS, na przykład w celu wykonania rotacji poświadczeń ze względów bezpieczeństwa.

Aby zmienić poświadczenia DBMS w środowisku Linux za pomocą narzędzia klsrvconfig:

1. Uruchom wiersz poleceń systemu Linux.

2. Określ narzędzie klsrvconfig w otwartym oknie wiersza poleceń:

```
sudo /opt/kaspersky/ksc64/sbin/klsrvconfig -set_dbms_cred
```

3. Podaj nową nazwę konta. Powinieneś określić poświadczenia konta, które istnieje w DBMS.

4. Wpisz nowe hasło.

5. Podaj nowe hasło w celu potwierdzenia.

Poświadczenia DBMS zostały zmienione.

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.

Pamiętaj, że nie są tworzone kopie zapasowe zainstalowanych wtyczek do zarządzania. Po przywróceniu danych Serwera administracyjnego z kopii zapasowej należy pobrać i ponownie zainstalować wtyczki dla zarządzanych aplikacji.

Zanim utworzysz kopię zapasową danych Serwera administracyjnego, sprawdź, czy do grupy administracyjnej został dodany wirtualny Serwer administracyjny. 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.

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 (profile, 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.

Odzyskanie danych Serwera administracyjnego jest możliwe tylko przy użyciu narzędzia klbackup.

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 **Zasoby (urządzenia)** → **Zadania**.
2. Kliknij **Dodaj**.

   Zostanie uruchomiony Kreator tworzenia nowego zadania.
3. W pierwszym kroku kreatora, na liście **Aplikacja** wybierz **Kaspersky Security Center 15**, a na liście **Typ zadania** wybierz **Kopia zapasowa danych Serwera administracyjnego**.
4. W odpowiednim kroku kreatora określ następujące informacje:
   - Folder do przechowywania kopii zapasowych
   - Hasło do kopii zapasowej (opcjonalnie)
   - Maksymalna liczba kopii zapasowych do zapisania
5. Jeśli na stronie **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.

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 [-logfile PLIKRAPORTU] [-use_ts]|[-restore] [-password HASŁO] [-online]
```

> Jeśli w wierszu polecenia narzędzia klbackup nie określono hasła, narzędzie zażąda wprowadzenie hasła interaktywnie.

Opisy przełączników:

- `-path BACKUP_PATH`—zapisuje informacje w folderze ŚCIEŻKA_DOSTĘPU_DO_KOPII_ZAPASOWEJ lub używa danych z folderu ŚCIEŻKA_DOSTĘPU_DO_KOPII_ZAPASOWEJ do ich przywrócenia (wymagany parametr).

- `-logfile LOGFILE`—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 ŚCIEŻKA_DOSTĘPU_DO_KOPII_ZAPASOWEJ.

- `-use_ts`— Podczas zapisywania danych kopiuje informacje do folderu BACKUP_PATH, do podfolderu z nazwą zawierającą bieżącą datę systemową i czas działania w formacie `klbackup RRRR-MM-DD # GG-MM-SS`. Jeśli przełącznik nie został określony, informacje są zapisywane w głównym folderze ŚCIEŻKA_DOSTĘPU_DO_KOPII_ZAPASOWEJ.

  Podczas próby zapisu informacji do folderu, w którym już znajduje się kopia zapasowa, zostaje wyświetlona wiadomość o błędzie. Żadne informacje nie zostaną zaktualizowane.

  Dostępność przełącznika `-use_ts` pozwala zachować archiwum danych Serwera administracyjnego. Na przykład jeśli klucz `-path` wskazuje folder `C:\KLBackups`, wówczas folder `klbackup 2022/6/19 # 11-30-18` przechowuje informacje o stanie Serwera administracyjnego na dzień 19 czerwca 2022 roku, godzina 11:30:18.

- `-restore`—przywraca dane Serwera administracyjnego. Przywracanie danych odbywa się w oparciu o informacje znajdujące się w folderze ŚCIEŻKA_DOSTĘPU_DO_KOPII_ZAPASOWEJ. Jeśli żaden parametr nie jest dostępny, kopie zapasowe danych są tworzone w folderze ŚCIEŻKA_DOSTĘPU_DO_KOPII_ZAPASOWEJ.

- `-password PASSWORD`—zapisuje lub przywraca certyfikat Serwera administracyjnego; aby zaszyfrować lub odszyfrować certyfikat, użyj hasła określonego przez parametr HASŁO.

  > 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. Zalecamy uruchomienie narzędzia na nowo zainstalowanym Serwerze administracyjnym.

- `-online`—utwórz kopię zapasową danych Serwera administracyjnego, tworząc migawkę woluminu, aby zminimalizować czas offline Serwera administracyjnego. Jeśli używasz narzędzia do odzyskiwania danych, ta opcja jest ignorowana.

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:

- Sprawdza, czy w bazie danych znajdują się jakiekolwiek błędy.
- Reorganizuje indeksy w bazie danych.
- Aktualizuje statystyki bazy danych.
- Zmniejsza bazę danych (jeśli to konieczne).

Zadanie Konserwacja Serwera administracyjnego nie obsługuje systemu MariaDB. Jeśli ten system DBMS jest używany w Twojej sieci, administratorzy będą musieli samodzielnie utrzymywać MariaDB.

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 **Zasoby (urządzenia)** → **Zadania**.
2. Kliknij przycisk **Dodaj**.

   Zostanie uruchomiony Kreator tworzenia nowego zadania.
3. W oknie Kreatora **Nowe zadanie** 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 aplikacji kliknij ikonę ustawienia ( ) obok nazwy głównego 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 za pomocą narzędzia klscflag:

1. Uruchom wiersz poleceń, a następnie zmień bieżący katalog na inny za pomocą narzędzia 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 następującą komendę:

   ```
   klscflag -fset -pv ".core/.independent" -s Transport -n ForceUseSystemDNS -t d -v 1
   ```

3. Aby włączyć korzystanie z publicznego DNS, wpisz na koncie root następującą komendę:

   ```
   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 ustawień konta i wybierz **Opcje interfejsu**.
2. W otwartym oknie **Opcje interfejsu** włącz lub wyłącz opcję **Pokaż szyfrowanie i ochronę danych**.
3. Kliknij **Zapisz**.

Następnie w menu głównym pojawi się sekcja **Operacje** → **Szyfrowanie i ochrona danych**.

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 inny za pomocą narzędzia 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 wstecznej z Kaspersky Security Center 11). 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 inny za pomocą narzędzia 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
     <value> -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
<value> -t d
```

Określ parametr <wartość> flagi:

- `1` — aby włączyć obsługę protokołu TLS.
- `0` — aby wyłączyć obsługę protokołu TLS.

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 Kaspersky Security Center i jego podrzędnych Serwerów administracyjnych.
- Urządzenia nieprzypisane zarządzane przez Serwer administracyjny Kaspersky Security Center 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 profile. 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 szybkiego startu 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.

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 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.

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**.

2. Kliknij przycisk **Właściwości**.

   Zostanie otwarte okno 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.

- **Co miesiąc, w określone dni wybranych tygodni**

  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.

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**.
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.
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 przeszukiwania 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 kontrolera domeny Microsoft Active Directory i kontrolera domeny Samba. 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 przeszukiwaniem kontrolera domeny upewnij się, że włączone są następujące protokoły:

- Simple Authentication and Security Layer (SASL)
- Lightweight Directory Access Protocol (LDAP)

Upewnij się, że na urządzeniu kontrolera domeny są dostępne następujące porty:

- 389 dla SASL
- 636 dla TLS

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**.
2. Kliknij **Ustawienia przeszukiwania**.

   Zostanie otwarte okno **Ustawienia odpytywania sterowników domeny**.
3. Wybierz opcję **Włącz przeszukiwanie sterowników domeny** .
4. W polu **Przeszukaj określone domeny** kliknij przycisk **Dodaj**, a następnie określ adres i dane uwierzytelniające użytkownika kontrolera domeny.
5. Jeśli to konieczne, w oknie **Ustawienia odpytywania sterowników domeny** określ terminarz 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.

   - Co miesiąc, w określone dni wybranych tygodni

     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 systemu Linux obsługiwane jest przeszukiwanie kontrolera domeny Microsoft Active Directory i kontrolera domeny Samba.
W przypadku punktu dystrybucji systemu Windows obsługiwane jest tylko przeszukiwanie kontrolera domeny Microsoft Active Directory.
Przeszukiwanie za pomocą punktu dystrybucji komputera 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. Wybierz opcję **Włącz przeszukiwanie sterowników domeny**.

4. 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**

5. 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

Podczas początkowego połączenia z kontrolerem domeny Serwer administracyjny identyfikuje protokół połączenia. Protokół ten będzie używany do wszystkich przyszłych połączeń z kontrolerem domeny.

Początkowe połączenie z kontrolerem domeny przebiega w następujący sposób:

1. Serwer administracyjny próbuje połączyć się z kontrolerem domeny poprzez protokół TLS.

   Domyślnie weryfikacja certyfikatu nie jest wymagana. Ustaw flagę KLNAG_LDAP_TLS_REQCERT na 1, aby wymusić weryfikację certyfikatu.

   Domyślnie do uzyskania dostępu do łańcucha certyfikatów używana jest ścieżka zależna od systemu operacyjnego do urzędu certyfikacji (CA). Użyj flagi KLNAG_LDAP_SSL_CACERT, aby określić ścieżkę niestandardową.

2. Jeżeli połączenie TLS nie powiedzie się, Serwer administracyjny spróbuje połączyć się z kontrolerem domeny poprzez SASL (DIGEST-MD5).

3. Jeżeli połączenie SASL (DIGEST-MD5) nie powiedzie się, Serwer administracyjny używa prostego uwierzytelniania poprzez nieszyfrowane połączenie TCP, aby połączyć się z kontrolerem domeny.

Do konfigurowania flag można użyć narzędzia klscflag.

Uruchom wiersz poleceń, a następnie zmień bieżący katalog na inny za pomocą narzędzia klscflag. Narzędzie klscflag znajduje się w katalogu, w którym zainstalowany jest serwer administracyjny. Domyślna ścieżka instalacji to /opt/kaspersky/ksc64/sbin.
Na przykład następujące polecenie wymusza weryfikację certyfikatu:

```
klscflag -fset -pv klserver -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.

Jeśli chcesz poprawnie przeszukiwać kontroler domeny Samba, musisz określić parametry `nazwy netbios` i `grupy roboczej` w pliku /etc/samba/smb.conf.

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 **Wykrywanie i wdrażanie** → **Wdrażanie i przypisywanie** → **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 **Zasoby (urządzenia)** → **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**.

Wdrażanie praktycznego zastosowania aplikacji

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 — podstawowe narzędzie administratora. Możesz zainstalować Kaspersky Security Center Web Console również na tym samym urządzeniu, na którym jest zainstalowany Serwer administracyjny, lub na innym.
- Agent sieciowy—zaprojektowany do zarządzania aplikacją zabezpieczającą, zainstalowaną na urządzeniu, a także do uzyskiwania informacji o tym urządzeniu i przesyłania tych informacji na Serwer administracyjny. Agenty sieciowe są instalowane na urządzeniach w organizacji.

Instalacja Kaspersky Security Center Linux w sieci organizacji odbywa się w następujący sposób:

- Instalacja Serwera administracyjnego
- Instalacja Kaspersky Security Center Web Console na urządzeniu administratora
- Instalacja Agenta sieciowego i aplikacji zabezpieczającej na urządzeniach w firmie

Przewodnik zwiększania bezpieczeństwa

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.

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

Przewodnik zwiększania bezpieczeństwa 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

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 instalacji 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 polityki bezpieczeństwa 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.

Konfigurowanie listy dozwolonych adresów IP do łączenia się z Serwerem administracyjnym

Domyślnie użytkownicy mogą logować się do Kaspersky Security Center Linux z dowolnego urządzenia, na którym zainstalowana jest konsola Kaspersky Security Center Web Console. Możesz skonfigurować serwer administracyjny tak, aby użytkownicy mogli łączyć się z nim tylko z urządzeń o dozwolonych adresach IP.

Konta i uwierzytelnianie

Używanie weryfikacji dwuetapowej z Serwerem administracyjnym

Kaspersky Security Center Linux zapewnia weryfikację dwuetapową dla użytkowników Kaspersky Security Center Web Console w oparciu o standard RFC 6238 (TOTP: algorytm jednorazowych haseł czasowych).

Jeśli weryfikacja dwuetapowa jest włączona dla Twojego konta, za każdym razem, gdy logujesz się do Kaspersky Security Center Web Console, wprowadzasz swoją nazwę użytkownika, hasło i dodatkowy jednorazowy kod zabezpieczający. Aby otrzymać jednorazowy kod zabezpieczający, 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.

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

Zalecamy używanie uwierzytelniania wieloskładnikowego (MFA) do uwierzytelniania na urządzeniu Serwera administracyjnego przy użyciu tokena, karty inteligentnej lub innej metody (jeśli to możliwe).

Zakaz 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 16 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.

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 przypisana jest rola głównego administratora na liście kontroli dostępu (ACL) 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

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

Zarządzanie ochroną Serwera administracyjnego

Wybieranie oprogramowania zabezpieczającego Serwer administracyjny

W zależności od typu instalacji 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 polityki bezpieczeństwa dla aplikacji zabezpieczającej

Zalecamy utworzenie oddzielnej zasady bezpieczeństwa dla aplikacji chroniącej urządzenie Serwera administracyjnego. Ta zasada musi różnić się od zasady bezpieczeństwa 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 politykę bezpieczeństwa.

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.

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, Agent sieciowy 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. Podczas instalacji Agenta sieciowego na urządzeniach klienckich narzędzie jest automatycznie kopiowane do folderu 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 profilu Agenta sieciowego.

Narzędzie klmover wymaga uprawnień administratora lokalnego. Zabezpieczenie hasłem do uruchomienia narzędzia klmover można pominąć w przypadku urządzeń obsługiwanych bez uprawnień administratora lokalnego.

Włączenie opcji **Użyj hasła dezinstalacyjnego** umożliwia również ochronę hasłem narzędzia do usuwania dla Kaspersky Security Center Web Console (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 polityki 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:

- Sprawdza, czy w bazie danych znajdują się jakiekolwiek błędy
- 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.

Przygotowanie do zdalnej instalacji

Ta sekcja opisuje kroki, jakie należy podjąć przed zainstalowaniem Kaspersky Security Center Linux.

Planowanie instalacji Kaspersky Security Center Linux

Ta sekcja zawiera informacje o najbardziej odpowiednich opcjach instalacji 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

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 instalacji jest zalecana w sytuacjach, gdy zdalna instalacja nie jest możliwa.

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

Informacje dotyczące planowania instalacji Kaspersky Security Center Linux w sieci organizacji

Jeden Serwer administracyjny może obsługiwać maksymalnie 20 000 urządzeń (z MariaDB jako DBMS). Jeśli całkowita liczba urządzeń w sieci organizacji przekroczy 20 000, 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 sekcja „Standardowa konfiguracja: Duże oddziały posiadające swoich 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 uaktualnienia zarówno z Serwera administracyjnego (domyślny scenariusz) oraz z serwerów Kaspersky dostępnych w Internecie (patrz sekcja „Standardowa konfiguracja: Małe zdalne biura”).

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 instalacji 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
- Określenia wymaganych wartości w polach certyfikatu
- Zapewnienia wymaganej siły szyfrowania certyfikatu

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 profili 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.

Standardowa konfiguracja 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 20 000 urządzeń (z MariaDB 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 profili 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. Należy zwrócić uwagę, że profile połączeń Agenta sieciowego są obsługiwane tylko dla hostów Windows i macOS.

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 temacie: Włączanie serwera push.

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.

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

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. Jeśli wymagane jest zarządzanie urządzeniami mobilnymi, możesz udostępnić port 13292 TCP.

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 wstępnej instalacji 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 instalacji przy użyciu zasad grupy systemu Microsoft Windows.

Możesz skorzystać z punktów dystrybucji zlokalizowanych w sieci organizacji. Aby przeprowadzić wstępną instalację 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).

Dostęp do internetu: Agent sieciowy jako brama połączenia w strefie zdemilitaryzowanej

Serwer administracyjny może znajdować się w wewnętrznej sieci organizacji, w strefie zdemilitaryzowanej (DMZ), gdzie może być urządzenie z Agentem sieciowym działającym jako brama połączenia z odwróconym połączeniem (Serwer administracyjny nawiązuje połączenie z Agentem sieciowym). W tym przypadku, w celu zapewnienia dostępu do Internetu muszą zostać spełnione następujące warunki:

- Agent sieciowy musi być zainstalowany na urządzeniu, które znajduje się w DMZ. Jeśli instalujesz Agenta sieciowego, w oknie **Brama połączenia** kreatora instalacji wybierz **Użyj Agenta sieciowego jako bramy połączenia w DMZ**.
- Urządzenie z zainstalowaną bramą połączenia musi zostać dodane do punktu dystrybucji. Po dodaniu bramy połączeniu, w oknie **Dodaj punkt dystrybucji** wybierz opcję **Wybierz** → **Dodaj bramę połączenia w DMZ na podstawie adresu**.
- Aby używać połączenia internetowego do podłączania zewnętrznych komputerów stacjonarnych z Serwerem administracyjnym, należy poprawić pakiet instalacyjny Agenta sieciowego. We właściwościach utworzonego pakietu instalacyjnego wybierz opcję **Zaawansowane** → **Połącz z Serwerem administracyjnym korzystając z bramy połączenia**, a następnie określ nowo utworzoną bramę połączenia.

Dla bramy połączenia w strefie DMZ Serwer administracyjny tworzy certyfikat podpisany przez certyfikat Serwera administracyjnego. Jeśli administrator zdecyduje przydzielić Serwerowi administracyjnemu certyfikat niestandardowy, musi to zrobić przed utworzeniem bramy połączenia w strefie DMZ.

Jeśli niektórzy pracownicy korzystają z laptopów, które mogą łączyć się z Serwerem administracyjnym z sieci lokalnej lub poprzez Internet, przydatne będzie utworzenie w zasadzie Agenta sieciowego reguły przełączania dla Agenta sieciowego.

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.

Instalacja 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 wstępnej konfiguracji
- 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.

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.

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.

Ustawienia sieciowe dotyczące interakcji z usługami zewnętrznymi

Kaspersky Security Center Linux używa następujących ustawień sieciowych do interakcji z usługami zewnętrznymi.

Ustawienia sieci

Ustawienia sieci	Address	Opis
Port: 443 Protokół: HTTPS	aktywacja-v2.kaspersky.com/activationservice/activationservice.svc	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.
Port: 80 Protokół: HTTP	http://p00.upd.kaspersky.com http://p01.upd.kaspersky.com http://p02.upd.kaspersky.com http://p03.upd.kaspersky.com	Aktualizowanie baz danych, modułów i aplikacji Kaspersky.

	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	
Port: 443 Protokół: HTTPS	ds.kaspersky.com	Używanie Kaspersky Security Network.
Port: 443, 1443 Protokół: HTTPS	ksn-a-stat-geo.kaspersky-labs.com ksn-file-geo.kaspersky-labs.com ksn-verdict-geo.kaspersky-labs.com ksn-url-geo.kaspersky-labs.com ksn-a-p2p-geo.kaspersky-labs.com ksn-info-geo.kaspersky-labs.com ksn-cinfo-geo.kaspersky-labs.com	Używanie Kaspersky Security Network.
Protokół: HTTPS	click.kaspersky.com redirect.kaspersky.com	Klikanie odnośników z poziomu interfejsu.
Port: 80	http://crl.kaspersky.com http://ocsp.kaspersky.com	Infrastruktura klucza publicznego (PKI).

Protokół: HTTP		
Port: 443 Protokół: HTTPS	https://ipm-klca.kaspersky.com	Ogłoszenia marketingowe.

W celu prawidłowej interakcji oprogramowania Kaspersky Security Center Linux z usługami zewnętrznymi należy wziąć pod uwagę następujące zalecenia:
- Nieszyfrowany ruch sieciowy musi być dozwolony na portach 443 i 1443 urządzeń sieciowych i serwera proxy Twojej organizacji.
– Podczas interakcji Serwera administracyjnego z serwerami aktualizacji Kaspersky i serwerami Kaspersky Security Network należy unikać przejmowania ruchu sieciowego za pomocą zastępowania certyfikatów (ataki MITM).

Aby pobrać aktualizacje poprzez protokół HTTP lub HTTPS za pomocą narzędzia klscflag:

1. Uruchom wiersz poleceń, a następnie zmień bieżący katalog na inny za pomocą narzędzia 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
     ```

Instalowanie Agenta sieciowego i aplikacji zabezpieczającej

Aby zarządzać urządzeniami w organizacji, na każdym z nich należy zainstalować Agenta sieciowego. Zdalna instalacja aplikacji Kaspersky Security Center Linux na urządzeniach w firmie zazwyczaj rozpoczyna się od zainstalowania na nich Agenta sieciowego.

W systemie Microsoft Windows XP Agent sieciowy może nie wykonywać poprawnie następujących operacji: pobierać aktualizacje bezpośrednio z serwerów Kaspersky (jako punkt dystrybucji) i działać jako serwer KSN Proxy (jako punkt dystrybucji).

Wstępna zdalna instalacja

Jeśli Agent sieciowy został już zainstalowany na urządzeniu, zdalna instalacja aplikacji na tym urządzeniu odbywa się poprzez 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. Więcej informacji dotyczących instalacji aplikacji na zarządzanych urządzeniach, na których jest już zainstalowany Agent sieciowy, można znaleźć poniżej.

Możesz przeprowadzić wstępną instalację Agenta sieciowego na urządzeniach działających pod kontrolą systemu Windows, korzystając z jednej z następujących metod:

- Używając narzędzi firm trzecich do zdalnej instalacji aplikacji.
- Klonując obraz dysku twardego administratora z systemem operacyjnym i Agentem sieciowym: przy pomocy narzędzi do zarządzania obrazami dysku, dostępnych w Kaspersky Security Center Linux, lub przy użyciu narzędzi firm trzecich.
- Korzystając z zasad grupy w systemie Windows: używając standardowych narzędzi do zarządzania systemu Windows dla zasad grupy lub w trybie automatycznym, poprzez odpowiednią, dedykowaną opcję w zadaniu zdalnej instalacji programu Kaspersky Security Center Linux.
- W trybie wymuszonym, korzystając ze specjalnych opcji w zadaniu zdalnej instalacji programu Kaspersky Security Center Linux.
- 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.
- Ręcznie, poprzez uruchomienie instalatorów aplikacji na urządzeniach.

Na platformach innych niż Microsoft Windows wstępna instalacja Agenta sieciowego na zarządzanych urządzeniach musi zostać wykonana z użyciem dostępnych narzędzi firm trzecich. Na platformach innych niż Windows możesz uaktualnić Agenta sieciowego do nowej wersji lub zainstalować inne aplikacje firmy Kaspersky, korzystając z Agentów sieciowych (już zainstalowanych na urządzeniach) przeznaczonych do wykonywania zadań zdalnej instalacji. W tym przypadku instalacja przebiega identycznie jak instalacja na urządzeniach działających pod kontrolą systemu Microsoft Windows.

Podczas wybierania metody i strategii zdalnej instalacji 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 Active Directory, 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 zastosowane na zdalnych urządzeniach w momencie uruchomienia zdalnej instalacji (na przykład, użycie UAC lub Prostego udostępniania plików).

Konfigurowanie instalatorów

Przed uruchomieniem zdalnej instalacji aplikacji Kaspersky w sieci, należy określić ustawienia instalacji (ustawienia definiowane podczas instalacji aplikacji). Podczas instalacji Agenta sieciowego należy określić przynajmniej adres połączenia z Serwerem administracyjnym; niektóre ustawienia zaawansowane też mogą być wymagane. W zależności od wybranej metody instalacji, ustawienia można zdefiniować w różny sposób. W najprostszym przypadku (ręczna instalacja interaktywna na wybranym urządzeniu) wszystkie odpowiednie ustawienia można skonfigurować z poziomu interfejsu instalatora.

Ta metoda definiowania ustawień jest nieodpowiednia w nieinteraktywnej („cichej") instalacji aplikacji w grupach urządzeń. Na ogół administrator musi określić wartości dla ustawień w sposób scentralizowany; te wartości mogą być następnie wykorzystane w instalacji cichej na wybranych urządzeniach w sieci.

Pakiety instalacyjne

Pierwsza i główna metoda definiowania ustawień instalacji aplikacji jest uniwersalna i tym samym jest odpowiednia dla wszystkich metod instalacji: przy użyciu narzędzi Kaspersky Security Center Linux oraz większości narzędzi firm trzecich. Ta metoda obejmuje utworzenie pakietów instalacyjnych aplikacji w Kaspersky Security Center Linux.

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 plików wykonywalnych instalatorów lub z instalatorów w formacie natywnym (.msi, .deb, .rpm), 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 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.

Instalacja przy użyciu zasad grupy Microsoft Windows nie jest obsługiwana.

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.

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 wskazanych 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.

Instalacja 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 przełącznikiem -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 przełącznikiem -dupfix przed (wymaganie obowiązkowe) pierwszym uruchomieniem usługi Agenta sieciowego na urządzeniach docelowych, przy pierwszym uruchomieniu systemu operacyjnego po zainstalowaniu 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 instalację 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 Windows 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`.

Wymuszona zdalna instalacja przy użyciu zadania zdalnej instalacji z Kaspersky Security Center Linux

Jeśli musisz natychmiast rozpocząć instalację Agentów sieciowych lub innych aplikacji, nie czekając na zalogowanie w domenie kolejnych urządzeń docelowych, lub jeśli są dostępne jakiekolwiek urządzenia docelowe, które nie znajdują się w domenie Active Directory, możesz wymusić instalację wybranych pakietów instalacyjnych poprzez zadanie zdalnej instalacji z Kaspersky Security Center Linux.

W tej sytuacji możesz bezpośrednio wskazać urządzenia docelowe lub wybrać grupę administracyjną Kaspersky Security Center Linux, do której należą, bądź też 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.

Ten rodzaj instalacji obejmuje kopiowanie plików do zasobu administracyjnego (admin$) na każdym urządzeniu oraz zdalną rejestrację usług pomocniczych na tych urządzeniach. Wymuszone wdrażanie na urządzeniach z systemem Windows z zasobu administracyjnego można przeprowadzić tylko przez wyznaczone punkty dystrybucji. W tym przypadku muszą być spełnione następujące warunki:

- Urządzenia muszą być dostępne dla połączenia albo po stronie Serwera administracyjnego, albo po stronie punktu dystrybucji.
- Rozwiązywanie nazw urządzeń docelowych musi działać poprawnie w sieci.
- Zasób administracyjny (admin$) musi pozostać włączony na urządzeniach docelowych.
- Na urządzeniach docelowych musi być uruchomiona usługa systemowa Serwer (domyślnie jest uruchomiona).
- W celu zezwolenia na zdalny dostęp przy użyciu narzędzi systemu Windows, na urządzeniach docelowych muszą być otwarte poniższe porty: TCP 139, TCP 445, UDP 137 i UDP 138.
- Tryb Proste udostępnianie plików musi być wyłączony na urządzeniach docelowych.
- Na urządzeniach docelowych udostępnianie i model zabezpieczeń muszą być ustawione na *Klasyczny - uwierzytelnianie użytkowników lokalnych jako samych siebie*. W żadnym wypadku nie może być ustawione *Tylko gość - uwierzytelnianie użytkowników lokalnych jako gościa*.
- Urządzenia docelowe muszą być członkami domeny lub wcześniej należy utworzyć na urządzeniach docelowych jednakowe konta z uprawnieniami administratora.

Urządzenia w grupach roboczych mogą zostać przystosowane zgodnie z powyższymi wymaganiami przy użyciu narzędzia riprep.exe, którego opis znajduje się na stronie działu pomocy technicznej firmy Kaspersky.

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.

Automatyczna instalacja jest uproszczonym sposobem tworzenia zadań dla wymuszonej instalacji aplikacji. We właściwościach grupy administracyjnej należy otworzyć listę pakietów instalacyjnych i 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.

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. Aby umożliwić instalację wymuszoną, w każdej odizolowanej sieci należy umieścić punkty dystrybucji.

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. Jednakże należy zauważyć, że ta metoda instalacji powoduje duże obciążenie urządzeń pełniących role punktów dystrybucji. Dlatego też zalecane jest wybranie jako punktów dystrybucji mocniejszych urządzeń z jednostkami przechowywania danych o wysokim poziomie wydajności. Co więcej, wolna przestrzeń na dysku, na którym znajduje się folder /var/opt/kaspersky/klnagent_srv/, musi wielokrotnie przekraczać całkowity rozmiar pakietów dystrybucyjnych instalowanych aplikacji.

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 jest przechowywany w folderze współdzielonym Kaspersky Security Center Linux.

Korzystając z Kaspersky Security Center Linux, możesz wysłać do wybranych użytkowników wiadomość e-mail zawierającą odnośnik do tego pliku w folderze współdzielonym oraz prośbę o jego uruchomienie (w trybie interaktywnym lub z przełącznikiem "-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 folderu współdzielonego Kaspersky Security Center Linux. Administrator może skopiować pakiet autonomiczny na nośnik 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 przełącznikiem "-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.

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.

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.

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.

Monitorowanie zdalnej instalacji

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.

Konfigurowanie instalatorów

Ta sekcja zawiera informacje na temat plików instalatorów Kaspersky Security Center Linux i ustawień instalacji, a także zalecenia dotyczące instalacji Serwera administracyjnego i Agenta sieciowego w trybie cichym.

Informacje ogólne

Programy instalacyjne komponentów oprogramowania Kaspersky Security Center Linux dla urządzeń z systemem Windows są zbudowane w oparciu o technologię Windows Installer. Pakiet MSI jest podstawą instalatora. Ten format pakietów umożliwia wykorzystanie wszystkich korzyści oferowanych przez Instalator Windows: skalowalność, dostępność systemu poprawek, system transformacji, scentralizowana instalacja za pośrednictwem rozwiązań firm trzecich oraz niewidoczna rejestracja w systemie operacyjnym.

Instalacja w trybie cichym (z plikiem odpowiedzi)

Instalator Agenta sieciowego może pracować z plikiem odpowiedzi (ss_install.xml), w którym zintegrowane są parametry instalacji w trybie cichym bez udziału użytkownika. Plik ss_install.xml znajduje się w tym samym folderze co pakiet MSI. Jest on używany automatycznie podczas instalacji w trybie cichym. Możesz włączyć tryb cichej instalacji z użyciem przełącznika „/s" wiersza polecenia.

Na przykład:

```
setup.exe /s
```

Przed uruchomieniem instalatora w trybie cichym przeczytaj Umowę licencyjną użytkownika końcowego (EULA). Jeśli pakiet dystrybucyjny Kaspersky Security Center Linux nie zawiera pliku TXT z treścią umowy EULA, możesz pobrać ten plik ze strony internetowej Kaspersky.

Plik ss_install.xml jest wewnętrznym formatem parametrów instalatora Kaspersky Security Center Linux. Pakiety dystrybucyjne zawierają plik ss_install.xml z domyślnymi parametrami.

Nie należy ręcznie modyfikować pliku ss_install.xml. Ten plik może być modyfikowany tylko przy użyciu narzędzi Kaspersky Security Center Linux podczas edytowania parametrów pakietów instalacyjnych w konsoli Kaspersky Security Center Web Console.

Częściowa konfiguracja instalacji poprzez setup.exe

Podczas uruchamiania instalacji aplikacji z pliku setup.exe, do pakietu MSI możesz dodać wartości dowolnych właściwości MSI.

To polecenie wygląda następująco:

Na przykład:
```
/v"PROPERTY_NAME1=PROPERTY_VALUE1 PROPERTYNAME2=PROPERTYVALUE2"
```

Parametry instalacji Serwera administracyjnego

W poniższej tabeli opisano właściwości, które możesz skonfigurować podczas instalacji Kaspersky Security Center Linux w trybie cichym.

Parametry instalacji Serwera Administracyjnego w trybie cichym

Nazwa zmiennej	Wymagane	Opis	Możliwe wa
EULA_ACCEPTED	Tak	Ten parametr potwierdza, że w pełni przeczytano, zrozumiano i zaakceptowano warunki Umowy licencyjnej.	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
KLSRV_UNATT_PORT_SRV	Nie	Wprowadź numer portu Serwera administracyjnego. Domyślna wartość to 14000.	Numer portu
KLSRV_UNATT_PORT_SRV_SSL	Nie	Wprowadź numer portu SSL Serwera administracyjnego. Domyślna wartość to 13000.	Numer portu
KLSRV_UNATT_PORT_KLOAPI	Nie	Numer portu KLOAPI Serwera administracyjnego. Domyślna wartość to 13299.	Numer portu
KLSRV_UNATT_PORT_GUI	Nie	Numer portu GUI Serwera administracyjnego. Opcja,	Numer portu

		domyślna wartość to 13291.	
`KLSRV_UNATT_NETRANGETYPE`	Nie	Oceń przybliżoną liczbę urządzeń, którymi zamierzasz zarządzać. Opcja, domyślna wartość to 1.	`1` dla od 1 do 10 urządzeń siecio `2` dla od 101 do urządzeń siecio `3` dla ponad 10(urządzeń siecio
`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.	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.	`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_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, p odpowiedzi musi zawierać następujące dodatkowe zmienne:			
`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.	`VirtualAdapt` lub `ExternalLoac`

W przypadku, gdy zmienna `KLFOC_UNATT_CONN_MODE` ma wartość `VirtualAdapter`, plik odpowiedzi musi zawie następujące zmienne dodatkowe:			
`KLFOC_UNATT_CONN_MODE_VA_NAME`		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

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—W pełni przeczytałem, rozumiem i akceptuję warunki Umowy licencyjnej. • 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.
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	• 1—uruchom. • Inna wartość lub brak wartości—nie uruchamiaj.
NAGENTTAGS	Znacznik dla Agenta sieciowego (ma priorytet nad znacznikiem podanym w pliku odpowiedzi)	Wartość wiersza.

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 profil 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).

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 "Zdalna instalacja 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.

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 %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\, 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 %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\ 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.

Lokalna instalacja aplikacji

Sekcja ta opisuje procedurę instalacji aplikacji, które można zainstalować tylko na urządzeniach lokalnych.

Aby przeprowadzić lokalną instalację aplikacji na określonym urządzeniu klienckim, musisz mieć uprawnienia administratora na tym urządzeniu.

W celu zainstalowania aplikacji lokalnie na określonym urządzeniu klienckim:

1. Zainstaluj Agenta sieciowego na urządzeniu klienckim i skonfiguruj połączenie pomiędzy urządzeniem klienckim a Serwerem administracyjnym.

2. Zainstaluj wymagane aplikacje na urządzeniu zgodnie z opisem w dokumentacji tych aplikacji.

3. Na stacji roboczej administratora zainstaluj wtyczkę zarządzającą dla każdej z zainstalowanych aplikacji.

Kaspersky Security Center Linux obsługuje również opcję lokalnej instalacji aplikacji przy pomocy autonomicznych pakietów instalacyjnych. Kaspersky Security Center Linux nie obsługuje instalacji wszystkich aplikacji Kaspersky.

Lokalna instalacja Agenta sieciowego

W celu zainstalowania Agenta sieciowego lokalnie:

1. Na urządzeniu uruchom plik setup.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 15**, 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 VDI**.

      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 profilu 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 w trybie cichym

Agent sieciowy może zostać zainstalowany w trybie cichym, czyli bez interaktywnego wprowadzania parametrów instalacji. W trybie cichej instalacji używany jest pakiet instalacyjny Windows (MSI) dla Agenta sieciowego. Plik MSI znajduje się w pakiecie dystrybucyjnym Kaspersky Security Center Linux, w folderze Packages\NetAgent\exec.

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.

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 11 i nowszych wersji 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 przełącznik 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.

Lokalna instalacja wtyczki zarządzającej aplikacją

W celu zainstalowania wtyczki zarządzającej aplikacją:

Na urządzeniu z zainstalowaną Konsolą administracyjną uruchom plik wykonywalny klcfginst.exe, wchodzący w skład pakietu dystrybucyjnego aplikacji.

Plik klcfginst.exe wchodzi w skład wszystkich aplikacji, którymi można zarządzać poprzez Kaspersky Security Center Linux. Instalacja jest wykonywana przez kreator i nie wymaga ręcznej konfiguracji ustawień.

Instalowanie aplikacji w trybie cichym

W celu zainstalowania aplikacji w trybie cichym:

1. Otwórz okno główne Kaspersky Security Center.

2. W folderze **Zdalna instalacja** drzewa konsoli, w podfolderze **Pakiety instalacyjne** wybierz pakiet instalacyjny odpowiedniej aplikacji lub utwórz nowy pakiet instalacyjny 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 przełącznika /s uruchom plik wykonywalny (plik z rozszerzeniem .exe).

   - Dla pozostałych aplikacji firmy Kaspersky, z otwartego folderu, przy pomocy przełącznika /s uruchom plik wykonywalny (plik z rozszerzeniem .exe).

Uruchomienie pliku wykonywalnego z parametrami `EULA=1` i `PRIVACYPOLICY=1` oznacza, że w pełni przeczytałeś, zrozumiałeś i akceptujesz warunki Umowy licencyjnej 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.

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. Nawiąż połączenie z żądanym Serwerem administracyjnym.
2. W folderze **Zdalna instalacja** drzewa konsoli wybierz podfolder **Pakiety instalacyjne**.
3. W obszarze roboczym wybierz pakiet instalacyjny wymaganej aplikacji.
4. Uruchom proces tworzenia autonomicznego pakietu instalacyjnego, korzystając z jednej z następujących metod:
   - Wybierając **Utwórz autonomiczny pakiet instalacyjny** z menu kontekstowego pakietu instalacyjnego.
   - Klikając odnośnik **Utwórz autonomiczny pakiet instalacyjny** w obszarze roboczym pakietu instalacyjnego.

   Zostanie uruchomiony Kreator tworzenia autonomicznego pakietu instalacyjnego. Postępuj zgodnie z instrukcjami kreatora.

   W ostatnim kroku kreatora wybierz metodę przesłania autonomicznego pakietu instalacyjnego na urządzenie klienckie.
5. Prześlij autonomiczny pakiet instalacyjny na urządzenie klienckie.
6. 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.

Ustawienia pakietu instalacyjnego Agenta sieciowego

W celu skonfigurowania pakietu instalacyjnego Agenta sieciowego:

1. W folderze **Zdalna instalacja** drzewa konsoli wybierz podfolder **Pakiety instalacyjne**.

Domyślnie folder **Zdalna instalacja** to podfolder folderu **Zaawansowane**.

2. Z menu kontekstowego pakietu instalacyjnego Agenta sieciowego wybierz **Właściwości**.

Zostanie otwarte okno właściwości pakietu instalacyjnego Agenta sieciowego.

Ogólne

Sekcja **Ogólne** wyświetla ogólne 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

Ustawienia

Ta sekcja przedstawia ustawienia wymagane do zapewnienia właściwego działania Agenta sieciowego natychmiast po jego zainstalowaniu. Ustawienia w tej sekcji są dostępne tylko na urządzeniach działających pod kontrolą systemu Windows.

W grupie ustawień **Folder docelowy** możesz wybrać folder na urządzeniu klienckim, w którym zostanie zainstalowany Agent sieciowy.

- **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.

W następującej grupie ustawień możesz określić hasło dla zadania zdalnej dezinstalacji Agenta sieciowego:

- **Użyj hasła dezinstalacyjnego**

  Jeśli ta opcja jest włączona, klikając przycisk **Modyfikuj** możesz wprowadzić hasło dezinstalacyjne (dostępne tylko dla Agenta sieciowego na urządzeniach działających pod kontrolą systemów operacyjnych Windows).

  Domyślnie opcja ta jest wyłączona.

- **Stan**

Stan hasła: **Hasło zostało określone** lub **Hasło nie zostało określone**.

Domyślnie hasło nie jest ustawione.

- 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, Serwera urządzeń mobilnych Exchange 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.

Połączenie

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:

- Serwer administracyjny

  Adres urządzenia z zainstalowanym Serwerem administracyjnym.

- Port

  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 **Przeglądaj**.

Jeśli ta opcja jest wyłączona, plik certyfikatu zostanie pobrany z Serwera administracyjnego przy pierwszym połączeniu Agenta sieciowego z adresem określonym w polu **Adres serwera**.

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 pole to jest zaznaczone.

- Użyj 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.

- Numer portu UDP

W tym polu możesz określić port do łączenia Serwera administracyjnego z Agentem sieciowym przy użyciu protokołu UDP.

Domyślny numer portu UDP to 15000.

- Otwórz porty dla Agenta sieciowego w Zaporze systemu Windows

Jeśli ta opcja jest włączona, porty UDP używane przez Agenta sieciowego są dodawane do listy wykluczeń Zapory sieciowej systemu Microsoft Windows.

Domyślnie opcja ta jest włączona.

Zaawansowane

W sekcji **Zaawansowane** możesz skonfigurować sposób korzystania z bramy połączenia. W tym celu możesz wykonać następujące czynności:

- Użyj 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 się z Serwerem administracyjnym 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**.

- Skonfiguruj połączenie dla infrastruktury pulpitu wirtualnego (VDI), jeśli sieć obejmuje maszyny wirtualne. W tym celu wykonaj następujące czynności:

  - **Włącz tryb dynamiczny VDI**

    Jeżeli ta opcja jest włączona, tryb dynamiczny Virtual Desktop Infrastructure będzie włączony dla Agenta sieciowego, zainstalowanego na maszynie wirtualnej.

    Domyślnie opcja ta jest wyłączona.

  - **Optymalizuj ustawienia dla VDI**

    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.

Dodatkowe składniki

W tej sekcji możesz wybrać dodatkowe komponenty do jednoczesnego zainstalowania z Agentem sieciowym.

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.

Historia rewizji

W tej sekcji możesz przejrzeć historię rewizji pakietu instalacyjnego. Możesz porównać rewizje, przejrzeć rewizje, zapisać rewizje do pliku oraz dodać i zmodyfikować opisy rewizji.

Ustawienia pakietu instalacyjnego Agenta sieciowego dostępne dla określonego systemu operacyjnego zostały podane w tabeli poniżej.

Ustawienia pakietu instalacyjnego Agenta sieciowego

Sekcja Właściwość	Windows	Mac	Linux
Ogólne	✓	✓	✓

Ustawienia	✓	–	–
Połączenie	✓	✓ (za wyjątkiem opcji **Otwórz porty dla Agenta sieciowego w Zaporze systemu Windows** i **Używaj wyłącznie automatycznego wykrywania serwera proxy**)	✓ (za wyjątkiem opcji **Otwórz porty dla Agenta sieciowego w Zaporze systemu Windows** i **Używaj wyłącznie automatycznego wykrywania serwera proxy**)
Zaawansowane	✓	✓	✓
Dodatkowe składniki	✓	✓	✓
Znaczniki	✓	✓ (za wyjątkiem reguł automatycznego znakowania)	✓ (za wyjątkiem reguł automatycznego znakowania)
Historia rewizji	✓	✓	✓

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.

Zarządzanie urządzeniami klienckimi

W tej sekcji można znaleźć opis sposobu zarządzania urządzeniami w grupach administracyjnych.

Ustawienia zarządzanego urządzenia

W celu sprawdzenia ustawień zarządzanego urządzenia:

1. W menu głównym przejdź do **Zasoby (urządzenia)** → **Zarządzane 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.

- 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

    W tym polu jest wyświetlany bieżący stan ochrony w czasie rzeczywistym urządzenia klienckiego.

    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 złośliwego oprogramowania przeprowadzonego na urządzeniu klienckim.

  - Wykryto wirusa

    Całkowita liczba zagrożeń wykrytych na urządzeniu klienckim od momentu zainstalowania aplikacji antywirusowej (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

  Ta zakładka zawiera listę wszystkich aplikacji firmy Kaspersky zainstalowanych na urządzeniu klienckim. 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 aktywne na zarządzanym 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. Jeśli połączenie nie jest nawiązane, stan nie jest wyświetlany.

- Zdarzenia

  Zakładka **Zdarzenia** wyświetla zdarzenia zarejestrowane na Serwerze administracyjnym dla wybranego urządzenia klienckiego.

- 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 programy 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.

- **Zdalna diagnostyka** W tej sekcji możesz przeprowadzić zdalną diagnostykę urządzeń klienckich.

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 **Zasoby (urządzenia)** → **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 **Zasoby (urządzenia)** → **Hierarchia grup**.
2. Kliknij przycisk **Importuj**.

Zostanie uruchomiony Kreator struktury nowej grupy administracyjnej. Postępuj zgodnie z instrukcjami Kreatora.

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 **Zasoby (urządzenia)** → **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 specjalnego profilu 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 itd.

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 **Zasoby (urządzenia)** → **Reguły przenoszenia**.
2. Kliknij **Dodaj**.
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.
   - **Aktywna reguła**

     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.
   - **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 zwiększyć lub zmniejszyć priorytet reguły przenoszenia, przesuń regułę odpowiednio w górę lub w dół na liście za pomocą myszy.

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 **Zasoby (urządzenia)** → **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.

   - Aktywna reguła

     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.

   - 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

Kiedy tworzysz lub kopiujesz regułę przenoszenia urządzeń klienckich do grup administracyjnych, na zakładce **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.
- Aplikacje zarządzane zainstalowane na urządzeniach klienckich, na przykład Agent sieciowy lub Serwer administracyjny.
- Maszyny wirtualne, które są urządzeniami klienckimi.

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 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.

- 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.

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 15** lub **Serwer administracyjny Kaspersky Security Center 15**.

  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.

- Typ systemu operacyjnego (bity)

  Urządzenia klienckie można usuwać według rozmiarów bitowych systemu operacyjnego. W polu **Typ systemu operacyjnego (bity)** możesz wybrać jedną z następujących wartości:

  - **Nieznany**
  - **x86**
  - **AMD64**
  - **IA64**

  Aby sprawdzić rozmiar bitowy systemu operacyjnego urządzeń klienckich:

  1. W menu głównym przejdź do **Zasoby (urządzenia)** → **Zarządzane urządzenia**.
  2. Kliknij przycisk **Ustawienia kolumn** ( ) po prawej.
  3. Wybierz opcję **Typ systemu operacyjnego (bity)**, a następnie kliknij przycisk **Zapisz**.

     Następnie rozmiar bitowy 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 infrastruktury pulpitu wirtualnego (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.

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 **Zasoby (urządzenia)** → **Zarządzane urządzenia**.
2. Kliknij odnośnik **Obecna ścieżka:** `<obecna ścieżka>` nad listą.
3. W otwartym oknie wybierz grupę administracyjną, do której chcesz dodać urządzenia.
4. Kliknij przycisk **Dodaj urządzenia**.

   Zostanie uruchomiony Kreator przenoszenia urządzeń.
5. 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.
     - 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: , \ / * ' " ; : & ` ~ ! @ # $ ^ ( ) = + [ ] { } | < > %
6. Przejrzyj listę urządzeń, które mają zostać dodane do grupy administracyjnej. Możesz edytować listę, dodając lub usuwając urządzenia.
7. 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, przejdź do **Zasoby (urządzenia)** → **Zarządzane urządzenia**, kliknij odnośnik ścieżki w polu **Bieżąca ścieżka** i wybierz grupę administracyjną w otwartym okienku po lewej stronie.

   - Aby otworzyć grupę **Urządzenia nieprzypisane**, w menu głównym przejdź do **Wykrywanie i wdrażanie** → **Urządzenia nieprzypisane**.

2. Jeżeli grupa administracyjna zawiera klastry lub macierze serwerowe, sekcja **Zarządzane 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 **Zarządzane 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 **Zasoby (urządzenia)** → **Zarządzane 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 wskazanych 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.

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.

Aby automatycznie przypisać punkty dystrybucji:

1. W menu aplikacji kliknij ikonę ustawienia ( ) obok nazwy żądanego 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 ich liczby i konfiguracji.

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

W celu ręcznego wskazania urządzenia jako punktu dystrybucji:

1. W menu aplikacji kliknij ikonę ustawienia ( ) obok nazwy żądanego 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.

     - Użyj multiemisji

       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 IPv4, za pośrednictwem którego urządzenia zdalne łączą się z punktem dystrybucji.

- **Roześlij aktualizacje**

  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.

- **Roześlij pakiety instalacyjne**

  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.

- **Uruchom serwer 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.

- **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 uaktualnień**

  Wybierz źródło uaktualnień 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.

- W podsekcji **Ustawienia połączenia z Internetem** możesz określić ustawienia dostępu do Internetu:

  - **Użyj serwera proxy**

    Jeśli to pole jest zaznaczone, w polach wejściowych możesz 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 Private KSN

    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.

- 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 konsoli internetowej znajdujący się w strefie DMZ lub w Internecie. Określ numer portu, który będzie używany do połączenia z konsoli internetowej 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)**.

  - 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. 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. 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.

- Skonfiguruj przeszukiwanie kontrolera domeny przez punkt dystrybucji.

  - Przeszukiwanie sterowników domeny

    Możesz włączyć wykrywanie urządzeń dla kontrolerów domeny.

    Jeśli wybierzesz opcję **Włącz przeszukiwanie sterowników domeny**, możesz wybrać kontrolery domeny do odpytywania, a także określić terminarz ich 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.

    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 przeszukiwania 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 przeszukiwania sieci IPv6** jest dostępna, jeśli w punkcie dystrybucji działa system Linux. Aby korzystać z odpytywania Zerocong 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.

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 **Zasoby (urządzenia)** → **Zarządzane urządzenia**.
2. W polu **Bieżąca ścieżka** nad listą zarządzanych urządzeń kliknij łącze ścieżki.
3. W otwartym okienku po lewej stronie wybierz grupę administracyjną, dla której chcesz wyświetlić przypisane punkty dystrybucji.

   Spowoduje to włączenie pozycji menu **Punkty dystrybucji**.
4. W menu głównym przejdź do **Zasoby (urządzenia)** → **Punkty dystrybucji**.
5. Aby dodać nowe punkty dystrybucji dla grupy administracyjnej, kliknij przycisk **Przypisz**.
6. 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 aplikacji kliknij ikonę ustawienia ( ) obok nazwy żądanego 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 **Uruchom serwer push**.
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.

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). 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	Agent sieciowy jest zainstalowany na urządzeniu, ale aplikacja zabezpieczająca nie jest zainstalowana.	• Przycisk

nie jest zainstalowana		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 złośliwego 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 złośliwego 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.
Wymagane jest ponowne uruchomienie	Urządzenie jest widoczne w sieci, ale aplikacja wymaga ponownego uruchomienia urządzenia dłużej niż określony przedział czasu i z jednego z wybranych powodów.	Więcej niż 0 minut.
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.

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.
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.
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.	• 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.

Jeśli Kaspersky Security Center Linux przypisze stan do urządzenia, dla niektórych warunków (patrz kolumna Opis warunku) brana jest pod uwagę flaga widoczności. 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*.

Konfigurowanie przełączania stanów urządzeń

Możesz zmienić warunki, aby przypisać stan *Krytyczny* lub *Ostrzeżenie* do urządzenia.

W celu włączenia zmiany stanu urządzenia na Krytyczny:

1. Otwórz okno właściwości w jeden z następujących sposobów:
   - W folderze **Zasady**, w menu kontekstowym profilu Serwera administracyjnego wybierz **Właściwości**.
   - Z menu kontekstowego grupy administracyjnej wybierz **Właściwości**.
2. W oknie **Właściwości**, które zostanie otwarte, w panelu **Sekcje** wybierz **Stan urządzenia**.
3. W sekcji **Ustaw stan Krytyczny, jeśli** zaznacz pole obok warunku na liście.

   Możesz zmienić tylko ustawienia, które nie są zablokowane w zasadzie nadrzędnej.

4. Dla wybranego warunku ustaw żądaną wartość.
   Możesz ustawić wartości dla niektórych, ale nie wszystkich, warunków.
5. Kliknij **OK**.

Jeśli określone warunki zostaną spełnione, zarządzanemu urządzeniu zostanie przypisany stan *Krytyczne*.

W celu włączenia zmiany stanu urządzenia na Ostrzeżenie:

1. Otwórz okno właściwości w jeden z następujących sposobów:
   - W folderze **Zasady**, w menu kontekstowym profilu Serwera administracyjnego wybierz **Właściwości**.
   - Z menu kontekstowego grupy administracyjnej wybierz **Właściwości**.
2. W oknie **Właściwości**, które zostanie otwarte, w panelu **Sekcje** wybierz **Stan urządzenia**.
3. W prawej części, w sekcji **Ustaw stan Ostrzeżenie, jeśli** zaznacz pole obok warunku na liście.

Możesz zmienić tylko ustawienia, które nie są zablokowane w zasadzie nadrzędnej.

4. Dla wybranego warunku ustaw żądaną wartość.

   Możesz ustawić wartości dla niektórych, ale nie wszystkich, warunków.

5. Kliknij **OK**.

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.

Wyświetlanie listy urządzeń z poziomu wyboru urządzenia

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 **Zasoby (urządzenia)** → **Wybory urządzeń** lub **Wykrywanie i wdrażanie** → **Wybory urządzeń**.

2. Na liście wyboru kliknij nazwę odpowiedniego wyboru.

   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 **Zasoby (urządzenia)** → **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 **Zasoby (urządzenia)** → **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

> Jeśli ta opcja jest włączona, określony warunek wyboru zostanie odwrócony. Wybór będzie zawierał wszystkie urządzenia, które nie spełniają warunku.
>
> Domyślnie opcja ta jest wyłączona.

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*, or *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 (*Brak danych z urządzenia, Zatrzymana, Uruchamianie, Wstrzymana, Uruchomiona, Niepowodzenie*).

- Stan ochrony serwerów współpracy

  Wyszukiwanie urządzeń według stanu ochrony serwerów współpracy (*Brak danych z urządzenia*, *Zatrzymana*, *Uruchamianie, Wstrzymana*, *Uruchomiona*, *Niepowodzenie*).

- Stan ochrony antywirusowej serwerów pocztowych

  Wyszukiwanie urządzeń według stanu ochrony dla serwerów pocztowych (*Brak danych z urządzenia, Zatrzymana, Uruchamianie, Wstrzymana, Uruchomiona, Niepowodzenie*).

- Stan czujnika Endpoint Sensor

  Wyszukiwanie urządzeń według stanu komponentu Endpoint Sensor (*Brak danych z urządzenia, Zatrzymana, Uruchamianie, Wstrzymana, Uruchomiona, Niepowodzenie*).

W sekcji **Problemy wpływające 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.

- Typ systemu operacyjnego (bity)

  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 infrastruktury pulpitu wirtualnego (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 infrastruktury pulpitu wirtualnego.
  - **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.

- **Musi zawierać**

  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.

- **Nie może zawierać**

  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.

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 **Zasoby (urządzenia)** → **Wybory urządzeń** lub **Wykrywanie i wdrażanie** → **Wybory urządzeń**.

2. Na liście wyboru kliknij nazwę odpowiedniego wyboru.

   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

Ta sekcja opisuje znaczniki urządzeń oraz zawiera instrukcje ich tworzenia i modyfikowania oraz ręcznego i automatycznego znakowania urządzeń.

Informacje o znacznikach urządzeń

Kaspersky Security Center Linux umożliwia *znakowanie* urządzeń. Znacznik to etykieta urządzenia, 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. Możesz użyć ręcznego znakowania, gdy chcesz oznakować pojedyncze urządzenie. Automatyczne znakowanie jest wykonywane przez Kaspersky Security Center Linux zgodnie z określonymi regułami znakowania.

Urządzenia są znakowane automatycznie, gdy spełnione są określone reguły. 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.

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 **Zasoby (urządzenia)** → **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 **Zasoby (urządzenia)** → **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

W celu usunięcia znacznika urządzenia:

1. W menu głównym przejdź do **Zasoby (urządzenia)** → **Znaczniki** → **Znaczniki urządzenia**.
2. Z listy 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.

Znacznik, który usunąłeś, nie zostanie usunięty automatycznie z reguł automatycznego znakowania. Po usunięciu znacznika, zostanie on przypisany do nowego urządzenia tylko wtedy, gdy urządzenie będzie spełniało wymagania reguły przypisującej znacznik.

Usunięty tag nie jest automatycznie usuwany z urządzenia, jeśli ten tag jest przypisany do urządzenia przez aplikację lub Agenta sieciowego. Aby usunąć tag z urządzenia, użyj narzędzia klscflag.

Przeglądanie urządzeń, do których przypisano znacznik

W celu przejrzenia urządzeń, do których przypisywany jest znacznik:

1. W menu głównym przejdź do **Zasoby (urządzenia)** → **Znaczniki** → **Znaczniki urządzenia**.
2. Kliknij odnośnik **Wyświetl urządzenia** obok znacznika, dla którego chcesz wyświetlić przypisane urządzenia.

   Wyświetlona lista urządzeń będzie zawierała tylko te urządzenia, do których został przypisany znacznik.

Aby wrócić do listy znaczników urządzenia, kliknij przycisk **Wstecz** w swojej przeglądarce.

Przeglądanie znaczników przydzielonych do urządzenia

W celu przejrzenia znaczników przydzielonych do urządzenia:

1. W menu głównym przejdź do **Zasoby (urządzenia)** → **Zarządzane 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.

Możesz przypisać inny znacznik do urządzenia lub usunąć już przypisany znacznik. Możesz także sprawdzić wszystkie znaczniki urządzenia, które znajdują się na Serwerze administracyjnym.

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 **Zasoby (urządzenia)** → **Zarządzane 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 kliknij **Tak**.

   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 usunąć te znaczniki, 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 **Zasoby (urządzenia)** → **Znaczniki** → **Reguły automatycznego znakowania**.

- W menu głównym przejdź do **Zasoby (urządzenia)** → **Znaczniki** → **Znaczniki urządzenia**, and then click the **Ustaw reguły automatycznego znakowania**.
- Przejrzyj znaczniki przypisane do urządzenia, a następnie kliknij przycisk **Ustawienia**.

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.

      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**.
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 ponownie kliknij **Usuń**.

   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.

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 możesz zarządzać następującymi typami szyfrowania:

- Szyfrowanie dysków funkcją BitLocker na urządzeniach z systemem operacyjnym Windows dla serwerów
- Kaspersky Disk Encryption na urządzeniach z systemem operacyjnym Windows dla stacji roboczych

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 Kaspersky Endpoint Security for Windows w Kaspersky Security Center Linux. Kaspersky Endpoint Security for Windows wykonuje szyfrowanie i deszyfrowanie 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 konsoli internetowej. Użyj podstawowego 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** → **Szyfrowanie i ochrona danych** → **Zaszyfrowane dyski**.

Jeśli sekcji nie ma w menu, oznacza to, że jest ukryta. W ustawieniach interfejsu użytkownika włącz opcję **Pokaż szyfrowanie i ochronę 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 deszyfrowania 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** → **Szyfrowanie i ochrona danych** → **Zdarzenia szyfrowania**.

Jeśli sekcji nie ma w menu, oznacza to, że jest ukryta. W ustawieniach interfejsu użytkownika włącz opcję **Pokaż szyfrowanie i ochronę 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 **Zasoby (urządzenia)** → **Zarządzane 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 polityka 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 deszyfrowania 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 i raportowanie** → **Raporty**). Alternatywnie w sekcji **Operacje** → **Szyfrowanie i ochrona 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 **Szyfrowanie i ochrona danych**:*

1. Upewnij się, że włączyłeś opcję **Pokaż szyfrowanie i ochronę danych** w opcjach interfejsu.
2. W menu głównym przejdź do **Operacje** → **Szyfrowanie i ochrona danych**.
3. 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.
4. 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 for Windows 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 for Windows.

W celu udzielenia dostępu do zaszyfrowanego dysku w trybie offline:

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** → **Szyfrowanie i ochrona 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.

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 nowego zadania wybierz aplikację **Kaspersky Security Center 15** 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.

   - **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.

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 **Zasoby (urządzenia)** → **Hierarchia grup**.
2. Kliknij nazwę żądanej grupy administracyjnej.

   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 potomnych, ale we właściwościach grup potomnych te ustawienia są zablokowane.

     Domyślnie opcja ta jest wyłączona.
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.

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 **Zasoby (urządzenia)** → **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 **Zasoby (urządzenia)** → **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). Opcjonalnie określ komunikat monitu dla użytkownika i opcję **Czas oczekiwania przed wymuszeniem zamknięcia aplikacji dla zablokowanych sesji (min)** dla poleceń wyłączania i ponownego uruchamiania.

6. Uruchom utworzone zadanie.

Po zakończeniu zadania, polecenie (włącz, wyłącz lub uruchom ponownie) zostanie wykonane na wybranych urządzeniach.

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 zdalnego zainstalowania 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 sieciowej 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 sieciową wtyczką zarządzającą. 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.

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 profili**

   Utwórz zasadę dla Kaspersky Endpoint Security ręcznie lub za pomocą kreatora wstępnej konfiguracji. Możesz użyć domyślnych ustawień profilu; możesz także zmodyfikować domyślne ustawienia profilu 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 profile 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 wtyczkę sieciową zarządzania dla aplikacji.

W celu pobrania sieciowej wtyczki zarządzającej dla aplikacji Kaspersky:

1. W menu głównym przejdź do **Ustawienia** → **Wtyczki sieciowe**.
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**.

   Sieciowa wtyczka administracyjna zostanie pobrana z domyślną konfiguracją i wyświetlona na liście sieciowych wtyczek administracyjnych.

Możesz dodać wtyczki i zaktualizować pobrane wtyczki z pliku. Wtyczki sieciowe do zarządzania można pobrać ze strony internetowej Kaspersky.

Aby pobrać lub zaktualizować wtyczkę internetową do zarządzania z pliku:

1. W menu głównym przejdź do **Ustawienia** → **Wtyczki sieciowe**.
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.

   Sieciowa wtyczka zarządzająca zostanie pobrana z pliku i zostanie wyświetlona na liście sieciowych wtyczek zarządzających.

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. Wykonaj jedną z poniższych czynności:
   - W menu głównym przejdź do **Wykrywanie i wdrażanie** → **Wdrażanie i przypisywanie** → **Pakiety instalacyjne**.
   - W menu głównym przejdź do **Operacje** → **Repozytoria** → **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.
2. Kliknij **Dodaj**.

   Zostanie uruchomiony Kreator tworzenia nowego pakietu. Przejdź przez kroki kreatora, korzystając z przycisku **Dalej**.
3. W pierwszym kroku kreatora wybierz **Utwórz pakiet instalacyjny dla aplikacji Kaspersky**.

   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.

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.

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**.

   Rozpocznie się pobieranie pakietu instalacyjnego na Serwer administracyjny. Możesz zamknąć okno kreatora lub przejść do następnego kroku instrukcji. Jeśli zamkniesz okno kreatora, proces pobierania będzie kontynuowany w tle.

   Jeśli chcesz śledzić proces pobierania pakietu instalacyjnego:

   a. W menu głównym przejdź do **Operacje** → **Repozytoria** → **Pakiety instalacyjne** → **W toku ()**.

   b. Śledź proces działania w kolumnie **Postęp pobierania** oraz w kolumnie **Stan pobierania** tabeli.

   Po zakończeniu procesu pakiet instalacyjny zostanie dodany do listy na zakładce **Pobrano**. Jeśli proces pobierania zostanie zatrzymany, a stan pobierania przełączy się na **Zaakceptuj Umowę licencyjną**, kliknij nazwę pakietu instalacyjnego, a następnie przejdź do kolejnego kroku instrukcji.

   > 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. Dla niektórych aplikacji Kaspersky, podczas pobierania wyświetlany jest przycisk **Pokaż Umowę licencyjną**. Jeśli przycisk jest wyświetlany, wykonaj następujące czynności:

   a. Kliknij przycisk **Pokaż Umowę licencyjną**, aby przeczytać Umowę licencyjną.

   b. Przeczytaj Umowę licencyjną, która zostanie wyświetlona na ekranie, i kliknij **Zaakceptuj**.

      Po zaakceptowaniu Umowy licencyjnej, proces pobierania będzie kontynuowany. Jeśli klikniesz **Odrzuć**, proces pobierania zostanie zatrzymany.

7. 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.

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.

W celu utworzenia niestandardowego pakietu instalacyjnego:

1. Wykonaj jedną z poniższych czynności:

   - W menu głównym przejdź do **Wykrywanie i wdrażanie** → **Wdrażanie i przypisywanie** → **Pakiety instalacyjne**.

   - W menu głównym przejdź do **Operacje** → **Repozytoria** → **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. W pierwszym kroku kreatora wybierz **Utwórz pakiet instalacyjny z pliku**.

4. W kolejnym kroku kreatora określ 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.

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. Wybierz opcję **Zaakceptuj warunki i postanowienia niniejszej Umowy licencyjnej użytkownika końcowego** tylko wtedy, gdy w pełni przeczytano, zrozumiano warunki umowy EULA i 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. W kolejnym kroku kreatora wybierz plik (z listy plików, które są wypakowywane z wybranego pliku archiwum) i określ parametry wiersza poleceń pliku wykonywalnego.

   Możesz określić parametry wiersza poleceń, aby zainstalować aplikację z pakietu instalacyjnego w trybie cichym. Określanie parametrów wiersza poleceń jest opcjonalne.

   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.
  - **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 (Installer.exe), 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.

Upewnij się, że autonomiczny pakiet instalacyjny nie jest dostępny dla innych osób.

W celu utworzenia autonomicznego pakietu instalacyjnego:

1. Wykonaj jedną z poniższych czynności:
   - W menu głównym przejdź do **Wykrywanie i wdrażanie** → **Wdrażanie i przypisywanie** → **Pakiety instalacyjne**.
   - W menu głównym przejdź do **Operacje** → **Repozytoria** → **Pakiety instalacyjne**.

   Zostanie wyświetlona lista pakietów instalacyjnych dostępnych na Serwerze administracyjnym.

2. Na liście pakietów instalacyjnych wybierz pakiet instalacyjny i nad listą kliknij przycisk **Wdrażaj**.

3. Wybierz opcję **Przy użyciu pakietów autonomicznych**.

   Zostanie uruchomiony Kreator tworzenia autonomicznego pakietu instalacyjnego. Przejdź przez kroki kreatora, korzystając z przycisku **Dalej**.

4. W pierwszym kroku kreatora, upewnij się, że opcja **Zainstaluj Agenta sieciowego wraz z aplikacją** jest włączona, jeśli chcesz zainstalować Agenta sieciowego wraz z wybraną aplikacją.

   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. Na stronie **Przenieś do listy zarządzanych urządzeń** kreatora domyślnie jest wybrana opcja **Nie przenoś urządzeń**. Jeśli chcesz przenieść urządzenie klienckie do dowolnej grupy administracyjnej po zainstalowaniu Agenta sieciowego, nie zmieniaj wyboru opcji.

   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**.

6. W kolejnym kroku kreatora, 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.

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.

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.

W celu przeprowadzenia instalacji Agenta sieciowego dla systemu Linux w trybie cichym:

1. Przygotuj odpowiednie urządzenie Linux do zdalnej instalacji. Pobierz i utwórz pakiet zdalnej instalacji, używając pakietu .deb lub .rpm Agenta sieciowego, korzystając z dowolnego odpowiedniego systemu do zarządzania pakietami.

2. 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.

3. Przeczytaj Umowę licencyjną. Wykonaj poniższe kroki tylko wtedy, gdy rozumiesz i akceptujesz warunki Umowy licencyjnej.

4. Ustaw wartość zmiennej środowiskowej KLAUTOANSWERS, wprowadzając pełną nazwę pliku odpowiedzi (w tym ścieżkę dostępu), na przykład, w następujący sposób:

   ```
   export KLAUTOANSWERS=/tmp/nagent_install/answers.txt
   ```

5. Utwórz plik odpowiedzi (w formacie TXT) w katalogu, który określiłeś w zmiennej środowiskowej. 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 Agenta sieciowego; jeśli brakuje wartości, może być interpretowane jako brak zgody na Umowę licencyjną.	1—Potwierdzam, że w pełni przeczytałem, rozumiem i akceptuję warunki tej Umowy licencyjnej. 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	Dowolny zestaw znaków alfanumerycznych

		zalogowania się do serwera proxy.	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. 4—Instancja Agenta sieciowego jest używana jako brama połączenia w strefie zdemilitaryzowanej (DMZ).
KLNAGENT_GW_ADDRESS	Nie	Definiuje adres bramy połączenia. Wartość jest stosowana tylko wtedy, gdy KLNAGENT_GW_MODE=3.	Nazwa DNS lub adres IP.

6. Zainstaluj agenta sieciowego:

- Aby zainstalować Agenta sieciowego z pakietu RPM w 32-bitowym systemie operacyjnym, wykonaj następujące polecenie:
  ```
  # rpm -i klnagent-<numer kompilacji>.i386.rpm
  ```
- Aby zainstalować Agenta sieciowego z pakietu RPM w 64-bitowym systemie operacyjnym, wykonaj następujące polecenie:
  ```
  # rpm -i klnagent64-<numer kompilacji>.x86_64.rpm
  ```
- Aby zainstalować Agenta sieciowego z pakietu RPM w 64-bitowym systemie operacyjnym dla architektury Arm, wykonaj następujące polecenie:
  ```
  # rpm -i klnagent64-<numer kompilacji>.aarch64.rpm
  ```
- Aby zainstalować Agenta sieciowego z pakietu DEB w 32-bitowym systemie operacyjnym, wykonaj następujące polecenie:
  ```
  # apt-get install ./klnagent_<numer kompilacji>_i386.deb
  ```
- Aby zainstalować Agenta sieciowego z pakietu DEB w 64-bitowym systemie operacyjnym, wykonaj następujące polecenie:
  ```
  # apt-get install ./klnagent64_<numer kompilacji>_amd64.deb
  ```
- Aby zainstalować Agenta sieciowego z pakietu DEB w 64-bitowym systemie operacyjnym dla architektury Arm, wykonaj następujące polecenie:
  ```
  # apt-get install ./klnagent64_<numer kompilacji>_arm64.deb
  ```

Instalacja Agenta sieciowego dla systemu Linux zostanie uruchomiona w trybie cichym; użytkownik nie zostanie zapytany o żadne działania podczas procesu.

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.

Czynności niezbędne do wykonania przed rozpoczęciem pracy:

- Upewnij się, że na urządzeniu, na którym chcesz zainstalować Agenta sieciowego dla systemu Linux, działa jedna z obsługiwanych dystrybucji systemu Linux.
- Pobierz niezbędny plik instalacyjny Agenta sieciowego ze strony Kaspersky.

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.

6. Wykonaj kroki przygotowawcze typowe dla dowolnego urządzenia z systemem Linux.

Urządzenie jest gotowe. Możesz teraz przystąpić do instalacji Agenta sieciowego.

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.
- **Suma kontrolna 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.

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**.

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 podstawowego Serwera administracyjnego, możesz rozesłać pakiety instalacyjne do pomocniczych 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 drugorzędne Serwery administracyjne są połączone z głównym Serwerem administracyjnym.

2. W menu głównym przejdź do **Zasoby (urządzenia)** → **Zadania**.

   Zostanie wyświetlona lista zadań.

3. Kliknij przycisk **Dodaj**.

   Zostanie uruchomiony Kreator tworzenia nowego zadania. Postępuj zgodnie z krokami kreatora.

4. Na stronie **Nowe zadanie**, 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 pomocniczych Serwerów administracyjnych w określonej grupie administracyjnej, wybierz tę grupę, a następnie utwórz dla niej zadanie grupowe.

   - Jeśli chcesz utworzyć zadanie dla określonych pomocniczych 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 dodatkowe 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 drugorzędne 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 pomocnicze Serwery administracyjne.

Przygotowanie urządzenia z systemem Linux i zdalna instalacja Agenta sieciowego na urządzeniu z systemem Linux

Instalacja Agenta sieciowego składa się z dwóch kroków:

- Przygotowanie urządzenia Linux
- Instalacja zdalnego Agenta sieciowego

Przygotowanie urządzenia Linux

W celu przygotowania urządzenia z systemem Linux do zdalnej instalacji Agenta sieciowego:

1. Upewnij się, że następujące oprogramowanie jest zainstalowane na docelowym urządzeniu Linux:
   - Sudo
   - Perl language interpreter wersja 5.10 lub wyższa
2. 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. Wyłącz hasło do programu sudo dla konta użytkownika, z poziomu którego nawiązywane jest połączenie.

   c. Użyj polecenia `visudo` w sudo, aby otworzyć plik konfiguracyjny sudoers.

      W otwartym pliku znajdź wiersz rozpoczynający się od `%sudo` (lub od `%wheel`, jeśli używasz systemu operacyjnego CentOS). W tym wierszu podaj następujące informacje: `< nazwa użytkownika > 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`

   d. Zapisz plik sudoers i zamknij go.

   e. 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. 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`.

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 `< username >` to konto użytkownika, które ma zostać użyte do połączenia urządzenia przez SSH.

W celu zastosowania zmienionych ustawień uruchom urządzenie Linux ponownie lub wykonaj następujące polecenie:

```
$ sudo systemctl restart systemd-logind.service
```

4. 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.

5. 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.

Instalacja zdalnego Agenta sieciowego

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. Pobierz pakiet instalacyjny Agenta sieciowego , korzystając z interfejsu aplikacji lub ze strony internetowej Kaspersky .

   c. 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`.

Może zostać zwrócony błąd, jeśli instalujesz Agenta sieciowego z SSH na urządzeniach działających pod kontrolą systemu Fedora w wersjach wcześniejszych niż 20. W tym przypadku, aby instalacja Agenta sieciowego zakończyła się pomyślnie, zakomentuj opcję Defaults requiretty (załącz w składni komentarza, aby usunąć z kodu przetwarzania) w pliku /etc/sudoers. Szczegółowy opis warunku opcji Defaults requiretty, która może powodować problemy podczas połączenia SSH, można znaleźć na stronie Bugzilla.

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, należy wskazać urządzenia w oknie kreatora w jeden z następujących sposobów:

- **Wybierz urządzenia wykryte w sieci przez Serwer administracyjny**. W tym przypadku zadanie jest przydzielane do określonych urządzeń. Określone urządzenia mogą obejmować urządzenia z grup administracyjnych oraz nieprzypisane urządzenia.
- **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.
- **Przypisz zadanie do grupy administracyjnej**. W tym przypadku zadanie jest przypisywane do urządzeń znajdujących się we wcześniej utworzonej grupie administracyjnej.

Aby zdalna instalacja została poprawnie przeprowadzona na urządzeniu, na którym nie został zainstalowany Agent sieciowy, muszą być otwarte następujące porty: a) TCP 139 i 445; b) UDP 137 i 138. Domyślnie porty te są otwarte dla wszystkich urządzeń z domeny. Porty te są otwierane automatycznie przy użyciu narzędzia do przygotowania zdalnej instalacji.

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 **Zasoby (urządzenia)** → **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.

- 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.

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 jednoczesnych pobierań** 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*.

- 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 Windows 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 Windows.

- **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.

  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.

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, aby zainstalować aplikację.

     Aby określić konto użytkownika, z poziomu którego zostanie uruchomiony instalator aplikacji, kliknij przycisk **Dodaj**, wybierz **Konto lokalne**, a następnie określ poświadczenia konta użytkownika.

     Możesz określić kilka kont użytkowników, na przykład, jeśli żadne z nich nie ma wszystkich wymaganych uprawnień na wszystkich urządzeniach, dla których definiujesz zadanie. W tym przypadku wszystkie dodane konta są używane do uruchomienia zadania, zaczynając od góry.

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.

Instalowanie aplikacji na podrzędnych Serwerach administracyjnych

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.

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 **Zasoby (urządzenia)** → **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.

Zastępowanie aplikacji zabezpieczających firm trzecich

Instalacja aplikacji zabezpieczających Kaspersky poprzez 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.

Instrukcje: Usuwanie niekompatybilnych aplikacji przed instalacją

Dezinstalowanie niekompatybilnych aplikacji przy użyciu dedykowanego zadania

Aby usunąć niekompatybilne aplikacje, użyj zadania **Zdalna dezinstalacja aplikacji**. Zadanie to powinno być uruchomione 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.

Dostępne instrukcje: Tworzenie zadania

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 **Zasoby (urządzenia)** → **Zadania**.

2. Kliknij **Dodaj**.

Zostanie uruchomiony Kreator tworzenia nowego zadania. Przejdź przez kroki kreatora, korzystając z przycisku **Next**.

3. Dla aplikacji Kaspersky Security Center wybierz typ zadania **Zdalna dezinstalacja aplikacji**.

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. 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.

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.

7. 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 Windows 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 Windows.

8. 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).

- **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.

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.

9. 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*.

  Określ konto użytkownika, z poziomu którego zostanie uruchomiony instalator aplikacji. Kliknij przycisk **Dodaj**, wybierz **Konto**, a następnie określ poświadczenia konta użytkownika.

  Możesz określić kilka kont użytkowników, na przykład, jeśli żadne z nich nie ma wszystkich wymaganych uprawnień na wszystkich urządzeniach, dla których definiujesz zadanie. W tym przypadku wszystkie dodane konta są używane do uruchomienia zadania, zaczynając od góry.

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**.

    Zadanie zostanie utworzone i będzie wyświetlane na liście zadań.

12. Kliknij nazwę utworzonego zadania, aby otworzyć okno właściwości zadania.

13. W oknie właściwości zadania określ ogólne ustawienia zadania.

14. Kliknij przycisk **Zapisz**.

15. Uruchom zadanie ręcznie lub poczekaj na jego uruchomienie zgodne z terminarzem określonym w ustawieniach zadania.

Po zakończeniu zadania zdalnej dezinstalacji, wybrana aplikacja zostanie usunięta z wybranych urządzeń.

Przygotowanie urządzenia z systemem SUSE Linux Enterprise Server 15 do instalacji Agenta sieciowego

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 opcję `i`, aby zignorować ostrzeżenie.

Po przygotowaniu urządzenia SUSE Linux Enterprise Server 15 wdróż i zainstaluj Agenta sieciowego.

Przygotowanie urządzenia z systemem Windows do zdalnej instalacji. Narzędzie Riprep

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. Należy włączyć urządzenie i ponownie uruchomić 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 rozwiązać problemy, które wystąpiły w trakcie instalowania aplikacji na urządzeniu klienckim bez zainstalowanego Agenta sieciowego, możesz użyć narzędzia do przygotowywania urządzeń do zdalnej instalacji (riprep).

Użyj narzędzia Riprep, aby przygotować urządzenie z systemem Windows do zdalnej instalacji. Aby pobrać narzędzie, kliknij ten link: https://media.kaspersky.com/utilities/CorporateUtilities/KSC/riprep.exe

Narzędzie do przygotowywania urządzenia do zdalnej instalacji nie zadziała na systemie Microsoft Windows XP Home Edition.

Przygotowanie urządzenia z systemem Windows do zdalnej instalacji w trybie interaktywnym

Aby przygotować urządzenie z systemem Windows do zdalnej instalacji w trybie interaktywnym:

1. Uruchom plik riprep.exe na urządzeniu klienckim.
2. W oknie głównym narzędzia przygotowującego do zdalnej instalacji wybierz następujące opcje:
   - **Wyłącz proste udostępnianie plików**
   - **Uruchom usługę Serwera administracyjnego**
   - **Otwórz porty**
   - **Dodaj konto**
   - **Wyłącz kontrolę konta użytkownika (UAC)** (opcja ta jest dostępna tylko dla urządzeń z systemami Microsoft Windows Vista, Microsoft Windows 7 oraz Microsoft Windows Server 2008)
3. Kliknij przycisk **Uruchom**.

   Etapy przygotowywania urządzenia do zdalnej instalacji będą wyświetlane w dolnej części okna głównego narzędzia.

Jeśli zaznaczyłeś opcję **Dodaj konto**, po utworzeniu konta zostanie wyświetlony monit o wprowadzenie nazwy konta i hasła. Spowoduje to utworzenie konta lokalnego należącego do grupy lokalnych administratorów.

Jeśli wybrałeś opcję **Wyłącz kontrolę konta użytkownika (UAC)**, próba wyłączenia Kontroli konta użytkownika zostanie wykonana nawet wtedy, gdy była ona wyłączona przed uruchomieniem narzędzia. Po wyłączeniu Kontroli konta użytkownika, zostaniesz poproszony o ponowne uruchomienie urządzenia.

Przygotowanie urządzenia z systemem Windows do zdalnej instalacji w trybie cichym

W celu przygotowania urządzenia z systemem Windows do zdalnej instalacji w trybie cichym:

Uruchom plik riprep.exe na urządzeniu klienckim z poziomu wiersza poleceń, podając wymagany zestaw przełączników.

Składnia wiersza poleceń narzędzia:

```
riprep.exe [-silent] [-cfg CONFIG_FILE] [-tl traceLevel]
```

Opisy przełączników:

- `-silent` — uruchamia narzędzie w trybie cichym.
- `-cfg CONFIG_FILE` — określa konfigurację narzędzia, gdzie `CONFIG_FILE` to ścieżka dostępu do pliku konfiguracyjnego (pliku posiadającego rozszerzenie .ini).
- `-tl traceLevel` — określa poziom śledzenia, gdzie `traceLevel` to cyfra od 0 do 5. Jeśli nie określono żadnego przełącznika, używana jest wartość 0.

Uruchamiając narzędzie w trybie cichym, możesz wykonać następujące zadania:

- Wyłączyć proste udostępnianie plików
- Uruchomić usługę serwera na urządzeniu klienckim
- Otworzyć porty
- Utworzyć konto lokalne
- Wyłączyć kontrolę konta użytkownika (UAC)

Możesz określić parametry dla przygotowywania urządzenia do zdalnej instalacji w pliku konfiguracyjnym podanym w przełączniku `-cfg`. W celu zdefiniowania tych parametrów, do pliku konfiguracyjnego należy dodać następujące informacje:

- W sekcji `Common` określ, które zadania mają zostać wykonane:
  - `DisableSFS` — wyłącza proste udostępnianie plików (0—zadanie jest wyłączone; 1—zadanie jest włączone).
  - `StartServer` — uruchamia usługę serwera (0—zadanie jest wyłączone; 1—zadanie jest włączone).
  - `OpenFirewallPorts` — otwiera potrzebne porty (0—zadanie jest wyłączone; 1—zadanie jest włączone).
  - `DisableUAC` — wyłącza Kontrolę konta użytkownika (UAC) (0—zadanie jest wyłączone; 1—zadanie jest włączone).
  - `RebootType` — określa zachowanie w przypadku, gdy konieczne jest ponowne uruchomienie urządzenia, a UAC jest wyłączona. Możesz użyć następujących wartości:
    - 0—nigdy nie uruchamiaj urządzenia ponownie.
    - 1—uruchom urządzenie ponownie, jeśli UAC była włączona przed uruchomieniem narzędzia.
    - 2—wymuś ponowne uruchomienie, jeśli UAC była włączona przed uruchomieniem narzędzia.
    - 4—zawsze uruchamiaj urządzenie ponownie.
    - 5—zawsze wymuszaj ponowne uruchomienie urządzenia.
- W sekcji `UserAccount` określ nazwę konta (`user`) i jego hasło (`Pwd`).

Przykładowa zawartość pliku konfiguracyjnego:

```
[Common]
DisableSFS=0
StartServer=1
OpenFirewallPorts=1
[UserAccount]
user=Admin
Pwd=Pass123
```

Po zakończeniu pracy narzędzia, w jego folderze zostaną utworzone następujące pliki:

- riprep.txt—raport z działania, w którym znajdują się wszystkie etapy działania narzędzia wraz z powodami takich działań.
- riprep.log—plik śledzenia (jest on tworzony, gdy poziom śledzenia został ustawiony powyżej 0).

Licencjonowanie

Ta sekcja zawiera następujące informacje:

- Ogólne pojęcia związane z licencjonowaniem oprogramowania Kaspersky Security Center Linux
- Instrukcje dotyczące zarządzania licencjami zarządzanych aplikacji Kaspersky

Informacje dotyczące licencjonowania oprogramowania Kaspersky Security Center Linux

Ta sekcja zawiera opis dotyczący ogólnych zasad związanych z licencjonowaniem Kaspersky Security Center Linux.

Informacje o Umowie licencyjnej

Umowa licencyjna 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.

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, 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 licencji to dokument, który otrzymujesz wraz z plikiem klucza lub kodem aktywacyjnym.

Certyfikat licencji zawiera następujące informacje o dostarczonej licencji:

- Klucz licencyjny lub numer zamówienia
- Informacje o użytkowniku, który otrzymał licencję
- Informacje o aplikacji, która może być aktywowana za pomocą zakupionej licencji
- Ograniczenie liczby urządzeń objętych zakupioną licencją
- Data rozpoczęcia okresu ważności licencji
- Data wygaśnięcia licencji lub okres ważności 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 jest dostarczany jako część aplikacji Kaspersky do ochrony sieci korporacyjnych. Można ją również pobrać ze strony firmy Kaspersky.

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 rozsyłanie 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.

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 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
- Aktywowanie aplikacji firmy Kaspersky na urządzeniach
- Zarządzanie kontami użytkowników
- Przeglądanie informacji o działaniu aplikacji firmy Kaspersky na urządzeniach
- Przeglądanie raportów

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 lub Samba lub poprzez skanowanie przedziałów czasu IP. Serwer administracyjny gromadzi dane niezależnie lub pobiera dane z Agenta sieciowego.
- Informacje z Active Directory i Samby o jednostkach organizacyjnych, domenach, użytkownikach i grupach. 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, 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: 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 lokalizacji, 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.

- 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.

- 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).

  - Informacje o oprogramowaniu zainstalowanym na zarządzanych urządzeniach (Rejestr oprogramowania). Oprogramowanie można porównać z informacjami o plikach wykonywalnych wykrytych na urządzeniach przez funkcję Kontroli aplikacji.

- 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.

- Informacje o zaszyfrowanych urządzeniach z systemem Windows i stanie szyfrowania. Zarządzana aplikacja przesyła dane z urządzenia na Serwer administracyjny poprzez Agenta sieciowego.

- Szczegóły dotyczące błędów szyfrowania danych na urządzeniach z systemem Windows, wykonane przy użyciu funkcji Szyfrowanie danych z aplikacji firmy Kaspersky. 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 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 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.

- Szczegóły wprowadzonych kodów aktywacyjnych oraz plików kluczy. Użytkownik wprowadza dane w Konsoli administracyjnej lub w interfejsie konsoli Kaspersky Security Center Web Console.

- Konta użytkowników: nazwa, opis, imię i nazwisko, adres e-mail, główny numer telefonu i hasło. 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.

- 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 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 Open API.

- 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.

Wymienione dane są przechowywane w bazie danych Serwera administracyjnego. Nazwy użytkowników i hasła 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 Konsoli administracyjnej lub konsoli 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 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 licencjonowane funkcje, aby korzystać z dodatkowej funkcjonalności Kaspersky Security Center Linux. Istnieją dwa sposoby wykonania tego zadania: użyj Kreatora wstępnej konfiguracji Serwera administracyjnego lub właściwości Serwera administracyjnego.

Aktywowanie licencjonowanych funkcji Kaspersky Security Center Linux:

1. W menu głównym kliknij ikonę ustawień ( ) obok nazwy żądanego 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 rozsyłanie
- Pakiet instalacyjny zarządzanej aplikacji
- Zadanie dodawania klucza licencyjnego 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 zapasowy klucz 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 rozsyłanie

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 rozesłany na urządzenie, ponieważ automatyczne rozesłanie 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 zdalną instalacją, 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

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

Rozesłanie 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 zdalną instalacją, 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** → **Licencjonowanie** → **Licencje 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.
   - **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 dodawania klucza.

Przed wdrożeniem należy dodać klucz licencyjny do repozytorium Serwera administracyjnego.

Aby rozesłać klucz licencyjny do urządzeń klienckich za pomocą zadania dodawania klucza:

1. W menu głównym przejdź do **Zasoby (urządzenia)** → **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 **Dodaj klucz**.
5. W polu **Nazwa zadania** podaj nazwę nowego zadania.
6. Wybierz urządzenia, do których zadanie zostanie przypisane.

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 dodawania klucza.

   - 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.

10. W kroku **Informacje o licencji** kreatora włącz opcję **Użyj jako klucza rezerwowego**, jeśli chcesz używać tego klucza jako klucza rezerwowego.

    W takim przypadku klucz rezerwowy zostaje zastosowany po wygaśnięciu klucza aktywnego.

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.

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 Kaspersky**.
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**.
4. Kliknij przycisk **Zapisz**.

   Klucz licencyjny zostanie automatycznie rozesłany 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.

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 później ręcznie rozpowszechniać klucz licencyjny.

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 Kaspersky**.

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 Kaspersky**.
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

W celu sprawdzenia, które klucze licencyjne zostały rozesłane na określone urządzenie klienckie:

1. W menu głównym przejdź do **Zasoby (urządzenia)** → **Zarządzane 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 ograniczeń licencyjnych

Kaspersky Security Center Linux pozwala uzyskać informacje o zdarzeniach, gdy pewne ograniczenia licencyjne zostaną przekroczone przez aplikacje firmy Kaspersky zainstalowane na urządzeniach klienckich.

Priorytet takich zdarzeń, gdy ograniczenia licencyjne zostaną przekroczone, jest definiowany zgodnie z następującymi regułami:

- Jeśli liczba aktualnie używanych jednostek objętych jedną licencją mieści się w 90% do 100% całkowitej liczby jednostek objętych licencją, publikowane zdarzenie posiada poziom istotności **Informacja**.
- Jeśli liczba aktualnie używanych jednostek objętych jedną licencją mieści się w 100% do 110% całkowitej liczby jednostek objętych licencją, publikowane zdarzenie posiada poziom istotności **Ostrzeżenie**.
- Jeśli liczba aktualnie używanych jednostek objętych jedną licencją przekracza 110% całkowitej liczby jednostek objętych licencją, publikowane zdarzenie posiada poziom istotności **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 aplikacji kliknij ikonę ustawień ( ) obok 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 Kaspersky**.

3. Wybierz wymagany plik klucza lub kod aktywacyjny, a następnie kliknij przycisk **Usuń**.

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 dla każdej zarządzanej aplikacji firmy Kaspersky. Przed wycofaniem zgody z Umową licencyjną należy odinstalować wybraną aplikację.

W celu anulowania Umowy licencyjnej 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, zaakceptowanych po utworzeniu pakietów instalacyjnych, w momencie bezproblemowej instalacji aktualizacji lub po zdalnym zainstalowaniu Kaspersky Security for Mobile.

2. Z listy wybierz Umowę licencyjną, którą chcesz anulować.

   Możesz sprawdzić następujące właściwości Umowy licencyjnej:

   - Datę zaakceptowania Umowy licencyjnej
   - Nazwę użytkownika, który zaakceptował Umowę licencyjną

3. Kliknij datę zaakceptowania dowolnej Umowy licencyjnej, aby otworzyć jej okno właściwości wyświetlające następujące dane:

   - Nazwę użytkownika, który zaakceptował Umowę licencyjną
   - Datę zaakceptowania Umowy licencyjnej
   - Unikatowy identyfikator (UID) Umowy licencyjnej

- Pełną treść Umowy licencyjnej
- Listę obiektów (pakiety instalacyjne, aktualizacje typu seamless, aplikacje mobilne) powiązanych z Umową licencyjną oraz ich odpowiednie nazwy i typy

4. W lewej części okna właściwości Umowy licencyjnej kliknij przycisk **Odrzuć Umowę licencyjną**.

   Jeśli istnieją jakiekolwiek obiekty (pakiety instalacyjne i ich odpowiednie zadania), które uniemożliwiają wycofanie Umowy licencyjnej, 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.

5. Kliknij przycisk, aby potwierdzić wycofanie.

   Umowa licencyjna zostanie wycofana. Nie jest już wyświetlana na liście Umów licencyjnych w sekcji **Umowy licencyjne użytkownika końcowego**. Okno właściwości Umowy licencyjnej 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 Kaspersky**.
   - W oknie głównym przejdź do **Monitorowanie i raportowanie** → **Pulpit nawigacyjny**, a następnie kliknij odnośnik **Zobacz wygasające licencje** obok powiadomienia.

   Zostanie otwarte okno **Licencje Kaspersky**, 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**:
  - Profil Kaspersky Endpoint Security
  - Grupowe zadanie aktualizacji Kaspersky Endpoint Security
  - Profil Agenta sieciowego

Etapy

Konfigurowanie ochrony sieci odbywa się w etapach:

1. **Konfiguracja i przesyłanie profili 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).

   Jak to zrobić: Konfigurowanie grupowego zadania aktualizacji Kaspersky Endpoint Security

   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 bezpieczeństwa aplikacji 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 określony profil aplikacji dla każdej grupy administracyjnej, a następnie utworzyć profile zasad dla jednej lub kilku ról użytkownika Twojej firmy. W tym przypadku profile i profile zasad są stosowane w następującej kolejności:

1. Zostaną zastosowane profile utworzone dla zarządzania ochroną skoncentrowaną na urządzeniu.
2. Są one modyfikowane przez profile zasad zgodnie z priorytetami profili zasad.

3. Profile są modyfikowane przez profile zasad skojarzone z rolami użytkownika.

Konfiguracja i przydzielanie profili: Metoda skoncentrowana na urządzeniu

Po zakończeniu tego scenariusza, aplikacje zostaną skonfigurowane na wszystkich zarządzanych urządzeniach zgodnie z profilami 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 profili aplikacji**

   Skonfiguruj ustawienia dla aplikacji firmy Kaspersky, zainstalowanych na zarządzanych urządzeniach poprzez utworzenie profilu dla każdej aplikacji. Zestaw profili zostanie przesłany na urządzenia klienckie.

   Podczas konfigurowania ochrony sieci w kreatorze szybkiego startu Kaspersky Security Center Linux tworzy domyślną politykę 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 nowego profilu dla tej aplikacji.

   Jeśli masz hierarchiczną strukturę kilku Serwerów administracyjnych i/lub grup administracyjnych, domyślnie podrzędne Serwery administracyjne i potomne grupy administracyjne dziedziczą zasady z głównego Serwera administracyjnego. Możesz wymusić dziedziczenie przez grupy potomne 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 profilu nadrzędnym. Pozostałe niezablokowane ustawienia będą dostępne do modyfikacji w profilach podrzędnych. Utworzona hierarchia zasad umożliwi efektywne zarządzanie urządzeniami w grupach administracyjnych.

   Dostępne instrukcje: Tworzenie profilu

2. **Tworzenie profili zasad (opcjonalnie)**

   Jeśli chcesz, żeby urządzenia w jednej grupie administracyjnej były uruchamiane z różnymi ustawieniami profilu, utwórz profile zasad dla tych urządzeń. Profil zasad jest to inaczej podzbiór ustawień profilu. Ten podzbiór jest stosowany na urządzeniach docelowych wraz z profilem i uzupełnia go zgodnie z określonym warunkiem zwanym *warunkiem aktywacji profilu*. Profile mogą zawierać tylko ustawienia różniące się od „podstawowego” profilu, który jest aktywny 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 profili i profili zasad na zarządzane urządzenia**

   Domyślnie Serwer administracyjny automatycznie synchronizuje się z zarządzanymi urządzeniami co 15 minut. Podczas synchronizacji nowe lub zmienione profile 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 profili i profili zasad do zainstalowanych aplikacji Kaspersky.

   Możesz sprawdzić, czy profile 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 profili.

Skonfigurowane profile i profile zasad aplikacji zostaną automatycznie zastosowane do nowych urządzeń dodanych do grup administracyjnych.

Konfiguracja i przydzielanie profili: 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 profilami 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 profili aplikacji**

   Skonfiguruj ustawienia dla aplikacji firmy Kaspersky, zainstalowanych na zarządzanych urządzeniach poprzez utworzenie profilu dla każdej aplikacji. Zestaw profili zostanie przesłany na urządzenia klienckie.

   Jeśli konfigurujesz ochronę swojej sieci w kreatorze wstępnej konfiguracji, Kaspersky Security Center Linux tworzy domyślny profil dla Kaspersky Endpoint Security. Jeśli zakończyłeś proces konfiguracji przy użyciu tego kreatora, nie musisz tworzyć nowego profilu dla tej aplikacji.

   Jeśli masz hierarchiczną strukturę kilku Serwerów administracyjnych i/lub grup administracyjnych, domyślnie podrzędne Serwery administracyjne i potomne grupy administracyjne dziedziczą zasady z głównego Serwera administracyjnego. Możesz wymusić dziedziczenie przez grupy potomne 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 profilu nadrzędnym. Pozostałe niezablokowane ustawienia będą dostępne do modyfikacji w profilach podrzędnych. Utworzona hierarchia profili umożliwi efektywne zarządzanie urządzeniami w grupach administracyjnych.

   Dostępne instrukcje: Tworzenie profilu

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 potomnych.

   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 profili 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 profile 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 profili i profili zasad do zainstalowanych aplikacji Kaspersky.

Możesz sprawdzić, czy profile 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 profili 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 profile i profile zasad aplikacji zostaną automatycznie zastosowane do urządzeń tego użytkownika.

Profile i profile zasad

W Kaspersky Security Center Web Console możesz tworzyć zasady dla aplikacji Kaspersky. Ta sekcja opisuje profile 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 zbiorów 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
Nie zdefiniowano	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*.
Wymuś	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 profili

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 profil dla grupy nadrzędnej jest też zwany *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 profili

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).

- 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).

- 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 profilami

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 **Zasoby (urządzenia)** → **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 **Zasoby (urządzenia)** → **Profile zasad**.

2. Kliknij **Dodaj**.

   Zostanie otwarte okno **Wybierz aplikację**.

3. Wybierz aplikację, dla której chcesz utworzyć zasadę.

4. Kliknij **Dalej**.

   Zostanie otwarte okno ustawień nowej zasady na zakładce **Ogólne**.

5. Jeśli chcesz, zmień domyślną nazwę, domyślny stan oraz domyślne ustawienia dziedziczenia zasady.

6. 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.

7. 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.

8. Kliknij **Zapisz**, aby zapisać zasadę.

Zasada zostanie wyświetlona na liście zasad.

Ogólne ustawienia zasady

Ogólne

Na zakładce **Ogólne** możesz zmodyfikować stan profilu oraz określić dziedziczenie ustawień profilu:

- 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 profilu 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 systemu**

- **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**.

Historia rewizji

Zakładka **Historia rewizji** umożliwia przeglądanie listy rewizji profilu i wycofanie zmian wprowadzonych do profilu (jeśli to konieczne).

Modyfikowanie zasady

W celu zmodyfikowania zasady:

1. W menu głównym przejdź do **Zasoby (urządzenia)** → **Profile zasad**.
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**.

Zmiany wprowadzone w zasadzie zostaną zapisane we właściwościach zasady i pojawią się w sekcji **Historia rewizji**.

Włączanie i wyłączanie opcji dziedziczenia zasady

Aby włączyć lub wyłączyć opcję dziedziczenia w zasadzie:

1. Otwórz wymaganą zasadę.
2. Otwórz zakładkę **Ogólne**.
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 żadnego profilu potomnego. 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.
4. Kliknij przycisk **Zapisz**, aby zapisać zmiany, lub kliknij przycisk **Anuluj**, aby odrzucić zmiany.

Domyślnie, opcja **Dziedzicz ustawienia z zasady nadrzędnej** jest włączona dla nowego profilu.

Jeśli zasada zawiera profile, wszystkie zasady podrzędne dziedziczą te profile.

Kopiowanie zasady

Możesz skopiować profile z jednej grupy administracyjnej do innej.

W celu skopiowania profilu do innej grupy administracyjnej:

1. W menu głównym przejdź do **Zasoby (urządzenia)** → **Profile zasad**.
2. Zaznacz pole obok profilu (profili), który (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 profil (profile).
5. W dolnej części okna kliknij przycisk **Kopiuj**.
6. Kliknij **OK**, aby potwierdzić działanie.

Profil (profile) zostanie skopiowany do grupy docelowej ze wszystkimi swoimi zasadami. Stan każdego skopiowanego profilu w grupie docelowej będzie **Nieaktywny**. W dowolnym momencie możesz zmienić stan na **Aktywny**.

Jeżeli profil z nazwą podobną do nazwy nowo przeniesionego profilu znajduje się już w grupie docelowej, do nazwy nowo przeniesionego profilu zostanie dodany przyrostek (<kolejny numer>), na przykład: (1).

Przenoszenie zasady

Możesz przenieść profile z jednej grupy administracyjnej do innej. Na przykład, chcesz usunąć grupę, ale chcesz używać jej profili dla innej grupy. W tym przypadku można przenieść profil ze starszej grupy do nowej zanim usuniesz starszą grupę.

W celu przeniesienia profilu do innej grupy administracyjnej:

1. W menu głównym przejdź do **Zasoby (urządzenia)** → **Profile zasad**.
2. Zaznacz pole obok profilu (profili), który (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 profil (profile).
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 profilu w grupie docelowej będzie **Nieaktywny**. W dowolnym momencie możesz zmienić stan na **Aktywny**.

   Jeśli profil jest dziedziczony z grupy źródłowej, pozostanie w grupie źródłowej. Zostanie skopiowany do grupy docelowej ze wszystkimi swoimi zasadami. Stan profilu w grupie docelowej będzie **Nieaktywny**. W dowolnym momencie możesz zmienić stan na **Aktywny**.

Jeżeli profil z nazwą podobną do nazwy nowo przeniesionego profilu znajduje się już w grupie docelowej, do nazwy nowo przeniesionego profilu zostanie dodany przyrostek (<kolejny numer>), na przykład: (1).

Eksportowanie profilu

Kaspersky Security Center Linux umożliwia zapisanie profilu, jego 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 profilu:

1. W menu głównym przejdź do **Zasoby (urządzenia)** → **Profile zasad**.
2. Zaznacz pole obok zasady, którą chcesz wyeliminować.

Nie można jednocześnie eksportować wielu zasad. Jeśli wybierzesz więcej niż jedną zasadę, przycisk **Eksportuj** będzie nieaktywny.

3. Kliknij przycisk **Eksportuj**.

4. W otwartym oknie **Zapisz jako** określ nazwę i ścieżkę dostępu pliku profilu. 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 profilu

Kaspersky Security Center Linux umożliwia importowanie profilu z pliku KLP. Plik KLP zawiera wyeksportowaną zasadę, jej ustawienia oraz profile zasad.

W celu zaimportowania profilu:

1. W menu głównym przejdź do **Zasoby (urządzenia)** → **Profile zasad**.

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 **Zasoby (urządzenia)** → **Zarządzane 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:
   - W menu głównym przejdź do **Zasoby (urządzenia)** → **Zarządzane urządzenia**, kliknij odnośnik ścieżki w polu **Bieżąca ścieżka** nad listą zarządzanych urządzeń, a następnie wybierz grupę administracyjną zawierającą urządzenia do synchronizacji.
   - Uruchom wybór urządzeń, aby przejrzeć listę urządzeń.
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 **Zasoby (urządzenia)** → **Zarządzane 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 profilu.

   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 **Zasoby (urządzenia)** → **Profile zasad**.
2. Zaznacz pole obok nazwy zasady, dla której chcesz przejrzeć stan dystrybucji na urządzeniach.
3. W wyświetlonym menu wybierz odnośnik **Dystrybucja**.

   Zostanie otwarte okno **Wyniki dystrybucji <nazwa 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 ustawień konta i wybierz **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.

Usuwanie zasady

Możesz usunąć profil, jeśli już go nie potrzebujesz. Możesz usunąć tylko ten profil, który nie jest dziedziczony w określonej grupie administracyjnej. Jeśli profil został odziedziczony, możesz go usunąć tylko w grupie wyższego poziomu, dla której został utworzony.

W celu usunięcia profilu:

1. W menu głównym przejdź do **Zasoby (urządzenia)** → **Profile zasad**.
2. Zaznacz pole obok profilu zasad, który chcesz usunąć, a następnie kliknij **Usuń**.

   Przycisk **Usuń** stanie się niedostępny (przyciemniony), jeśli wybierzesz profil dziedziczony.
3. Kliknij **OK**, aby potwierdzić działanie.

Profil jest usuwany ze wszystkimi swoimi zasadami.

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 i usuwaniu profilu zasad.

Przeglądanie profili zasad

W celu przejrzenia profili zasad:

1. W menu głównym przejdź do **Zasoby (urządzenia)** → **Profile zasad**.
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.

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.

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.

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 zasad możesz skopiować do tego samego profilu lub do profilu, który określiłeś.

5. Kliknij **Kopiuj**.

Profil zasad został skopiowany do wybranego profilu. 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.

     - Reguła dla połączenia Serwera administracyjnego jest aktywna na tym urządzeniu

       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.

Liczba dodatkowych okien w kreatorze zależy od ustawień wybranych w pierwszym kroku. Reguły aktywacji profili zasad można zmodyfikować w późniejszym czasie.

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 profil jest dziedziczony 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.

Ustawienia zasady Agenta sieciowego

W celu skonfigurowania zasady Agenta sieciowego:

1. W menu głównym przejdź do **Zasoby (urządzenia)** → **Profile zasad**.

2. Kliknij nazwę zasady Agenta sieciowego.

   Zostanie otwarte okno właściwości zasady Agenta sieciowego.

Weź pod uwagę, że dla urządzeń z systemem Linux i Windows dostępne są różne ustawienia.

Ogólne

Na tej zakładce możesz zmodyfikować stan zasady oraz określić dziedziczenie ustawień zasady:

- W sekcji **Stan zasady** możesz wybrać jeden z trybów zasady:

  - **Zasada aktywna**

    Jeśli wybrano tę opcję, zasada jest aktywna.

    Domyślnie opcja ta jest zaznaczona.

  - **Zasada nieaktywna**

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. Zdarzenia są rozsyłane zgodnie z priorytetem w następujących sekcjach na zakładce **Konfiguracja zdarzenia**:

- **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 wykrył 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 uaktualnień 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 lub zasady użytkownika mobilnego w momencie dostarczenia zasady na zarządzane urządzenie
  - Nazwę i pełną ścieżkę do grupy administracyjnej, która zawierała zarządzane urządzenie w momencie dostarczenia zasady na zarządzane urządzenie
  - Lista aktywnych profili zasad

    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.

  Domyślnie opcja ta jest wyłączona.

Repozytoria

W sekcji **Repozytoria** możesz wybrać typy obiektów, których szczegóły zostaną wysłane z Agenta sieciowego na Serwer administracyjny. Jeśli modyfikacja niektórych ustawień w tej sekcji jest zablokowana przez zasadę Agenta sieciowego, nie można ich modyfikować.

- 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.

- 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.

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 pulsem) na 15 minut dla 10 000 zarządzanych urządzeń.

  Jeśli okres synchronizacji wynosi mniej niż 15 minut, synchronizacja odbywa się co każde 15 minut. Jeśli okres synchronizacji jest ustawiony na 15 minut lub więcej, synchronizacja odbywa się w określonym przedziale synchronizacji.

- 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 systemu Windows

  Jeżeli ta opcja jest włączona, port UDP, niezbędny do pracy Agenta sieciowego, zostanie dodany do listy wykluczeń Zapory 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 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. Domyślny port UDP do nawiązywania połączenia z serwerem KSN Proxy to 15111.

- Numer portu UDP

W tym polu możesz wprowadzić numer portu UDP. Domyślny numer portu to 15000.

Używany jest system dziesiętny.

W podsekcji **Profile połączenia** możesz określić ustawienia lokalizacji sieciowej i włączyć tryb użytkownika mobilnego, gdy Serwer administracyjny nie jest dostępny. Ustawienia w sekcji **Profile połączenia** są dostępne tylko na urządzeniach działających pod kontrolą systemu Windows:

- 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

  Profile połączenia są obsługiwane tylko dla urządzeń działających pod kontrolą systemu Windows.

  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:

- 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.

- Zakresy IP

  Jeśli opcja jest włączona, punkt dystrybucji automatycznie przeszuka zakresy IP zgodnie z terminarzem skonfigurowanym po kliknięciu odnośnika **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.

- 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.

- **Nazwa użytkownika**
- **Hasło**

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

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 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. Domyślny port UDP do nawiązywania połączenia z serwerem KSN Proxy to 15111.

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 ponownym uruchamianiem

W sekcji **Zarządzanie ponownym uruchamianiem** możesz określić działanie, jakie zostanie wykonane, jeśli system operacyjny musi być uruchomiony ponownie, gdy korzystasz, instalujesz lub dezinstalujesz aplikację. Ustawienia w sekcji **Zarządzanie ponownym uruchamianiem** są dostępne tylko na urządzeniach działających pod kontrolą systemu Windows:

- 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.

  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.

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.

Porównanie funkcji Agenta sieciowego

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	✓	✓	–

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	✓	✓	✓
Punkt dystrybucji			
Przy użyciu punktu dystrybucji	✓	✓	✓
Automatyczne przypisywanie punktów dystrybucji	✓	✓ Bez korzystania z funkcji rozpoznawania lokalizacji w sieci (NLA).	✓ Bez korzystania z funkcji rozpoznawania lokalizacji w sieci (NLA).
Tryb offline pobierania uaktualnień	✓	✓	✓
Przeszukiwanie sieci	✓ • Przeszukiwanie zakresu IP • Przeszukiwanie kontrolera domeny	✓ • Przeszukiwanie zakresu IP • Przeszukiwanie Zeroconf • Przeszukiwanie kontrolera domeny (Microsoft Active Directory, Samba 4	–

		Active Directory)	
Uruchamianie usługi KSN proxy po stronie punktu dystrybucji	✓	✓	–
Pobieranie aktualizacji za pośrednictwem serwerów aktualizacji Kaspersky do repozytoriów punktów dystrybucji, które dystrybuują aktualizacje do zarządzanych urządzeń	✓	✓	– (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	✓	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	✓	✓	–
Informacje o aplikacjach innych firm			
Zdalne instalowanie aplikacji na urządzeniach	✓	–	–
Konfigurowanie aktualizacji systemu operacyjnego w zasadzie Agenta sieciowego	✓	–	–
Przeglądanie informacji o lukach w oprogramowaniu	✓	–	–
Skanowanie aplikacji w poszukiwaniu luk	✓	–	–
Aktualizacje oprogramowania	✓	–	–
Inwentaryzacja oprogramowania zainstalowanego na urządzeniach	✓	✓	–
Maszyny wirtualne			
Instalowanie Agenta	✓	✓	✓

sieciowego na maszynie wirtualnej			
Ustawienia optymalizacji dla infrastruktury pulpitu wirtualnego (VDI)	✓	✓	✓
Obsługa dynamicznych maszyn wirtualnych	✓	✓	✓
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	✓	✓	✓
Przełączanie Agenta sieciowego z jednego Serwera administracyjnego na inny (automatycznie według lokalizacji sieciowej)	✓	–	✓
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	✓	✓	✓

Porównanie ustawień Agenta sieciowego według systemów operacyjnych

Poniższa tabela pokazuje, które ustawienia 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**	–
Łączność → Sieć	✓	✓ Za wyjątkiem opcji **Otwórz porty dla Agenta sieciowego w Zaporze systemu Windows**.	✓
Łączność → Profile połączenia	✓	–	✓
Łączność → Terminarz połączeń	✓	✓	✓
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	✓	✓	✓

Ręczna konfiguracja zasady Kaspersky Endpoint Security

Ta sekcja zawiera zalecenia dotyczące konfigurowania profilu Kaspersky Endpoint Security. Możesz przeprowadzić konfigurację w oknie właściwości zasady. Podczas edytowania ustawienia kliknij ikonę kłódki po prawej stronie odpowiedniej grupy ustawień, aby zastosować określone wartości do stacji roboczej.

Konfigurowanie Kaspersky Security Network

Kaspersky Security Network (KSN) to infrastruktura usług w chmurze, która zawiera informacje o reputacji plików, zasobach sieciowych i oprogramowaniu. Kaspersky Security Network umożliwia Kaspersky Endpoint Security for Windows szybsze reagowanie na różnego rodzaju zagrożenia, zwiększa wydajność komponentów ochrony i zmniejsza prawdopodobieństwo fałszywych trafień. Więcej informacji na temat Kaspersky Security Network można znaleźć w Pomocy Kaspersky Endpoint Security for Windows.

W celu określenia zalecanych ustawień KSN:

1. W menu głównym przejdź do **Zasoby (urządzenia)** → **Profile zasad**.
2. Kliknij zasadę dla Kaspersky Endpoint Security for Windows.

   Zostanie otwarte okno właściwości wybranej zasady.
3. We właściwościach zasady przejdź do **Ustawienia aplikacji** → **Zaawansowana ochrona przed zagrożeniami** → **Kaspersky Security Network**.
4. Upewnij się, że opcja **Użyj KSN Proxy** jest włączona. Użyj tej opcji do redystrybucji i optymalizacji ruchu w sieci.

   > Jeśli korzystasz z zarządzanego wykrywania i reagowania , musisz włączyć opcję **KSN Proxy** dla punktu dystrybucji i włączyć rozszerzony tryb KSN .
5. [Opcjonalne] Włącz korzystanie z serwerów KSN, jeśli usługa KSN proxy jest niedostępna. Serwery KSN mogą znajdować się po stronie Kaspersky (jeśli używana jest KSN) lub po stronie firm trzecich (jeśli używana jest KPSN).
6. Kliknij **OK**.

Zostaną określone zalecane ustawienia KSN.

Sprawdzanie listy sieci chronionych przez Zaporę sieciową

Upewnij się, że Kaspersky Endpoint Security for Windows Firewall chroni wszystkie Twoje sieci. Domyślnie Zapora sieciowa chroni sieci z następującymi typami połączeń:

- **Sieć publiczna**. Aplikacje antywirusowe, zapory ogniowe czy filtry nie chronią urządzeń w takiej sieci.
- **Sieć lokalna**. Dostęp do plików i drukarek jest ograniczony dla urządzeń w tej sieci.

- **Zaufana sieć**. Urządzenia w takiej sieci są chronione przed atakami oraz nieautoryzowanym dostępem do plików i danych.

Jeśli skonfigurowano niestandardową sieć, upewnij się, że zapora sieciowa ją chroni. W tym celu sprawdź listę sieci we właściwościach Kaspersky Endpoint Security for Windows. Lista może nie zawierać wszystkich sieci.

Więcej informacji na temat Zapory sieciowej można znaleźć w Pomocy Kaspersky Endpoint Security for Windows.

W celu sprawdzenia listy sieci:

1. W menu głównym przejdź do **Zasoby (urządzenia)** → **Profile zasad**.
2. Kliknij zasadę dla Kaspersky Endpoint Security for Windows.

   Zostanie otwarte okno właściwości wybranej zasady.
3. We właściwościach zasady przejdź do **Ustawienia aplikacji** → **Podstawowa ochrona przed zagrożeniami** → **Zapora sieciowa**.
4. Pod sekcją **Dostępne sieci** kliknij odnośnik **Ustawienia sieci**.

   Zostanie otwarte okno **Połączenia sieciowe**. To okno będzie wyświetlało listę sieci.
5. Jeśli na liście brakuje sieci, dodaj ją.

Wyłączanie skanowania urządzeń sieciowych

Gdy Kaspersky Endpoint Security for Windows skanuje dyski sieciowe, może to spowodować ich znaczne obciążenie. Praktyczniejsze jest wykonywanie bezpośredniego skanowania na serwerach plików.

Możesz wyłączyć skanowanie dysków sieciowych we właściwościach Kaspersky Endpoint Security for Windows. Opis tych właściwości profilu znajduje się w Pomocy Kaspersky Endpoint Security for Windows.

W celu wyłączenia skanowania dysków sieciowych:

1. W menu głównym przejdź do **Zasoby (urządzenia)** → **Profile zasad**.
2. Kliknij zasadę dla Kaspersky Endpoint Security for Windows.

   Zostanie otwarte okno właściwości wybranej zasady.
3. We właściwościach zasady przejdź do **Ustawienia aplikacji** → **Podstawowa ochrona przed zagrożeniami** → **Ochrona plików**.
4. W sekcji **Obszar ochrony** wyłącz opcję **Wszystkie dyski sieciowe**.
5. Kliknij **OK**.

Skanowanie dysków sieciowych zostanie wyłączone.

Wykluczanie szczegółów oprogramowania z pamięci Serwera administracyjnego

Zalecamy, aby Serwer administracyjny nie zapisywał informacji o modułach oprogramowania uruchamianych na urządzeniach sieciowych. W rezultacie pamięć Serwera administracyjnego nie jest przepełniona.

Możesz wyłączyć zapisywanie tych informacji we właściwościach Kaspersky Endpoint Security for Windows.

W celu wyłączenia zapisywania informacji o zainstalowanych modułach oprogramowania:

1. W menu głównym przejdź do **Zasoby (urządzenia)** → **Profile zasad**.
2. Kliknij zasadę dla Kaspersky Endpoint Security for Windows.

   Zostanie otwarte okno właściwości wybranej zasady.
3. We właściwościach zasady przejdź do **Ustawienia aplikacji** → **Ustawienia ogólne** → **Raporty i pliki danych**.
4. Pod sekcją **Przesyłanie danych do Serwera administracyjnego** wyłącz pole **Informacje o uruchomionych aplikacjach**, jeśli wciąż jest włączone w zasadzie najwyższego poziomu.

   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).

Informacje o zainstalowanych modułach oprogramowania nie są już zapisywane w bazie danych Serwera administracyjnego.

Konfigurowanie dostępu do interfejsu Kaspersky Endpoint Security for Windows na stacjach roboczych

Jeśli ochrona antywirusowa w sieci organizacji musi być zarządzana w trybie scentralizowanym poprzez Kaspersky Security Center Linux, określ ustawienia interfejsu we właściwościach Kaspersky Endpoint Security for Windows, jak opisano poniżej. W rezultacie zapobiegniesz nieautoryzowanemu dostępowi do Kaspersky Endpoint Security for Windows na stacjach roboczych i zmianie ustawień Kaspersky Endpoint Security for Windows.

Opis tych właściwości profilu znajduje się w Pomocy Kaspersky Endpoint Security for Windows.

W celu określenia zalecanych ustawień interfejsu:

1. W menu głównym przejdź do **Zasoby (urządzenia)** → **Profile zasad**.
2. Kliknij zasadę dla Kaspersky Endpoint Security for Windows.

   Zostanie otwarte okno właściwości wybranej zasady.
3. We właściwościach zasady przejdź do **Ustawienia aplikacji** → **Ustawienia ogólne** → **Interfejs**.
4. Pod sekcją **Interakcja z użytkownikiem** wybierz opcję **Bez interfejsu**. To wyłącza wyświetlanie interfejsu użytkownika Kaspersky Endpoint Security for Windows na stacjach roboczych, więc ich użytkownicy nie mogą zmieniać ustawień Kaspersky Endpoint Security for Windows.

5. Pod sekcją **Ochrona hasłem** włącz przycisk przełącznika. Zmniejszy to ryzyko nieautoryzowanych lub niezamierzonych zmian w ustawieniach Kaspersky Endpoint Security for Windows na stacjach roboczych.

Zalecane ustawienia dla interfejsu Kaspersky Endpoint Security for Windows zostały określone.

Zapisywanie ważnych zdarzeń dot. zasad w bazie danych Serwera administracyjnego

Aby uniknąć przepełnienia bazy danych Serwera administracyjnego, zalecane jest zapisywanie tylko ważnych zdarzeń w bazie danych.

W celu skonfigurowania rejestracji ważnych zdarzeń w bazie danych Serwera administracyjnego:

1. W menu głównym przejdź do **Zasoby (urządzenia)** → **Profile zasad**.
2. Kliknij zasadę dla Kaspersky Endpoint Security for Windows.
   Zostanie otwarte okno właściwości wybranej zasady.
3. We właściwościach zasady otwórz zakładkę **Konfiguracja zdarzenia**.
4. W sekcji **Krytyczny** kliknij **Dodaj zdarzenie** i zaznacz pola tylko obok następujących zdarzeń:
   - *Uwaga! Sprawdź licencję*
   - *Automatyczne uruchamianie aplikacji jest wyłączone*
   - *Błąd aktywacji*
   - *Wykryto aktywne zagrożenie Należy uruchomić zaawansowane leczenie*
   - *Leczenie nie jest możliwe*
   - *Wykryto wcześniej otwarty niebezpieczny odnośnik*
   - *Proces został przerwany*
   - *Zablokowano aktywność sieciową*
   - *Wykryto atak sieciowy*
   - *Zablokowano uruchomienie aplikacji*
   - *Dostęp zabroniony (bazy lokalne)*
   - *Dostęp zabroniony (KSN)*
   - *Błąd aktualizacji lokalnej*
   - *Nie można uruchomić dwóch zadań jednocześnie*
   - *Błąd interakcji z Kaspersky Security Center*

- *Nie wszystkie komponenty zostały zaktualizowane*
- *Błąd zastosowania reguł szyfrowania/deszyfrowania pliku*
- *Błąd włączenia trybu przenośnego*
- *Błąd wyłączenia trybu przenośnego*
- *Nie można załadować modułu szyfrującego*
- *Nie można zastosować profilu*
- *Błąd zmiany komponentów aplikacji*

5. Kliknij **OK**.
6. W sekcji **Błąd funkcjonalny** kliknij **Dodaj zdarzenie** i zaznacz pole wyboru obok zdarzenia *Nieprawidłowe ustawienia zadania. Ustawienia nie zostały zastosowane*.
7. Kliknij **OK**.
8. W sekcji **Ostrzeżenie** kliknij **Dodaj zdarzenie** i zaznacz pola tylko obok następujących zdarzeń:
   - *Autoochrona jest wyłączona*
   - *Składniki ochrony są wyłączone*
   - *Nieprawidłowy klucz zapasowy*
   - *Wykryto legalne oprogramowanie, które może zostać użyte do uszkodzenia komputera lub danych osobowych (bazy lokalne)*
   - *Wykryto legalne oprogramowanie, które może zostać użyte do uszkodzenia komputera lub danych osobowych (KSN)*
   - *Usunięty obiekt*
   - *Wyleczony obiekt*
   - *Użytkownik zrezygnował z profilu szyfrowania*
   - *Plik został przywrócony z kwarantanny przez administratora na serwerze Kaspersky Anti Targeted Attack Platform*
   - *Plik został poddany kwarantannie przez administratora na serwerze Kaspersky Anti Targeted Attack Platform*
   - *Wiadomość do administratora o zakazie uruchamiania aplikacji*
   - *Wiadomość do administratora dotycząca zakazu dostępu do urządzenia*
   - *Wiadomość do administratora dotycząca zakazu dostępu do strony internetowej*
9. Kliknij **OK**.
10. W sekcji **Informacja** kliknij **Dodaj zdarzenie** i zaznacz pola tylko obok następujących zdarzeń:

- *Została utworzona kopia zapasowa obiektu*
- *Zablokowane uruchomienie aplikacji w trybie testowym*

11. Kliknij **OK**.

Zostanie skonfigurowana rejestracja ważnych zdarzeń w bazie danych Serwera administracyjnego.

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**.

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.

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 modułów 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 KSN z ich własnych komputerów. 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 **Ustawienia 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 lub uaktualniania 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. Jeżeli dostęp do serwerów za pomocą systemowego DNS nie jest możliwy, aplikacja korzysta z publicznych serwerów DNS. Jest to konieczne, aby zapewnić utrzymanie poziomu bezpieczeństwa zarządzanych urządzeń.

Urządzenia klienckie zarządzane przez Serwer administracyjny wchodzą w interakcję z KSN poprzez serwer KSN proxy. Serwer proxy KSN posiada następujące cechy:

- Urządzenia klienckie mogą wysyłać żądania do 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 **Ustawienia 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 aplikacji kliknij ikonę ustawienia ( ) obok nazwy żądanego Serwera administracyjnego.

   Zostanie otwarte okno właściwości Serwera administracyjnego.

2. Na zakładce **Ogólne** wybierz sekcję **Ustawienia KSN Proxy**.

3. Ustaw przycisk przełącznika w pozycji **Włącz KSN Proxy na Serwerze administracyjnym Włączono**.

   Dane są wysyłane z urządzeń klienckich do KSN zgodnie z profilem Kaspersky Endpoint Security, który jest aktywny 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. Profil Kaspersky Endpoint Security, aktywny na urządzeniach klienckich, określa, które dane będą wysyłane bezpośrednio z tych urządzeń do KSN (z pominięciem Kaspersky Security Center Linux).

4. Przełącz przycisk przełącznika na pozycję **Użyj Kaspersky Security Network Włączono**.

Jeśli ta opcja jest włączona, urządzenia klienckie będą wysyłać wyniki instalacji łat do Kaspersky. 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 **Ustawienia 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 Private KSN**. 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.

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 **Ustawienia 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 aplikacji kliknij ikonę ustawienia ( ) obok nazwy żądanego 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 KSN

W celu włączenia KSN:

1. W menu aplikacji kliknij ikonę ustawienia ( ) obok nazwy żądanego Serwera administracyjnego.

   Zostanie otwarte okno właściwości Serwera administracyjnego.
2. Na zakładce **Ogólne** wybierz sekcję **Ustawienia KSN Proxy**.
3. Ustaw przycisk przełącznika w pozycji **Włącz KSN Proxy na Serwerze administracyjnym Włączono**.

   Serwer KSN proxy zostanie włączony.
4. Przełącz przycisk przełącznika na pozycję **Użyj Kaspersky Security Network Włączono**.

   Usługa KSN zostanie włączona.

   Jeśli przycisk przełącznika jest włączony, urządzenia klienckie będą wysyłać wyniki instalacji poprawek do Kaspersky. Przed włączeniem tego przycisku przełącznika należy przeczytać i zaakceptować warunki Oświadczenia KSN.
5. Kliknij przycisk **Zapisz**.

W celu wyłączenia KSN:

1. W menu aplikacji kliknij ikonę ustawienia ( ) obok nazwy żądanego Serwera administracyjnego.

Zostanie otwarte okno właściwości Serwera administracyjnego.

2. Na zakładce **Ogólne** wybierz sekcję **Ustawienia KSN Proxy**.

3. Ustaw przycisk przełącznika w pozycji **Włącz KSN Proxy na Serwerze administracyjnym Wyłączono**, aby wyłączyć usługę KSN proxy lub ustawić przycisk przełącznika w pozycji **Użyj Kaspersky Security Network Wyłączono**.

   Jeśli jeden z tych przycisków przełączników jest wyłączony, urządzenia klienckie nie będą wysyłać wyników instalacji poprawek do Kaspersky.

   Jeśli korzystasz z sieci KPSN, ustaw przycisk przełącznika **Użyj Kaspersky Private Security Network Wyłączono**.

   Usługa KSN zostanie wyłączona.

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 aplikacji kliknij ikonę ustawienia ( ) obok nazwy żądanego Serwera administracyjnego.

   Zostanie otwarte okno właściwości Serwera administracyjnego.

2. Na zakładce **Ogólne** wybierz sekcję **Ustawienia 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 lub uaktualniania 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 aktualizacji lub uaktualnieniu Serwera administracyjnego zaktualizowane Oświadczenie KSN jest wyświetlane 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 punktu dystrybucji wyświetl listę uruchomionych procesów.
2. Na liście uruchomionych procesów sprawdź, czy proces `/opt/kaspersky/ksc64/sbin/ksnproxy` jest uruchomiony.

Jeśli proces `/opt/kaspersky/ksc64/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.

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.

- 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 **Zasoby (urządzenia)** → **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.

Ręczne uruchamianie zadania

Aplikacja jest uruchamiana zgodnie z ustawieniami terminarza, określonymi we właściwościach każdego zadania. Możesz ręcznie uruchomić zadanie w dowolnym momencie.

W celu ręcznego uruchomienia zadania:

1. W menu głównym przejdź do **Zasoby (urządzenia)** → **Zadania**.
2. Na liście zadań zaznacz pole obok zadania, które chcesz uruchomić.
3. Kliknij przycisk **Uruchom**.

   Zadanie zostanie uruchomione. Możesz sprawdzić stan zadania w kolumnie **Stan** lub klikając przycisk **Wynik**.

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 **Zasoby (urządzenia)** → **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.

    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:
  - **Ustawienia Zaplanowane uruchomienie**
    - Co N godzin

      Zadanie jest uruchamiane regularnie, w określonych przedziałach czasu, począwszy od określonego dnia i godziny.

      Domyślnie, zadanie jest uruchamiane co sześć 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 poniedziałek o godzinie zgodnej z bieżącym czasem systemowym.

- 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.

- Codziennie (czas letni nie jest obsługiwany)

Zadanie jest uruchamiane regularnie, w określonych przedziałach czasu. Ten terminarz nie obsługuje czasu letniego (DST). Oznacza to, że gdy zegar przeskoczy o jedną godzinę do przodu lub tyłu na początku lub końcu DST, aktualny czas uruchomienia zadania nie ulegnie zmianie.

Nie jest zalecane korzystanie z tego terminarza. Jest on potrzebny w celu zapewnienia wstecznej kompatybilności Kaspersky Security Center Linux.

Domyślnie, zadanie jest uruchamiane codziennie o godzinie zgodnej z bieżącym czasem systemowym.

- Co tydzień

Zadanie jest uruchamiane co tydzień, w określonym dniu i o określonej godzinie.

- 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 włączona.

- Co miesiąc, w określone dni wybranych tygodni

Zadanie jest uruchamiane regularnie, w określone dni każdego miesiąca i o określonej godzinie.

Domyślnie nie wybrano dni miesiąca; domyślny czas uruchomienia to 18:00:00.

- 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. Możesz wybrać sposób zakończenia poprzedniego zadania (pomyślnie lub z błędem), aby wyzwolić uruchomienie bieżącego zadania. Parametr ten działa tylko wtedy, gdy oba zadania są przypisane do tych samych urządzeń.

- 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.

  Jeżeli ta opcja jest wyłączona, na urządzeniach klienckich będą uruchamiane tylko zaplanowane zadania, a dla trybu **Ręcznie**, **Raz** i **Natychmiast** zadania będą 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 włączona.

- 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 losowego opóźnienia dla zadań uruchamianych w przedziale (min)

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.

- 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 podstawowym serwerze administracyjnym jest również stosowane na pomocniczych (drugorzędnych) serwerach administracyjnych (w tym wirtualnych). Jeżeli zadanie tego samego typu już istnieje na pomocniczym serwerze administracyjnym, oba zadania są stosowane na pomocniczym serwerze administracyjnym — istniejące i odziedziczone z podstawowego 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 (min) 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 (min)

  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 **Zasoby (urządzenia)** → **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.

W celu zaimportowania zadania:

1. W menu głównym przejdź do **Zasoby (urządzenia)** → **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.

   - **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 **Zasoby (urządzenia)** → **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 wskazanych urządzeń oraz zadań Serwera administracyjnego. Nie można przeglądać wyników wykonywania zadań lokalnych.

W celu przejrzenia wyników wykonania zadania:

1. W oknie właściwości zadania wybierz sekcję **Ogólne**.
2. Kliknij odnośnik **Wyniki**, aby otworzyć okno **Wyniki zadania**.

Znaczniki aplikacji

Ta sekcja opisuje znaczniki aplikacji oraz zawiera instrukcje ich tworzenia i modyfikowania oraz znakowania aplikacji firm trzecich.

Informacje o znacznikach aplikacji

Kaspersky Security Center Linux umożliwia znakowanie aplikacji firm trzecich (aplikacje utworzone przez producentów oprogramowania innych niż firma Kaspersky). 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 **Operacje** → **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 **Operacje** → **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 **Operacje** → **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 **Operacje** → **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 **Operacje** → **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.

Udzielanie dostępu offline urządzeniu zewnętrznemu, zablokowanemu przez Kontrolę urządzeń

W komponencie Kontrola urządzeń zasady Kaspersky Endpoint Security możesz zarządzać dostępem użytkownika do urządzeń zewnętrznych, które są instalowane na lub podłączane do urządzenia klienckiego (na przykład: dyski twarde, aparaty lub moduły Wi-Fi). To umożliwia ochronę urządzenia klienckiego przed infekcją, gdy podłączone są takie urządzenia zewnętrzne, oraz zapobiega utracie lub wyciekowi danych.

Jeśli chcesz udzielić tymczasowego dostępu do urządzenia zewnętrznego, zablokowanego przez Kontrolę urządzeń, ale nie jest możliwe dodanie urządzenia do listy zaufanych urządzeń, możesz udzielić tymczasowego dostępu offline do urządzenia zewnętrznego. Dostęp offline oznacza, że urządzenie klienckie nie ma dostępu do sieci.

Możesz przyznać dostęp w trybie offline do urządzenia zewnętrznego zablokowanego przez Kontrolę urządzeń tylko wtedy, gdy opcja **Zezwól na żądanie tymczasowego dostępu** jest włączona w ustawieniach Kaspersky Endpoint Security, w sekcji **Ustawienia aplikacji** → **Kontrola bezpieczeństwa** → **Kontrola urządzeń**.

Udzielanie dostępu offline urządzeniu zewnętrznemu, zablokowanemu przez Kontrolę urządzeń obejmuje następujące etapy:

1. W oknie dialogowym Kaspersky Endpoint Security użytkownik urządzenia, który chce mieć dostęp do zablokowanego urządzenia zewnętrznego, wygeneruj plik prośby o dostęp i wyślij go do administratora Kaspersky Security Center Linux.

2. Po otrzymaniu tego zgłoszeni, administrator Kaspersky Security Center Linux tworzy plik klucza dostępu i wysyła go do użytkownika.

3. W oknie dialogowym Kaspersky Endpoint Security użytkownik urządzenia aktywuje plik klucza dostępu i uzyskuje tymczasowy dostęp do urządzenia zewnętrznego.

W celu udzielenia tymczasowego dostępu do urządzenia zewnętrznego, zablokowanego przez Kontrolę urządzeń:

1. W menu głównym przejdź do **Zasoby (urządzenia)** → **Zarządzane urządzenia**.

   Zostanie wyświetlona lista zarządzanych urządzeń.

2. Na tej liście wybierz urządzenie użytkownika, który żąda dostępu do urządzenia zewnętrznego zablokowanego przez Kontrolę urządzeń.

   Możesz wybrać tylko jedno urządzenie.

3. Nad listą zarządzanych urządzeń kliknij ikonę, a następnie kliknij owalny przycisk (...) **Udziel dostępu do urządzenia w trybie offline**.

4. W otwartym oknie **Ustawienia aplikacji**, w sekcji **Kontrola urządzeń** kliknij przycisk **Przeglądaj**.

5. Wybierz plik żądania dostępu otrzymany od użytkownika, a następnie kliknij przycisk **Otwórz**. Plik powinien mieć format AKEY.

   Zostaną wyświetlone szczegóły dotyczące zablokowanego urządzenia, do którego o dostęp poprosił użytkownik.

6. Określ wartość ustawienia **Czas trwania dostępu**.

   To ustawienie definiuje długość czasu, na jaki udzielasz użytkownikowi dostępu do zablokowanego urządzenia. Domyślna wartość to wartość, która została określona przez użytkownika podczas tworzenia pliku żądania dostępu.

7. Określ wartość ustawienia **Okres aktywacji**.

   To ustawienie definiuje przedział czasu, w trakcie którego użytkownik może aktywować dostęp do zablokowanego urządzenia przy użyciu dostarczonego klucza dostępu.

8. Kliknij przycisk **Zapisz**.

9. W oknie, które zostanie otwarte, wybierz folder docelowy, w którym chcesz zapisać plik zawierający klucz dostępu do zablokowanego urządzenia.

10. Kliknij przycisk **Zapisz**.

W rezultacie, po wysłaniu do użytkownika pliku klucza dostępu i aktywowaniu go przez użytkownika w oknie dialogowym Kaspersky Endpoint Security, użytkownik posiada tymczasowy dostęp do zablokowanego urządzenia dla określonego przedziału czasu.

Użycie narzędzia klscflag do otwarcia portu 13291

Port 13291 na serwerze administracyjnym jest używany do odbierania połączeń z konsoli administracyjnej opartej na MMC. Na komputerach z systemem innym niż Windows ten port jest domyślnie zamknięty.

Jeśli chcesz umożliwić połączenie z konsolą administracyjną opartą na MMC lub używać narzędzi klakaut, możesz otworzyć ten port za pomocą narzędzia klscflag. Należy pamiętać, że funkcjonalność Konsoli administracyjnej opartej na MMC jest ograniczona, gdy jest ona połączona z Kaspersky Security Center Linux. Zalecamy, aby do połączenia z Kaspersky Security Center Linux użyć Kaspersky Security Center Web Console.

Narzędzie klscflag zmienia wartość parametru KLSRV_SP_SERVER_SSL_PORT_GUI_OPEN.

Zalecamy, aby do połączenia z Kaspersky Security Center Linux użyć Kaspersky Security Center Web Console.

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:

   - Pobrano i zainstalowano 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. 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 **Discovery & deployment** → **Unassigned devices**.

   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 Kaspersky Security Center Network Agent.

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 internetowa 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 **Monitoring & Reporting** → **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 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 umożliwia zarządzanie kontami użytkowników i grupami bezpieczeństwa. Aplikacja obsługuje dwa typy kont:

- Konta pracowników firmy. Serwer administracyjny pobiera dane kont tych użytkowników lokalnych podczas przeszukiwania sieci organizacji.
- Konta użytkowników wewnętrznych Kaspersky Security Center Linux. W portalu możesz tworzyć konta użytkowników wewnętrznych. Konta te są używane wyłącznie w 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 **Podtyp** odpowiednio na **Wewnętrzny** lub **Lokalny**.

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 drugorzędne 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 potomnych.

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.

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**.

Prawa dostępu do funkcji aplikacji

Obszar funkcjonalny	Uprawnienie	Akcja użytkownika: uprawnienia wymagane do wykonania akcji	Zadanie	Raport
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
Funkcje ogólne: **Uzyskuj dostęp do obiektów bez względu na ich listy ACL**	**Odczyt**	Uzyskaj dostęp do odczytu do wszystkich obiektów: **Odczyt**	Brak	Brak
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**	• „Pobierz aktualizacje do repozytorium serwera administracyjnego” • „Dostarczaj raporty” • „Roześlij pakiet instalacyjny” • „Zdalnie zainstaluj aplikację na podrzędnych Serwerach administracyjnych”	• „Raport o sta ochrony” • „Raport o zagrożeniach” • „Raport o najbardziej zainfekowany urządzeniach” • „Raport o sta antywirusowy baz danych” • „Raport o błę • „Raport o ata sieciowych”

		• Ustaw certyfikat niestandardowy protokołu Mobile (LWNGT): **Zapisz** • Uzyskaj listę sieci zdefiniowaną przez NLA: **Odczytaj** • Dodaj, zmodyfikuj lub usuń listę sieci zdefiniowaną przez NLA: **Wpisz** • Wyświetl listę kontroli dostępu grup: **Odczytaj** • Wyświetl dziennik systemu operacyjnego: **Przeczytaj**		• „Raport podsumowuja na temat zainstalowany aplikacji ochro obwodowej” • „Raport podsumowuja na temat typo zainstalowany aplikacji” • „Raport o użytkownikac zainfekowany urządzeń” • "Raport o incydentach związanych z bezpieczeńst • „Raport wyda • „Raport o aktywności punktów dystrybucji” • „Raport o podrzędnych Serwerach administracyj • „Raport zdarz Kontroli urząc • „Raport o zabronionych aplikacjach” • „Raport Kontr sieci” • "Raport o star szyfrowania zarządzanych urządzeń" • "Raport o star szyfrowania urządzeń pam masowej" • "Raport o prav dostępu do

				zaszyfrowany dysków" • "Raport o błęd podczas szyfrowania plików" • "Raport o zablokowanyr dostępie do zaszyfrowany plików" • „Raport o efektywnych uprawnieniacl użytkowników • „Raport dotyc uprawnień"
Funkcje ogólne: **Obiekty usunięte**	• **Odczyt** • **Wpisz**	• Wyświetl usunięte obiekty w Koszu: **Odczytaj** • Usuń obiekty z Kosza: **Wpisz**	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
Funkcje ogólne: **Operacje na Serwerze administracyjnym**	• **Odczyt** • **Wpisz** • **Wykonaj** • **Modyfikuj listy ACL obiektów**	• Określ porty Serwera administracyjnego dla połączenia agenta sieciowego: **Wpisz** • Określ porty Serwera proxy aktywacji	• „Tworzenie kopii zapasowych danych Serwera administracyjnego" • „Konserwacja baz danych"	Brak

	• **Wykonaj operacje na wyborach urządzeń**	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** • 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 dotyc użycia klucza licencyjnego p wirtualny serw administracyjn • „Raport o wer oprogramowa Kaspersky" • „Raport o niekompatybi aplikacjach" • „Raport o wer aktualizacji m oprogramowa Kaspersky" • „Raport wdraz ochrony"
Cechy ogólne: **Zarządzanie kluczami**	• **Eksportuj plik klucza** • **Wpisz**	• Eksportuj plik klucza: **Eksportuj plik klucza** • Zmodyfikuj ustawienia klucza licencyjnego Serwera administracyjnego: **Wpisz**	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
Funkcje ogólne:	**Skonfiguruj**	• Zarejestruj,	Brak	Brak

Hierarchia serwerów administracyjnych	**hierarchię Serwerów administracyjnych**	zaktualizuj lub usuń podrzędne Serwery administracyjne: **Skonfiguruj hierarchię Serwerów administracyjnych**		
Cechy ogólne: **Uprawnienia użytkownika**	**Modyfikuj listy ACL obiektów**	• Zmień właściwości Zabezpieczenia dowolnego obiektu: **Modyfikuj 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**	Brak	Brak
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**	Brak	Brak

		serwerami administracyjnymi • Przenieś wirtualny Serwer administracyjny do innej grupy: **Zarządzaj wirtualnymi serwerami administracyjnymi** • Ustaw uprawnienia do administracyjnego Serwera wirtualnego: **Zarządzaj wirtualnymi serwerami administracyjnymi**		
Funkcje ogólne: **Zarządzanie kluczami szyfrowania**	**Wpisz**	Zaimportuj klucze szyfrowania: **Wpisz**	Brak	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

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 i samodzielnie skonfigurować wymagane uprawnienia. 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 działania na wszystkich typach raportów, na wszystkie działania przeglądania, w tym przeglądanie usuniętych obiektów (nadaje uprawnienia **Odczyt** i **Zapisz** w obszarze **Usunięte obiekty**). Nie zezwala na pozostałe działania. Tę rolę można przypisać do osoby, która przeprowadza audyt w Twojej organizacji.
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.

Funkcje obszarów funkcjonalnych **Zarządzanie urządzeniami mobilnymi: Zarządzanie ogólne** i **Zarządzanie systemem** nie są dostępne w Kaspersky Security Center Linux. Użytkownik z rolami **Administrator / Operator zarządzania lukami i poprawkami** lub **Administrator / Operator zarządzania urządzeniami mobilnymi** ma dostęp tylko do uprawnień z funkcji **Ogólne**: **Podstawowy obszar funkcjonalny**.

Prawa dostępu do predefiniowanych ról użytkowników

Rola	Opis
Administrator serwera administracyjnego	Zezwala na następujące operacje w obszarach funkcjonalnych, w **Cechach ogólnych**: • **Podstawowa funkcjonalność** • **Przetwarzanie zdarzeń** • **Hierarchia Serwerów administracyjnych** • **Wirtualne Serwery administracyjne** Przyznaje uprawnienia do **Odczytu** i **Wpisania** w obszarze **Funkcje ogólne: obszar funkcjonalny zarządzania kluczami szyfrowania**.
Operator serwera administracyjnego	Przyznaje uprawnienia do **odczytu** i **wykonywania** we wszystkich następujących obszarach funkcjonalnych, w **Funkcjach ogólnych:** • **Podstawowa funkcjonalność** • **Wirtualne Serwery administracyjne**
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 następujące operacje w obszarach funkcjonalnych, w **Cechach ogólnych**: • **Podstawowa funkcjonalność** • **Zdalna instalacja oprogramowania Kaspersky**

	• **Zarządzanie kluczami licencyjnymi** Przyznaje uprawnienia do **odczytu** i **wykonywania** w obszarze funkcjonalnym **Funkcje ogólne: Wirtualne serwery administracyjne**.
Operator instalacji	Przyznaje uprawnienia do **odczytu** i **wykonywania** we wszystkich następujących obszarach funkcjonalnych, w **Funkcjach ogólnych:** • **Podstawowa funkcjonalność** • **Zdalna instalacja oprogramowania Kaspersky** (zapewnia również **Zarządzanie poprawkami Kaspersky Lab** bezpośrednio w tym obszarze) • **Wirtualne Serwery administracyjne**
Administrator Kaspersky Endpoint Security	Zezwala na wszystkie operacje w następujących obszarach funkcjonalnych: • **Cechy ogólne: Podstawowa funkcjonalność** • Obszar Kaspersky Endpoint Security zawierający wszystkie funkcje Przyznaje uprawnienia do **Odczytu** i **Wpisania** w obszarze **Funkcje ogólne: obszar funkcjonalny zarządzania kluczami szyfrowania**.
Operator Kaspersky Endpoint Security	Przyznaje uprawnienia do **odczytu** i **wykonywania** we wszystkich następujących obszarach funkcjonalnych: • **Cechy ogólne: Podstawowa funkcjonalność** • 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** Przyznaje uprawnienia do **Odczytu** i **Wpisania** w obszarze **Funkcje ogólne: obszar funkcjonalny zarządzania kluczami szyfrowania**.
Główny operator	Przyznaje prawa **odczytu** i **wykonywania** (w stosownych przypadkach) we wszystkich następujących obszarach funkcjonalnych: • **Funkcje ogólne**: • **Podstawowa funkcjonalność** • **Usunięte obiekty** • **Operacje na Serwerze administracyjnym** • **Wdrażanie oprogramowania Kaspersky Lab** • **Wirtualne Serwery administracyjne** • Obszar Kaspersky Endpoint Security zawierający wszystkie funkcje
Administrator	Pozwala na wszystkie operacje w obszarze **Funkcje ogólne: Podstawowa**

zarządzania urządzeniami mobilnymi	**funkcjonalność** w obszarze funkcjonalnym.
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 uprawnienia **Odczytu**, **Wpisania**, **Wykonywania**, **Zapisywania** plików z urządzeń na stacji roboczej administratora i **wykonywania działań dla wyborów urządzeń w obszarze funkcjonalnym Zarządzanie systemami: Łączność**. 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**. Ta funkcja nie jest obsługiwana w Kaspersky Security Center 11 i nowszej wersji.
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.

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:
   - **Zasoby (urządzenia) → Hierarchia grup**
   - **Zasoby (urządzenia) → Zadania**
   - **Monitorowanie i raportowanie → Raporty**
   - **Zasoby (urządzenia) → Wybory urządzeń**
   - **Monitorowanie i raportowanie → 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 uprawnień dostępu użytkownikom i grupom

Użytkownikom i grupom możesz nadać uprawnienia dostępu do używania różnych funkcji Serwera administracyjnego i aplikacji Kaspersky, dla których posiadasz wtyczki zarządzające, na przykład, Kaspersky Endpoint Security for Linux.

W celu przypisania uprawnień dostępu do użytkownika lub grupy użytkowników:

1. W menu głównym kliknij ikonę ustawienia ( ) obok nazwy żądanego 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 **Uprawnienia 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 (tylko dla Kaspersky Security Center Linux 11 lub nowszej wersji)
  - Uzyskuj dostęp do obiektów bez względu na ich listy ACL (tylko dla Kaspersky Security Center Linux 11 lub nowszej wersji)
  - Podstawowa funkcjonalność
  - Usunięte obiekty (tylko dla Kaspersky Security Center Linux 11 lub nowszej wersji)
  - Zarządzanie kluczami szyfrowania
  - Przetwarzanie zdarzeń
  - Operacje na Serwerze administracyjnym (tylko w oknie właściwości Serwera administracyjnego)
  - Zdalna instalacja oprogramowania Kaspersky
  - Zarządzanie kluczami licencyjnymi
  - Integracja aplikacji
  - Wymuszone zarządzanie raportami
  - Hierarchia Serwerów administracyjnych
  - Uprawnienia użytkownika
  - Wirtualne Serwery administracyjne
- Zarządzanie urządzeniami mobilnymi:
  - Ogólne
  - Portal Self Service Portal
- Zarządzanie poprawkami i lukami:
  - Łączność
  - Inwentaryzacja sprzętu
  - Kontrola dostępu do sieci
  - Nazwa systemu operacyjnego

- Instalacja zdalna
- 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.

Dodawanie konta użytkownika wewnętrznego

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 16 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 wprowadzony tajny klucz, kliknij i przytrzymaj przycisk **Pokaż**.

Liczba prób wprowadzenia hasła jest ograniczona. Domyślnie jest to 10 prób. Możesz zmienić dozwoloną liczbę prób wprowadzenia hasła, jak opisano to w sekcji „Zmienianie liczby dozwolonych prób wprowadzenia hasła".

Jeśli użytkownik wprowadzi nieprawidłowe hasło określoną liczbę razy, konto użytkownika zostanie zablokowane na jedną godzinę. Możesz odblokować konto użytkownika tylko poprzez zmianę hasła.

4. Kliknij **Zapisz**, aby zachować zmiany.

Nowe konto użytkownika zostanie dodane do listy użytkowników.

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

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:
   - **Opis**
   - **Pełna nazwa**
   - **Adres e-mail**

- **Główny numer telefonu**
- **Określ nowe hasło** dla połączenia użytkownika z Kaspersky Security Center Linux.

  Hasło musi być zgodne z następującymi zasadami:

  - Hasło musi zawierać od 8 do 16 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 i przytrzymaj przycisk **Pokaż**.

  > Liczba prób wprowadzenia hasła jest ograniczona. Domyślnie jest to 10 prób. Możesz zmienić dozwoloną liczbę prób; jednak ze względów bezpieczeństwa nie zalecamy zmniejszania tej liczby. Jeśli użytkownik wprowadzi nieprawidłowe hasło określoną liczbę razy, konto użytkownika zostanie zablokowane na jedną godzinę. Możesz odblokować konto użytkownika tylko poprzez zmianę hasła.

- Jeśli to konieczne, przesuń przełącznik na **Wyłączone**, aby zabronić użytkownikowi możliwość łączenia z aplikacją. Możesz wyłączyć konto, na przykład, gdy pracownik opuści teren firmy.

4. Na zakładce **Bezpieczeństwo uwierzytelniania** 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. Kliknij **Zapisz**, aby zachować zmiany.

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 potomnych.

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 Security for Mobile.

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 podstawowego 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 **Zasoby (urządzenia)** → **Zarządzane urządzenia**, klikając nazwę urządzenia, które chcesz przypisać, a następnie klikając odnośnik **Zarządzaj właścicielem 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 **Bezpieczeństwo uwierzytelniania**.

4. Na zakładce **Bezpieczeństwo uwierzytelniania** wybierz opcję **Żądaj uwierzytelnienia w celu sprawdzenia uprawnień do modyfikacji tego konta**, jeśli chcesz żądać poświadczeń 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. Kliknij przycisk **Zapisz**.

Weryfikacja dwuetapowa

Ta sekcja opisuje sposób korzystania z weryfikacji dwuetapowej do zmniejszenia ryzyka nieautoryzowanego dostępu do Kaspersky Security Center Web Console.

Scenariusz: konfigurowanie weryfikacji dwuetapowej dla wszystkich użytkowników

W tym scenariuszu opisano sposób włączenia weryfikacji dwuetapowej dla wszystkich użytkowników oraz sposób wykluczenia konta użytkowników z weryfikacji dwuetapowej. Jeśli nie włączyłeś weryfikacji dwuetapowej dla swojego konta przed włączeniem go dla innych użytkowników, aplikacja najpierw otworzy okno umożliwiające włączenie weryfikacji dwuetapowej dla Twojego konta. W tym scenariuszu opisano również sposób włączenia weryfikacji dwuetapowej na swoim koncie.

Jeśli włączyłeś weryfikację dwuetapową na swoim koncie, możesz przejść do etapu włączenia weryfikacji dwuetapowej dla wszystkich użytkowników.

Wymagania wstępne

Zanim zaczniesz:

- Upewnij się, że Twoje konto użytkownika ma uprawnienie Modyfikuj listy ACL obiektów w obszarze funkcjonalnym **Cechy ogólne: Uprawnienia użytkownika** służącym do modyfikacji ustawień zabezpieczeń dla kont innych użytkowników.

- Upewnij się, że inni użytkownicy Serwera administracyjnego zainstalowali aplikację uwierzytelniającą na swoich urządzeniach.

Etapy

Włączenie weryfikacji dwuetapowej dla wszystkich użytkowników przebiega etapami:

1. **Instalowanie aplikacji uwierzytelniającej na urządzeniu**

   Można zainstalować dowolną aplikację obsługującą algorytm czasowego hasła jednorazowego (TOTP), np:

   - Google Authenticator
   - Microsoft Authenticator
   - Bitrix24 OTP
   - Yandex Key
   - Avanpost Authenticator
   - Aladyn 2FA

   Aby sprawdzić, czy Kaspersky Security Center Linux obsługuje aplikację uwierzytelniającą, której chcesz użyć, włącz weryfikację dwuetapową 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.

2. **Synchronizacja czasu aplikacji uwierzytelniającej 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, korzystając z zewnętrznych źródeł czasu. W przeciwnym razie mogą wystąpić awarie podczas uwierzytelniania i aktywacji weryfikacji dwuetapowej.

3. **Włączenie weryfikacji dwuetapowej dla Twojego konta i otrzymanie tajnego klucza do Twojego konta**

   Po włączeniu weryfikacji dwuetapowej na koncie możesz włączyć weryfikację dwuetapową dla wszystkich użytkowników.

4. **Włączanie weryfikacji dwuetapowej dla wszystkich użytkowników**

   Użytkownicy z włączoną weryfikacją dwuetapową muszą jej używać do logowania się do Serwera administracyjnego.

5. **Uniemożliwienie nowym użytkownikom konfigurowania dla siebie weryfikacji dwuetapowej**

   Aby jeszcze bardziej poprawić bezpieczeństwo dostępu Kaspersky Security Center Web Console, możesz zabronić nowym użytkownikom konfigurowania dla siebie weryfikacji dwuetapowej.

6. **Edytowanie nazwy wystawcy kodu zabezpieczającego**

   Jeśli masz kilka Serwerów administracyjnych o podobnych nazwach, konieczna może być zmiana nazw wystawców kodów zabezpieczających w celu lepszego rozpoznawania różnych Serwerów administracyjnych.

7. **Z wyłączeniem kont użytkowników, dla których nie musisz włączać weryfikacji dwuetapowej**

   W razie potrzeby możesz wykluczyć użytkowników z weryfikacji dwuetapowej. Użytkownicy z wykluczonymi kontami nie muszą używać weryfikacji dwuetapowej, aby zalogować się do Serwera administracyjnego.

8. **Konfigurowanie weryfikacji dwuetapowej dla własnego konta**

   Jeśli użytkownicy nie są wykluczeni z weryfikacji dwuetapowej, a weryfikacja dwuetapowa nie została jeszcze skonfigurowana dla posiadanych przez nich kont, należy ją skonfigurować w oknie otwieranym po zalogowaniu się do Kaspersky Security Center Web Console. W przeciwnym razie nie będą mogli uzyskać dostępu do Serwera administracyjnego zgodnie ze swoimi uprawnieniami.

Wyniki

Po zakończeniu tego scenariusza:

- Weryfikacja dwuetapowa jest włączona na Twoim koncie.
- Weryfikacja dwuetapowa jest włączona dla wszystkich kont użytkowników Serwera administracyjnego, z wyjątkiem kont użytkowników, które zostały wykluczone.

Informacje o dwuetapowej weryfikacji konta

Kaspersky Security Center Linux zapewnia weryfikację dwuetapową dla użytkowników Kaspersky Security Center Web Console. Jeśli weryfikacja dwuetapowa jest włączona dla Twojego konta, za każdym razem, gdy logujesz się do Kaspersky Security Center Web Console, wprowadzasz swoją nazwę użytkownika, hasło i dodatkowy jednorazowy kod zabezpieczający. Aby otrzymać jednorazowy kod zabezpieczający, musisz mieć aplikację uwierzytelniającą na swoim komputerze lub urządzeniu mobilnym.

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 wydawcy kodu zabezpieczającego. Nazwa wystawcy kodu zabezpieczającego ma domyślną wartość, która jest taka sama jak nazwa Serwera administracyjnego. Nazwa wystawcy jest używana jako identyfikator Serwera administracyjnego w aplikacji uwierzytelniającej. Jeśli zmienisz nazwę wystawcy kodu zabezpieczającego, musisz wydać nowy tajny klucz i przekazać go do aplikacji uwierzytelniającej. Kod zabezpieczający jest jednorazowy i ważny do 90 sekund (dokładny czas może się różnić).

Każdy użytkownik, dla którego włączono weryfikację dwuetapową, może ponownie wydać swój własny tajny klucz. Jeśli użytkownik uwierzytelnia się za pomocą ponownie wydanego tajnego klucza i używa go do logowania, Serwer administracyjny zapisuje nowy tajny klucz dla konta użytkownika. Jeśli użytkownik wprowadzi nowy tajny klucz niepoprawnie, Serwer administracyjny nie zapisze nowego tajnego klucza i pozostawi aktualny tajny klucz ważny do dalszej autoryzacji.

> Każde oprogramowanie uwierzytelniające, które obsługuje algorytm jednorazowego hasła czasowego (TOTP), może być używane jako aplikacja uwierzytelniająca, na przykład Google Authenticator. Aby wygenerować kod zabezpieczający, musisz zsynchronizować czas ustawiony w aplikacji uwierzytelniającej z czasem ustawionym dla Serwera administracyjnego.

Aby sprawdzić, czy Kaspersky Security Center Linux obsługuje aplikację uwierzytelniającą, której chcesz użyć, włącz weryfikację dwuetapową 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.

Aplikacja uwierzytelniająca generuje kod zabezpieczający w następujący sposób:

1. Serwer administracyjny generuje specjalny tajny klucz i kod QR.
2. Przekazujesz wygenerowany tajny klucz lub kod QR do aplikacji uwierzytelniającej.
3. Aplikacja uwierzytelniająca generuje jednorazowy kod zabezpieczający, który należy przekazać do okna uwierzytelniania Serwera administracyjnego.

Zdecydowanie zalecamy zainstalowanie aplikacji uwierzytelniającej na więcej niż jednym urządzeniu. Zapisz tajny klucz (lub kod QR) i przechowuj go w bezpiecznym miejscu. Pomoże to w przywróceniu dostępu do Kaspersky Security Center Web Console w przypadku utraty dostępu do urządzenia mobilnego.

Aby zabezpieczyć korzystanie z Kaspersky Security Center Linux, możesz włączyć weryfikację dwuetapową dla swojego konta i włączyć weryfikację dwuetapową dla wszystkich użytkowników.

Możesz wykluczyć konta z weryfikacji dwuetapowej. Może to być konieczne w przypadku kont usług, które nie mogą otrzymać kodu zabezpieczającego dla uwierzytelnienia.

Weryfikacja dwuetapowa działa według następujących zasad:

- Tylko konto użytkownika z uprawnieniem Modyfikuj listy ACL obiektów bezpośrednio w obszarze funkcjonalnym **Cechy ogólne: Uprawnienia użytkownika** umożliwia weryfikację dwuetapową dla wszystkich użytkowników.
- Tylko użytkownik, który włączył weryfikację dwuetapową na swoim koncie, może włączyć opcję weryfikacji dwuetapowej dla wszystkich użytkowników.
- Tylko użytkownik, który włączył weryfikację dwuetapową na swoim koncie, może wykluczyć inne konta użytkowników z listy weryfikacji dwuetapowej włączonej dla wszystkich użytkowników.
- Użytkownik może włączyć weryfikację dwuetapową tylko dla swojego konta.
- Konto użytkownika, który posiada uprawnienie Modyfikuj listy ACL obiektów w obszarze funkcyjnym **Cechy ogólne: Uprawnienia użytkownika** i jest zalogowany do Kaspersky Security Center Web Console przy użyciu weryfikacji dwuetapowej, może wyłączyć weryfikację dwuetapową: dla każdego innego użytkownika tylko wtedy, gdy weryfikacja dwuetapowa dla wszystkich użytkowników jest wyłączona, dla użytkownika wykluczonego z listy weryfikacji dwuetapowej, która jest włączona dla wszystkich użytkowników.
- Każdy użytkownik, który zalogował się do Kaspersky Security Center Web Console przy użyciu weryfikacji dwuetapowej, może ponownie wydać swój własny tajny klucz.
- Możesz włączyć opcję weryfikacji dwuetapowej dla wszystkich użytkowników dla Serwera administracyjnego, z którym aktualnie pracujesz. Jeśli włączysz tę opcję na Serwerze administracyjnym, włączysz tę opcję również dla jego kont użytkowników jego wirtualnych Serwerów administracyjnych i nie włączysz weryfikacji dwuetapowej dla kont użytkowników podrzędnych Serwerów administracyjnych.

Włączanie weryfikacji dwuetapowej dla własnego konta

Użytkownik może włączyć weryfikację dwuetapową tylko dla swojego konta.

Zanim włączysz weryfikację dwuetapową na swoim koncie, upewnij się, że aplikacja uwierzytelniająca jest zainstalowana na Twoim urządzeniu mobilnym. Upewnij się, że czas ustawiony w aplikacji uwierzytelniającej jest zsynchronizowany z czasem ustawionym na urządzeniu, na którym jest zainstalowany Serwer administracyjny.

W celu włączenia weryfikacji dwuetapowej na koncie użytkownika:

1. W menu głównym przejdź do opcji **Użytkownicy i role** → **Użytkownicy i grupy**, a następnie wybierz zakładkę **Użytkownicy**.

2. Kliknij nazwę swojego konta.

3. W otwartym oknie ustawień użytkownika wybierz zakładkę **Bezpieczeństwo uwierzytelniania**:

   a. Wybierz opcję **Zażądaj nazwę użytkownika, hasło i kod zabezpieczający (weryfikacja dwuetapowa)**. Kliknij przycisk **Zapisz**.

   b. W otwartym oknie weryfikacji dwuetapowej kliknij **Zobacz, jak skonfigurować weryfikację dwuetapową**.

      Wprowadź tajny klucz w aplikacji uwierzytelniania lub też kliknij **Wyświetl kod QR** i zeskanuj kod QR za pomocą aplikacji uwierzytelniania na urządzeniu mobilnym, aby uzyskać jednorazowy kod zabezpieczający.

   c. W oknie weryfikacji dwuetapowej określ kod zabezpieczający, wygenerowany przez aplikację uwierzytelniającą, a następnie kliknij przycisk **Sprawdź i zastosuj**.

4. Kliknij przycisk **Zapisz**.

Weryfikacja dwuetapowa jest włączona na Twoim koncie.

Włączanie weryfikacji dwuetapowej dla wszystkich użytkowników

Możesz włączyć weryfikację dwuetapową dla wszystkich użytkowników Serwera administracyjnego, jeśli Twoje konto ma uprawnienie Modyfikuj listy ACL obiektów bezpośrednio w obszarze funkcjonalnym **Cechy ogólne: Uprawnienia użytkownika** i jeśli jesteś uwierzytelniony za pomocą weryfikacji dwuetapowej.

W celu włączenia weryfikacji dwuetapowej dla wszystkich użytkowników:

1. W menu aplikacji kliknij ikonę ustawienia ( ) obok nazwy żądanego Serwera administracyjnego.

   Zostanie otwarte okno właściwości Serwera administracyjnego.

2. Na zakładce **Bezpieczeństwo uwierzytelniania** w oknie właściwości ustaw przycisk przełącznika opcji **weryfikacja dwuetapowa dla wszystkich użytkowników** w pozycji włączenia.

3. Jeśli nie włączyłeś weryfikacji dwuetapowej na swoim koncie, aplikacja otworzy okno dla włączenia weryfikacji dwuetapowej dla Twojego konta.

   a. W oknie weryfikacji dwuetapowej kliknij **Zobacz, jak skonfigurować weryfikację dwuetapową**.

   b. Wprowadź ręcznie tajny klucz w aplikacji uwierzytelniania lub kliknij **Wyświetl kod QR** i zeskanuj kod QR za pomocą aplikacji uwierzytelniania na urządzeniu mobilnym, aby uzyskać jednorazowy kod zabezpieczający.

   c. W oknie weryfikacji dwuetapowej określ kod zabezpieczający, wygenerowany przez aplikację uwierzytelniającą, a następnie kliknij przycisk **Sprawdź i zastosuj**.

Weryfikacja dwuetapowa jest włączona dla wszystkich użytkowników. Od teraz wszyscy użytkownicy Serwera administracyjnego, w tym użytkownicy dodani po włączeniu weryfikacji dwuetapowej dla wszystkich użytkowników, muszą konfigurować weryfikację dwuetapową dla swoich kont, z wyjątkiem użytkowników, których konta są wykluczone z weryfikacji dwuetapowej.

Wyłączanie weryfikacji dwuetapowej dla konta użytkownika

Możesz wyłączyć weryfikację dwuetapową na swoim koncie, a także na koncie dowolnego innego użytkownika.

> Możesz wyłączyć weryfikację dwuetapową konta innego użytkownika, gdy masz uprawnienie Modyfikuj listy ACL obiektów w obszarze funkcyjnym **Cechy ogólne: Uprawnienia użytkownika.**

W celu wyłączenia weryfikacji dwuetapowej dla konta użytkownika:

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 wyłączyć weryfikację dwuetapową. Może to być Twoje własne konto lub konto innego użytkownika.
3. W otwartym oknie ustawień użytkownika wybierz zakładkę **Bezpieczeństwo uwierzytelniania**.
4. Wybierz opcję **Zażądaj tylko nazwę użytkownika i hasło**, jeśli chcesz wyłączyć weryfikację dwuetapową dla użytkownika konto.
5. Kliknij przycisk **Zapisz**.

Weryfikacja dwuetapowa jest wyłączona dla konta użytkownika.

Wyłączanie weryfikacji dwuetapowej dla wszystkich użytkowników

Możesz wyłączyć weryfikację dwuetapową dla wszystkich użytkowników, jeśli weryfikacja dwuetapowa jest włączona dla Twojego konta, a Twoje konto posiada uprawnienie Modyfikuj listy ACL obiektów w obszarze funkcyjnym **Cechy ogólne: Uprawnienia użytkownika.** Jeśli weryfikacja dwuetapowa nie jest włączona na Twoim koncie, musisz włączyć weryfikację dwuetapową dla swojego konta przed wyłączeniem jej dla wszystkich użytkowników.

W celu wyłączenia weryfikacji dwuetapowej dla wszystkich użytkowników:

1. W menu aplikacji kliknij ikonę ustawienia ( ) obok nazwy żądanego Serwera administracyjnego.

   Zostanie otwarte okno właściwości Serwera administracyjnego.
2. Na zakładce **Bezpieczeństwo uwierzytelniania** w oknie właściwości ustaw przycisk przełącznika opcji **weryfikacja dwuetapowa dla wszystkich użytkowników** w pozycji wyłączenia.
3. Wprowadź poświadczenia swojego konta w oknie uwierzytelniania.

Weryfikacja dwuetapowa jest wyłączona dla wszystkich użytkowników.

Wykluczanie kont z weryfikacji dwuetapowej

Możesz wykluczyć konta użytkowników z weryfikacji dwuetapowej, jeśli masz uprawnienie Modyfikuj listy ACL obiektów w obszarze funkcyjnym **Cechy ogólne: Uprawnienia użytkownika.**

Jeśli konto użytkownika jest wykluczone z listy weryfikacji dwuetapowej dla wszystkich użytkowników, ten użytkownik nie musi korzystać z weryfikacji dwuetapowej.

Wykluczenie kont z weryfikacji dwuetapowej może być konieczne w przypadku kont usług, które nie mogą przekazać kodu zabezpieczającego podczas uwierzytelniania.

Jeśli chcesz wykluczyć niektóre konta użytkowników z weryfikacji dwuetapowej:

1. W menu aplikacji kliknij ikonę ustawienia ( ) obok nazwy żądanego Serwera administracyjnego.

   Zostanie otwarte okno właściwości Serwera administracyjnego.

2. Na zakładce **Bezpieczeństwo uwierzytelniania** w oknie właściwości, w tabeli wykluczeń weryfikacji dwuetapowej kliknij przycisk **Dodaj**.

3. W oknie, które zostanie otwarte:

   a. Wybierz konta użytkowników, które chcesz wykluczyć.

   b. Kliknij przycisk **OK**.

Wybrane konta użytkowników są wykluczone z weryfikacji dwuetapowej.

Konfigurowanie weryfikacji dwuetapowej dla własnego konta

Gdy po raz pierwszy zalogujesz się do Kaspersky Security Center Linux po włączeniu weryfikacji dwuetapowej, otworzy się okno umożliwiające skonfigurowanie weryfikacji dwuetapowej konta.

Zanim verification weryfikację dwuetapową na swoim koncie, upewnij się, że aplikacja uwierzytelniająca jest zainstalowana na Twoim urządzeniu mobilnym. Upewnij się, że czas na urządzeniu z aplikacją uwierzytelniającą i czas na urządzeniu z Serwerem administracyjnym są zsynchronizowane z czasem UTC, korzystając z zewnętrznych źródeł czasu.

W celu skonfigurować weryfikacji dwuetapowej na swoim koncie:

1. Wygeneruj jednorazowy kod zabezpieczający korzystając z aplikacji uwierzytelniającej na urządzeniu mobilnym. W tym celu wykonaj jedną z następujących czynności:

   - Wprowadź ręcznie tajny klucz w aplikacji uwierzytelniającej.
   - Kliknij **Wyświetl kod QR** i zeskanuj kod QR za pomocą aplikacji uwierzytelniającej.

   Na urządzeniu mobilnym wyświetli się kod zabezpieczający.

2. W oknie Konfiguruj weryfikacji dwuetapowej określ kod zabezpieczający, wygenerowany przez aplikację uwierzytelniającą, a następnie kliknij przycisk **Sprawdź i zastosuj**.

   Weryfikacja dwuetapowa jest skonfigurowany na Twoim koncie. Możesz uzyskać dostęp do Serwera administracyjnego zgodnie ze swoimi uprawnieniami.

Uniemożliwienie nowym użytkownikom konfigurowania dla siebie weryfikacji dwuetapowej

Aby jeszcze bardziej poprawić bezpieczeństwo dostępu do Kaspersky Security Center Web Console, możesz zabronić nowym użytkownikom konfigurowania dla siebie weryfikacji dwuetapowej.

Jeśli ta opcja jest włączona, użytkownik z wyłączoną weryfikacją dwuetapową, na przykład nowy administrator domeny, nie może skonfigurować dla siebie weryfikacji dwuetapowej. W związku z tym taki użytkownik nie może zostać uwierzytelniony na Serwerze administracyjnym ani zalogować się do Kaspersky Security Center Web Console bez zgody innego administratora Kaspersky Security Center Linux, który ma już włączoną weryfikację dwuetapową.

Ta opcja jest dostępna, jeśli dla wszystkich użytkowników włączona jest weryfikacja dwuetapowa.

Aby zabronić nowym użytkownikom konfigurowania dla siebie weryfikacji dwuetapowej:

1. W menu głównym kliknij ikonę ustawienia ( ) obok nazwy żądanego Serwera administracyjnego.

   Zostanie otwarte okno właściwości Serwera administracyjnego.

2. Na karcie **Bezpieczeństwo uwierzytelniania** okna właściwości przełącz przycisk przełączania **Zabroń nowym użytkownikom konfigurowania weryfikacji dwuetapowej dla siebie** w pozycję włączenia.

Ta opcja nie ma wpływu na konta użytkowników dodane do wykluczeń weryfikacji dwuetapowej.

Aby przyznać użytkownikowi z włączoną weryfikacją dwuetapową dostęp do Kaspersky Security Center Web Console, wyłącz tymczasowo opcję **Zabroń nowym użytkownikom konfigurowania weryfikacji dwuetapowej dla siebie**, poproś użytkownika o włączenie weryfikacji dwuetapowej, a następnie włącz tę opcję z powrotem.

Generowanie nowego tajnego klucza

Możesz wygenerować nowy tajny klucz do weryfikacji dwuetapowej dla swojego konta tylko wtedy, gdy jesteś autoryzowany za pomocą weryfikacji dwuetapowej.

W celu wygenerowania nowego tajnego klucza dla konta użytkownika:

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 wygenerować nowy tajny klucz dla weryfikacji dwuetapowej.

3. W otwartym oknie ustawień użytkownika wybierz zakładkę **Bezpieczeństwo uwierzytelniania**.

4. Na zakładce **Bezpieczeństwo uwierzytelniania** kliknij odnośnik **Wygeneruj nowy tajny klucz**.

5. W otwartym oknie weryfikacji dwuetapowej określ nowy klucz zabezpieczeń wygenerowany przez aplikację uwierzytelniającą.

6. Kliknij przycisk **Sprawdź i zastosuj**.

Dla użytkownika jest generowany nowy tajny klucz.

Jeśli zgubisz swoje urządzenie mobilne, możesz zainstalować aplikację uwierzytelniającą na innym urządzeniu mobilnym i wygenerować nowy tajny klucz, aby przywrócić dostęp do Kaspersky Security Center Web Console.

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, jeśli 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.

Po zmianie nazwy wystawcy kodu zabezpieczającego należy ponownie wystawić nowy tajny klucz i przekazać go do aplikacji uwierzytelniającej.

W celu określenia nowej nazwy wystawcy kodu zabezpieczającego:

1. W menu aplikacji kliknij ikonę ustawienia ( ) obok nazwy żądanego Serwera administracyjnego.

   Zostanie otwarte okno właściwości Serwera administracyjnego.

2. W otwartym oknie ustawień użytkownika wybierz zakładkę **Bezpieczeństwo uwierzytelniania**.

3. Na zakładce **Bezpieczeństwo uwierzytelniania** kliknij odnośnik **Edytuj**.

   Zostanie otwarta sekcja **Edytuj wystawcę kodu zabezpieczającego**.

4. Określ nową nazwę wydawcy kodu zabezpieczającego.

5. Kliknij przycisk **OK**.

Nowa nazwa wystawcy kodu zabezpieczającego została określona dla Serwera administracyjnego.

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.
3. Kliknij **Usuń**.
4. W otwartym oknie potwierdzenia kliknij **OK**.

Użytkownik lub grupa bezpieczeństwa zostanie usunięta.

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 obszar 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 obszar 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 potomnych.

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.

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 **Profile zasad**.

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.

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

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 profile, 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 uaktualnień 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 uaktualnień 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 uaktualnień do repozytoriów punktów dystrybucji

4. **Konfigurowanie punktów dystrybucji**

   Jeśli w Twojej sieci są przypisane punkty dystrybucji, upewnij się, że opcja **Roześlij aktualizacje** 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 Twoja sieć zawiera urządzenia obsługujące tylko protokół IPv6 i chcesz regularnie aktualizować aplikacje zabezpieczające zainstalowane na tych urządzeniach, upewnij się, że na zarządzanych urządzeniach zainstalowany jest Serwer administracyjny w wersji 13.2 oraz Agent sieciowy w wersji 13.2.

   Jeśli aktualizacja wymaga przejrzenia i zaakceptowania warunków Umowy licencyjnej, następnie musisz najpierw zaakceptować warunki. Dopiero wtedy aktualizacja będzie mogła zostać przesłana na zarządzane urządzenia.

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 nie może automatycznie aktualizować aplikacji Kaspersky. Aby zaktualizować aplikacje, pobierz najnowsze wersje aplikacji z witryny internetowej Kaspersky i zainstaluj je ręcznie:

  - Serwer administracyjny Kaspersky Security Center Linux, Kaspersky Security Center Web Console
  - Agent sieciowy, Kaspersky Endpoint Security, sieciowa wtyczka administracyjna

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:

- Kaspersky Endpoint Security for Linux — pomoc
- 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:

- Kaspersky Endpoint Security for Linux — pomoc
- 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*.

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 szybkiego startu 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 **Zasoby (urządzenia)** → **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 ("*<>?\:|).
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.
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 serwerów aktualizacji Kaspersky, folderu lokalnego lub sieciowego albo głównego serwera administracyjnego.

W zadaniach Pobierz uaktualnienia do repozytorium *Serwera administracyjnego* i *Pobierz uaktualnienia do repozytoriów punktów dystrybucji* uwierzytelnianie użytkownika nie będzie działać, jeśli jako źródło uaktualnień 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. W innym przypadku 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.

  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 Linux 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 uaktualnień do repozytorium**). Zadanie pobierania uaktualnień do repozytorium zostaje zakończone dopiero po zakończeniu zadania *weryfikacji uaktualnień*.

  Domyślnie opcja ta jest wyłączona.

9. W oknie właściwości zadania, na zakładce **Terminarz** utwórz terminarz uruchamiania zadania. Jeśli to konieczne, określ następujące ustawienia:

   - **Zaplanowane uruchomienie**:

     - **Ręcznie** (zaznaczone domyślnie)

       Zadanie nie jest uruchamiane automatycznie. Możesz je uruchomić tylko ręcznie.

       Domyślnie opcja ta jest włączona.

     - **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 sześć 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 poniedziałek o godzinie zgodnej z bieżącym czasem systemowym.

- Codziennie (czas letni nie jest obsługiwany)

Zadanie jest uruchamiane regularnie, w określonych przedziałach czasu. Ten terminarz nie obsługuje czasu letniego (DST). Oznacza to, że gdy zegar przeskoczy o jedną godzinę do przodu lub tyłu na początku lub końcu DST, aktualny czas uruchomienia zadania nie ulegnie zmianie.

Nie jest zalecane korzystanie z tego terminarza. Jest on potrzebny w celu zapewnienia wstecznej kompatybilności Kaspersky Security Center Linux.

Domyślnie, zadanie jest uruchamiane codziennie o godzinie zgodnej z bieżącym czasem systemowym.

- Co tydzień

Zadanie jest uruchamiane co tydzień, w określonym dniu i o określonej godzinie.

- 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.

- Co miesiąc, w określone dni wybranych tygodni

Zadanie jest uruchamiane regularnie, w określone dni każdego miesiąca i o określonej godzinie.

Domyślnie nie wybrano dni miesiąca; domyślny czas uruchomienia to 18:00:00.

- Po zakończeniu wykonywania innego zadania

  Bieżące zadanie jest uruchamiane po zakończeniu innego zadania. Możesz wybrać sposób zakończenia poprzedniego zadania (pomyślnie lub z błędem), aby wyzwolić uruchomienie bieżącego zadania. Parametr ten działa tylko wtedy, gdy oba zadania są przypisane do tych samych urządzeń.

- 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.

    Jeżeli ta opcja jest wyłączona, na urządzeniach klienckich będą uruchamiane tylko zaplanowane zadania, a dla trybu **Ręcznie**, **Raz** i **Natychmiast** zadania będą 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 włączona.

  - 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 losowego opóźnienia dla zadań uruchamianych w przedziale (min)

    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 (min)

  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.

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 uaktualnień*. Zadanie *Weryfikacja uaktualnień* 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 programu firmy 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 uaktualnień*, 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 złośliwego oprogramowania określ grupę administracyjną z urządzeniami testowymi.

   Zadanie *Weryfikacja uaktualnień* uruchamia kolejno zadania Aktualizacja i Skanowanie w poszukiwaniu złośliwego oprogramowania na urządzeniach testowych, aby sprawdzić, czy wszystkie aktualizacje są prawidłowe. Ponadto podczas tworzenia zadania *Weryfikacja uaktualnień* 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 **Zasoby (urządzenia)** → **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**.

4. Jeśli zadanie *weryfikacji aktualizacji* istnieje, kliknij przycisk **Wybierz zadanie**. W oknie, które zostanie otwarte, wybierz zadanie *Weryfikacja uaktualnień* w grupie administracyjnej z urządzeniami testowymi.

5. Jeśli wcześniej nie utworzono zadania *Weryfikacja uaktualnień*, wykonaj następujące czynności:

   a. Kliknij przycisk **Nowe zadanie**.

   b. W otwartym kreatorze nowego zadania określ nazwę zadania, jeśli chcesz zmienić nazwę ustawienia wstępnego.

   c. Wybierz grupę administracyjną z urządzeniami testowymi, którą utworzono wcześniej.

   d. Najpierw wybierz zadanie aktualizacji wymaganej aplikacji obsługiwanej przez Kaspersky Security Center Linux, a następnie wybierz zadanie 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 uaktualnień* 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.

e. Określ konto, z którego zostanie uruchomione zadanie *Weryfikacja uaktualnień*. 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 uaktualnień zostanie włączona. Teraz możesz uruchomić zadanie *Pobierz aktualizacje do repozytorium Serwera administracyjnego*, które rozpocznie się od weryfikacji aktualizacji.

Tworzenie zadania pobierania uaktualnień 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 **Zasoby (urządzenia)** → **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 ("*<>?\:|).

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.

     - 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. 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 uaktualnień 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 Linux 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:

- **Zaplanowane uruchomienie**:

  - Ręcznie (zaznaczone domyślnie)

    Zadanie nie jest uruchamiane automatycznie. Możesz je uruchomić tylko ręcznie.

    Domyślnie opcja ta jest włączona.

  - 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 sześć 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 poniedziałek o godzinie zgodnej z bieżącym czasem systemowym.

- Codziennie (czas letni nie jest obsługiwany)

  Zadanie jest uruchamiane regularnie, w określonych przedziałach czasu. Ten terminarz nie obsługuje czasu letniego (DST). Oznacza to, że gdy zegar przeskoczy o jedną godzinę do przodu lub tyłu na początku lub końcu DST, aktualny czas uruchomienia zadania nie ulegnie zmianie.

  Nie jest zalecane korzystanie z tego terminarza. Jest on potrzebny w celu zapewnienia wstecznej kompatybilności Kaspersky Security Center Linux.

  Domyślnie, zadanie jest uruchamiane codziennie o godzinie zgodnej z bieżącym czasem systemowym.

- Co tydzień

  Zadanie jest uruchamiane co tydzień, w określonym dniu i o określonej godzinie.

- 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.

- Co miesiąc, w określone dni wybranych tygodni

  Zadanie jest uruchamiane regularnie, w określone dni każdego miesiąca i o określonej godzinie.

  Domyślnie nie wybrano dni miesiąca; domyślny czas uruchomienia to 18:00:00.

- Po epidemii wirusa

Zadanie jest uruchamiane po wystąpieniu zdarzenia *Epidemia wirusa*. Wybierz typy aplikacji, które będą monitorować epidemie wirusów. 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 antywirusowej, która zgłosiła epidemię wirusa. W tym przypadku, usuń wybór typów aplikacji, których nie potrzebujesz.

- Po zakończeniu wykonywania innego zadania

  Bieżące zadanie jest uruchamiane po zakończeniu innego zadania. Możesz wybrać sposób zakończenia poprzedniego zadania (pomyślnie lub z błędem), aby wyzwolić uruchomienie bieżącego zadania. Parametr ten działa tylko wtedy, gdy oba zadania są przypisane do tych samych urządzeń.

- 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.

  Jeżeli ta opcja jest wyłączona, na urządzeniach klienckich będą uruchamiane tylko zaplanowane zadania, a dla trybu **Ręcznie**, **Raz** i **Natychmiast** zadania będą 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 włączona.

- 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 losowego opóźnienia dla zadań uruchamianych w przedziale (min)

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 uaktualnień.

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 uaktualnień 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 należy określić folder na urządzeniu z zainstalowanym Serwerem administracyjnym. Folderem sieciowym może być serwer FTP lub HTTP lub udostępnienie 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.

Jeśli dodasz oba serwery aktualizacji Kaspersky oraz folder lokalny lub sieciowy, aktualizacje będą pobierane najpierw z folderu. W przypadku błędu podczas pobierania zostaną użyte serwery aktualizacji Kaspersky.

Jeśli folder współdzielony zawierający aktualizacje jest chroniony hasłem, włącz opcję **Określ konto, które posiada dostęp do udostępnionego folderu źródła aktualizacji (jeśli takie jest)** i wprowadź dane konta wymagane do uzyskania dostępu.

Aby dodać źródła aktualizacji:

1. W menu głównym przejdź do **Zasoby (urządzenia)** → **Zadania**.
2. Kliknij **Pobierz aktualizacje do repozytorium Serwera administracyjnego**.
3. Przejdź do zakładki **Ustawienia aplikacji**.
4. W wierszu **Źródła aktualizacji** kliknij przycisk **Konfiguruj**.
5. W otwartym oknie kliknij przycisk **Dodaj**.
6. Na liście źródeł aktualizacji dodaj niezbędne źródła. Jeśli zaznaczysz pole wyboru **Folder lokalny lub sieciowy**, określ ścieżkę do folderu.
7. Kliknij przycisk **OK**, a następnie zamknij okno właściwości źródła uaktualnień.
8. W oknie zaktualizuj źródło kliknij przycisk **OK**.
9. Kliknij przycisk **Zapisz** w oknie zadania.

Teraz aktualizacje są pobierane do repozytorium Serwera administracyjnego z określonych źródeł.

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.

Włączania funkcji Pobierz pliki diff: scenariusz

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 profilu 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 polityki Agenta sieciowego i — jeśli punkty dystrybucji są przypisywane ręcznie i jeśli chcesz zastąpić ustawienia polityki — 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 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 aplikacji kliknij ikonę ustawienia ( ) obok nazwy żądanego 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 uaktualnień**

Wybierz źródło uaktualnień 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 uaktualnień, 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 uaktualnień 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: \\<nazwa serwera>\KLSHARE\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:

   - Kaspersky Endpoint Security for Linux — pomoc
   - 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.

Tworzenie kopii zapasowych i przywracanie wtyczek webowych

Kaspersky Security Center Web Console umożliwia wykonanie kopii zapasowej bieżącego stanu wtyczki webowej, aby móc później przywrócić zapisany stan. Na przykład, możesz utworzyć kopię zapasową wtyczki webowej przed aktualizacją jej do nowszej wersji. Po aktualizacji, jeśli nowsza wersja nie spełnia Twoich wymagań lub oczekiwań, możesz przywrócić poprzednią wersję wtyczki webowej z kopii zapasowej.

W celu utworzenia kopii zapasowej wtyczek webowych:

1. W menu głównym przejdź do **Ustawienia** → **Wtyczki sieciowe**.

2. W sekcji **Wtyczki sieciowe** wybierz wtyczki sieciowe, których kopię zapasową chcesz utworzyć, a następnie kliknij przycisk **Utwórz kopię zapasową**.

Kopia zapasowa wybranych wtyczek webowych zostanie utworzona. Utworzone kopie zapasowe można przeglądać w sekcji **Kopie zapasowe**.

W celu przywrócenia wtyczki webowej z kopii zapasowej:

1. W menu głównym przejdź do sekcji **Ustawienia** → **Kopie zapasowe**.

2. W sekcji **Kopie zapasowe** wybierz kopię zapasową wtyczki webowej, którą chcesz przywrócić, a następnie kliknij przycisk **Przywróć z kopii zapasowej**.

Wtyczka webowa zostanie przywrócona z wybranej kopii zapasowej.

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 priorytetami *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.

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 i raportowanie** 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 i raportowanie** → **Pulpit nawigacyjny**.
2. Kliknij przycisk **Dodaj lub przywróć widżet sieciowy**.
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.
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 i raportowanie** → **Pulpit nawigacyjny**.
2. Kliknij ikonę ustawienia(⚙), znajdującą się obok widżetu, który chcesz ukryć.
3. Wybierz **Ukryj widżet sieciowy**.
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 i raportowanie** → **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 i raportowanie** → **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 i raportowanie** → **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:

- **Obszar widżetu webowego** (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 stan Krytyczny, jeśli** i **Ustaw stan Ostrzeżenie, jeśli** (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 i raportowanie** → **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 samego pulpitu

Możesz skonfigurować tryb samego 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 samego 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 samego 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 samego pulpitu

Zanim zaczniesz konfigurować tryb samego 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 samego 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 samego 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 tylko w trybie samego 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 i raportowanie** → **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 samego 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 samego 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 samego pulpitu.

Raporty

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 i raportowanie** 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 i raportowanie** → **Raporty**.

Lista szablonów raportów w podsekcji Raporty

2. Kliknij **Dodaj**.

   Zostanie uruchomiony Kreator tworzenia nowego szablonu raportu. Przejdź przez kroki kreatora, korzystając z przycisku **Dalej**.

3. W pierwszym kroku kreatora wprowadź nazwę raportu i wybierz typ raportu.

Kreator tworzenia nowego szablonu raportu. Określenie nazwy i typu szablonu 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.

Kreator tworzenia nowego szablonu raportu. Określenie zakresu szablonu raportu

5. Na stronie **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.

Kreator tworzenia nowego szablonu raportu. Określenie 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.

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 i raportowanie** → **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**.

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 i raportowanie** → **Raporty**.

2. Wybierz raporty, które chcesz wyeksportować.

   Jeśli wybierzesz więcej niż 10 raportów, przycisk **Eksportuj raport** będzie nieaktywny.

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.

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 i raportowanie** → **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 i raportowanie** → **Raporty**.

2. [Opcjonalnie] Zaznacz pole obok szablonów raportu, dla którego chcesz utworzyć zadanie dostarczania raportu.

3. Kliknij przycisk **Nowe zadanie dostarczania raportu**.

4. Zostanie uruchomiony Kreator tworzenia nowego zadania. Przejdź przez kroki kreatora, korzystając z przycisku **Dalej**.

5. W pierwszym kroku kreatora wprowadź nazwę zadania. Domyślna nazwa to **Dostarcz raporty (<N>)**, gdzie <N> to numer seryjny zadania.

6. W kroku ustawień zadania określ następujące ustawienia:

   a. Szablony raportu, które zostaną dostarczone przez zadanie. Jeśli wybrałeś je w kroku 2, pomiń ten krok.

   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.

   d. Czy raporty są zapisywane do folderu, czy wcześniej zapisane raporty w tym folderze są nadpisywane i czy określone konto będzie używane do uzyskania dostępu do tego folderu (dla folderu współdzielonego).

7. Jeśli chcesz zmodyfikować inne ustawienia zadania po utworzeniu zadania, na stronie **Zakończ tworzenie zadania** kreatora włącz opcję **Otwórz szczegóły zadania po jego utworzeniu**.

8. Kliknij przycisk **Utwórz**, aby utworzyć zadanie i zamknąć kreator.

   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 i raportowanie** → **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.

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 Epidemia 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 poziomu ważności

Każde zdarzenie posiada priorytet. W zależności od warunków wystąpienia zdarzenia, może ono posiadać różne priorytety. Istnieją cztery priorytety 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 wymienione są typy zdarzeń, które występują w Serwerze administracyjnym Kaspersky Security Center 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, możesz określić ustawienia powiadomień i ustawienia przechowywania na zakładce **Konfiguracja zdarzenia** w zasadach aplikacji. 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 Kaspersky Security Center, które mają priorytet **Krytyczny**.

Dla każdego zdarzenia, które może być generowane przez aplikację, możesz określić ustawienia powiadomień i ustawienia przechowywania na zakładce **Konfiguracja zdarzenia** w zasadach aplikacji. 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	Domyśln przechow
Limit licencji został przekroczony	4099	KLSRV_EV_LICENSE_CHECK_MORE_110	Raz dziennie Kaspersky Security Center Linux sprawdza, czy ograniczenia 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:	180 dni

			• 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 ograniczenia licencjonowania zostaną przekroczone.	
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
Plik klucza został dodany do listy zablokowanych	4124	KLSRV_LICENSE_BLACKLISTED	Zdarzenia tego typu występują, gdy firma Kaspersky dodała kod aktywacyjny lub plik	180 dni

			klucza, którego używasz, do listy blokowanych. Aby uzyskać więcej informacji, skontaktuj się z działem pomocy technicznej.	
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	180 dni

			automatycznie, jeśli została opłacona w odpowiednim terminie.	
Certyfikat wygasł	4132	KLSRV_CERTIFICATE_EXPIRED	Zdarzenia tego typu występują, gdy certyfikat Serwera administracyjnego dla Zarządzania urządzeniami mobilnymi utraci ważność. Należy zaktualizować certyfikat, który utracił ważność. Możesz skonfigurować automatyczne aktualizacje certyfikatów, zaznaczając pole **Odnów certyfikat automatycznie, jeśli jest to możliwe** w ustawieniach wydawania certyfikatów.	180 dni

Zdarzenia błędu funkcyjnego Serwera administracyjnego

Poniższa tabela wyświetla zdarzenia Kaspersky Security Center Administration Server, które posiadają priorytet **Błąd funkcjonalny**.

Dla każdego zdarzenia, które może być generowane przez aplikację, możesz określić ustawienia powiadomień i ustawienia przechowywania na zakładce **Konfiguracja zdarzenia** w zasadach aplikacji. 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 błędu funkcyjnego Serwera administracyjnego

Nazwa wyświetlanego typu zdarzenia	ID typu zdarzenia	Typ zdarzenia	Opis	Do prze
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.	180

			Szczegóły zdarzenia można znaleźć w opisie zdarzenia.	
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
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	180

			folderu(ów) posiada prawo do zapisu. • Sprawdź, czy nazwa użytkownika i/lub hasło do folderu(ów) uległy zmianie. • Sprawdź połączenie z internetem, gdyż to może być przyczyną zdarzenia. Aby zaktualizować bazy danych i moduły oprogramowania, postępuj zgodnie z instrukcjami.	
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
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
Baza danych Serwera administracyjnego jest niedostępna	4109	KLSRV_DATABASE_UNAVAILABLE	Zdarzenia tego typu występują, jeśli baza danych Serwera administracyjnego stała się niedostępna.	180

			Możesz zareagować na zdarzenie w następujące sposoby: • Sprawdź, czy zdalny serwer, na którym jest zainstalowany serwer SQL, jest dostępny. • Przejrzyj raporty systemu DBMS, aby odkryć przyczynę braku dostępności bazy danych Serwera administracyjnego. Na przykład, ze względu na profilaktyczną obsługę, zdalny serwer z zainstalowanym serwerem SQL może być niedostępny.	
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: • Korzystasz z SQL Server Express Edition DBMS: • W dokumentacji SQL Server Express sprawdź ograniczenie rozmiaru bazy danych dla wersji, której używasz. Prawdopodobnie Twoja baza danych Serwera administracyjnego przekroczyła ograniczenie	180

			rozmiaru bazy danych. • 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. • Używasz systemu DBMS innego niż SQL Server Express Edition: • Nieograniczanie liczby zdarzeń przechowywanych w bazie danych Serwera administracyjnego. • Zmniejszanie listy zdarzeń przechowywanych w bazie danych Serwera administracyjnego. Przeglądanie informacji dotyczących wyboru systemu DBMS.	

Zdarzenia ostrzegające Serwera administracyjnego

Poniższa tabela prezentuje zdarzenia Serwera administracyjnego Kaspersky Security Center, których istotność to **Ostrzeżenie**.

Dla każdego zdarzenia, które może być generowane przez aplikację, możesz określić ustawienia powiadomień i ustawienia przechowywania na zakładce **Konfiguracja zdarzenia** w zasadach aplikacji. 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	Do prze
Wykryto często występujące zdarzenie		KLSRV_EVENT_SPAM_EVENTS_DETECTED	Zdarzenia tego typu występują, gdy Serwer administracyjny wykryje częste zdarzenie na zarządzanym urządzeniu. Aby uzyskać szczegółowe informacje, zapoznaj się z następującą sekcją: Blokowanie częstych zdarzeń.	90 d
Limit licencji został przekroczony	4098	KLSRV_EV_LICENSE_CHECK_100_110	Raz dziennie Kaspersky Security Center Linux sprawdza, czy ograniczenia 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:	90 d

			• 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 ograniczenia licencjonowania zostaną przekroczone.	
Urządzenie było nieaktywne w sieci od dłuższego czasu	4103	KLSRV_EVENT_HOSTS_NOT_VISIBLE	Zdarzenia tego typu występują, gdy do zarządzanego urządzenia zostanie przypisany stan Ostrzeżenie. 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,	90 d

			przy użyciu Kaspersky Security Center Web Console.	
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 d
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 d
Limit instalacji w jednej z grup licencjonowanych aplikacji zostanie wkrótce przekroczony	4127	KLSRV_INVLICPROD_FILLED	Zdarzenia tego typu występują, gdy liczba instalacji aplikacji firm trzecich, zawartych w grupie licencjonowanych aplikacji osiągnie 90% maksymalnej dozwolonej wartości określonej we	90 d

			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.	
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	90 d

			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.	
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 d
Certyfikat APNs	4135	KLSRV_APN_CERTIFICATE_EXPIRED	Zdarzenia tego typu	Nie

wygasł			występują, gdy certyfikat APNs utraci ważność. Należy ręcznie odnowić certyfikat APNs i zainstalować go na serwerze iOS MDM.	prze
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 j prze
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.	90 d

			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”).	
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 serwer FCM zwróci żądanie do 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	90 c

			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.	
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 c
Pozostała niewielka ilość wolnego miejsca na dysku twardym	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 c
Mała ilość 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	90 c

			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. Korzystasz z SQL Server Express Edition DBMS: • W dokumentacji SQL Server Express sprawdź ograniczenie rozmiaru bazy danych dla wersji, której używasz. Prawdopodobnie Twoja baza danych Serwera administracyjnego zaraz osiągnie ograniczenie rozmiaru bazy danych. • 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.

			Używasz systemu DBMS innego niż SQL Server Express Edition: • Nieograniczanie liczby zdarzeń przechowywanych w bazie danych Serwera administracyjnego. • Zmniejszenie listy zdarzeń przechowywanych w bazie danych Serwera administracyjnego. Przeglądanie informacji dotyczących wyboru systemu DBMS.	
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 c
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 c
Zarejestrowano nowe aktualizacje dla modułów oprogramowania Kaspersky	4141	KLSRV_SEAMLESS_UPDATE_REGISTERED	Zdarzenia tego typu występują, gdy Serwer administracyjny zarejestruje nowe aktualizacje dla	90 c

			oprogramowania firmy Kaspersky, zainstalowanego na zarządzanych urządzeniach, których instalacja wymaga zatwierdzenia. Zatwierdź lub odrzuć aktualizacje, korzystając z Kaspersky Security Center Web Console.	
Przekroczono limit wydarzeń w bazie danych. Rozpoczęto usuwanie wydarzeń	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 j prze
Przekroczono limit wydarzeń w bazie danych. Usunięto wydarzenia	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	Nie j prze

			dozwolonej liczby zdarzeń przechowywanych w bazie danych Serwera administracyjnego. • Zmniejszenie listy zdarzeń przechowywanych w bazie danych Serwera administracyjnego.	

Zdarzenia informacyjne Serwera administracyjnego

Poniższa tabela prezentuje zdarzenia Serwera administracyjnego Kaspersky Security Center, których istotność to **Informacja**.

Dla każdego zdarzenia, które może być generowane przez aplikację, możesz określić ustawienia powiadomień i ustawienia przechowywania na zakładce **Konfiguracja zdarzenia** w zasadach aplikacji. 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 informacyjne Serwera administracyjnego

Nazwa wyświetlanego typu zdarzenia	ID typu zdarzenia	Typ zdarzenia	Domyślny czas przechowywania	Uv
Ponad 90% tego klucza licencyjnego jest wykorzystane	4097	KLSRV_EV_LICENSE_CHECK_90	30 dni	
Wykryto nowe urządzenie	4100	KLSRV_EVENT_HOSTS_NEW_DETECTED	30 dni	
Urządzenie zostało automatycznie dodane do grupy	4101	KLSRV_EVENT_HOSTS_NEW_REDIRECTED	30 dni	
Urządzenie zostało usunięte z grupy: nieaktywność w sieci od dłuższego czasu	4104	KLSRV_INVISIBLE_HOSTS_REMOVED	30 dni	
Limit instalacji w jednej z grup licencjonowanych aplikacji zostanie wkrótce przekroczony (wykorzystywanych jest więcej niż 95%)	4128	KLSRV_INVLICPROD_EXPIRED_SOON	30 dni	
Wykryto pliki do przesłania do firmy	4131	KLSRV_APS_FILE_APPEARED	30 dni	

Kaspersky w celu analizy				
ID instancji FCM na tym urządzeniu mobilnym zmieniło się	4137	KLSRV_GCM_DEVICE_REGID_CHANGED	30 dni	
Aktualizacje zostały pomyślnie skopiowane do wskazanego folderu	4122	KLSRV_UPD_REPL_OK	30 dni	
Nawiązano połączenie z podrzędnym Serwerem administracyjnym	4115	KLSRV_EV_SLAVE_SRV_CONNECTED	30 dni	
Nawiązano połączenie z głównym Serwerem administracyjnym	4117	KLSRV_EV_MASTER_SRV_CONNECTED	30 dni	
Bazy danych zostały zaktualizowane	4144	KLSRV_UPD_BASES_UPDATED	30 dni	
Audyt: Połączenie z Serwerem administracyjnym zostało nawiązane	4147	KLAUD_EV_SERVERCONNECT	30 dni	
Audyt: Obiekt został zmodyfikowany	4148	KLAUD_EV_OBJECTMODIFY	30 dni	To zdarze zmiany w następuj obiektac • Grupa admir • Grupa bezpi • Użytk • Pakie • Zadar • Zasac • Serwe • Wirtu Serwe
Audyt: Stan obiektu zmienił się	4150	KLAUD_EV_TASK_STATE_CHANGED	30 dni	Na przyk zdarzenie występuj zadanie r

				powiodło powodu l
Audyt: Ustawienia grupy zostały zmodyfikowane	4149	KLAUD_EV_ADMGROUP_CHANGED	30 dni	
Audyt: Połączenie z Serwerem administracyjnym zostało zakończone	4151	KLAUD_EV_SERVERDISCONNECT	30 dni	
Audyt: Właściwości obiektu zostały zmodyfikowane	4152	KLAUD_EV_OBJECTPROPMODIFIED	30 dni	To zdarze zmiany w następują właściwo • Użytk • Licen • Serwe • Wirtu serwe
Audyt: uprawnienia użytkownika zostały zmodyfikowane	4153	KLAUD_EV_OBJECTACLMODIFIED	30 dni	
Audyt: Klucze szyfrowania zostały zaimportowane lub wyeksportowane z Serwera administracyjnego	5100	KLAUD_EV_DPEKEYSEXPORT	30 dni	

Zdarzenia Agenta sieciowego

Ta sekcja zawiera informacje o zdarzeniach dotyczących Agenta sieciowego.

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 profilu 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	Domyślny czas przechowywania

Wystąpił incydent związany z bezpieczeństwem	549	GNRL_EV_APP_INCIDENT_OCCURED	30 dni
Serwer KSN proxy został uruchomiony. Sprawdzenie dostępności KSN nie powiodło się	7718	KSNPROXY_STARTED_CON_CHK_FAILED	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 profilu 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
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
Urządzenie zostało usunięte	7709	KLNAG_EV_DEVICE_REMOVE	30 dni
Wykryto nowe urządzenie	7710	KLNAG_EV_NAC_DEVICE_DISCOVERED	30 dni
Urządzenie zostało zautoryzowane	7711	KLNAG_EV_NAC_HOST_AUTHORIZED	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

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 i raportowanie** po kliknięciu **Wybory 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**
  - **Zdarzenie 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 i raportowanie** → **Wybory 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.
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 i raportowanie** → **Wybory zdarzeń**.
2. Zaznacz pole obok wyboru zdarzeń, który chcesz edytować.
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 i raportowanie** → **Wybory zdarzeń**.
2. Zaznacz pole obok wyboru zdarzeń, który chcesz uruchomić.

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.

     c. Kliknij nazwę wyboru.

   - W innej sytuacji, jeśli chcesz przejrzeć listę zdarzeń posortowanych na Serwerze administracyjnym, kliknij nazwę wyboru.

   Zostanie wyświetlony 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 i raportowanie** → **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 i raportowanie** → **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**.

3. W wyświetlonym oknie możesz wykonać następujące czynności:

   - Przejrzeć informacje o wybranym zdarzeniu
   - Przejść do kolejnych i poprzednich zdarzeń w wyniku wyboru zdarzeń
   - 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

W celu wyeksportowania zdarzeń do pliku:

1. Uruchom wybór zdarzeń.

2. Zaznacz pole obok żądanego zdarzenia.

3. Kliknij przycisk **Eksportuj do pliku**.

   Wybrane zdarzenie zostanie wyeksportowane do pliku.

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 jednego lub kilku zdarzeń:

1. Uruchom wybór zdarzeń.
2. Zaznacz pola obok żądanych zdarzeń.
3. Kliknij przycisk **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 i raportowanie** → **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 domyślne wartości. 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 **Zasoby (urządzenia)** → **Profile zasad**.

2. Wykonaj jedną z poniższych czynności:

   - Aby skonfigurować okres przechowywania zdarzeń Agenta sieciowego lub zarządzanej aplikacji firmy Kaspersky, kliknij nazwę odpowiedniej zasady.

     Zostanie otwarte okno właściwości zasady.

   - Aby skonfigurować zdarzenia Serwera administracyjnego, w menu głównym kliknij ikonę ustawienia ( ) obok nazwy żądanego Serwera administracyjnego.

     Jeśli masz zasadę dla Serwera administracyjnego, zamiast tego możesz kliknąć nazwę tej zasady.

     Zostanie otwarta strona właściwości Serwera administracyjnego (lub strona właściwości zasady Serwera administracyjnego).

3. Wybierz zakładkę **Konfiguracja zdarzenia**.

   Zostanie wyświetlona lista typów zdarzeń dotyczących sekcji **Krytyczny**.

4. Wybierz sekcję **Błąd funkcjonalny**, **Ostrzeżenie** lub **Informacja**.

5. Na liście typów zdarzeń w prawej części okna kliknij odnośnik dla zdarzenia, którego okres przechowywania chcesz zmienić.

   W sekcji **Rejestracja zdarzenia** otwartego okna włączona jest opcja **Przechowuj w bazie danych Serwera administracyjnego przez (dni)**.

6. W polu edycji znajdującym się pod tym przyciskiem przełącznika wprowadź liczbę dni, przez jaką zdarzenie ma być przechowywane.

7. Jeśli nie chcesz przechowywać zdarzenia w bazie danych Serwera administracyjnego, wyłącz opcję **Przechowuj w bazie danych Serwera administracyjnego przez (dni)**.

Jeśli konfigurujesz zdarzenia Serwera administracyjnego w oknie właściwości Serwera administracyjnego i jeśli ustawienia zdarzeń są blokowane w zasadzie Serwera administracyjnego Kaspersky Security Center, nie możesz ponownie zdefiniować wartości okresu przechowywania dla zdarzenia.

8. Kliknij **OK**.

   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 aplikacji kliknij ikonę ustawienia ( ) obok nazwy żądanego 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 aplikacji kliknij ikonę ustawienia ( ) obok nazwy żądanego 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 wyświetlane 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.

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.

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 priorytetów (*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 i raportowanie** → **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 i raportowanie** → **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 i raportowanie** → **Powiadomienia**.

   Kategoria **Wszystkie powiadomienia** została wybrana w lewej części okna, a w prawej części okna są wyświetlane wszystkie powiadomienia.

2. W lewej części okna wybierz jedną z kategorii:

   - **Wdrażanie**

   - **Urządzenia**

   - **Ochrona**

- **Aktualizacje** (ta kategoria zawiera powiadomienia dotyczące aplikacji Kaspersky, dostępnych do pobrania, i powiadomienia na temat pobranych aktualizacji antywirusowych baz danych)
- **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)
- **Aktualności od Kaspersky** (ta kategoria obejmuje informacje o publikacji aplikacji firmy 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 i raportowanie**.

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). 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 złośliwego 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 złośliwego 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.
Wymagane jest	Urządzenie jest widoczne w sieci, ale aplikacja wymaga	Więcej niż 0 minut.

ponowne uruchomienie	ponownego uruchomienia urządzenia dłużej niż określony przedział czasu i z jednego z wybranych powodów.	
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.
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.
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.
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.	• 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	Urządzenie jest widoczne w sieci, a aplikacja zabezpieczająca jest zainstalowana na urządzeniu, ale nie jest uruchomiona.	• Przycisk przełącznika jest ustawiony

nie jest uruchomiona		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.

Jeśli Kaspersky Security Center Linux przypisze stan do urządzenia, dla niektórych warunków (patrz kolumna Opis warunku) brana jest pod uwagę flaga widoczności. 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*.

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 **Zasoby (urządzenia)** → **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 **Krytyczny**.
5. W prawej części okna, w sekcji **Ustaw stan Krytyczny, jeśli** 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**.

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 **Zasoby (urządzenia)** → **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 stan Ostrzeżenie, jeśli** 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**.

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 aplikacji kliknij ikonę ustawienia ( ) obok nazwy żądanego 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 **Wybierz szablon** 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 **Wybierz szablon** 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.

3. Na zakładce zdefiniuj ustawienia powiadamiania.

4. Kliknij przycisk **OK**, aby 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 wskazanych 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 i raportowanie** → **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 z symbolami zastępczymi zdarzenia przekazywanymi administratorowi.

Symbole zastępcze opisujące zdarzenie

Symbol zastępczy	Opis symbolu zastępczego
%SEVERITY%	Priorytet zdarzenia
%COMPUTER%	Nazwa urządzenia, na którym wystąpiło zdarzenie
%DOMAIN%	Domena
%EVENT%	Zdarzenie
%DESCR%	Opis zdarzenia
%RISE_TIME%	Czas wystąpienia zdarzenia
%KLCSAK_EVENT_TASK_DISPLAY_NAME%	Nazwa zadania
%KL_PRODUCT%	Agent sieciowy
%KL_VERSION%	Numer wersji Agenta sieciowego
%HOST_IP%	Adres IP
%HOST_CONN_IP%	Adres IP połączenia.

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) z symbolem zastępczym %COMPUTER%. Po wystąpieniu zdarzenia, plik script1.bat jest uruchamiany na urządzeniu administratora, który uruchamia plik script2.bat z symbolem zastępczym %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 i raportowanie** → **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 można wysłać do serwerów, opisano w Umowie licencyjnej użytkownika końcowego, którą akceptujesz podczas instalacji Serwera administracyjnego Kaspersky Security Center.

- 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 poziomowi 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 i raportowanie** → **Ogłoszenia Kaspersky**.
2. Kliknij odnośnik **Ustawienia**.

   Zostanie otwarte okno ustawień ogłoszeń Kaspersky.
3. Określ następujące ustawienia:
   - Wybierz poziom ważności 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 raportowanie** i jego podsekcjach.
4. Kliknij przycisk **OK**.

   Zostaną określone ustawienia ogłoszeń firmy Kaspersky.

Wyłączanie ogłoszeń Kaspersky

Sekcja Zapowiedzi firmy Kaspersky (**Monitorowanie i raportowanie** → **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 aplikacji kliknij ikonę ustawienia ( ) obok nazwy żądanego 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 aplikacji kliknij ikonę ustawienia ( ) obok nazwy żądanego 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.

Eksportowanie zdarzeń do systemów SIEM

Ta sekcja opisuje sposób skonfigurowania eksportowania zdarzeń do systemów SIEM.

Scenariusz: Konfigurowanie eksportowania zdarzeń do systemów SIEM

Kaspersky Security Center Linux umożliwia skonfigurowanie eksportu zdarzeń do systemów SIEM za pomocą jednej z następujących metod: eksport do dowolnego systemu SIEM używającego formatu Syslog 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/IP, 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 ostrzeżeń 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 ostrzeżeń w celu powiadomienia administratorów o nagłych problemach z bezpieczeństwem. Wysyłanie ostrzeżeń 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.

Format Syslog eksportu zdarzeń

Możesz wysyłać zdarzenia w formacie Syslog do dowolnego systemu SIEM. Korzystając z formatu Syslog, możesz przekazywać wszelkie zdarzenia, które występują na Serwerze administracyjnym oraz w aplikacjach Kaspersky, które są zainstalowane na zarządzanych urządzeniach. Podczas eksportowania zdarzeń w formacie Syslog możesz wybrać dokładne typy zdarzeń, które będą przesyłane do systemu SIEM.

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.

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: ID 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.

Oznaczenie zdarzeń do wyeksportowania do systemów SIEM w formacie Syslog

W tej sekcji opisano, jak oznaczyć zdarzenia do dalszego eksportu do systemów SIEM w formacie Syslog.

Informacje dotyczące oznaczania zdarzeń do wyeksportowania do systemu 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 profilu, nie będziesz mógł ich ponownie zdefiniować dla aplikacji zarządzanej przez ten profil.

- 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.

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 **Zasoby (urządzenia)** → **Profile zasad**.

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 Syslog**.

   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 **Syslog** 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 **Zasoby (urządzenia)** → **Zarządzane 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 Syslog**.

   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 **Syslog** 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. Wykonaj jedną z poniższych czynności:

   - W menu aplikacji kliknij ikonę ustawienia (🔧) obok nazwy żądanego Serwera administracyjnego.

   - W menu głónym przejdź do **Zasoby (urządzenia)** → **Profile zasad**, a następnie kliknij odnośnik do zasady.

2. W otwartym oknie przejdź na zakładkę **Konfiguracja zdarzenia**.

3. Kliknij **Zaznacz do eksportu do systemu SIEM poprzez Syslog**.

   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 **Syslog** 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.

W celu skonfigurowania eksportowania do systemów SIEM w Kaspersky Security Center Web Console:

1. W menu głównym kliknij ikonę ustawienia ( ) obok nazwy żądanego Serwera administracyjnego.

   Zostanie otwarte okno właściwości Serwera administracyjnego.

2. Na karcie **Ogólne** wybierz sekcję **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/IP, UDP lub TLS przez 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 plik z listą certyfikatów od zaufanych urzędów certyfikacji (CA) i przesłać go do Kaspersky Security Center Linux. Kaspersky Security Center Linux sprawdza, czy certyfikat 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 SHA-1 certyfikatów systemu SIEM w Kaspersky Security Center Linux. Aby dodać odcisk palca SHA-1, 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.

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. Przełącz opcję na pozycję **Automatycznie eksportuj zdarzenia do bazy danych systemu SIEM Włączone.**

7. Kliknij przycisk **Zapisz**.

Eksportowanie do systemu SIEM zostało skonfigurowane. Od teraz, jeśli skonfigurowano odbieranie zdarzeń w systemie SIEM, Serwer administracyjny eksportuje zaznaczone zdarzenia do systemu SIEM. Jeśli ustawisz datę rozpoczęcia eksportu, Serwer administracyjny wyeksportuje również zaznaczone zdarzenia przechowywane w bazie danych Serwera administracyjnego od określonej daty.

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 tej sekcji 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 /opt/kaspersky/ksc64/sbin/klsql2 na urządzeniu z zainstalowanym Serwerem administracyjnym Kaspersky Security Center.

2. W tym katalogu utwórz pusty plik src.sql.

3. Otwórz plik src.sql w dowolnym edytorze tekstu.

4. W pliku src.sql wpisz typ żądanego zapytania SQL, a następnie zapisz plik.

5. Na urządzeniu z zainstalowanym Serwerem administracyjnym Kaspersky Security Center, w wierszu polecenia wpisz następujące polecenie do uruchomienia zapytania SQL z pliku src.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.

Możesz zmodyfikować plik src.sql i utworzyć dowolne zapytanie 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, utworzonego przy użyciu narzędzia klsql2.

Poniższy przykład ilustruje otrzymanie zdarzeń, które wystąpiły na urządzeniach w ciągu ostatnich siedmiu dni, oraz wyświetlenie zdarzeń według czasu ich wystąpienia (najnowsze są wyświetlane jako pierwsze).

Na przykład:
```
SELECT
e.nId, /* identyfikator zdarzenia */
e.tmRiseTime, /* godzina wystąpienia zdarzenia */
e.strEventType, /* wewnętrzna nazwa typu zdarzenia */
e.wstrEventTypeDisplayName, /* wyświetlona nazwa zdarzenia */
e.wstrDescription, /* wyświetlony opis zdarzenia */
e.wstrGroupName, /* nazwa grupy, w której znajduje się zdarzenie */
h.wstrDisplayName, /* wyświetlona nazwa urządzenia, na którym wystąpiło zdarzenie */
CAST(((h.nIp / 16777216) & 255) AS varchar(4)) + '.' +
CAST(((h.nIp / 65536) & 255) AS varchar(4)) + '.' +
CAST(((h.nIp / 256) & 255) AS varchar(4)) + '.' +
CAST(((h.nIp) & 255) AS varchar(4)) as strIp /* adres IP urządzenia, na którym
wystąpiło zdarzenie */
FROM v_akpub_ev_event e
INNER JOIN v_akpub_host h ON h.nId=e.nHostId
WHERE e.tmRiseTime>=DATEADD(Day, -7, GETUTCDATE())
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 SQL 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 aplikacji kliknij ikonę ustawienia ( ) obok nazwy żądanego 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 aplikacji, które obsługują zarządzanie rewizjami, obejmują:

- Serwery administracyjne
- Zasady
- Zadania
- Grupy administracyjne
- Konta użytkowników
- Pakiety instalacyjne

Na rewizjach obiektów możesz wykonać następujące działania:

- Porównać wybraną rewizję z bieżącą rewizją
- Porównać wybrane rewizje
- Porównać obiekt wybranej rewizji z innym obiektem tego samego typu
- Przejrzeć wybraną rewizję
- Wycofać zmiany wprowadzone w obiekcie do wybranej rewizji
- Zapisać rewizje jako plik .txt

W oknie właściwości dowolnego obiektu obsługującego zarządzanie rewizjami sekcja **Historia rewizji** wyświetla listę rewizji obiektów z następującymi szczegółami:

- Liczbę rewizji obiektu
- Datę i godzinę modyfikacji obiektu
- Nazwę użytkownika, który zmodyfikował obiekt
- Działanie wykonane na obiekcie
- 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 **Opis**. W oknie **Opis rewizji obiektu** wprowadź opis rewizji.

Informacje o rewizjach obiektów

Na rewizjach obiektów możesz wykonać następujące działania:

- Porównać wybraną rewizję z bieżącą rewizją
- Porównać wybrane rewizje
- Porównać obiekt wybranej rewizji z innym obiektem tego samego typu
- Przejrzeć wybraną rewizję
- Wycofać zmiany wprowadzone w obiekcie do wybranej rewizji
- Zapisać rewizje jako plik .txt

W oknie właściwości dowolnego obiektu obsługującego zarządzanie rewizjami sekcja **Historia rewizji** wyświetla listę rewizji obiektów z następującymi szczegółami:

- Liczbę rewizji obiektu
- Datę i godzinę modyfikacji obiektu
- Nazwę użytkownika, który zmodyfikował obiekt
- Działanie wykonane na obiekcie
- Opis rewizji związanej ze zmianą wprowadzoną w ustawieniach obiektu

Przywracanie poprzedniej wersji obiektu

Jeśli to konieczne, możesz wycofać zmiany wprowadzone w obiekcie. Na przykład, konieczne może być przywrócenie ustawień profilu 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.

Usuwanie obiektów

Ta sekcja zawiera informacje dotyczące usuwania obiektów i przeglądania informacji o obiektach po ich usunięciu.

Możesz usuwać obiekty, w tym:

- Zasady
- Zadania
- Pakiety instalacyjne
- Wirtualne Serwery administracyjne
- Użytkownicy
- Grupy bezpieczeństwa
- Grupy administracyjne

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 Nieprzypisane urządzenia 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. W takim przypadku, 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.

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 Kopii zapasowej

Ta sekcja zawiera informacje na temat pobierania i usuwania plików z Kwarantanny i Kopii zapasowej 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 Kopii zapasowej 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** → **Kopia zapasowa**.
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 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**, **Kopia zapasowa** lub **Aktywne zagrożenia** w Kaspersky Security Center Linux. Po otwarciu jednej z tych sekcji, wybierz obiekt z listy i kliknij przycisk **Usuń**, a Kaspersky Security Center Linux wykona jedną z następujących akcji lub obie akcje:

- Usunie wybrany obiekt z listy
- Usunie wybrany obiekt 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**. Zapoznaj się z dokumentacją aplikacji Kaspersky, aby uzyskać szczegółowe informacje o tym, jaka akcja ma zostać wykonana.

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 **Zasoby (urządzenia)** → **Zarządzane urządzenia**.
   - Jeśli urządzenie należy do grupy Urządzenia nieprzypisane, w menu głównym przejdź do **Wykrywanie i wdrażanie** → **Urządzenia nieprzypisane**.
2. Kliknij nazwę żądanego urządzenia.
3. W otwartym oknie właściwości urządzenia wybierz zakładkę **Zaawansowane**.
4. W otwartym oknie kliknij opcję **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 z rotacją plików

     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.

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.

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 sekcji **Pliki aplikacji** kliknij przycisk **Przeglądaj**, aby wybrać archiwum ZIP zawierające aplikację, którą chcesz uruchomić na urządzeniu klienckim.

   Archiwum ZIP musi zawierać folder z narzędziami. Ten folder zawiera plik wykonywalny do uruchomienia na urządzeniu zdalnym.

   W razie potrzeby można określić nazwę pliku wykonywalnego i w razie potrzeby argumenty wiersza polecenia. W tym celu należy wypełnić **pole Plik wykonywalny w archiwum do uruchomienia na urządzeniu zdalnym** oraz pola **Argumenty wiersza polecenia**.
4. Kliknij przycisk **Wczytaj i uruchom**, aby uruchomić określoną aplikację na urządzeniu klienckim.

5. Postępuj zgodnie z instrukcjami specjalisty działu pomocy Kaspersky.

Generowania pliku zrzutu dla aplikacji

Plik zrzutu aplikacji umożliwia przeglądanie parametrów aplikacji uruchomionej na urządzeniu klienckim w danym momencie. Ten plik zawiera również informacje o modułach, które zostały załadowane dla aplikacji.

Generowanie plików zrzutu jest dostępne tylko dla procesów 32-bitowych działających na urządzeniach klienckich z systemem Windows. W przypadku urządzeń klienckich z systemem Linux i procesów 64-bitowych ta funkcja nie jest obsługiwana.

Tworzenie pliku zrzutu dla aplikacji:

1. Otwórz okno do zdalnej diagnostyki urządzenia klienckiego.
2. W oknie zdalnej diagnostyki wybierz kliknięciem kartę **Uruchamianie aplikacji zdalnej**.
3. W sekcji **Generowanie plik zrzutu procesu** określ plik wykonywalny aplikacji, dla której chcesz wygenerować plik zrzutu.
4. Kliknij przycisk **Pobierz**, aby zapisać plik zrzutu dla określonej aplikacji.

   Jeśli określona aplikacja nie jest uruchomiona na urządzeniu klienckim, zostanie wyświetlony komunikat o błędzie.

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 firm trzecich na urządzeniach klienckich

Ta sekcja opisuje funkcje Kaspersky Security Center Linux które dotyczą zarządzania aplikacjami firm trzecich uruchomionymi na urządzeniach klienckich.

Scenariusz: Zarządzanie aplikacjami

Możesz zarządzać uruchamianiem aplikacji na urządzeniach użytkowników. Możesz zezwolić na lub zablokować uruchamianie aplikacji na zarządzanych urządzeniach. Ta funkcjonalność jest realizowana przez komponent Kontrola aplikacji. Możesz zarządzać aplikacjami zainstalowanymi na urządzeniach Windows lub 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.
- Kaspersky Endpoint Security for Linux lub Kaspersky Endpoint Security for Windows został utworzony i jest aktywny.

Etapy

Scenariusz korzystania z Kontroli aplikacji podzielony jest na etapy:

1. **Tworzenie i przeglądanie listy aplikacji na urządzeniach klienckich**

   Ten etap pomaga w odnalezieniu aplikacji, które są zainstalowane na zarządzanych urządzeniach. Możesz przejrzeć listę aplikacji i zdecydować, na które aplikacje chcesz zezwolić, a które chcesz zablokować zgodnie z polityką bezpieczeństwa organizacji. Ograniczenia mogą dotyczyć polityki bezpieczeństwa informacji, obowiązującej w Twojej organizacji. Możesz pominąć ten etap, jeśli wiesz dokładnie, jakie aplikacje są zainstalowane na zarządzanych urządzeniach.

   Wskazówki jak to zrobić: Uzyskiwanie i przeglądanie listy aplikacji zainstalowanych na urządzeniach klienckich

2. **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. Możesz pominąć ten etap, jeśli wiesz dokładnie, jakie pliki wykonywalne są zainstalowane na zarządzanych urządzeniach.

   Jak to zrobić: Uzyskiwanie i przeglądanie listy plików wykonywalnych przechowywanych na urządzeniach klienckich

3. **Tworzenie kategorii aplikacji dla aplikacji używanych w Twojej organizacji**

   Przeanalizuj listy aplikacji i plików wykonywalnych, przechowywanych na zarządzanych urządzeniach. W oparciu o analizę, utwórz kategorie aplikacji. Zalecane jest utworzenie kategorii „Aplikacje do pracy”, która obejmuje standardowy zestaw aplikacji używanych w Twojej organizacji. Jeśli różne grupy bezpieczeństwa używają różnych zestawów aplikacji w swojej pracy, oddzielna kategoria aplikacji może zostać utworzona dla każdej grupy bezpieczeństwa.

W zależności od zestawu kryteriów do utworzenia kategorii aplikacji możesz utworzyć kategorie aplikacji dwóch typów.

Instrukcje: Tworzenie kategorii aplikacji z zawartością dodaną ręcznie, Tworzenie kategorii aplikacji zawierającej pliki wykonywalne z wybranych urządzeń

4. **Konfigurowanie Kontroli aplikacji w zasadzie Kaspersky Endpoint Security**

   Skonfiguruj komponent Kontrola aplikacji w zasadzie Kaspersky Endpoint Security for Linux, korzystając z kategorii aplikacji, które utworzono w poprzednim kroku.

   Wskazówki jak to zrobić: Konfigurowanie Kontroli aplikacji w zasadzie Kaspersky Endpoint Security for Windows

5. **Włączanie komponentu Kontrola aplikacji w trybie testowym**

   Aby zapewnić, że reguły Kontroli aplikacji nie będą blokowały aplikacji 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 aplikacji, 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.

6. **Zmienianie ustawień kategorii aplikacji 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 aplikacji z zawartością dodaną ręcznie.

   Wskazówki jak to zrobić: Kaspersky Security Center Web Console: Dodawanie plików wykonywalnych dotyczących zdarzeń do kategorii aplikacji

7. **Stosowanie reguł Kontroli aplikacji w trybie działania**

   Po przetestowaniu reguł Kontroli aplikacji i zakończeniu konfiguracji kategorii aplikacji 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.

8. **Weryfikowanie konfiguracji Kontroli aplikacji**

   Upewnij się, że wykonałeś następujące czynności:

   - Utworzyłeś kategorie aplikacji.
   - Skonfigurowałeś Kontrolę aplikacji przy użyciu kategorii aplikacji.
   - Zastosowałeś reguły Kontroli aplikacji w trybie działania.

Wyniki

Po zakończeniu scenariusza uruchamianie aplikacji na zarządzanych urządzeniach jest kontrolowane. Użytkownicy mogą uruchamiać tylko te aplikacje, które są dozwolone w Twojej organizacji, a nie mogą uruchamiać aplikacji, 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.

Informacje o Kontroli aplikacji

Komponent Kontrola aplikacji monitoruje próby użytkowników mające na celu uruchomienie aplikacji i regulowanie uruchamiania aplikacji przy użyciu reguł Kontroli aplikacji.

Komponent Kontrola aplikacji jest dostępny dla Kaspersky Endpoint Security 11.2 for Linux i nowszych wersji.

Uruchamianie aplikacji, których ustawienia nie odpowiadają żadnym regułom Kontroli aplikacji, jest regulowane przez wybrany tryb działania komponentu:

- *Lista blokowanych*. Tryb jest używany, jeśli chcesz zezwolić na uruchamianie wszystkich aplikacji, za wyjątkiem aplikacji określonych w regułach blokowania. Ten tryb jest wybrany domyślnie.
- *Lista dozwolonych*. Tryb jest używany, jeśli chcesz zablokować uruchamianie wszystkich aplikacji, za wyjątkiem aplikacji określonych w regułach zezwalania.

Reguły Kontroli aplikacji są implementowane poprzez kategorie aplikacji. Tworzysz kategorie aplikacji definiujące określone kryteria. W Kaspersky Security Center Linux istnieją trzy typy kategorii aplikacji:

- Ręcznie dodana kategoria z zawartością. Definiujesz warunki, na przykład metadane plików, wartość skrótu 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.

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 **Urządzenia** → **Zarządzane 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.

Uzyskiwanie i przeglądanie listy plików wykonywalnych przechowywanych na urządzeniach klienckich

Możesz uzyskać listę plików wykonywalnych przechowywanych na zarządzanych urządzeniach. Aby przeprowadzić inwentaryzację plików wykonywalnych, należy utworzyć zadanie inwentaryzacji.

Dla Kaspersky Endpoint Security for Linux funkcja inwentaryzacji plików wykonywalnych jest dostępna nie wcześniej niż w wersji 11.2.

W celu utworzenia zadania dla plików wykonywalnych na urządzeniach klienckich:

1. W menu głównym przejdź do **Zasoby (urządzenia)** → **Zadania**.

   Zostanie wyświetlona lista zadań.

2. Kliknij przycisk **Dodaj**.

   Zostanie uruchomiony Kreator tworzenia nowego zadania. Postępuj zgodnie z krokami kreatora.

3. Na stronie **Nowe zadanie**, 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 wykrywane są pliki wykonywalne w następujących formatach: MZ, COM, PE, NE, SYS, CMD, BAT, PS1, JS, VBS, REG, MSI, CPL, DLL, JAR oraz HTML.

W celu przejrzenia listy plików wykonywalnych przechowywanych na urządzeniach klienckich:

W menu głównym przejdź do **Operacje** → **Aplikacje innych firm** → **Pliki wykonywalne**.

Strona wyświetla listę plików wykonywalnych przechowywanych na urządzeniach klienckich.

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 **Operacje** → **Aplikacje innych firm** → **Kategorie aplikacji**.

   Zostanie wyświetlona strona z listą kategorii aplikacji.

2. Kliknij przycisk **Dodaj**.

   Zostanie uruchomiony Kreator tworzenia nowej kategorii. Postępuj zgodnie z krokami kreatora.

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 **Dodaj**, aby dodać kryterium warunku do uwzględnienia plików w tworzonej kategorii.

5. W kroku **Kryteria warunku** wybierz typ reguły dla tworzenia kategorii z listy:

   - **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. Pliki wykonywalne, które zostały podpisane zgodnie z określonymi certyfikatami, zostaną dodane do kategorii użytkownika.

   - **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 (dowolne urządzenie lub urządzenie przenośne), 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. Możesz wybrać aplikację z rejestru i określić następujące metadane plików:

    - 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.

  - Określ ręcznie

Jeśli ta opcja jest zaznaczona, możesz określić sumę kontrolną pliku lub metadane lub certyfikat jako warunek dodawania aplikacji do kategorii użytkownika.

Suma kontrolna 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 obliczonych wartościach sum kontrolnych są przechowywane w bazie danych Serwera administracyjnego. Przechowywanie wartości sum kontrolnych nie zwiększa znacząco rozmiaru bazy danych.

SHA-256 jest kryptograficzną funkcją skrótu: w algorytmie nie znaleziono usterek, dlatego jest obecnie najbardziej aktualną funkcją kryptograficzną. Kaspersky Endpoint Security for Linux obsługuje obliczenia SHA-256.

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 **SHA-256**.
- 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. Metadane zostaną przesłane do Serwera administracyjnego. Pliki wykonywalne, które zawierają te same metadane, zostaną dodane do kategorii aplikacji.

Certyfikat

Jeśli ta opcja jest zaznaczona, możesz określić certyfikaty z repozytorium. Pliki wykonywalne, które zostały podpisane zgodnie z określonymi certyfikatami, zostaną dodane do kategorii użytkownika.

- 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:

- **Suma kontrolna pliku**

  Wybierz funkcję skrótu (MD5 lub SHA-256), 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.

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:

- **Suma kontrolna pliku**

  Wybierz funkcję skrótu (MD5 lub SHA-256), 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.

Wybrane kryterium zostanie dodane do listy warunków.

Możesz dodać tyle kryteriów tworzenia kategorii aplikacji, ile potrzebujesz.

6. W kroku **Wykluczenia** kliknij przycisk **Add**, aby dodać kryterium warunku wykluczenia w celu wykluczenia plików z tworzonej kategorii.

7. W kroku **Kryteria warunku** wybierz typ reguły z listy w taki sam sposób, w jaki wybierałeś typ reguły dla tworzenia kategorii.

Jeśli kreator zakończy działanie, zostanie utworzona kategoria aplikacji. Jest wyświetlana 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.

W celu utworzenia kategorii aplikacji, która zawiera pliki wykonywalne z wybranych urządzeń:

1. W menu głównym przejdź do **Operacje** → **Aplikacje innych firm** → **Kategorie aplikacji**.

   Zostanie wyświetlona strona z listą kategorii aplikacji.

2. Kliknij przycisk **Dodaj**.

Zostanie uruchomiony Kreator tworzenia nowej kategorii. Postępuj zgodnie z krokami kreatora.

3. W kroku **Wybierz metodę tworzenia kategorii** kreatora określ nazwę kategorii i wybierz opcję **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 obliczonych wartościach sum kontrolnych są przechowywane w bazie danych Serwera administracyjnego. Przechowywanie wartości sum kontrolnych nie zwiększa znacząco rozmiaru bazy danych.

  SHA-256 jest kryptograficzną funkcją skrótu: w algorytmie nie znaleziono usterek, dlatego jest obecnie najbardziej aktualną funkcją kryptograficzną. Kaspersky Endpoint Security for Linux obsługuje obliczenia SHA-256.

  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 **SHA-256**.

  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 sumy SHA-256 plików należących do tej kategorii (obsługiwane przez Kaspersky Endpoint Security 10 Service Pack 2 for Windows i nowsze)** 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.

Jeśli kreator zakończy działanie, zostanie utworzona kategoria aplikacji. Jest wyświetlana na liście kategorii aplikacji. Po skonfigurowaniu Kontroli aplikacji możesz użyć utworzonej kategorii aplikacji.

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 składnika Kontrola aplikacji.

W celu utworzenia kategorii aplikacji, która zawiera pliki wykonywalne z wybranego folderu:

1. W menu głównym przejdź do **Operacje** → **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 **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 aplikacji.

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.

     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.

Domyślnie pole to nie jest zaznaczone.

- Algorytm obliczania wartości sumy kontrolnej **Oblicz sumy SHA-256 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 obliczonych wartościach sum kontrolnych są przechowywane w bazie danych Serwera administracyjnego. Przechowywanie wartości sum kontrolnych nie zwiększa znacząco rozmiaru bazy danych.

  SHA-256 jest kryptograficzną funkcją skrótu: w algorytmie nie znaleziono usterek, dlatego jest obecnie najbardziej aktualną funkcją kryptograficzną. Kaspersky Endpoint Security for Linux obsługuje obliczenia SHA-256.

  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 **SHA-256**.

  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 sumy SHA-256 plików należących do tej kategorii (obsługiwane przez Kaspersky Endpoint Security 10 Service Pack 2 for Windows i nowsze)** 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.

Jeśli kreator zakończy działanie, zostanie utworzona kategoria aplikacji. Jest wyświetlana na liście kategorii aplikacji. Podczas konfiguracji Kontroli aplikacji możesz użyć 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.

Przeglądanie listy kategorii aplikacji

Możesz przejrzeć listę konfigurowanych kategorii aplikacji i ustawień każdej kategorii aplikacji.

W celu przejrzenia listy kategorii aplikacji:

W menu głównym przejdź do **Operacje** → **Aplikacje innych firm** → **Kategorie aplikacji**.

Zostanie wyświetlona strona z listą kategorii aplikacji.

W celu przejrzenia właściwości kategorii aplikacji:

Kliknij nazwę kategorii aplikacji.

Zostanie wyświetlone okno właściwości kategorii aplikacji. Właściwości zostaną pogrupowane na kilku zakładkach.

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 **Zasoby (urządzenia)** → **Profile zasad**.

   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 komputer 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 blokowanych** lub **Lista dozwolonych**.

   Domyślnie, wybrany jest tryb **Lista blokowanych**.

9. Kliknij odnośnik **Ustawienia list reguł**.

   Zostanie otwarte okno **Lista blokowanych i lista dozwolonych**, w którym można dodać kategorię aplikacji. Domyślnie, wybrana jest zakładka **Lista blokowanych**, jeśli wybrany jest tryb **Lista blokowanych** lub wybrana jest zakładka **Lista dozwolonych**, jeśli wybrany jest tryb **Lista dozwolonych**.

10. W oknie **Lista blokowanych i lista dozwolonych** 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 blokowanych i lista dozwolonych**, kliknij przycisk **OK**.

17. Aby zapisać ustawienia i zamknąć okno **Kontrola aplikacji**, kliknij przycisk **OK**.

18. Zamknij okno z ustawieniami profilu 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.

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 i raportowanie** → **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 SHA-256 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 SHA-256. Jeśli wybierzesz funkcję skrótu SHA-256, 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 SHA-256 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 SHA-256 (pliki bez sumy kontrolnej zostaną pominięte)**

  Każdy plik posiada swoją unikatową funkcję skrótu SHA-256. Jeśli wybierzesz funkcję skrótu SHA-256, tylko jeden odpowiadający plik, na przykład, zdefiniowana wersja aplikacji, zostanie przydzielony do kategorii.

  Wybierz tę opcję, jeśli chcesz dodać tylko szczegóły funkcji skrótu SHA-256 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.

Przewodnik po API

Ten podręcznik informacyjny Kaspersky Security Center OpenAPI 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 przewodniku po OpenAPI.

PRZEWODNIK PO OPENAPI

Próbki skryptów

Przewodnik referencyjny 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:

1. Pobierz archiwum KlAkOAPI.tar.gz. To archiwum zawiera pakiet KlAkOAPI i próbki (możesz je skopiować z archiwum lub z przewodnika referencyjnego OpenAPI). Archiwum KlAkOAPI.tar.gz znajduje się również w folderze instalacyjnym Kaspersky Security Center Linux.

2. Zainstaluj pakiet KlakOAPI z archiwum KlAkOAPI.tar.gz na urządzeniu, na którym zainstalowany jest Serwer administracyjny.

   Możesz wywoływać metody OpenAPI, uruchamiać przykłady i własne skrypty tylko na urządzeniach, na których zainstalowany jest Serwer administracyjny i pakiet KlAkOAPI.

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 pomocniczego Serwera administracyjnego i usuwanie hierarchii Serwerów administracyjnych
Pobierz pliki listy sieci	Możesz nawiązać połączenie z Agentem	Dostosowanie punktów

przez bramę połączenia do określonego hosta	sieciowym na żądanym urządzeniu za pomocą bramy połączenia, a następnie pobrać plik z listą sieci na swoje urządzenie.	dystrybucji i bram połączenia
Zainstaluj klucz licencyjny przechowywany w głównym repozytorium Serwera administracyjnego na dodatkowych 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.	Monitorowanie wykonywania zadania
Utwórz i uruchom zadanie	Możesz utworzyć zadanie. W przykładzie określ następujące parametry zadania: • Typ • Metoda uruchamiania	Tworzenie zadania

	• 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.	
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.	Wybieranie konta do uruchamiania Serwera administracyjnego
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 kontami użytkowników

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 dozwolonych 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.

Podręcznik szacowania rozmiaru

Ta sekcja zawiera informacje na temat szacowania rozmiaru dla komponentów Kaspersky Security Center Linux.

Informacje o podręczniku

Podręcznik szacowania rozmiaru 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
- 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.

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.

Serwer administracyjny, DBMS i konsola internetowa, każde na osobnym urządzeniu, sieć obejmuje 50 000 urządzeń

Konfiguracja urządzenia z zainstalowanym Serwerem administracyjnym

Sprzęt	Wartość
Procesor	8 rdzeni, 2500 MHz
Pamięć RAM	16 GB
Dysk twardy	300 GB, zalecana macierz RAID 10
Karta sieciowa	1 Gbit

Konfiguracja urządzenia z zainstalowanym DBMS

Sprzęt	Wartość
Procesor	16 rdzenie, 2500 MHz
Pamięć RAM	32 GB
Dysk twardy	300 GB, zalecana macierz RAID 10
Karta sieciowa	1 Gbit

Konfiguracja urządzenia z zainstalowaną konsolą internetową

Sprzęt	Wartość
Procesor	4 rdzenie, 2500 MHz
Pamięć RAM	8 GB
Dysk twardy	40 GB
Karta sieciowa	1 Gbit

Serwer administracyjny i konsola internetowa na tym samym urządzeniu, DBMS na oddzielnym urządzeniu, sieć obejmuje 50 000 urządzeń

Konfiguracja urządzenia z zainstalowanym Serwerem administracyjnym i konsolą internetową

Sprzęt	Wartość
Procesor	12 rdzenie, 2500 MHz
Pamięć RAM	24 GB
Dysk twardy	340 GB, zalecana macierz RAID 10
Karta sieciowa	1 Gbit

Konfiguracja urządzenia z zainstalowanym DBMS

Sprzęt	Wartość
Procesor	16 rdzenie, 2500 MHz
Pamięć RAM	32 GB
Dysk twardy	300 GB, zalecana macierz RAID 10
Karta sieciowa	1 Gbit

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.
- Zadanie tworzenia kopii zapasowej zapisuje kopie zapasowe w zasobie plików znajdującym się na dedykowanym serwerze.

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.
- 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 profilu 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 (domyślnie jest to plik KAV.MDF, jeśli jako DBMS używasz serwera SQL) okazuje się być około dwukrotnie większy niż ilość miejsca zajmowanego przez bazę danych.

Nie jest zalecane wyraźne ograniczenie rozmiaru dziennika transakcji (domyślnie, plik KAV_log.LDF, jeśli używasz serwera SQL jako systemu DBMS). Zalecane jest pozostawienie domyślnej wartości parametru MAXSIZE. Jednakże, jeśli musisz ograniczyć rozmiar tego pliku, weź pod uwagę fakt, że typowa niezbędna wartość parametru MAXSIZE dla KAV_log.LDF to 20480 MB.

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.
- 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 celu zarządzania maksymalnie 10 000 urządzeń klienckich, punkt dystrybucji musi spełniać przynajmniej następujące wymagania (dostępna jest konfiguracja dla środowiska test stand):

- Procesor: Intel® Core™ i7-7700 CPU, 3.60 GHz 4 rdzenie.
- Pamięć RAM: 8 GB.
- Wolne miejsce na dysku: 120 GB.

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 uaktualnień (łat) i naprawy luk, urządzenie z zainstalowanym punktem dystrybucji będzie także wymagało dodatkowej wolnej przestrzeni na dysku równej podwojonej wartości całkowitego rozmiaru wszystkich łat przeznaczonych do zainstalowania.

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.

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 profili

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 profilu zapewniają przechowywanie wszystkich zdarzeń związanych z wykonywaniem zadań i wymuszeniem profilu.

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 profil został zdefiniowany 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 profilu 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 profilem. Domyślny okres wynosi 7 dni dla zdarzeń związanych z zadaniem oraz 30 dni dla zdarzeń związanych z profilem. 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 profili 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).

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 baz danych

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 **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 Inwentaryzacja oprogramowania

Możesz zmniejszyć obciążenie bazy danych, jednocześnie uzyskując informacje o zainstalowanych aplikacjach. W tym celu zalecamy uruchomienie zadania inwentaryzacji na urządzeniach referencyjnych, 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 zarządzaną aplikacją w różnych scenariuszach.

Domyślnie, urządzenia są synchronizowane z Serwerem administracyjnym co 15 minut lub w dłuższych odstępach czasu. Jednakże, jeśli zmodyfikujesz ustawienia profilu lub zadania na Serwerze administracyjnym, wczesna synchronizacja będzie miała miejsce na urządzeniach, do których profil (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
Równoległa instalacja 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 profili 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 profilu grupowym (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.

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). 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.

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.

Znane problemy

Kaspersky Security Center Linux ma szereg ograniczeń, które nie są krytyczne dla działania aplikacji:

- 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 konkretnych urządzeń. W przypadku przypisania zadania *Pobierz uaktualnienia do repozytoriów punktów dystrybucji* lub zadania *Weryfikacja uaktualnień* do konkretnych urządzeń, zadanie zostanie zaimportowane niepoprawnie.

- Jeśli Twoja sieć obejmuje domenę Microsoft Active Directory zawierającą kilkadziesiąt tysięcy obiektów (zarządzanych urządzeń, grup zabezpieczeń i kont użytkowników), a rozmiar strony odpowiedzi (parametr `MaxPageSize`) jest mniejszy niż 5000, przeszukiwanie kontrolera domeny nie jest dostępne i informacje o obiektach domeny nie są odbierane. Podczas próby przeszukiwania kontrolera domeny pojawia się błąd *Przekroczono limit rozmiaru*. Zwiększenie rozmiaru strony odpowiedzi może pomóc w naprawieniu błędu. Można użyć narzędzia Ntdsutil.exe, aby w razie potrzeby zwiększyć wartość parametru `MaxPageSize` do `5000` lub do `10 000`.

- Jeśli włączysz KPSN we właściwościach Serwera administracyjnego i użyjesz portu HTTPS 17111, połączenie z ds.kaspersky.com nie zostanie przerwane.

- Kaspersky Endpoint Security for Windows nie obsługuje usługi KSN Proxy, jeśli włączona jest opcja **Użyj HTTPS** w ustawieniach KSN Proxy we właściwościach Serwera administracyjnego, a adres Serwera administracyjnego zawiera znaki inne niż łacińskie.

- Po przełączeniu się na serwer podrzędny z interfejsu podstawowego Serwera administracyjnego Kaspersky Security Center Linux, nie można w menu głównym otworzyć sekcji **Aktualizacje oprogramowania Kaspersky**.

- Kiedy tworzysz zadanie *Dodaj klucz* dla Kaspersky Endpoint Security 11.3 for Mac, kreator wyświetla tabelę kluczy licencyjnych, która może zawierać puste linie.

- Poziom ochrony wyświetlany w profilu Kaspersky Endpoint Security for Windows nie odpowiada poziomowi ochrony w interfejsie Kaspersky Endpoint Security for Windows.

- Jeśli uruchomisz zadanie *Zdalna dezinstalacja aplikacji* w celu usunięcia aplikacji Kaspersky z zarządzanego urządzenia, zadanie zakończy się pomyślnie, ale aplikacja nie zostanie usunięta. Ten problem dotyczy Kaspersky Endpoint Security for Linux, Kaspersky Embedded Systems Security for Linux i Kaspersky Industrial CyberSecurity for Linux Nodes.

- Okno właściwości Serwera administracyjnego zawiera ustawienia dla urządzeń mobilnych, chociaż Kaspersky Security Center Linux nie obsługuje zarządzania urządzeniami mobilnymi.

- Jeśli aplikacja z sekcji **Rejestr aplikacji** została wykryta na urządzeniu z systemem Linux, właściwości aplikacji nie zawierają informacji o powiązanych plikach wykonywalnych.

- Jeśli instalujesz Agenta sieciowego na urządzeniu z systemem operacyjnym ALT Linux za pomocą zadania zdalnej instalacji i uruchamiasz to zadanie na koncie z uprawnieniami użytkownika innego niż root, zadanie kończy się niepowodzeniem. Uruchom zadanie zdalnej instalacji z poziomu konta root lub utwórz i użyj autonomicznego pakietu instalacyjnego Agenta sieciowego, aby zainstalować aplikację lokalnie.

- W raportach o formacie literowym podział strony może przecinać linię tekstu w poziomie.

- W kreatorze **Dodaj podrzędny Serwer administracyjny**, jeśli określisz konto z włączoną weryfikacją dwuetapową do uwierzytelniania na przyszłym Serwerze pomocniczym, kreator zakończy działanie z błędem. Aby rozwiązać ten problem, określ konto, dla którego weryfikacja dwuetapowa jest wyłączona, lub utwórz hierarchię z przyszłego serwera pomocniczego.

- 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.

- 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.

- W 64-bitowej wersji Astra Linux pakietu klnagent-astra nie można uaktualnić za pomocą pakietu klnagent64_14: stary pakiet klnagent64-astra zostanie usunięty, a nowy pakiet klnagent64 zostanie zainstalowany zamiast uaktualnienia, więc zostanie dodana nowa ikona urządzenia z pakietem klnagent64_14. Możesz usunąć starą ikonę tego urządzenia.

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.

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 dodatkowym Serwerem administracyjnym

Certyfikat jest tworzony automatycznie podczas instalacji Serwera administracyjnego, a następnie jest przechowywany na Serwerze administracyjnym.

Dodatkowy klucz subskrypcyjny

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.

Folder Kopia zapasowa

Specjalny folder do przechowywania kopii danych Serwera administracyjnego utworzonych przy użyciu narzędzia kopii zapasowej.

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 grupowe i zadania grupowe mogą być tworzone dla każdej zainstalowanej aplikacji w grupie.

Grupa licencjonowanych aplikacji

Grupa aplikacji utworzona w oparciu o kryterium ustalone przez administratora (na przykład, przez dostawcę), dla których zbierane są statystyki instalacji na urządzeniach klienckich.

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.

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

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.

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 komputerów 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 uaktualnień 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.

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.

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, Shockwave i PostScript 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.

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 Systems, IOS są zastrzeżonymi znakami towarowymi lub znakami towarowymi firmy Cisco Systems, Inc. i/lub jej podmiotów w Stanach Zjednoczonych i innych krajach.

Citrix, XenServer są znakami towarowymi firmy Citrix Systems, Inc. i/lub jednego lub więcej oddziałów i mogą być zarejestrowane w Urzędzie patentowym w Stanach Zjednoczonych i 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.

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 w Stanach Zjednoczonych i/lub innych krajach.

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.

Microsoft, Active Directory, ActiveSync, BitLocker, Excel, Forefront, Internet Explorer, InfoPath, Hyper-V, Microsoft Edge, MultiPoint, MS-DOS, PowerShell, PowerPoint, SharePoint, SQL Server, 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 Fundacji Mozilla w Stanach Zjednoczonych i innych krajach.

Novell jest zastrzeżonym znakiem towarowym firmy Novell Enterprises Inc. w Stanach Zjednoczonych i innych krajach.

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.

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.

VMware, VMware vSphere, VMware Workstation są zastrzeżonymi znakami towarowymi lub znakami towarowymi firmy VMware, Inc., zarejestrowanymi w Stanach Zjednoczonych i/lub innych jurysdykcjach.

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.