kaspersky

Kaspersky Security Center 16.3 Linux

© 2026 АО "Лаборатория Касперского"

Мазмұны

Kaspersky Security Center Linux бағдарламасына анықтама

Не жаңалық

Мәселелер шешілді

Kaspersky Security Center Linux туралы

- Жеткізу жиынтығы
- Аппараттық және бағдарламалық талаптар
  - Басқару серверіне қойылатын талаптар
  - Web Console консоліне қойылатын талаптар
  - Желілік агентіне қойылатын талаптар
- Kaspersky үйлесімді бағдарламалары мен шешімдері
- Kaspersky Security Center Linux құрамдастарының үйлесімділігі туралы ақпарат
- Kaspersky Security Center нұсқаларын салыстыру: Windows негізінде және Linux негізінде
- Kaspersky Next Expert View туралы

Архитектура және негізгі ұғымдар

- Бағдарлама архитектурасы
- Kaspersky Security Center Linux Басқару сервері мен Kaspersky Security Center Web Console бағдарламасын орналастыру схемасы
- Kaspersky Security Center Linux қолданатын порттар
- Kaspersky Security Center Web Console бағдарламасы қолданатын порттар
- Негізгі ұғымдар
  - Басқару сервері
  - Басқару серверлерінің иерархиясы
  - Виртуалды Басқару сервері
  - Веб-сервер
  - Kaspersky Security Center Linux Web Server
  - Желілік агент
  - Басқару топтары
  - Басқарылатын құрылғы
  - Тағайындалмаған құрылғы
  - Әкімшінің жұмыс станциясы
  - Басқару веб-плагиндері
  - Саясаттар
  - Саясат профильдері
  - Тапсырмалар
  - Тапсырманың әрекет ету ауқымы
  - Саясат пен бағдарламаның жергілікті параметрлерінің өзара байланысы
  - Тарату нүктесі
  - Қосылым шлюзі
  - Виртуалды Басқару серверлері

Деректер трафигі және порттарды пайдалану схемалары

- Жергілікті желідегі (LAN) Басқару сервері және басқарылатын құрылғылар
- Жергілікті желідегі (LAN) негізгі Басқару сервері және екі қосалқы Басқару сервері
- Жергілікті желі (LAN) ішіндегі басқару сервері, интернеттегі басқарылатын құрылғылар; кері прокси-серверді пайдалану

Жергілікті желі (LAN) ішіндегі Басқару сервері, интернеттегі басқарылатын құрылғылар; қосылым шлюзін қолдану
Демилитаризацияланған аймақтың (DMZ) ішіндегі Басқару сервері, интернеттегі басқарылатын құрылғылар
Kaspersky Security Center Linux құрамдастары мен қауіпсіздік қолданбаларының өзара әрекеттесуі: қосымша мәліметтер
Өзара әрекеттесу схемаларындағы шартты белгілер
Басқару сервері және ДҚБЖ
Басқару сервері және клиент құрылғысы: Қауіпсіздік бағдарламасын басқару
Тарату нүктесін пайдаланып клиент құрылғысындағы бағдарламалық жасақтаманы жаңарту
Басқару серверлерінің иерархиясы: негізгі Басқару сервері және қосалқы Басқару сервері
Демилитаризацияланған аймақта қосалқы Сервері бар Басқару серверлері иерархиясы
Басқару сервері, желі сегментіндегі қосылымдар шлюзі және клиент құрылғысы
Басқару сервері және демилитаризацияланған аймағы екі құрылғы: қосылымдар шлюзі және клиент құрылғысы
Басқару сервері және Kaspersky Security Center Web Console
Жұмысқа кірісу
Қорғанысты күшейту нұсқаулығы
Қорғанысты күшейтудің тексеру тізімі
Басқару серверін орналастыру
Қосылым қауіпсіздігі
Есептік жазбалар және авторизация
Басқару серверін қорғауды басқару
Клиент құрылғыларын қорғауды басқару
Басқарылатын қолданбалар қорғанысын конфигурациялау
Басқару серверіне техникалық қызмет көрсету
Оқиғаларды үшінші тарап жүйелеріне беру
Үшінші тарап ақпараттық жүйелерінің қауіпсіздігі бойынша ұсыныстар
Kaspersky қауіпсіздік қолданбаларын пайдалануға қатысты ұсыныстар
Сценарий: MySQL Server серверінің аутентификациясы
Сценарий: PostgreSQL Server серверінің аутентификациясы
Орналастыруға дайындық
Kaspersky Security Center Linux конфигурациясын таңдау
Типтік конфигурация: бір кеңсе
Типтік конфигурация: өзіндік әкімшілері бар бірнеше үлкен кеңсе
Типтік конфигурация: қашықтағы көптеген шағын кеңселер
Ұйымның қорғаныс құрылымын таңдау
Қорғаныс жүйесін орналастырудың типтік тәсілдері
ДҚБЖ таңдау
Басқару серверіне интернеттен қатынасуды ұсыну
Интернеттен қатынасу: жергілікті желідегі Басқару сервері
Интернеттен қатынасу: Демилитаризацияланған аймақтағы Басқару сервері
Орнату
Kaspersky Security Center Linux нұсқасымен жұмыс істеу үшін MariaDB x64 серверінің конфигурациясы
Kaspersky Security Center Linux бағдарламасымен жұмыс істеу үшін PostgreSQL немесе Postgres Pro серверін конфигурациялау
Kaspersky Security Center Linux нұсқасымен жұмыс істеу үшін MySQL x64 серверінің конфигурациясы
Жоғары қолжетімділікті ДҚБЖ кластерін Kaspersky Security Center Linux жүйесімен жұмыс істеуге дайындау

Kaspersky Security Center Linux орнату
Kaspersky Security Center Linux бағдарламасын тыныш режимде орнату
Тұйық бағдарламалық орта режимінде Astra Linux-ке Kaspersky Security Center Linux орнату
Kaspersky Security Center Web Console орнату
Kaspersky Security Center Web Console веб-консолін орнату параметрлері
Тұйық бағдарламалық орта режимінде Astra Linux-ке Kaspersky Security Center Web Console орнату
Kaspersky Security Center Linux жүйесін скриптпен орнату
Ақауларға төзімді Kaspersky Security Center Linux кластерін орналастыру
Ақауларға төзімді Kaspersky Security Center Linux кластері. Орналастыру схемалары
Ақауларға төзімді Kaspersky Security Center Linux кластері
Сценарий: Ақауларға төзімді Kaspersky Security Center Linux кластерін орналастыру
Ақауларға төзімді Kaspersky Security Center Linux кластері. Аппараттық және бағдарламалық талаптар
Ақауларға төзімді Kaspersky Security Center Linux кластері үшін файлдық серверді дайындау
Ақауларға төзімді Kaspersky Security Center Linux кластері үшін түйіндерді дайындау
Kaspersky Security Center Linux бағдарламасын ақауларға төзімді Kaspersky Security Center Linux кластерінің түйіндеріне орнату
Кластер түйінін қолмен іске қосу және тоқтату
Ақауларға төзімді кластер түйінін қайта орнату
Ақауларға төзімді Kaspersky Security Center Linux кластерінің түйіндерінде орнатылған басқару серверіне қосылған Kaspersky Security Center Web Console орнату
Kaspersky Security Center Linux ақауларға төзімді кластері.
PostgreSQL DBMS жүйесімен Ubuntu жұмыс істейтін географиялық таратылған кластер
Кластер түйіндерінің файлдық жүйесін дайындау
Көшірмелі кластер файлдық жүйесін конфигурациялау
Түйіндерде Corosync және Pacemaker орнату және конфигурациялау
PostgreSQL ДҚБЖ орнату және конфигурациялау
Kaspersky Security Center Linux бағдарламасын географиялық таралған ақауларға төзімді кластерінің түйіндеріне орнатыңыз
Platform V Pangolin DBMS жүйесімен SberLinux жұмыс істейтін географиялық таратылған кластер
Кластер түйіндерінің файлдық жүйесін дайындау
Көшірмелі кластер файлдық жүйесін конфигурациялау
Түйіндерде Corosync және Pacemaker орнату және конфигурациялау
Platform V Pangolin ДҚБЖ орнату және конфигурациялау
Kaspersky Security Center Linux бағдарламасын географиялық таралған ақауларға төзімді кластерінің түйіндеріне орнатыңыз
Kaspersky Security Center веб-консолін географиялық таратылған ақауларға төзімді кластер түйіндеріне орнату
ДҚБЖ-мен жұмыс істеуге арналған есептік жазбалар
MySQL және MariaDB-мен жұмыс істеу үшін ДҚБЖ есептік жазбасын конфигурациялау
PostgreSQL және Postgres Pro жүйесімен жұмыс істеу үшін ДҚБЖ есептік жазбасын конфигурациялау
Деректерді MySQL және MariaDB ДҚБЖ-лардағы ортақ кесте кеңістігінен әр кестедегі файл кеңістігіне жіберу
Kaspersky Security Center Linux-пен жұмыс істеуге арналған сертификаттар
Kaspersky Security Center сертификаттары туралы
Kaspersky Security Center Linux-те қолданылатын пайдаланушы сертификаттарына қойылатын талаптар
Kaspersky Security Center Web Console үшін сертификатты қайта шығару
Kaspersky Security Center Web Console үшін сертификатты ауыстыру
Сертификатты PFX пішімінен PEM пішіміне түрлендіру
Сценарий: Басқару серверінің пайдаланушы сертификатын белгілеу
klsetsrvcert утилитасын пайдаланып, Басқару сервері сертификатын ауыстыру

Желілік агенттерді klmover утилитасын пайдаланып Басқару серверіне қосу
Веб-сервер сертификатын қайта шығару
Әдепкі IAM сертификатын арнаулы сертификатқа өзгерту
IAM серверінің конфигурациясына Басқару серверінің мекенжайын қосу
Ортақ қатынасы бар қалтаны белгілеу
Kaspersky Security Center Web Console бағдарламасына кіру және одан шығу
Kaspersky Security Center Web Console интерфейсі
Kaspersky Security Center Web Console интерфейсінің тілін өзгерту
Kaspersky Security Center Web Console басты бетін өзгерту
Бетбелгілерді қосу және өшіру
Kaspersky Security Center Web Console веб-консолін жою
Бағдарламаны жылдам іске қосу шебері
1-қадам. Интернетке қосылу параметрлерін көрсету
2-қадам. Талап етілетін жаңартуларды жүктеп алу
3-қадам. Қорғау үшін активтерді таңдау
4-қадам. Шифрлауды таңдау
5-қадам. Басқарылатын бағдарламалардың плагиндерін орнатуды конфигурациялау
6-қадам. Дистрибутивтерді жүктеу және орнату пакеттерін жасау
7-қадам. Kaspersky Security Network конфигурациялау
8-қадам. Бағдарламаны белсендіру тәсілін таңдау
9-қадам. Үшінші тарап бағдарламаларының жаңартуларын басқару параметрлерін көрсету
10-қадам. Желі қорғанысының базалық конфигурациясын жасау
11-қадам. Электрондық пошта арқылы хабарландыруларды жіберу әдісін конфигурациялау
12-қадам. Бағдарламаны жылдам іске қосу шеберінің жұмысын аяқтау
Қорғанысты орналастыру шебері
1-қадам. Қорғанысты орналастыру шеберін іске қосу
2-қадам. Орнату пакетін таңдау
3-қадам. Кілт файлын немесе белсендіру кодын тарату тәсілін таңдау
4-қадам. Желілік агенттің нұсқасын таңдау
5-қадам. Құрылғыларды таңдау
6-қадам. Қашықтан орнату тапсырмасының параметрлерін орнату
7-қадам. Өшіріп қайта қосуды басқару
8-қадам. Орнатудың алдында үйлесімді емес бағдарламаларды жою
9-қадам. Құрылғыларды басқарылатын құрылғылар қалтасына жылжыту
10-қадам. Құрылғыларға қатынасу үшін есептік жазбаларды таңдау
11-қадам. Орнатуды бастау
Kaspersky Security Center Linux алдыңғы нұсқасын жаңарту
Kaspersky Security Center Linux жүйесін 16 немесе одан кейінгі нұсқасынан жаңарту
Kaspersky Security Center Linux жүйесін 16 немесе одан кейінгі нұсқасынан орнату файлын пайдаланып жаңарту
Kaspersky Security Center Linux жүйесін 16 немесе одан кейінгі нұсқасынан сақтық көшірме арқылы жаңарту
Kaspersky Security Center Linux бағдарламасын 16-нұсқадан немесе одан кейінгі нұсқадан Kaspersky Security Center Linux ақауларға төзімді кластер тораптарында жаңарту
Kaspersky Security Center Linux 15.4 немесе одан алдыңғы нұсқасынан жаңарту
Kaspersky Security Center Linux жүйесін 15.4 немесе одан алдыңғы нұсқасынан орнату файлын пайдаланып жаңарту
Kaspersky Security Center Linux жүйесін 15.4 немесе одан алдыңғы нұсқасынан сақтық көшірме арқылы жаңарту
Kaspersky Security Center Linux бағдарламасын 15.4-нұсқадан немесе одан алдыңғы нұсқадан Kaspersky Security Center Linux ақауларға төзімді кластер тораптарында жаңарту

- Kaspersky Security Center Web Console жаңарту
- Тұйық бағдарламалық орта режимінде Astra Linux-ке Kaspersky Security Center Web Console жаңарту

Kaspersky Security Center Linux бағдарламасына тасымалдау

- Басқару сервері деректерінің сақтық көшірмесін пайдалану арқылы Kaspersky Security Center Linux жүйесіне көшіру
- Оқулық бейне: басқару сервері деректерінің сақтық көшірмесін жасау арқылы Kaspersky Security Center Linux жүйесіне көшіру
- Kaspersky Security Center Linux серверіне тасымалдау шеберімен тасымалдау
  - Kaspersky Security Center Windows жүйесінен топтық нысандарды экспорттау
  - Экспорттық файлын Kaspersky Security Center Linux жүйесіне импорттау
  - Kaspersky Security Center Linux басқаруындағы басқарылатын құрылғыларды ауыстыру

Басқару серверін конфигурациялау

- Басқару серверінің қосылу мекенжайын конфигурациялау
- Kaspersky Security Center Web Console веб-консолін Басқару серверіне қосу параметрлерін конфигурациялау
- Kaspersky Security Center Linux бағдарламасына кіру үшін IP мекенжайларының рұқсат тізімін конфигурациялау
- Басқару серверінің интернетке қатынасу параметрлерін конфигурациялау
- Басқару серверлерінің иерархиясы
- Басқару серверлерінің иерархиясын жасау: қосалқы Басқару серверін қосу
- Қосалқы Басқару серверлері тізімін қарау
- Виртуалды Басқару серверлерін басқару
  - Виртуалды Басқару серверін жасау
  - Виртуалды Басқару серверін қосу және өшіру
  - Виртуалды Басқару сервері әкімшісін тағайындау
  - Клиент құрылғылары үшін Басқару серверін ауыстыру
  - Виртуалды Басқару серверін жою
- Басқару серверіне қосылу оқиғасының журналын реттеу
- Оқиғалар қоймасындағы оқиғалар санын конфигурациялау
- Басқару серверін басқа құрылғыға тасымалдау
- Басқару серверінің атауын өзгерту
  - Жаңа DNS жазбасын қосу арқылы қосылымдарды сақтау
  - IP мекенжайына негізделген қосылымға ауысу арқылы қосылымдарды сақтау
  - Сервер атауын өзгерткеннен кейін үзілген қосылымдарды қалпына келтіру
- ДҚБЖ есептік деректерін өзгерту
- Басқару сервері деректерін сақтық көшірмелеу және қалпына келтіру
  - Басқару серверінің деректерін сақтық көшірмелеу тапсырмасын жасау
  - Деректердің сақтық көшірмесін жасау және қалпына келтіру үшін klbackup утилитасын пайдалану
  - Басқа басқару серверінің басқаруымен басқарылатын құрылғыларды ауыстыру үшін klbackup утилитасын пайдалану
  - MySQL немесе MariaDB пайдалану кезінде басқару сервері деректерінің сақтық көшірмесін жасау және қалпына келтіру
- Басқару серверіне техникалық қызмет көрсету
- Басқару серверлерінің иерархиясын жою
- Жалпыға қолжетімді DNS серверлеріне қатынасу
- Интерфейсті конфигурациялау
- Басқару серверіне қорғалған қосылым
- TLS қосылымын шифрлау
- Сыртқы қызметтермен әрекеттесуге арналған желі параметрлері
- Глобалды қосалқы желілердің тізімі
- klscmodchk және integrity_checker утилиталарын пайдалану арқылы модульдердің тұтастығын тексеру

Желідегі құрылғыларды табу
Сценарий: Желілік құрылғыларды табу
Windows желісінің сауалнамасы
IP ауқымдарының сауалнамасы
IP ауқымын қосу және өзгерту
Zeroconf сауалнамасы
Домен контроллері сауалнамасы
Домен контроллерін аутентификациялау және қосу
Samba домен контроллерлерін конфигурациялау
Жабдықты түгендеу
Жаңа құрылғылар туралы ақпаратты қосу
Кәсіпорын құрылғыларын анықтау критерийлерін конфигурациялау
Клиент құрылғыларында VDI динамикалық режимін пайдалану
Желілік агенттің орнату пакетінің сипаттарында VDI динамикалық режимін қосу
VDI құрамына кіретін құрылғыларды басқару тобына жылжыту
Клиент құрылғыларын басқару
Басқарылатын құрылғының параметрлері
Клиент құрылғысы мен Басқару серверінің арасындағы қосылымды қолмен тексеру. klnagchk утилитасы
Құрылғыны жылжыту ережелері
Құрылғыны жылжыту ережелерін жасау
Құрылғыны жылжыту ережелерін көшіру
Құрылғыны жылжыту ережелеріне арналған шарттар
Басқару тобы құрамына құрылғыларды қолмен қосу
Құрылғыларды немесе кластерлерді басқару тобының құрамына қолмен жылжыту
Кластерлер мен серверлердің массивтері туралы
Кластерлердің немесе серверлердің массивтерінің сипаттары
Тарату нүктелері мен қосылым шлюздерін конфигурациялау
Тарату нүктелері туралы
Тарату нүктелерінің типтік конфигурациясы: бір кеңсе
Тарату нүктелерінің типтік конфигурациясы: қашықтағы көптеген шағын кеңселер
Тарату нүктелерінің саны мен конфигурациясын есептеу
Тарату нүктелерін автоматты түрде тағайындау
Тарату нүктелерін қолмен тағайындау
Қосылым шлюзін тарату нүктесі ретінде демилитаризацияланған аймаққа қосу
Басқару тобы үшін тарату нүктелерінің тізімін өзгерту
Push серверін қосу
klnagent қызметі үшін файл дескрипторларының шектеуін арттыру
Құрылғы күйлері туралы
Құрылғылардың күйлерін ауыстыруды конфигурациялау
Құрылғыны таңдаулары
Құрылғы таңдауларынан құрылғылар тізімін қарау
Құрылғы таңдауларын жасау
Құрылғы таңдауларын конфигурациялау
Құрылғы таңдауларынан құрылғылар тізімін экспорттау
Таңдаудағы басқару топтарынан құрылғыларды жою

- Құрылғы тегтері
  - Құрылғы тегтерін жасау
  - Құрылғы тегтерін өзгерту
  - Құрылғы тегтерін жою
  - Тег тағайындалған құрылғыларды қарап шығу
  - Құрылғыға тағайындалған тегтерді қарап шығу
  - Құрылғыға тегтерді қолмен тағайындау
  - Тағайындалған тегті құрылғыдан жою
  - Құрылғыларға автоматты түрде тег қою ережелерін қарап шығу
  - Құрылғыларға автоматты түрде тег қою ережелерін өзгерту
  - Құрылғыларға автоматты түрде тег қою ережелерін жасау
  - Құрылғыларға автоматты түрде тег қою ережелерін орындау
  - Құрылғылардан автоматты түрде тег қою ережелерін жою
  - klscflag утилитасы арқылы құрылғылар тегтерін басқару
- Деректерді шифрлау және қорғау
  - Шифрланған қатты дискілер тізімін қарау
  - Шифрлау оқиғалары тізімін қарау
  - Шифрлау туралы есептерді қалыптастыру және қарау
  - Шифрланған қатты дискіге автономды режимде қатынасу мүмкіндігін ұсыну
  - Басқару серверлері арасында шифрлау кілттерін беру
- Клиент құрылғылары үшін Басқару серверін ауыстыру
- Басқару серверлері арасындағы қақтығыстардан аулақ болу
- Басқа Басқару серверіне қосылу шлюздері арқылы Басқару серверіне қосылған құрылғыларды жылжыту
- Құрылғы белсенді емес кезде әрекеттерді қарау және конфигурациялау
- Құрылғылардың пайдаланушыларына хабар жіберу
- Клиент құрылғыларын қашықтан қосу, өшіру және қайта іске қосу
- Басқарылатын құрылғыларға қашықтан қатынасу
  - Kaspersky Security Center Web Console бар Linux негізіндегі құрылғыдан Linux негізіндегі басқарылатын құрылғыға қашықтан қол жеткізу
  - Kaspersky Security Center Web Console бар Linux негізіндегі құрылғыдан Windows негізіндегі басқарылатын құрылғыға қашықтан қол жеткізу
  - Kaspersky Security Center Web Console бар Windows негізіндегі құрылғыдан Linux негізіндегі басқарылатын құрылғыға қашықтан қол жеткізу
  - Kaspersky Security Center Web Console бар Windows негізіндегі құрылғыдан Windows негізіндегі басқарылатын құрылғыға қашықтан қол жеткізу
- Ұялы құрылғыларды басқару үшін
  - Firebase Cloud Messaging қолдану
  - Жалпыға ортақ кілттер инфрақұрылымымен біріктіру

Басқару топтарын басқару

- Басқару топтарын жасау
- Бағдарламаларды басқару тобының құрылғыларына автоматты түрде орнату
- Басқару топтарын жылжыту
- Басқару топтарын жою

Kaspersky бағдарламалық жасақтамасын орналастыру

- Сценарий: Kaspersky бағдарламалық жасақтамасын орналастыру
- Kaspersky бағдарламаларын басқаруға арналған плагинін қосу

Орнату пакеттері
Kaspersky бағдарламаларына арналған орнату пакеттерін жүктеп алу және жасау
Файлдан орнату пакетін жасау
Автономды орнату пакетін жасау
Желілік агенттің орнату пакетінің параметрлері
Kaspersky Security Center Linux қалыптастырған автономды пакеттерді іске қосу
Бағдарламаларды автономды пакеттердің көмегімен орнату
Қауіпсіздік бағдарламасының орнату пакетіндегі дерекқорларды жаңартудың орындылығы
Пайдаланушының орнату пакетінің өлшеміне қойылған шектеулерді өзгерту
Орнату пакеттерін қосалқы Басқару серверлеріне тарату
Жеке орнату пакеттері тізімін қарау
Linux үшін желілік агент орнату
Linux құрылғысын желілік агентті орнатуға дайындау
SUSE Linux Enterprise Server 15 басқаратын құрылғыны Желілік агентті орнатуға дайындау
Желілік агентті орнату үшін жабық бағдарлама ортасы режимінде Astra Linux басқаратын құрылғыны дайындау
glibc 2.5 (ескі ОС) бар Linux операциялық жүйесіне Желілік агент орнатуға дайындалуда
OpenSSH 6.4 нұсқасы (ескірген ОЖ) бар Linux операциялық жүйесіне Желілік агентті орнатуға дайындық
Linux құрылғысына желілік агентті қашықтан орнату
Linux үшін Желілік агентті тыныш режимде орнату (жауап файлымен)
Linux үшін Желілік агентті интерактивті режимде орнату
Желілік агенті бар құрылғылар үшін файлдық жүйені шегіндіруді қолдау
Windows үшін желілік агент орнату
Windows үшін желілік агентті өзара әрекет режимінде орнату
Windows үшін Желілік агентті тыныш режимде орнату
Құрылғының бейнесін қармау және көшіру арқылы енгізу
Желілік агенттің дискісін клондау режимі
Желілік агентті орнату параметрлері
Қашықтан орнату тапсырмасын пайдаланып бағдарламаларды орнату
Kaspersky Security Center Linux қолданбаларын қашықтан орнату тапсырмалары туралы
Бағдарламаны қашықтан орнату
Қолданбаларды macOS құрылғыларына қашықтан орнату
Қосалқы Басқару серверлеріне бағдарламаларды орнату
Желілік агенті орнатылған құрылғыларға бағдарламаларды қашықтан орнату
Қашықтан орнату тапсырмасында құрылғыларды қайта жүктеуді басқару
Kaspersky Security Center Linux қолданбаларын қашықтан орнату тапсырмасы арқылы мәжбүрлеп орналастыру
Бағдарламаларды тыныш режимде орнату
macOS операциялық жүйесі бар құрылғыны Желілік агентті қашықтан орнатуға дайындау
Виртуалды инфрақұрылым
Виртуалды машиналарға түсетін жүктемені азайту бойынша ұсынымдар
Динамикалық виртуалды машиналарды қолдау
Виртуалды машиналарды көшіруді қолдау
Unix басқаруымен жұмыс істейтін құрылғыларда қашықтан орнату параметрлерін көрсету
Орналастыру мониторингі
Kaspersky бағдарламаларын іске қосу және тоқтату
Үшінші тарап қауіпсіздік бағдарламаларын алмастыру
Бағдарламаларды немесе бағдарламалық жасақтама жаңартуларын қашықтан жою
Windows басқаратын құрылғыны қашықтан орнатуға дайындау

- Скрипттерді қашықтан орындау тапсырмасын жасау
  - Манифест-файлы негізінде орнату пакетін жасау
  - Скрипттерді қашықтан орындау тапсырмасы үшін мұрағатты дайындау
  - Скрипттерді қашықтан орындау тапсырмасын пайдаланып құрылғыларға қолданбаларды қашықтан орнату
  - Скрипттерді қашықтан орындау тапсырмасы үшін хабарландыруларды конфигурациялау және бақылау
- Бағдарламаны лицензиялау
  - Kaspersky Security Center Linux лицензиясы
    - Лицензиялық келісім туралы
    - Лицензия туралы
    - Лицензиялық сертификат туралы
    - Лицензиялық кілт туралы
    - Құпиялылық саясатын қарау
    - Kaspersky Security Center лицензиялау нұсқалары
    - Кілт файлы туралы
    - Деректерді беру туралы
    - Жазылым туралы
    - Kaspersky Security Center Linux-ті белсендіру
  - Kaspersky басқарылатын қолданбаларын лицензиялау
    - Басқарылатын бағдарламаларды лицензиялау
    - Лицензиялық кілтті Басқару серверінің қоймасына қосу
    - Лицензиялық кілтті клиент құрылғыларына тарату
    - Лицензиялық кілтті автоматты түрде тарату
    - Қолданылатын лицензиялық кілттер туралы ақпаратты қарап шығу
    - Лицензия шектеуден асып кету оқиғалары
    - Лицензиялық кілтті қоймадан жою
    - Лицензиялық келісімге берілген келісімді кері қайтарып алу
    - Kaspersky бағдарламалары лицензиясының әрекет ету мерзімін ұзарту
    - Бизнес шешімдерін таңдау үшін Kaspersky Marketplace пайдалану
- Kaspersky қолданбаларын конфигурациялау
  - Сценарий: Желі қорғанысын конфигурациялау
  - Құрылғыларға және пайдаланушыларға бағытталған қауіпсіздікті басқару тәсілдемелері
  - Саясаттарды конфигурациялау және тарату: құрылғыларға бағытталған тәсілдеме
  - Саясаттарды конфигурациялау және тарату: пайдаланушыларға бағытталған тәсілдеме
  - Саясаттар және профильдер
    - Саясаттар мен саясат профильдері туралы
    - Бұғаттау (құлып) және бұғатталған параметрлер
    - Саясат пен саясат профильдерін иелену
      - Саясаттар иерархиясы
      - Саясаттар иерархиясындағы саясат профильдері
      - Басқарылатын құрылғының параметрлері қалай іске асырылады
    - Саясатты басқару
      - Саясаттар тізімін қарап шығу
      - Саясатты жасау
      - Саясаттардың жалпы параметрлері
      - Саясатты өзгерту
      - Саясатты иелену параметрін қосу және өшіру
      - Саясатты көшіру

Саясатты жылжыту

Саясатты экспорттау

Саясатты импорттау

Мәжбүрлеп синхрондау

Саясатты қолдану күйінің диаграммасын қарау

"Вирустық шабуыл" оқиғасы бойынша саясатты автоматты түрде белсендіру

Саясатты жою

Саясат профильдерін басқару

Саясат профильдерін қарау

Саясат профилі басымдығын өзгерту

Саясат профилін жасау

Саясат профилін көшіру

Саясатын профилін белсендіру ережесін жасау

Саясат профилін жою

Саясат профилін экспорттау және импорттау

Желілік агент саясатының параметрлері

Желілік агентті Windows, Linux және macOS үшін қолдану: салыстыру

Желілік агенттің параметрлерін операциялық жүйелер бойынша салыстыру

Желілік агент үшін ресурстарды аз тұтыну режимін қосу немесе өшіру

Басқарылатын қолданбалардың қорғаныс параметрлерін конфигурациялау

Kaspersky Endpoint Security жаңарту топтық тапсырмасын қолмен конфигурациялау

Kaspersky Endpoint Security құрылғысын тексеру топтық тапсырмасын қолмен конфигурациялау

Kaspersky Security Network (KSN)

KSN туралы

KSN бағдарламасына қатынасуды конфигурациялау

KSN қолданысын қосу және өшіру

Қабылданған KSN мәлімдемесін қарау

Жаңартылған KSN мәлімдемесін қабылдау

Тарату нүктесі KSN прокси-сервері ретінде жұмыс істейтінін тексеру

KSN прокси-серверінің статистикасын көру

Тапсырмаларды басқару

Тапсырмалар туралы

Тапсырма аймағы

Тапсырманы жасау

Тапсырманы қолмен іске қосу

Таңдалған құрылғылар үшін тапсырманы іске қосу

Тапсырмалар тізімін қарап шығу

Тапсырмалардың жалпы параметрлері

Тапсырманы экспорттау

Тапсырманы импорттау

Тапсырмалардың құпиясөзін өзгерту шеберін іске қосу

1-қадам. Есептік деректерді таңдау

2-қадам. Орындалып жатқан әрекетті таңдау

3-қадам. Нәтижелерді қарап шығу

Басқару серверінде сақталатын тапсырмаларды орындау нәтижелерін қарап шығу

Бағдарлама тегтері
Бағдарлама тегтері
Бағдарлама тегтерін жасау
Қолданба тегтерін өзгерту
Бағдарламаларға тегтер тағайындау
Бағдарламаларға тағайындалған тегтерді алып тастау
Қолданба тегтерін жою
13291-портты ашу үшін klscflag утилитасын пайдалану
Kaspersky Security Center Web Console веб-консолінде Kaspersky Industrial CyberSecurity for Networks бағдарламаларын тіркеу
Пайдаланушылар мен пайдаланушы рөлдерді басқару
Пайдаланушылардың есептік жазбалары туралы
Пайдаланушы рөлдері туралы
Бағдарлама функцияларына қатынасу құқықтарын конфигурациялау. Рөлге негізделген қатынасуды басқару
Бағдарлама функцияларына қатынасу құқықтары
Алдын ала анықталған пайдаланушы рөлдері
Нысандар жиынтығына қатынасу құқықтарын тағайындау
Пайдаланушыларға немесе қауіпсіздік топтарына құқықтарды тағайындау
Ішкі пайдаланушының есептік жазбасын қосу
Пайдаланушылар тобын жасау
Ішкі пайдаланушының есептік жазбасын өзгерту
Пайдаланушылар тобын өзгерту
Пайдаланушыға немесе қауіпсіздік тобына рөл тағайындау
Пайдаланушылардың есептік жазбаларын ішкі қауіпсіздік топқа қосу
Пайдаланушыны құрылғының иесі етіп тағайындау
Желілік агентті орнату кезінде пайдаланушыны құрылғы иесі ретінде тағайындау
Желілік агентті орнатқаннан кейін пайдаланушыны Linux құрылғысының иесі ретінде тағайындау
Пайдаланушыны құрылғының иесі етіп тағайындаудың күшін жою
Есептік жазбаны рұқсатсыз өзгертуден қорғауды қосу
Екі факторлы аутентификацияны конфигурациялау
Есептік жазбаның екі факторлы аутентификациясы туралы
Kaspersky Security Center Web Console веб-консолiне кіру кезінде екі факторлы аутентификация құпия кілтін баптау
Пайдаланушыларға екі факторлы аутентификацияны конфигурациялауға мүмкіндік беру
Екі факторлы аутентификация құпия кілтін қалпына келтіру және жою
Есептік жазбаларды екі факторлы аутентификациядан алып тастау
Қауіпсіздік кодын шығарушының атын өзгерту
Құпиясөзді енгізу әрекеттерінің санын өзгерту
Пайдаланушыларды немесе қауіпсіздік топтарын жою
Пайдаланушы есептік жазбасының құпиясөзін өзгерту
Пайдаланушы рөлін жасау
Пайдаланушы рөлін өзгерту
Пайдаланушы рөлі үшін аймақты өзгерту
Пайдаланушы рөлін жою
Саясат профильдерінің рөлдермен байланысы
Қосалқы Басқару серверлеріне пайдаланушы рөлдерін тарату
Есептік жазбаның құпиясөзін ауыстыру

- Жергілікті әкімші құқықтарын кері қайтарып алу
- Kerberos домен аутентификациясын конфигурациялау

Kaspersky дерекқорлары мен бағдарламаларын жаңарту

- Сценарий: Kaspersky бағдарламалары мен дерекқорларын үнемі жаңартып тұру
- Kaspersky дерекқорларын, бағдарламалық модульдерін және бағдарламаларын жаңарту туралы
- Жаңартуларды Басқару серверінің қоймасына жүктеп алу тапсырмасын жасау
- Алынған жаңартуларды тексеру
- Жаңартуларды тарату орындарының қоймаларына жүктеп алу тапсырмасын жасау
- Басқару серверінің қоймасына жаңартуларды жүктеп алу тапсырмасы үшін жаңарту көздерін қосу
- Бағдарламалық жасақтама жаңартуын мақұлдау және қабылдамау
- Kaspersky Endpoint Security for Windows жаңартуларын автоматты түрде орнату
- Kaspersky дерекқорлары мен бағдарламалық модульдерін жаңарту үшін айырмашылық файлдарын пайдалану туралы
- Айырмашылық файлдарын жүктеу функциясын қосу
- Тарату нүктелері арқылы жаңартуларды жүктеп алу
- Автономды құрылғыларда Kaspersky дерекқорлары мен бағдарламалық жасақтама модульдеріне арналған жаңартулар

Мониторинг, есеп беру және аудит

- Сценарий: Бақылау және есеп беру
- Бақылау түрлері және есеп беру туралы
- Ережелердің Смарт оқыту режимінде іске қосылуы
  - Аномалияларды бейімделумен басқару ережелері арқылы орындалған анықтау әрекеттерін қарау және растау
  - Аномалияларды бейімделумен басқару ережесіне ерекшеліктер қосу
- Бақылау тақтасы және веб-виджеттер
  - Бақылау тақтасын қолдану
  - Ақпараттық тақтаға веб-виджетті қосу
  - Веб-виджетті ақпараттық тақтадан жою
  - Веб-виджетті ақпараттық тақтадан жылжыту
  - Виджеттің өлшемін немесе сыртқы түрін өзгерту
  - Веб-виджет параметрлерін өзгерту
  - Тек бақылау тақтасын қарау режимі туралы
  - Тек бақылау тақтасын қарау режимін конфигурациялау
- Басқару және қорғау есептері
  - Есептерді қолдану
  - Есеп үлгісін жасау
  - Есеп үлгісінің сипаттарын қарау және өзгерту
  - Есепті файлға экспорттау
  - Есепті жасау және қарау
  - Есептерді жеткізу тапсырмасын жасау
  - Есеп үлгілерін жою
- Қорғаныс деңгейінің индикаторы
  - Қауіпсіздік бағдарламасы орнатылған
  - Қолданылған саясат
  - Антивирустық дерекқорларды жаңарту схемасы
  - Сақтық көшірме конфигурацияланған
  - Басқару серверіне техникалық қызмет көрсету тапсырмасы
  - TLS шифрлау қосылған

Оқиғалар және оқиғаларды таңдау
Kaspersky Security Center Linux-тегі оқиғалар туралы
Оқиғалар: Kaspersky Security Center Linux құрамдасы
Оқиға түрі сипаттамасы деректерінің құрылымы
Басқару сервері оқиғалары
Басқару серверінің критикалық оқиғалары
Басқару серверінің функционалдық ақауы оқиғалары
Басқару серверінің ескерту оқиғалары
Басқару серверінің ақпараттық оқиғалары
Желілік агент оқиғалары
Желілік агенттің функционалдық ақауы оқиғалары
Желілік агенттің ескертулері оқиғалары
Желілік агенттің ақпараттық оқиғалары
Оқиға таңдауларын пайдалану
Оқиғалар таңдауын жасау
Оқиғалар таңдауын өзгерту
Оқиғалар таңдауы тізімін қарау
Оқиғалар таңдауын экспорттау
Оқиғалар таңдауын импорттау
Оқиға туралы ақпаратты көру
Оқиғаларды файлға экспорттау
Оқиғадан нысан тарихын қарау
Оқиғаларды жою
Оқиға таңдауларын жою
Оқиғаны сақтау мерзімін конфигурациялау
Жиі болатын оқиғаларды бұғаттау
Жиі болатын оқиғаларды бұғаттау туралы
Жиі болатын оқиғаларды бұғаттауды басқару
Жиі болатын оқиғады бұғаттауды болдырмау
Басқару серверінде оқиғаларды өңдеу және сақтау
Хабарландырулар және құрылғылар күйлері
Хабарландыруларды қолдану
Экрандағы хабарландыруларды қарау
Құрылғы күйлері туралы
Құрылғылардың күйлерін ауыстыруды конфигурациялау
Хабарландыруларды жеткізу параметрлерін конфигурациялау
Хабарландыруларды таратуды тексеру
Орындалатын файл көмегімен оқиғалар туралы хабарлау
Kaspersky хабарландырулары
Kaspersky хабарландырулары туралы
Kaspersky хабарландыру параметрлерін конфигурациялау
Kaspersky хабарландыруларын өшіру
Табылған қауіптер туралы ақпаратты қарап шығу
Дабылдарға жауап беруге арналған интеграциялар
Жауап әрекеттерін орындау үшін Active Directory көмегімен интеграцияны конфигурациялау
Kaspersky Automated Security Awareness Platform-мен интеграцияны конфигурациялау
Kaspersky Threat Intelligence Portal Sandbox интеграциясын конфигурациялау

Дабылдарды атрибуттар бойынша топтау
Cloud Discovery
Веб-виджетті пайдаланып, Cloud Discovery функциясын қосу
Cloud Discovery веб-виджетін бақылау тақтасына қосу
Бұлттық сервистерді пайдалану туралы ақпаратты қарау
Бұлттық сервистің тәуекел деңгейі
Қажетсіз бұлттық сервистерге қол жеткізуді бұғаттау
Оқиғаларды SIEM жүйелеріне экспорттау
Оқиғаларды SIEM жүйелеріне экспорттауды конфигурациялау
Алдын ала шарттар
Оқиғаларды экспорттау туралы
Оқиғаларды SIEM жүйесінде экспорттауды конфигурациялау туралы
CEF және LEEF пішіміндегі оқиғаларды экспорттау туралы
Оқиғаларды CEF немесе LEEF форматына түрлендіру
SIEM жүйелеріне Syslog пішімінде экспортталатын оқиғаларды таңдау
Kaspersky бағдарламалары оқиғаларын Syslog пішімінде экспорттау үшін таңдау
Syslog пішімінде экспорттау үшін жалпы оқиғаларды таңдау
Syslog пішіміндегі оқиғаларды экспорттау туралы
Оқиғаларды SIEM жүйесіне экспорттау үшін Kaspersky Security Center Linux конфигурациялау
Саясат пен саясат профилінің өзгерістерін бақылау
Оқиғаларды тікелей дерекқордан экспорттау
klsql2 утилитасы арқылы SQL сұрауын жасау
klsql2 утилитасы арқылы жасалған SQL сұрауының мысалы
Kaspersky Security Center Linux дерекқорының атауын қарау
Экспорт нәтижелерін қарау
Нысанды тексерумен жұмыс
Саясаттың нұсқасын қарау және сақтау
Саясат тексерістерін салыстыру
Нысанның өзгерістерін алдыңғы тексеруге шегіндіру
Белсенді қауіптер
Кейін өңделетін файлды дезинфекциялау
Кейін өңделетін файлды жүктеу
Белсенді қауіптер бөліміндегі файлдарды жою
Нысандарды жою
Файлдарды Карантинге және Файлдардың сақтық көшірмелері жүктеу және одан жою
Файлдарды Карантиннен және Файлдардың сақтық көшірмелерінен жүктеп алу
Нысандарды Карантин, Сақтық көшірмелеу файлдары немесе Белсенді қауіптерден жою туралы
Қолданбаны SNMP арқылы басқару
Операциялық жүйеде snmpd қызметін конфигурациялау
SNMP арқылы хабарландыруды қосу және өшіру
Kaspersky Security Center Linux жүйесінде SNMP қосу және өшіру
SNMP үшін нысан идентификаторларының мәндері

Kaspersky Security: Бизнеске арналған Кәсіби лицензиясында Kaspersky Security Center Linux жүйесімен жұмыс істеу
Дабылдарға жауап беруге арналған интеграциялар
Жауап әрекеттерін орындау үшін Active Directory көмегімен интеграцияны конфигурациялау
Kaspersky Automated Security Awareness Platform-мен интеграцияны конфигурациялау
Kaspersky Threat Intelligence Portal Sandbox интеграциясын конфигурациялау
Дабылдарды атрибуттар бойынша топтау
Kaspersky Security Center Web Console-ін Kaspersky басқа шешімдерімен біріктіру
Фондық қосылым орнату
Прокси-сервер қосылымын конфигурациялау
Клиент құрылғыларын қашықтан диагностикалау
Қашықтан диагностикалау терезесін ашу
Бағдарламалар үшін трассалауды қосу және өшіру
Бағдарламаны трассалау файлын жүктеу
Трассалау файлдарын жою
Бағдарламалар параметрлерін жүктеу
Клиенттік құрылғыдан жүйелік ақпаратын жүктеп алу
Оқиғалар журналдарын жүктеу
Бағдарламаны іске қосу, тоқтату және қайта іске қосу
Kaspersky Security Center Linux Желілік агент қашықтағы диагностикасын іске қосу және нәтижелерді жүктеп алу
Бағдарламаны клиент құрылғысында іске қосу
Linux операциялық жүйесі бар клиенттік құрылғыда қашықтағы диагностиканы іске қосу
Клиент құрылғыларындағы қолданбалар мен орындалатын файлдарды басқару
Орындалатын файлдарды басқару үшін Бағдарламаларды басқару компонентін пайдалану
Клиент құрылғыларында сақталған орындалатын файлдардың тізімін алу және қарау
Қолмен толықтырылатын бағдарламалар санатын жасау
Таңдалған құрылғылардан орындалатын файлдарды қамтитын бағдарламалар санатын жасау
Таңдалған қалталардан орындалатын файлдарды қамтитын бағдарламалар санатын құру
Бағдарлама санаттары тізімін қарап шығу
Бағдарлама санатына оқиғамен байланысты орындалатын файлдарды қосу
Kaspersky Endpoint Security for Windows саясатындағы Бағдарламаларды басқару конфигурациялау
Клиент құрылғыларында орнатылған бағдарламалар тізімін алу және қарау
Үшінші тарап бағдарламалары туралы
Үшінші тарап бағдарламаларының жаңартуларын орнату
Сценарий: Үшінші тарап бағдарламаларын жаңарту
Үшінші тарап бағдарламалық жасақтама жаңартуларын орнату нұсқалары
Осалдықтарды және қажетті жаңартуларды іздеу тапсырмасы параметрлері
Осалдықтарды және қажетті жаңартуларды іздеу тапсырмасын жасау
Үшінші тарап бағдарламаларының қолжетімді жаңартулары туралы ақпаратты қарау
Қолжетімді жаңартулар тізімін файлға экспорттау
Үшінші тарап бағдарламаларының жаңартуларын мақұлдау және қабылдамау
Қажетті жаңартуларды орнату және осалдықтарды түзету тапсырмасын жасау
Жаңартуларды орнату үшін ережелер қосу
Тапсырма жасалғаннан кейін көрсетілген Қажетті жаңартуларды орнату және осалдықтарды жабу тапсырмасының параметрлері
Үшінші тарап бағдарламаларын автоматты түрде жаңарту

- Үшінші тарап қолданбаларында осалдықтарды түзету
  - Бағдарламалық жасақтама осалдықтарын анықтау және түзету туралы
  - Сценарий: Үшінші тарап бағдарламаларындағы осалдықтарды анықтау және түзету
  - Үшінші тарап қолданбаларында осалдықтарды түзету
  - Осалдықтарды түзету тапсырмасын жасау
  - Үшінші тарап бағдарламаларындағы осалдықтарға арналған пайдаланушы түзетулері
  - Барлық басқарылатын құрылғыларда анықталған бағдарламалардағы осалдықтар туралы ақпаратты қарау
  - Таңдалған басқарылатын құрылғыларда анықталған бағдарламалардағы осалдықтар туралы ақпаратты қарау
  - Басқарылатын құрылғылардағы осалдықтардың статистикасын қарау
  - Бағдарламалардағы осалдықтар тізімін мәтіндік файлға экспорттау
  - Бағдарламалардағы осалдықтарды елемеу
- Kaspersky дерекқорынан үшінші тарап бағдарламасы үшін орнату пакетін жасау
- Kaspersky дерекқорынан үшінші тарап бағдарламасына арналған орнату пакетінің параметрлерін қарау және өзгерту
- Kaspersky дерекқорынан үшінші тарап бағдарламасына арналған орнату пакетінің параметрлері
- Оқшауланған желіде осалдықтарды түзету
  - Оқшауланған желідегі үшінші тарап бағдарламаларының осалдықтарын түзету
  - Оқшауланған желідегі үшінші тарап бағдарламаларының осалдықтарын түзету туралы
  - Оқшауланған желідегі осалдықтарды түзету үшін интернетке қатынасу мүмкіндігі бар Басқару серверін конфигурациялау
  - Оқшауланған желідегі осалдықтарды түзету үшін оқшауланған Басқару серверлерін конфигурациялау
  - Оқшауланған желіде түзетулерді беру және жаңартуларды орнату
  - Оқшауланған желіде патчтарды жіберу және жаңартуларды орнату мүмкіндігін өшіру
- API анықтамалық нұсқаулығы
- Провайдерлер үшін үздік тәжірибелер
- Kaspersky Security Center Linux орналастыруды жоспарлау
  - Басқару серверіне интернеттен қатынасуды ұсыну
  - Kaspersky Security Center Linux стандартты конфигурациясы
  - Тарату нүктелері туралы
  - Басқару серверлерінің иерархиясы
  - Виртуалды Басқару серверлері
- Орналастыру және бастапқы конфигурациялау
  - Басқару серверін орнату бойынша ұсыныстар
    - Істен шығуға төзімді кластерде Басқару серверінің қызметтеріне арналған есептік жазбалар жасау
    - ДҚБЖ таңдау
    - Басқару серверінің мекенжайын көрсету
    - Әрекетсіз қосылымдарды жүргізу
  - Желілік агент пен қауіпсіздік қолданбаларын орналастыру
  - Ұйым-клиент желісінде қорғанысты конфигурациялау
    - Kaspersky Endpoint Security саясатын қолмен конфигурациялау
      - Кеңейтілген қорғаныс бөлімінде саясатты конфигурациялау
      - Негізгі қорғаныс бөліміндегі саясатты конфигурациялау
      - Қосымша параметрлер бөліміндегі саясатты конфигурациялау
      - Оқиғаларды конфигурациялау бөліміндегі саясатты конфигурациялау
    - Kaspersky Endpoint Security жаңарту топтық тапсырмасын қолмен конфигурациялау
    - Kaspersky Endpoint Security құрылғысын тексеру топтық тапсырмасын қолмен конфигурациялау
    - Осалдықтарды және қажетті жаңартуларды іздеу тапсырмасы кестесін конфигурациялау
    - Жаңартуларды орнату және осалдықты түзету топтық тапсырмасын қолмен конфигурациялау

Басқару топтары құрылымын құру және тарату нүктелерін тағайындау
MSP клиентінің типтік конфигурациясы: бір кеңсе
MSP клиентінің типтік конфигурациясы: көптеген шағын оқшауланған кеңселер
Саясаттар иерархиясы, саясат профильдерін қолдану
Саясаттар иерархиясы
Саясат профильдері
Тапсырмалар
Құрылғыны жылжыту ережелері
Бағдарламалық жасақтаманы санаттау
Басқару сервері параметрлерін сақтық көшірмелеу және қалпына келтіру
Басқару сервері бар құрылғы істен шықты
Басқару серверінің параметрлері немесе дерекқор зақымдалған
Автономды пайдаланушыларға арналған қосылым профильдері туралы
Желілік агентті басқа Басқару серверіне ауыстырып қосу туралы
Автономды пайдаланушылар үшін қосылым профилін жасау
Басқарылатын құрылғыларға қашықтан қатынасу
Басқарылатын құрылғы мен Басқару сервері арасындағы тұрақты байланысты қамтамасыз ету үшін "Басқару серверімен байланысты үзбеу" параметрін қолдану
Құрылғыны Басқару серверіне қосу уақытын тексеру туралы
Мәжбүрлеп синхрондау туралы
Өлшеу нұсқаулығы
Осы нұсқаулық туралы
Басқару серверлері үшін есептеулер
Басқару сервері үшін аппараттық ресурстарды есептеу
ДҚБЖ және Басқару серверіне арналған аппараттық талаптар
Дерекқорда орынды есептеу
Дискідегі орынды есептеу
Басқару серверлерінің саны мен конфигурациясын есептеу
Динамикалық виртуалды машиналарды Kaspersky Security Center бағдарламасына қосу бойынша ұсыныстар
Тарату нүктелері мен қосылым шлюздеріне арналған есептеулер
Тарату нүктесі үшін талаптар
Тарату нүктелерінің саны мен конфигурациясын есептеу
Қосылым шлюздерінің санын есептеу
Тапсырмалар мен саясаттар үшін оқиғалар туралы ақпаратты сақтау
Көптеген құрылғыны басқаратын басқару серверіне арналған ең озық тәжірибелер
Кейбір тапсырмалардың ерекшеліктері мен оңтайлы параметрлері
Құрылғыны табу жиілігі
Басқару сервері деректерінің резервтік қоймасы және дерекқорға қызмет көрсету тапсырмалары
Kaspersky Endpoint Security жаңарту топтық тапсырмалары
Түгендеу тапсырмасы
Басқару сервері мен қорғалатын құрылғылар арасында желіге түсетін жүктеме туралы ақпарат
Әртүрлі сценарийлерді орындау кезіндегі трафик шығыны
Трафиктің тәулік ішіндегі орташа шығыны
Шектеулер тізімі

Техникалық қолдау қызметіне жүгіну
Техникалық қолдау алу жолдары
Kaspersky CompanyAccount арқылы техникалық қолдау
Басқару серверінің қоқыс файлдарын алу
Бағдарлама мәліметтері көздері
Глоссарий
Cloud Discovery
FileTransferBridge
HTTPS
iOS MDM құрылғы
iOS MDM сервері
JavaScript
Kaspersky Private Security Network (KPSN)
Kaspersky Security Center Linux Web Server
Kaspersky Security Center Linux әкімшісі
Kaspersky Security Center System Health Validator (SHV)
Kaspersky Security Center операторы
Kaspersky жаңарту серверлері
Network Location Awareness (NLA)
Provisioning профилі
SSL
Антивирустық дерекқорлар
Антивирустық қорғаныс провайдері
Арнайы құрылғыға арналған тапсырма
Әкімшілік құқықтар
Әкімшінің жұмыс станциясы
Бағдарлама параметрлері
Бағдарламаларды орталықтандырылған басқару
Бағдарламаны тікелей басқару
Басқару консолі
Басқару сервері
Басқару сервері деректерін сақтық көшірмелеу
Басқару сервері сертификаты
Басқару серверінің деректерін қалпына келтіру
Басқару серверінің клиенті (Клиент құрылғысы)
Басқару тобы
Басқарылатын құрылғылар
Белсенді кілт
Виртуалды Басқару сервері
Вирустық шабуыл
Демилитаризацияланған аймақ (DMZ)
Есептік деректер және қатынасу диспетчері (IAM)
Жалпы сертификат
Жаңарту
Желілік агент
Желінің антивирустық қорғанысы
Желінің қорғаныс күйі

Жеңіл N агенті (LWNGT)
Жергілікті тапсырма
Жергілікті түрде орнату
Ішкі пайдаланушылар
Кеңінен таратын домен
Кілт файлы
Клиент әкімшісі
Конфигурациялық профиль
Қалпына келтіру
Қашықтан орнату
Қолданбалар дүкені
Қолжетімді жаңарту
Қолмен орнату
Қорғаныс күйі
Қосылым шлюзі
Қосымша (немесе резервтегі) лицензиялық кілт
Құрылғының иесі
Лицензия мерзімі
Оқиғалар қоймасы
Оқиғаның маңыздылық деңгейі
Орнату пакеті
Осалдық
Патчтың маңыздылық деңгейі
Провайдер әкімшісі
Профиль
Рөлдік топ
Сақтық көшірме қоймасы
Саясат
Тапсырма
Тапсырма параметрлері
Тарату нүктесі
Топтық тапсырма
Түпнұсқалық растама агенті
Үйдегі Басқару сервері
Үйлесімсіз бағдарлама
Үшінші тарап коды туралы ақпарат
Тауар белгілері туралы хабарландырулар

Kaspersky Security Center Linux бағдарламасына анықтама

Жаңа функциялар

- Не жаңалық

Аппараттық және бағдарламалық талаптар

- Басқару серверіне қойылатын талаптар
- Web Console консоліне қойылатын талаптар
- Желілік агентіне қойылатын талаптар

Жұмысқа кірісу

- Орнату
- Бағдарламаны жылдам іске қосу шебері
- Қорғанысты орналастыру шебері

Лицензиялау және белсендіру

- Kaspersky Security Center Linux-ті белсендіру
- Басқарылатын бағдарламаларды лицензиялау

Орналастыру және конфигурациялау

- Желідегі құрылғыларды табу
- Тарату нүктелері мен қосылым шлюздерін конфигурациялау
- Үшінші тарап қауіпсіздік бағдарламаларын алмастыру

- Kaspersky бағдарламалары. Орталықтандырылған орналастыру
- Желі қорғанысын конфигурациялау
- Kaspersky бағдарламалары. Дерекқорлар мен бағдарламалық модульдерді жаңарту
- Басқару серверінің қосылу мекенжайын конфигурациялау
- Kaspersky Security Center Linux бағдарламасына тасымалдау
- Kaspersky Security Center Linux нұсқасын жаңарту туралы ақпарат

Мониторинг

- Бақылау және есеп беру
- Cloud Discovery

Клиент құрылғыларын басқару

- Басқарылатын құрылғыларға қашықтан қатынасу

Осалдықтар мен патчтарды басқару

- Үшінші тарап бағдарламаларындағы осалдықтарды анықтау және түзету

Кеңейтілген мүмкіндіктер

- Оқиғаларды SIEM жүйелеріне экспорттау
- KSN прокси-серверінің статистикасын көру
- Өлшеу нұсқаулығы (тек онлайн анықтама)

Не жаңалық

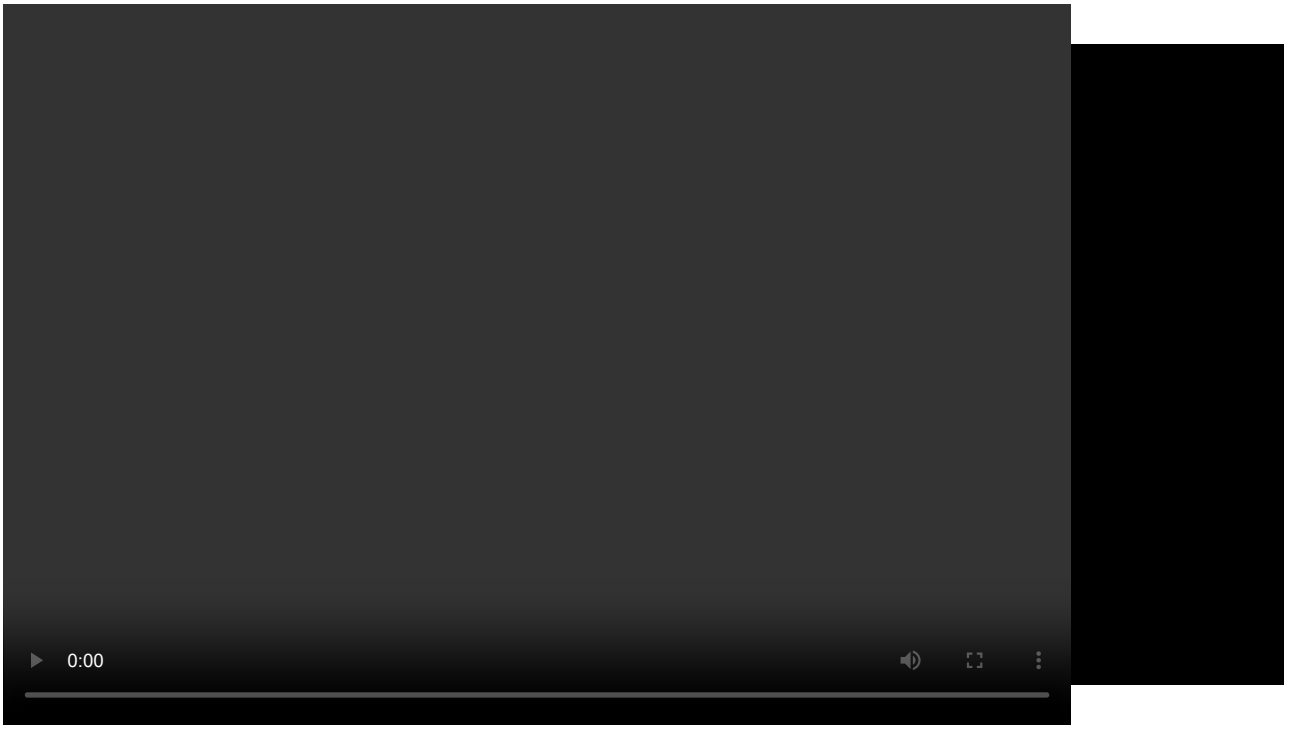
Kaspersky Security Center 16.3 Linux

Kaspersky Security Center 16.3 Linux бағдарламасында бірнеше жаңа функциялар мен жақсартулар іске асырылған:

- Егер сіз саясатты өзгертсеңіз, өзгертілген әрбір параметр үшін бөлек аудит оқиғасы жасалады. Оқиғалар SIEM-ге экспортталады.
- **Kaspersky SIEM** (KUMA) қолдауы енді SIEM жүйелеріне оқиғаларды экспорттау функциясына қосылды.
- Kaspersky Security Center Linux енді Kaspersky Vulnerability Management шешімімен жұмысты қолдайды.
- Қауіпсіздікті күшейту жөніндегі нұсқаулыққа сәйкес болу үшін біз Басқару сервері, Web Console және ДҚБЖ бар құрылғыларға орнатуға, сондай-ақ Kaspersky Security Center Linux ақауларға төзімді кластерін орналастыруға арналған оңтайландырылған Kaspersky Endpoint Security for Linux конфигурациясын әзірледік.
- Енді Kaspersky Security Center Linux жүйесін орнатқан кезде арнайы дерекқор схемасын көрсете аласыз.
- **Мониторинг → Бақылау тақтасы** қорғаныс деңгейінің индикаторы Басқару серверіңіз бен тарату нүктелеріңіздің қауіпсіздігін бағалауға көмектеседі. Егер индикатор сары немесе қызыл болса, мәселелерді шешу және индикатор күйін жасылға өзгерту үшін әрекеттерді орындау керек.
- Kaspersky Security Center Linux орналастырудың жеңілдетілген әдісі қолжетімді: енді орнату скриптін пайдалана аласыз.
- Келесі ескірген операциялық жүйелерді қолдау үшін glibc 2.5 нұсқасы бар Linux Legacy-ге арналған Kaspersky Желілік агентінің арнайы дистрибутиві қолжетімді:
  - CentOS 5.2
  - CentOS 5.4
  - CentOS 6.4
  - CentOS 6.6
  - Astra Linux Special Edition RUSB.10015-01 (1.4 операциялық жаңартуы) 64 разрядты
- Желілік агент енді операциялық жүйенің келесі жаңа нұсқаларымен жұмыс істеуге қолдау көрсетеді:
  - Microsoft Windows 11 IoT Enterprise, 25H2 нұсқасы 64-бит
  - SberOS 3.6.1
  - Ubuntu Server 26.04 LTS (Noble Numbat)

- Келесі ДҚБЖ енді қолдау көрсетілмейді:
  - MySQL 5.7
  - MariaDB 10.1.30
- Пайдаланушы тәжірибесін жақсарту:
  - Тапсырмалар мен Саясаттар кестелері үшін жақсартылған сүзгілеу. Енді `OR` логиканы, сондай-ақ бір қасиет үшін бірнеше мәндерді таңдауға және көрсетілген критерийлердің кем дегенде біреуіне сәйкес келетін жазбаларды көрсетуге мүмкіндік беретін жаңа операторды пайдаланып, бірнеше шартты қосуға болады.
  - Негізгі мәзірде:
    - **Бағдарламалық жасақтаманы басқару** жаңа бөлімі қолжетімді. Келесі бөлімдер енді **Бағдарламалық жасақтаманы басқару** көшірілді: **Орнату пакеттері**, **Kaspersky бағдарламалары**, **Үшінші тарап бағдарламалары**, **Ағымдағы бағдарлама нұсқалары** және **Патчтарды басқару**.
    - **Тағайындалмаған құрылғылар** және **Жабдық** бөлімдер енді **Активтерді басқару** бөліміне ауыстырылды.
    - **Тапсырмалар** және **Қоймалар** бөлімдері мәзірдің бірінші деңгейіне ауыстырылды.
    - **Веб-плагиннің сақтық көшірмелері** бөлімі енді пайдаланылмайды және Web Console-ден жойылады.

Kaspersky Security Center 16.2 Linux



16.2 нұсқасындағы жаңа мүмкіндіктерге шолу. Бейне

Kaspersky Security Center 16.2 Linux бағдарламасында бірнеше жаңа функциялар мен жақсартулар іске асырылған:

- Kaspersky Security Center Web Console веб-консолінде енді демилитаризацияланған аймақта (DMZ) қосылым шлюзін конфигурациялауға болады.

  Қосылым шлюзін конфигурациялау үшін **DMZ қосылу шлюзін мекенжайы бойынша пайдалану** опциясын пайдаланыңыз.

- Linux құрылғыларында Желілік агент құрылғысының идентификаторын сақтау алгоритмі (`Device ID` параметр) жақсартылды. Егер құрылғының BIOS сериялық нөмірі, аналық тақшаның сериялық нөмірі, сақтау дискілерінің идентификаторлары немесе MAC мекенжайы бұрын белгілі мәндерге сәйкес келсе, Басқару сервері құрылғыны операциялық жүйе жаңартылғаннан немесе MAC мекенжайы өзгергеннен кейін бұрын анықталған құрылғы ретінде дұрыс анықтайды.

- Әртүрлі деректерді өңдеу орталығында орналасқан түйіндері бар географиялық таралған Kaspersky Security Center Linux ақаулық кластеріне қолдау қосылды. Географиялық таралған кластер конфигурациясында барлық компоненттер ақаулық болып табылады.

- Енді оқиғаларды SIEM жүйесіне CEF немесе LEEF форматтарында экспорттай аласыз.

- Автоматты ақаулық үшін Patroni және жүктемені теңестіру үшін HAProxy бар жоғары қолжетімді PostgreSQL кластеріне қолдау қосылды.

- Саясат түзетулерін салыстыра аласыз. Бұл опция Басқару сервері, Желілік агент, Kaspersky Endpoint Security for Windows (14.0 веб-плагин нұсқасынан бастап) және Kaspersky Endpoint Security for Mac (12.2.1 Patch A веб-плагин нұсқасынан бастап) саясаттары үшін қолжетімді. Бұл мүмкіндікті қолдайтын Kaspersky қолданбаларының тізімі болашақ нұсқаларда кеңейтіледі.

- SNMP енді қолдау көрсетіледі. SNMP арқылы үшінші тарап клиенттік қолданбаларына Басқару сервері туралы ақпаратты, статистиканы және оқиғаларды бере аласыз.

- Windows желісіндегі сауалнама енді Windows негізіндегі тарату нүктелері үшін қолдау көрсетіледі.

- Linux үшін Желілік агент үшін енді бірыңғай орнату пакеті қолжетімді. Бұл орнату пакетіне әртүрлі пакет менеджерлері мен CPU архитектураларына арналған нұсқалар кіреді. Орнату кезінде орта автоматты түрде анықталады және тиісті Желілік агент орнату пакеті орнатылады.

- Енді оқиғаларға мобильді құрылғыларда орындалатын пәрмендердің бастамашысы туралы ақпарат кіреді.

- NSQ компоненті Kaspersky Security Center Web Console дистрибутивінен жойылды. KSCWebConsoleMessageQueue.service қызметі енді пайдаланылмайды және Kaspersky Security Center Web Console жаңартылғаннан кейін жойылады.

- Оқшауланған желілерде Windows құрылғыларына арналған орнату пакеттерін жасау енді Kaspersky веб-сайтынан қосымша модульдерді жүктеуді қажет етеді (ri_utils_win32.zip and ri_utils_arm64.zip мұрағаттары).

- Желілік агент енді Windows ARM 64-биттік архитектурасын қолдайды. Басқарылатын қолданбалармен үйлесімділікті тиісті анықтама құжаттамасынан тексеруге болады.

- Kaspersky Security Center Linux жүйесі Kaspersky Sandbox-пен жұмыс істеуді қолдайды.

- Пайдаланушы тәжірибесін жақсарту:
  - Енді сіз оқиғалар таңдауынан және құрылғылар оқиғалары тізімінен барлық оқиғаларды бірден жоя аласыз.

    Барлығын таңдау және **Ағымдағы беттегінің барлығын таңдау** опциялары оқиғалар таңдау және құрылғылар оқиғалары тізімінде қолжетімді.
  - Сіз жылжытылатын ережелердің басымдығын енді қолмен көрсете аласыз.

    Басымдықты өзгерту түймесі жылжыту ережесін таңдағанда қолжетімді болады және жаңа басымдықты көрсетуге мүмкіндік береді.
- Kaspersky Security Center Linux жүйесі Platform V SberLinux OS Server (SLO) 9.6 нұсқасымен жұмыс істеуді қолдайды.
- Kaspersky Security Center Linux енді келесі ДҚБЖ-мен жұмысты қолдайды:
  - MySQL Standard Edition 8.4
  - MySQL Enterprise Edition 8.4
  - PostgreSQL 18
  - Postgres Pro 18 (барлық басылым)
  - Postgres Pro 18 Enterprise (Built-in High Availability кластері)
- Желілік агент енді операциялық жүйенің келесі жаңа нұсқаларымен жұмыс істеуге қолдау көрсетеді:
  - Windows 11 Home/Pro/Pro for Workstations/Enterprise/Education ARM
  - Platform V SberLinux OS Server (SLO) 9.6

Kaspersky Security Center 16.1 Linux

Kaspersky Security Center 16.1 Linux бағдарламасында бірнеше жаңа функциялар мен жақсартулар іске асырылған:

- Екі факторлы аутентификация енді әдепкі бойынша қосылған. Екі факторлы аутентификацияны өшірудің жаһандық опциясы енді қолжетімді емес. Пайдаланушылардың Kaspersky Security Center Web Console-ге кіріп, OpenAPI автоматтандыру скрипттерін пайдалануды жалғастыра алатынына көз жеткізу үшін жаңарту алдында барлық пайдаланушылар үшін екі факторлы аутентификацияны қосыңыз.
- Енді саясат профилін саясатты экспорттамастан KLPROF файлына сақтауға болады, содан кейін сақталған профильді саясатқа импорттау үшін осы KLPROF файлын пайдалануға болады.
- Желілік агент енді жабық бағдарламалық жасақтама ортасы режимінде ALT OS жұмыс істейтін құрылғыда жұмыс істейді.
- SCRIL протоколын пайдалану арқылы құпия сөзсіз домен пайдаланушылары үшін Kerberos негізіндегі домен аутентификациясын қолдау қосылды, бұл сертификатқа негізделген бірыңғай кіруді (SSO) қосады.

- Пайдаланушы тәжірибесін жақсарту:
  - Клиент құрылғыларын операциялық жүйе нұсқасы және пакет менеджері бойынша сүзу енді Linux операциялық жүйесінің нұсқаларын қамтиды.
  - Kaspersky Security Center Web Console веб-консоліндегі кестелер үшін беттеу механизмі жақсартылды: көрсетілген элементтердің әдепкі саны 50-ге дейін арттырылды және көрсетілген элементтердің реттелетін саны енді сеанстар арасында сақталады.
  - Санаттағы қолданбаларды қосу және алып тастау ережелерінің сипаттамаларын қосуға мүмкіндік беретін қолданба санаттарына түсініктемелер.
  - Әдепкі бойынша, қолжетімді орнату пакеттерінің тізімі енді тек Kaspersky Security Center Web Console интерфейс тілінде және ағылшын тілінде Касперский Зертханасы қолданбасын орнату пакеттерін көрсетеді.
- Kaspersky Security Center Linux Kaspersky Endpoint Security for Linux 12.4 үшін жұмысты қолдайды.
- Желілік агент енді операциялық жүйенің келесі жаңа нұсқаларымен жұмыс істеуге қолдау көрсетеді:
  - Debian GNU/Linux 13 (Trixie)
  - CentOS Stream 10
  - Red Hat Enterprise Linux Server 10.x
- Желілік агент енді операциялық жүйенің келесі жаңа нұсқаларымен жұмыс істеуге қолдау көрсетеді:
  - ALT Workstation 11
  - Альт Сервер 11
  - ALT Education 11
  - AlterOS 2025
  - SberOS 3.4.0
  - SberOS 3.5.0
  - OSnova 3.*

Kaspersky Security Center 16 Linux

Kaspersky Security Center 16 Linux бағдарламасында бірнеше жаңа функциялар мен жақсартулар іске асырылған:

- FreeIPA және ALD Pro домен контроллерлеріне қолдау көрсетіледі.
- Домен аутентификациясы (бірыңғай кіру) ендірілді. Бірыңғай кіру функциясы корпоративтік желіде құпиясөзді қайта енгізбей-ақ Kaspersky Security Center 16 Web Console веб-консолінде қауіпсіз аутентификацияны қосуға мүмкіндік береді. Домен аутентификациясын пайдалану үшін Kaspersky Security Center Web Console орнату кезінде жауап файлында қосымша параметрлерді көрсету керек.
- Kaspersky Security Center 16 Linux басқару сервері тек Kaspersky Security Center 16 Web Console-мен үйлесімді. Kaspersky Security Center Web Console бұрынғы нұсқаларын пайдалану мүмкін емес.
- Қосалқы басқару серверін қосып, осы серверді сынақ лицензиясы бойынша белсендірсеңіз және лицензия кілтін қосалқы басқару сервері басқаратын құрылғыларға орналастырсаңыз, енді Kaspersky Security: Бизнеске арналған Кәсіби функционалдығын сынақ лицензиясы бойынша пайдалана аласыз.
- Пайдаланушы тәжірибесін жақсарту:
  - Басқару топтары және басқару серверлері арқылы навигация жаңартылды: бір навигация панелінен топтар мен серверлер арасында оңай ауысуға болады.
  - Профиль параметрлері жоғарғы панельге жылжытылады.
  - Негізгі мәзірдің келесі бөлімдерінің атауы өзгертілді:
    - **Активтер (Құрылғылар)** бөлімі енді **Активтерді басқару** деп аталады.
    - **Басқарылатын құрылғылар Активтер (құрылғылар)** деп аталады.
    - **Жылдам сілтемелер** атауы **Консольді шарлау** деп өзгертілді.
  - Қажет болса, негізгі мәзірді белгішелерге дейін кішірейтуге болады.
  - **Kaspersky жаңалықтары** бөлімі **Мониторинг → Хабарландырулар** бөлімінен жойылды.
- **Операциялар → Патчтарды басқару → Бағдарламалық жасақтама осалдықтары** және **Операциялар → Патчтарды басқару → Бағдарламалық жасақтама жаңартулары** бөлімдеріндегі кестелерге қолданылатын сүзгілер енді сәтті сақталды және қалпына келтірілмейді.
- Kaspersky Security Center Linux келесі жұмыстарға қолдау көрсетеді:
  - Kaspersky NGFW
  - Келесі операциялық жүйе нұсқаларымен (басқарылатын құрылғылар үшін):
    - MosOS 15.5 Arbat
    - Microsoft Windows 11 25H2

- CentOS 6.4
- CentOS 6.6

Kaspersky Security: Бизнеске арналған Кәсіби лицензиясындағы Kaspersky Security Center 15.4 Linux

Kaspersky Security: Бизнеске арналған Кәсіби лицензиясында басқару серверін белсендірсеңіз және басқарылатын қолданбаларға Kaspersky Security: Бизнеске арналған Кәсіби лицензия кілтін қолдансаңыз, келесі әрекеттерді орындауға болады:

- Дабылдарды атрибуттар бойынша топтау.
- Қауіптерге жауап беру үшін интеграцияларды конфигурациялау.

Kaspersky Security Center 15.4 Linux

Kaspersky Security Center 15.4 Linux бағдарламасында бірнеше жаңа функциялар мен жақсартулар іске асырылған:

- Linux құрылғылары бар кеңседе емес пайдаланушылар үшін қосылым профильдері енді қолжетімді. Қосылым профильдерінің көмегімен сіз Linux құрылғыларындағы желілік агенттерді құрылғының орналасқан жеріне байланысты бірдей немесе әртүрлі басқару серверлеріне қосу ережелерін конфигурациялай аласыз.
- Басқару серверлері арасында шифрлау кілттерін тасымалдау енді қолжетімді.
- Kaspersky Thin Client клиентіне енді қолдау көрсетіледі.
- Platform V Pangolin кірістірілген жоғары деңгейдегі қолжетімділік кластеріне енді қолдау көрсетіледі.
- Postgres Pro кірістірілген жоғары деңгейдегі қолжетімділік кластеріне енді қолдау көрсетіледі. Бұл ДҚБЖ кластерінің түйіндері Kaspersky Security Center Linux орнату кезінде қосылым жолында көрсетіледі.
- Kaspersky Security Center Linux енді келесі ДҚБЖ-мен жұмысты қолдайды:
  - Platform V Pangolin 6.5.1
  - Tantor SE 1C for Astra Linux Special Edition RUSB.10015-01 (операциялық жаңарту 1.8)
  - Jatoba 5
- Platform V SberLinux OS Server (SLO) 8.10.1, 9.0.1, 9.5.1 нұсқаларына қолдау көрсетіледі.
- KlAkOAPI.tar.gz мұрағаты анықтамадан жойылды. KlAkOAPI.tar.gz мұрағаты Kaspersky Security Center Linux орнату қалтасында орналасқан.

- **Сканерлеу** түймесі **Карантин** бөлімінен жойылады.
- Өлшемі, файл хэші және жолы туралы ақпарат желілік агент автономды пакеті немесе виртуалды басқару серверлерінде жасалған кез келген пакет үшін орнату пакеттерінің тізімінде қолжетімді емес, себебі бұл автономды пакеттер жүктеп алу кезінде жасалады.

Kaspersky Security Center 15.3 Linux

Kaspersky Security Center 15.3 Linux бағдарламасында бірнеше жаңа функциялар мен жақсартулар іске асырылған:

- klcsngtgui утилитасы Kaspersky Security Center Linux тарату жинағынан жойылған. klcsngtgui утилитасының орнына klnagchk утилитасын пайдалануды ұсынамыз.
- Желілік агент енді операциялық жүйенің келесі жаңа нұсқаларымен жұмыс істеуге қолдау көрсетеді:
  - Windows Server 2025
  - Fedora Linux Server 41
  - Fedora Linux Workstation 41
- Kaspersky Security Center Linux енді келесі ДҚБЖ-мен жұмысты қолдайды:
  - PostgreSQL 17
  - Postgres Pro 17
- Kaspersky жаңарту утилитасын қолданып, енді Kaspersky қауіпсіздік қолданбаларына арналған дерекқорлар мен бағдарламалық жасақтама модульдерінің тек қажетті жаңартуларын жүктеп алуға болады. **Жаңартуларды Басқару серверінің қоймасына жүктеп алу** тапсырмасының сипаттар терезесінде **Жаңарту сұрауының файлын автоматты түрде жүктеп алу** опциясын қосыңыз, содан кейін Kaspersky Security Center Linux жүктеп алынатын жаңартулар туралы ақпараты бар жаңарту сұрауларының файлын жасайтын жолды көрсетіңіз.
- KSN прокси-серверін пайдалану статистикасын енді көруге болады.
- Kaspersky Security Center Windows басқару серверінің деректерін klbackup утилитасын пайдалану арқылы Kaspersky Security Center Linux жүйесіне көшіру әрекеті жаңартылды. Енді Microsoft SQL Server дерекқорында сақталған басқару сервері деректерін PostgreSQL немесе Postgres Pro жүйесіне көшіруге болады.
- Басқару серверінің қосылым мекенжайын конфигурациялау енді қолжетімді. Басқару серверінің қосылым мекенжайы желілік агенттің орнату пакеттерін жасау кезінде әдепкі мекенжай ретінде және басқарылатын құрылғыларды KSN-ге қосу кезінде KSN прокси-серверінің мекенжайы ретінде пайдаланылады.
- Енді басқарылатын құрылғыларды орталықтан қайта іске қосуға болады.
- Қазіргі уақытта Linux басқарылатын құрылғысына кірген пайдаланушылар туралы ақпарат енді құрылғы сипаттары терезесінің **Жалпы** → **Сеанстар** бөлімінде көрсетіледі.

- Енді осы құрылғыларға орнатылған желілік агент арқылы Linux және Windows басқарылатын құрылғыларына қашықтан қол жеткізуге болады. Қосылым RDP, VNC немесе WDS арқылы орнатылады. Құрылғыға қосылғаннан кейін, әкімші осы құрылғыдағы ақпаратқа толық қатынас алады және онда орнатылған бағдарламаларды басқара алады.

- Басқарылатын құрылғыда диагностикаға арналған қолданбаны (немесе скриптіні) жүктеп салыңыз және іске қосыңыз. Енді орындалатын файлды қамтитын каталогті не мұрағатты немесе орындалатын файлдың өзін жүктеп салуға болады. Қолданба сәтті орындалғаннан кейін, орындау нәтижелерін жүктеп алуға болады.

- Пайдаланушы тәжірибесі жақсартылды, соның ішінде жаңа **Жылдам сілтемелер** бөлімі қосылды. Бұл бөлім негізгі мәзір картасын көрсетеді және Kaspersky Security Center Web Console барлық бөліміне жылдам кіруге мүмкіндік береді. Әдепкісінше **Жылдам сілтемелер** басты бет ретінде орнатылады.

Kaspersky Security Center 15.2 Linux

Kaspersky Security Center 15.2 Linux бағдарламасында бірнеше жаңа функциялар мен жақсартулар іске асырылған:

- Ішкі пайдаланушы есептік жазбаларының құпиясөздерін басқаруға арналған жаңа мүмкіндіктер:

  - Енді Kaspersky Security Center Web Console жүйесіне бірінші (немесе келесі) рет кіру кезінде ішкі пайдаланушыны құпиясөзді өзгертуге мәжбүрлеуге болады.

  - Ішкі пайдаланушы есептік жазбаларына арналған құпиясөздің жарамдылық мерзімін конфигурациялаудың жаңа опциясы.

- Енді klbackup утилитасын қолданып, Kaspersky Security Center Windows басқару сервері деректерінің сақтық көшірмесін жасап, оларды Kaspersky Security Center Linux жүйесінде қалпына келтіруге болады. Тасымалдау әрекетін бірдей түрдегі ДҚБЖ немесе Microsoft SQL сервері > MySQL не MariaDB арқылы деректерді жоғалтпай орындауға болады.

- Kaspersky Security Center Linux енді келесі ДҚБЖ-мен жұмысты қолдайды:

  - PostgreSQL 16.x

  - Postgres Pro 16.x

- Kaspersky Security Center Linux енді PostgreSQL және Postgres Pro кластерлерінің кейбір түрлеріне қолдау көрсетеді.

- Жаңа операциялық жүйелерге және операциялық жүйенің жаңа нұсқаларына, соның ішінде OS MES (Moscow Electronic School), MosTech және MosTech Server жаңа нұсқаларына қолдау көрсету.

- Пайдаланушы тәжірибесін жақсарту, соның ішінде:

  - Саясат параметрлері терезесіндегі жаңа **Сақтау** түймесі. Саясат параметрлері терезесін жаппай-ақ өзгерістерді сақтағыңыз келсе, осы түймені пайдаланыңыз.

- Енді файлдарды Android құрылғыларына жіберу әрекетін басқаруға, алдыңғы жіберілген файлдарды жоюға және олардың параметрлерін Kaspersky Mobile Devices Protection and Management плагинінің жаңа "Қолданбалар және файлдар" бөлімінде конфигурациялауға болады.

- Енді қосылым шлюзінің жаңа веб-сервер қызметін пайдаланып, қолданбаны орнату пакеттері мен құрылғыны басқару профильдерін мобильдік құрылғыларға оларды басқару серверіне тікелей қоспай-ақ тасымалдауға болады.

Kaspersky Security Center 15.1 Linux

Kaspersky Security Center 15.1 Linux бағдарламасында бірнеше жаңа функциялар мен жақсартулар іске асырылған:

- Kaspersky Security Center Web Console енді Kaspersky мобильдік құрылғыларды қорғау және басқару плагині арқылы мобильдік құрылғыларды басқаруға қолдау көрсетеді.

- Енді iOS MDM құрылғыларын басқару үшін iOS MDM серверлерін iOS MDM серверінің параметрлері плагині арқылы орнатуға және конфигурациялауға болады.

- Енді мобильдік құрылғылардың сертификаттарын басқара аласыз.

- Kaspersky Endpoint Security for Android бағдарламасына енді қолдау көрсетіледі.

- Kaspersky Security for iOS қолданбасына енді қолдау көрсетіледі.

- Kaspersky Endpoint Security for Aurora бағдарламасына енді қолдау көрсетіледі.

- Windows операциялық жүйесімен жұмыс істейтін басқарылатын құрылғылар үшін осалдықтар мен патчтарды басқару. Windows операциялық жүйелерімен жұмыс істейтін басқарылатын құрылғыларда орнатылған үшінші тарап бағдарламалық жасақтамасының жаңартуларын басқаруға және қажетті жаңартуларды орнату арқылы мұндай қолданбалардағы осалдықтарды жабуға болады.

- Kaspersky Security Center Linux енді бір уақытта бүкіл домен контроллерін емес, бет бойынша домен контроллерлерін сұрайды. Бұл жазбалардың көп санын қамтитын домен контроллерлеріне сұрау салуға мүмкіндік береді.

- Аномалияларды бейімделумен басқару. Бұл клиент құрылғыларындағы әдеттен тыс әрекетті бақылау үшін ережелер жинағын пайдаланатын және аномалды әрекеттерді бұғаттауға мүмкіндік беретін Windows жүйесіне арналған Kaspersky Endpoint Security функциясы.

- Windows басқаруымен жұмыс істейтін құрылғыларда орнатылған Kaspersky басқарылатын қолданбаларға, сондай-ақ Linux жүйесі үшін Желілік агентке арналған жаңартулар. Орнатылуы тиіс жаңартуларды мақұлдау және орнатылмауы тиіс жаңартуларды қабылдамау арқылы жаңартуды орнату процесін басқаруға болады.

- Кеңейтілген саясаттар аудиті. Енді сіз саясаттың тексерісін көре аласыз және саясаттың тексерісін файлға сақтай аласыз. Қазіргі уақытта бұл мүмкіндіктер тек Басқару сервері және Желілік агент саясаттары үшін қолжетімді.

- Cloud Discovery. Kaspersky Security Center Linux қолданбасының жаңа функционалдығы Windows операциялық жүйесімен жұмыс істейтін басқарылатын құрылғыларда бұлттық сервистерді пайдалануды бақылауға және қажетсіз бұлттық сервистерге кіруді бұғаттауға мүмкіндік береді.

- Негізгі мәзірдің **Мониторинг** бөліміндегі жаңа **Дабылдар** бөлікшесі. **Дабылдар** бөлімінде, құрылғыларда табылған қауіптер туралы ақпаратты қарай аласыз. Қауіптерді Kaspersky қауіпсіздік қолданбалары анықтайды.

- Kaspersky Security Center Linux енді Kaspersky Managed Detection and Response шешімінің құрамдасы болып табылады.

- Kaspersky Security for Virtualization Жеңіл агентке қолдау көрсетіледі.

- macOS құрылғыларының кеңейтілген түгендемесі. macOS құрылғысындағы Желілік агент құрылғының MAC мекенжайы мен сериялық нөмірін Басқару серверіне жібереді.

- Басқарылатын құрылғыларға бағдарламалық жасақтаманы пайдаланушылық скрипттерді пайдаланып орнатқанда, енді қашықтан орнату есебін алуға болады.

- Басқарылатын құрылғыда бірнеше пайдаланушылық скриптті орындаған кезде, олардың орындалу ретін анықтау үшін әрбір сценарийге басымдық беруге болады. Скрипттер ең жоғары басымдықты скрипттен ең төменгі басымдықты скриптке дейін орындалады.

- Kaspersky Endpoint Security for Linux және Linux үшін Желілік агент пайдаланатын жедел жад көлемін азайту үшін Linux үшін Желілік агентке арналған арнайы жұмыс режимін қосуға болады. Бұл режимде Linux үшін Желілік агент азырақ жедел жадты қажет етеді, бірақ оның функционалдығы шектеулі.

- Басқарылатын құрылғылардан үйлеспейтін бағдарламалық жасақтаманы *Бағдарламаны қашықтан жою* тапсырмасы арқылы жоюға болады.

- Желілік шабуылдар туралы есеп енді шабуылдаушы құрылғының MAC мекенжайы мен портын қамтиды.

- Ішкі пайдаланушы үшін құпиясөздің максималды ұзындығы 256 таңбаға дейін ұлғайтылды.

- Пайдаланушы тәжірибесін жақсарту, соның ішінде:

  - **Бетбелгілер** бөлімінен жылдам кіру үшін бетбелгілерге Kaspersky Security Center Web Console бөлімдерін қосу арқылы негізгі мәзірді жекелендіру.

  - Кестелермен жұмыс оңтайландырылды. Әрбір кесте үшін әдепкі көрініс енді ең жиі қолданылатын бағандарды қамтиды. Сондай-ақ, енді ағымдағы беттегі немесе бүкіл кестедегі барлық элементтерді таңдап, элементтерді бүкіл кесте бойынша сұрыптауға болады.

  - Есептерді тарату конфигурациясы жақсартылды. Енді есепті тарату үшін 20 электрондық пошта мекенжайына дейін көрсетуге және есепті тарату кестесін белгілеуге болады.

- Операциялық жүйелердің кең ауқымын және операциялық жүйелердің жаңа нұсқаларын қолдау.

- Өлшеу нұсқаулығының жаңа нұсқасы әзірленді және онлайн анықтамада жарияланды.

- Пайдаланушы интерфейсін талдау нәтижесінде Басқару серверінің сипаттары терезесінде **Қашықтан диагностикалау** бөлімінің пайда болуына себеп болған мәселе шешілді.

- Клиенттік құрылғыда орнату пакетін орындау және қолданбаны қашықтан орнату үшін *Скрипттерді қашықтан орындау* тапсырмасын жасауға болады.

- Пайдаланушы Желілік агентті Linux жүйесімен жұмыс істейтін клиенттік құрылғыға орнату кезінде немесе орнатқаннан кейін құрылғы иесі ретінде тағайындалуы мүмкін.

- Сізге құрылғы иесіне, құрылғы иесінің қауіпсіздік тобындағы мүшелігіне және құрылғы иесінің рөліне негізделген құрылғы таңдауын конфигурациялауға немесе құрылғыларды жылжыту ережесін жасауға болады.

- Есептік жазбалар үшін жергілікті әкімші құқықтарын жоюға болады. Бұл пайдаланушы есептік жазбаларын бақылаудың қосымша деңгейін береді. Мысалы, бір реттік тапсырманы орындағаннан кейін жергілікті әкімші құқықтарын жоя аласыз.

- Жергілікті есептік жазбаның құпиясөзін өзгертуге болады, мысалы, пайдаланушы жергілікті есептік жазба құпиясөзін ұмытып қалғанда немесе құпиясөзді кесте бойынша өзгерту үшін.

- **Пайдаланушы сертификаттарын басқару** ішкі бөлімінде қай түбірлік сертификаттарды орнату керектігін көрсетуге болады. Бұл сертификаттарды, мысалы, веб-сайттардың немесе веб-серверлердің түпнұсқалығын тексеру үшін пайдалануға болады.

Kaspersky Security Center 15 Linux

Kaspersky Security Center 15 Linux бағдарламасында бірнеше жаңа функциялар мен жақсартулар іске асырылған:

- Домен контроллерін сұрау, ол Microsoft Active Directory домен контроллерін және Samba домен контроллерін сұрауға мүмкіндік береді. Microsoft Active Directory каталогін сұрау үшін Басқару серверді немесе тарату нүктесін пайдалануға болады. Samba домен контроллерлерін тек Linux операциялық жүйесі бар тарату нүктесін пайдаланып сұрауға болады. Домен контроллерін сұрау кезінде Басқару сервер немесе тарату нүктесі домен құрылымы, пайдаланушы тіркелгілері, қауіпсіздік топтары және доменге кіретін құрылғылардың DNS атаулары туралы ақпаратты алады.

- Kaspersky Security Center Linux енді келесі ДҚБЖ-мен жұмысты қолдайды:

  - PostgreSQL 15.x

  - Postgres Pro 15.x

- ДҚБЖ ретінде PostgreSQL немесе Postgres Pro пайдалансаңыз, Kaspersky Security Center Linux 50 000 басқарылатын құрылғыларға дейін қолдайды.

- Деректерді Kaspersky Security Center Windows жүйесінен Kaspersky Security Center Linux жүйесіне тасымалдау. Kaspersky Security Center нысан деректерін, соның ішінде тапсырмаларды, саясаттарды және басқару топтар құрылымын тасымалдауға арналған шеберді іске қосуға болады. Осыдан кейін импортталған басқарылатын құрылғыларды Kaspersky Security Center Linux басқаруымен тасымалдауға болады.

- Kaspersky Security Center Linux енді келесі Kaspersky қолданбаларымен жұмысты қолдайды:

  - Kaspersky Security for Virtualization Жеңіл агент

  - 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 Жеңіл агент

- Windows және Linux операциялық жүйелерімен басқарылатын құрылғыларды қашықтан диагностикалау.
- Жақсартылған Қолданбаны бақылау компоненті. Таңдалған қалтадағы орындалатын файлдар тізімі негізінде немесе Kaspersky қолданбаларының санаты негізінде қолданбалар санатын жасауға болады. Содан кейін ұйымыңызда жасалған санаттағы қолданбаларға рұқсат беруді немесе тыйым салуды көрсетуге болады.
- Оқиға таңдауларын экспорттау және импорттау. Пайдаланушы анықтаған оқиғалар таңдауын және оның параметрлерін KLO файлына экспорттай аласыз, содан кейін оқиғалардың сақталған таңдауын Kaspersky Security Center Windows немесе Kaspersky Security Center Linux жүйесіне импорттай аласыз.
- Қауіп-қатер туралы есепте енді **Дабылды көру** сілтемесін басу арқылы қауіптердің даму тізбегін ашуға болады.
- Kaspersky Security Center Linux енді кластерлік технологияны қолдайды. Басқару топта серверлердің кластерлері немесе массивтері болса, **Активтер (құрылғылар)** бетінде екі қойынды көрсетіледі: біреуі жеке құрылғылар үшін, екіншісі серверлердің кластерлері мен массивтері үшін. Басқарылатын құрылғылар кластер түйіндері ретінде анықталғаннан кейін, кластер **Кластерлер және серверлердің массивтері** қойындысына бөлек нысан ретінде қосылады. Кластер түйіндері басқа басқарылатын құрылғылармен бірге **Құрылғылар** қойындысында берілген.
- Kaspersky Security Center Linux қолданбасы кейбір платформаларға қолдау көрсетуді тоқтатты, себебі бұл платформаларға олардың жеткізушілері енді қолдау көрсетпейді.

Kaspersky Security Center 14.2 Linux

Kaspersky Security Center 14.2 Linux бағдарламасында бірнеше жаңа функциялар мен жақсартулар іске асырылған:

- Басқару серверлерінің иерархиясында Linux операциялық жүйесі бар Басқару сервері енді Басты сервер ретінде әрекет ете алады және Linux немесе Windows операциялық жүйелері бар Серверлерді құл ретінде басқара алады.
- Kaspersky Security Center Linux енді Kaspersky Security Network (KSN), KSN прокси сервер қызметін және Kaspersky Private Security Network (KPSN) қызметін қолдайды.
- Kaspersky Security Center Linux енді Windows үшін Kaspersky Endpoint Security басқарылатын бағдарлама ретінде қолдайды.

  Желілік агентті Windows операциялық жүйесімен клиент құрылғыларға қашықтан орнату Windows операциялық жүйесі бар тарату нүктесінің операциялық жүйесінің құрылғыларын пайдалану арқылы ғана мүмкін болады.
- Windows операциялық жүйесі бар құрылғыларындағы деректерді шифрлау портативті құрылғы немесе қатты диск ұрланған/жоғалған жағдайда абайсызда ақпараттың ағып кету қаупін азайтады. Бұл функция Windows үшін Kaspersky Endpoint Security арқылы жүзеге асырылады.

- Kaspersky Security Center Linux жүйесі Kaspersky Security Center Linux пайдаланушы интерфейсінде Kaspersky бағдарламаларының дистрибутивтерін және басқару веб-плагиндерін жүктеп алуға және жаңартуға мүмкіндік береді.

- Әдепкі бойынша, Linux және Windows жүйесімен жұмыс істеп басқарылатын құрылғыларда орнатылған бағдарламалар туралы ақпарат Басқару серверіне жіберіледі.

- Kaspersky серверлеріне қатынасу енді автоматты түрде тексеріледі. Жүйелік DNS арқылы серверлерге қатынасу мүмкін болмаса, бағдарлама жалпыға ортақ DNS жүйесін пайдаланады.

- Басты Басқару сервері, қосалқы Басқару серверлері және Желілік агенттер арасында жіберілетін құпия деректер енді AES шифрлау алгоритмімен қорғалған.

- Виртуалды Басқару сервері пайдаланушысының құқықтары басты Басқару сервері пайдаланушыларының құқықтарына қарамастан конфигурацияланады. Сондай-ақ, сіз басты Сервер пайдаланушыларына виртуалды Серверді басқару құқығын да бере аласыз.

- Kaspersky Security Center Linux енді келесі ДҚБЖ-мен жұмысты қолдайды:

  - PostgreSQL 13.x

  - PostgreSQL 14.x

  - Postgres Pro 13.x (барлық басылым)

  - Postgres Pro 14.x (барлық басылым)

- Сіз Kaspersky Security Center Web Console веб-консолін саясаттар мен тапсырмаларды файлға экспорттау, содан соң саясаттар мен тапсырмаларды Kaspersky Security Center Windows немесе Kaspersky Security Center Linux операциялық жүйелеріне импорттау үшін қолдана аласыз.

- **Прокси-серверді пайдаланбау** параметрі келесі тапсырмалардан жойылған:

  - *Жаңартуларды Басқару серверінің қоймасына жүктеп алу*

  - *Жаңартуларды тарату нүктесінің қоймаларына жүктеп алу*

Kaspersky Security Center 14 Linux

Kaspersky Security Center Linux бағдарламасында бірнеше жаңа функциялар мен жақсартулар іске асырылған:

- *Жаңартуларды Басқару серверінің қоймасына жүктеп алу* тапсырмасынан бөлек, Kaspersky қауіпсіздік бағдарламаларына арналған антивирустық дерекқорларды енді *Жаңартуларды тарату нүктесінің қоймаларына жүктеп алу* тапсырмасы арқылы жүктеп алуға болады.

- Басқарылатын құрылғылардағы антивирустық дерекқорлар мен бағдарлама модульдерін Басқару сервері немесе тарату нүктелері арқылы таратуға және жаңартуға болады. Басқару серверіндегі жүктемені азайту және корпоративтік желідегі деректер трафигін оңтайландыру үшін ұйымыңыз үшін оңтайлы жаңарту схемасын таңдауға болады.

- Kaspersky Security Center Linux жүйесі Kaspersky жаңартулар серверлерінен тек Kaspersky қауіпсіздік бағдарламалары сұраған жаңартуларды жүктейді. Бұл жүктелген деректердің өлшемін азайтады.

- Енді сіз антивирустық дерекқорлар мен бағдарлама модульдерін жүктеп алу үшін айырмашылық файлдардың жүктеу функциясын пайдалана аласыз. Айырмашылықтар файлы дерекқор немесе бағдарламалық модуль файлдарының екі нұсқасы арасындағы айырмашылықтарды сипаттайды. Айырмашылық файлдарын пайдалану трафикті ұйымыңыздың желісінде сақтайды, өйткені айырмашылық файлдары бүкіл дерекқор және бағдарламалық модуль файлдарына қарағанда аз орын алады.

- *Жаңартуды тексеру* тапсырмасы қосылды. Бұл тапсырма арқылы жүктелген жаңартуларды басқарылатын құрылғыларға орнатпас бұрын, жүктелетін жаңартулардың жұмысқа жарамдылығын және қателердің болуын автоматты түрде тексеруге болады.

- Kaspersky Security Center Linux енді Kaspersky Industrial CyberSecurity for Linux Nodes 1.3 бағдарламасын басқарылатын бағдарлама ретінде қолдайды.

Мәселелер шешілді

Төмендегі кестеде алдыңғы Kaspersky Security Center Linux нұсқаларында табылған және ағымдағы нұсқада түзетілген барлық мәселелер көрсетілген.

Kaspersky Security Center Linux 16.3 мәселелер тізімі

Kaspersky Security Center Linux нұсқасында мәселе алғаш рет	Мәселе идентификаторында	Мәселе сипаттамасы
16.2	9959974	Құрылғы сипаттары терезесінің **Оқиғалар** қойындысында Басқару серверінің дерекқорынан барлық оқиғаларды жоюы мүмкін **Барлығын таңдау** опциясының болуына байланысты мәселе шешілді.
16.2	9392997	ALD Pro немесе FreeIPA домен контроллерін сәтті сұрағаннан кейін оқиға журналына қате туралы хабарлама қосылған мәселе шешілді.
16.2	9504495	Пайдаланушының дұрыс тағайындалмауына әкелуі мүмкін мәселе шешілді — құрылғының иесі Желілік агенттің орнату пакетінің параметрлері арқылы тағайындалады.
16.1	9316206	Қойындыны ашқаннан кейін шолғышты жаңартқан кезде басқару түймелері **Екі факторлы аутентификация** қойындысынан жоғалып кетуі мүмкін мәселе шешілді.
16.1	7555541	*Тіркелгі құпиясөзін өзгерту (тек Linux)* тапсырмасын жасаған кезде **Бір реттік құпиясөз ретінде орнату (пайдаланушы есептік жазбаға бірінші кіргеннен кейін, құпиясөзді өзгертуі керек)** опциясын қосқан жағдайда, Web Console жүйесіне кірудің сәтсіз аяқталуына әкелетін мәселе шешілді.
15.4	7555788	SELinux пайдаланушы құрылғысында қосылған болса, *Тіркелгі құпия сөзін өзгерту* тапсырмасы дұрыс жұмыс істемеуі мүмкін мәселе шешілді.
16.2	9603496	Бұл құрылғы туралы диагностикалық ақпарат алу үшін Басқару сервері құрылғысына Желілік агентті орнату қажет болған мәселе шешілді.
16.2	9704308	Басқару топтарының саны көп орталарда бетті жүктеу кезінде **Топтардың иерархиясы** бөлімін ашу `429 Too Many Requests` қатесін тудыруы, Басқару серверімен байланысты үзуі және пайдаланушыларды кіру бетіне қайта бағыттауы мүмкін болған мәселе жойылды.
16.2	9989231	Құрылғыларды қосылымның IP-мекенжайы бойынша сүзгілеу кезінде дұрыс емес нәтижелердің қайтарылу мәселесі шешілді.
16.2	9990025	Беттер арасында шарлау кезінде **Саясаттар** және **Тапсырмалар** бөлімдеріндегі кесте көрінісі параметрлерінің сақталмау мәселесі шешілді.
15.3	9632613	LDAP домен контроллерлері қолжетімсіз болғанда немесе онда пайдаланушы тіркелгісі болмаған кезде, домендік пайдаланушының Web Console консольге кіруі айтарлықтай кешіктірілу мәселесі шешілді.
15.1	9829027	**Антивирустық дерекқорларды пайдалану туралы есеп** есебінде **Күйді жаңарту** сүзгісін баптау кезінде қате орын алу мәселесі шешілді.
15.1	9844707	Прокси-сервер бапталған болса да, Kaspersky Security Center және FCM (Firebase Cloud Messaging) тікелей өзара әрекеттесті.

Kaspersky Security Center Linux 16.2 мәселелер тізімі

Kaspersky Security Center Linux нұсқасында мәселе алғаш рет	Мәселе идентификаторында	Мәселе сипаттамасы
15.1	10071566	Егер кестеде "Апта күндері бойынша" параметрі қолданылса, тапсырма кестесіне енгізілген өзгерістер басқарылатын құрылғыларға таратылмаған мәселе шешілді.
15.4	9067754	Kaspersky Mobile Devices Protection and Management плагинін жаңартқаннан кейін бұрын жасалған саясатта жаңа оқиғалардың дұрыс көрсетілмеуіне әкелетін мәселе шешілді.
16	9329729	Егер жаңарту алдында белгілі бір пайдаланушылар үшін екі факторлы аутентификация конфигурацияланған болса, Kaspersky Security Center Linux жүйесін 16 нұсқасынан 16.1 нұсқасына жаңартқаннан кейін Kaspersky оқиғалар журналында қате пайда болған мәселе шешілді.
16.1	9256000	Microsoft Windows XP жүйесіне Желілік агент орнатылған жағдайда, басқарылатын бағдарлама компоненттері туралы ақпараттың қолжетімсіз болуына әкеп соққан қате түзетілді.
16.1	9251629	Kaspersky Security Center Web Console веб-консоліне кірген кезде кейбір қажетті HTTP жауап тақырыптары қосылмаған мәселе шешілді.

Kaspersky Security Center Linux туралы

Бұл бөлімде Kaspersky Security Center Linux мақсаты, өзекті мүмкіндіктері мен құрамдастары, сондай-ақ Kaspersky Security Center Linux сатып алу тәсілдері туралы ақпарат беріледі.

Kaspersky Security Center Linux (бұдан әрі - Kaspersky Security Center деп те аталады) Linux негізіндегі Басқару сервері арқылы клиент құрылғыларын қорғауды орналастыруға және басқаруға арналған.

Kaspersky Security Center Linux корпоративтік желідегі құрылғыларға Kaspersky қауіпсіздік бағдарламаларын орнатуға, тексеру және жаңарту тапсырмаларын қашықтан іске қосуға, сондай-ақ басқарылатын бағдарламалардың қауіпсіздік саясаттарын басқаруға мүмкіндік береді. Әкімші ретінде сіз корпоративтік құрылғылардың ағымдағы күйін көрсететін, егжей-тегжейлі есептерді және егжей-тегжейлі саясат параметрлерін көрсететін бақылау тақтасын пайдалана аласыз.

Windows® негізіндегі Kaspersky Security Center Басқару серверімен салыстырғанда, Kaspersky Security Center Linux жүйесінде басқа функциялар жиынтығы бар.

Kaspersky Security Center Linux бағдарламасы ұйымдардың желі әкімшілеріне және ұйымдардағы құрылғыларды қорғауға жауапты қызметкерлерге арналған.

Kaspersky Security Center көмегімен сіз:

- Өзіндікұйымның желісін, сондай-ақ қашықтағы кеңселердің немесе клиенттік ұйым-клиенттердің желілерін басқару үшін Басқару серверлерінің иерархиясын қалыптастыру.

  Мұндағы *Ұйым-клиенттер* дегеніміз – провайдер антивирустық қорғанысты қамтамасыз ететін ұйымдар.

- Клиент құрылғылары жиынтығын тұтастай басқару үшін басқару топтарының иерархиясын құру.

- Kaspersky бағдарламалары негізінде құрылған антивирустық қауіпсіздік жүйесін басқару.

- Kaspersky бағдарламаларын және басқа үшінші тарап бағдарламаларын қашықтан орнатуды орындау.

- Kaspersky бағдарламаларының лицензиялық кілттерін клиент құрылғыларына орталықтан тарату, кілттердің қолданылуын бақылау және лицензиялардың жарамдылық мерзімін ұзарту.

- Бағдарламалар мен құрылғылардың жұмысы туралы статистика мен есептер алу.

- Kaspersky бағдарламаларының жұмысындағы маңызды оқиғалар туралы хабарландырулар алу.

- Windows операциялық жүйесі бар құрылғылардың қатты дискілерінде және алынбалы дискілерде сақталған деректерді шифрлауды басқару.

- Windows операциялық жүйесі бар құрылғыларындағы шифрланған деректерге пайдаланушы қатынасын басқару.

- Ұйымның желісіне қосылған жабдықтарды түгендеу.

- Қауіпсіздік бағдарламалары карантинге немесе сақтық көшірмелеуге орналастырылған файлдармен, сондай-ақ қауіпсіздік бағдарламалары өңдеуді кейінге қалдырған файлдармен орталықтандырылған түрде жұмыс істеу.

Kaspersky Security Center Linux бағдарламасын Kaspersky арқылы (мысалы, https://www.kaspersky.ru сайтында) немесе серіктес компаниялар арқылы сатып алуға болады.

Kaspersky Security Center Linux бағдарламасын Kaspersky арқылы сатып алсаңыз, бағдарламаны біздің сайттан жүктеп алуға болады. Бағдарламаны іске қосу үшін қажетті ақпарат төлем жасалғаннан кейін сізге электрондық пошта арқылы жіберіледі.

Жаңарту функционалдығы (антивирустық қолтаңба жаңартуларын және код дерекқоры жаңартуларын қоса) және KSN функционалдығы АҚШ аймағындағы бағдарламада қолжетімді болмауы мүмкін.

Жеткізу жиынтығы

Kaspersky веб-сайты нда, сіз қолданбаның барлық қажетті дистрибутив пакеттерін жүктей аласыз.

Kaspersky Security Center Linux дистрибутиві келесі файлдарды қамтиды:

Kaspersky Security Center Linux Басқару сервері:

- Debian негізіндегі операциялық жүйе жұмыс істейтін құрылғыға орнатылатын Басқару сервері:
  ksc64_16.3.0-<build>_amd64.deb
- Red Hat Enterprise Linux негізіндегі операциялық жүйе жұмыс істейтін құрылғыға орнатылатын Басқару сервері:
  ksc64-16.3.0-<build>.x86_64.rpm

Kaspersky Security Center Web Console:

- Debian негізіндегі операциялық жүйе жұмыс істейтін құрылғыға орнатылатын веб-консоль:
  ksc-web-console-16.3.<build>.x86_64.deb
- Red Hat Enterprise Linux негізіндегі операциялық жүйе жұмыс істейтін құрылғыға орнатылатын веб-консоль жүйе:
  ksc-web-console-16.3.<build>.x86_64.rpm

Kaspersky Security Center орнату скрипті

- ksc_fast_install.tar.gz

Windows үшін Желілік агент:

- ARM архитектурасы бар құрылғыға арналған Желілік агенттің орнату бағдарламасы:
  klnagent_winarm64-16.3.0.<build>-win_<localization>.zip
- x86-32 немесе x64 архитектурасы бар құрылғыға Желілік агентті қашықтан орнатуға арналған файлдар:
  ksc_16_16.3.0.<build>_NetAgent_<localization>.zip
- Arm архитектурасы бар құрылғыға Желілік агентті қашықтан орнатуға арналған файлдар:
  ksc_16_16.3.0.<build>_NetAgent_arm64_<localization>.zip
- Arm архитектурасы бар құрылғыда Kaspersky Security Center арқылы қашықтан орнатуға арналған файлдар:
  ri_utils_arm64.zip

- x86-32 немесе x64 архитектурасы бар құрылғыда Kaspersky Security Center арқылы қашықтан орнатуға арналған файлдар:

  ri_utils_win32.zip

Linux үшін Желілік агент

- Debian негізіндегі операциялық жүйе бар құрылғыға орнатылатын Желілік агент:

  klnagent64_16.3.0-<build>_<architecture>.deb

- Red Hat Enterprise Linux негізіндегі операциялық жүйені іске қосатын құрылғыға орнатылатын Желілік агент:

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

- Debian негізіндегі операциялық жүйені іске қосатын құрылғыға Желілік агентті қашықтан орнатуға арналған файлдар:

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

- Red Hat Enterprise Linux негізіндегі операциялық жүйені іске қосатын құрылғыға Желілік агентті қашықтан орнату үшін арналған файлдар:

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

- Linux жүйесіне арналған Желілік агенттерді қашықтан орнатудың бірыңғай дистрибутив пакеті:

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

  Егер сізде әртүрлі CPU архитектурасы және әртүрлі Linux негізіндегі операциялық жүйелері бар көптеген клиенттік құрылғылар болса, бірыңғай тарату пакеті пайдалы болуы мүмкін. Желілік агенттердің қажетті нұсқалары құрылғыларға одан әрі орнату үшін автоматты түрде таңдалады.

- glibc 2.5 бар Debian немесе Red Hat Enterprise Linux негізіндегі ескі операциялық жүйеде жұмыс істейтін құрылғыға Желілік агентті қашықтан орнатуға арналған файлдар:

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

Kaspersky Endpoint Detection and Response Optimum веб-плагині:

- signed_irp.zip

> Веб-плагинді тек қашықтан орнатуға арналған қолданбалардың тарату пакеттерінің қоймасынан жүктей аласыз.

Егер сізге Linux жүйесіне арналған Желілік агент орнату пакетін таңдау қиын болса, келесі мақаланы қараңыз: Linux жүйесіне арналған Желілік агент орнату пакетін қалай таңдауға болады.

Аппараттық және бағдарламалық талаптар

- Басқару серверіне қойылатын талаптар
- Web Console консоліне қойылатын талаптар
- Желілік агентіне қойылатын талаптар

Мобильді құрылғыларды қорғауды орналастыру және басқаруға арналған Android және iOS нұсқаларының талаптарымен танысу үшін Kaspersky Security for Mobile Help және Kaspersky Secure Mobility Management Help анықтамалықтарын қараңыз.

Басқару серверіне қойылатын талаптар

Ең төменгі аппараттық талаптар:

- Жұмыс жиілігі 2,5 ГГц немесе одан жоғары 2 ядролық процессор.
- Жедел жад: 6 ГБ.

  Басқару сервері орнатылған құрылғыда swap файлын қосу керек. swap файлының ең аз өлшемі жедел жад көлемінен 1,5 есе үлкен болуы керек.
- Дискідегі бос орын көлемі: басқару серверінің деректері (/var/opt/kaspersky/klnagent_srv) сақталатын қалта үшін 10 ГБ қажет.

Құрылғыға әкімшілік серверді орнатқаннан кейін, осы құрылғыға Kaspersky Endpoint Security for Linux бағдарламасын орнатуды ұсынамыз.
Бірлесіп орнату үшін сізде кемінде 300 IOPS болуы керек, сондай-ақ Басқару сервері талаптарына 1,5 ГБ жедел жады және процессорға 15% қосу керек.
Kaspersky Endpoint Security аппараттық құралдарына қойылатын талаптарды Kaspersky Endpoint Security for Linux анықтамасынан қараңыз.
Басқару серверімен жұмыс істеу үшін қажетті ұсынылатын ең аз қауіпсіздік параметрлері туралы ақпарат алу үшін Kaspersky Endpoint Security for Linux анықтамасын қараңыз.

Келесі операциялық жүйелерге қолдау көрсетіледі:

Операциялық жүйеде процестер арасындағы байланыс үшін циклдік интерфейс қолжетімді болуы керек.

- Debian GNU/Linux 12 (Bookworm) 64 разрядты
- Debian GNU/Linux 12 (Bookworm) 64 разрядты
- Ubuntu Server 22.04 LTS (Jammy Jellyfish) 64 разрядты
- Ubuntu Server 24.04 LTS (Noble Numbat), 64 разрядты
- Ubuntu Server 26.04 LTS (Resolute Raccoon), 64 разрядты
- CentOS Stream 9 64 разрядты
- CentOS Stream 10 64 разрядты
- Red Hat Enterprise Linux Server 7.x 64 разрядты
- Red Hat Enterprise Linux Server 8.x 64 разрядты
- Red Hat Enterprise Linux Server 9.x 64 разрядты
- Red Hat Enterprise Linux Server 10.x 64 разрядты

- SUSE Linux Enterprise Server 12 (барлық жаңарту пакеттері) 64 разрядты
- SUSE Linux Enterprise Server 15 (барлық жаңарту пакеттері) 64 разрядты
- Astra Linux Special Edition RUSB.10015-01 (кезекті жаңарту 1.6) 64 разрядты
- Astra Linux Special Edition RUSB.10015-01 (кезекті жаңарту 1.7) 64 разрядты
- Astra Linux Special Edition РУСБ.10015-01 (кезекті жаңарту 1.8) 64 разрядты
- Astra Linux Special Edition RUSB.10015-16 (1-орындау) (кезекті жаңарту 1.6) 64 разрядты
- Astra Linux Special Edition RUSB.10015-17 (кезекті жаңарту 1.7.3) 64 разрядты
- Astra Linux Special Edition RUSB.10015-03 (7.6 жаңартуы) 64 разрядты
- Astra Linux Special Edition RUSB.10015-37 (кезекті жаңарту 7.7) 64 разрядты
- Astra Linux Common Edition (кезекті жаңарту 2.12) 64 разрядты
- Альт СП Сервер 10 64 разрядты
- Альт СП Жұмыс станциялары 10 64 разрядты
- Oracle Linux 7 64 разрядты
- Oracle Linux 8 64 разрядты
- Oracle Linux 9 64 разрядты
- Platform V SberLinux OS Server (SLO) 8.10.1 64 разрядты
- Platform V SberLinux OS Server (SLO) 9.5.1 64 разрядты
- Platform V SberLinux OS Server (SLO) 9.6 64 разрядты
- Platform V SberLinux OS Server (SLO) 9.7 нұсқасы, 64 разрядты
- РЕД ОС 7.3 Сервер 64 разрядты
- РЕД ОС 7.3 Сертификатталған редакция 64 разрядты
- РЕД ОС 8 64 разрядты
- РОСА "КОБАЛЬТ" 7.9 64 разрядты
- M ОС (Moscow Electronic School) 12 сервері, 64 разрядты
- Mostech Server 64 разрядты
- МосОС 15.5 Arbat, 64 разрядты

Әдепкі параметрлері бар EXT4 файлдық жүйесін пайдалану ұсынылады.

Келесі дерекқор серверлеріне қолдау көрсетіледі (басқа машинада орнатылуы мүмкін):

- MySQL Standard Edition 8.0 (релизі 8.0.20 және одан да жоғары) 32 разрядты/64 разрядты
- MySQL Enterprise Edition 8.0 (релизі 8.0.20 және одан да жоғары) 32 разрядты/64 разрядты
- MySQL стандартты нұсқасы 8.4 32-бит/64-бит
- MySQL Enterprise Edition 8.4 32-бит/64-бит
- MariaDB 10.3 (жинағы 10.3.22 және одан да жоғары) 32 разрядты/64 разрядты
- MariaDB 10.4 (жинағы 10.4.20 және одан да жоғары) 32 разрядты/64 разрядты
- MariaDB 10.5 (жинағы 10.5.27 және одан да жоғары) 32 разрядты/64 разрядты
- MariaDB 10.6 (жинағы 10.6.20 және одан да жоғары) 32 разрядты/64 разрядты
- MariaDB 10.11 (жинағы 10.11.10 және одан да жоғары) 32 разрядты/64 разрядты
- MariaDB Galera Cluster 10.3 32 разрядты/64 разрядты, InnoDB қоймасы ішкі жүйесімен
- PostgreSQL 13.x 64 разрядты
- PostgreSQL 14.x 64 разрядты
- PostgreSQL 15.x 64 разрядты
- PostgreSQL 15.x 64 бит (Corosync/Pacemaker кластері)
- PostgreSQL 16.x 64 разрядты
- PostgreSQL 17 64 разрядты
- PostgreSQL 18 64 разрядты
- Postgres Pro 13.x (барлық редакция) 64 разрядты
- Postgres Pro 14.x (барлық редакция) 64 разрядты
- Postgres Pro 15.x (барлық редакция) 64 разрядты
- Postgres Pro 15.x 64 бит (Corosync/Pacemaker кластері)
- Postgres Pro 16.x (барлық редакция) 64 разрядты
- Postgres Pro 16.x Enterprise 64 бит (Built-in High Availability кластері)
- Postgres Pro 17 64 разрядты (барлық редакция)
- Postgres Pro 17 Enterprise 64 разрядты (Built-in High Availability кластері)
- Postgres Pro 18 64 разрядты (барлық редакция)
- Postgres Pro 18 Enterprise 64 разрядты (Built-in High Availability кластері)

- Platform V Pangolin 6.5.1 64 разрядты
- Platform V Pangolin 6.5.1 64 разрядты (кластер ендірілген жоғары деңгейдегі қолжетімділік)
- Jatoba 4 64 разрядты
- Jatoba 5 64 разрядты
- Tantor SE 1C 64 разрядты

Сенімділігі жоғары PostgreSQL кластерлеріне қолдау көрсетіледі. Толығырақ ақпарат алу үшін келесі мақаланы қараңыз: Kaspersky Security Center Linux жүйесімен жұмыс істеу үшін жоғары қолжетімді ДҚБЖ кластерін дайындау.

Қолдау көрсетілетін виртуалдандыру платформалары туралы ақпарат алу үшін Kaspersky Security for Virtualization Light Agent онлайн анықтамасын қараңыз.

Web Console консоліне қойылатын талаптар

Kaspersky Security Center Web Console Server сервері

Ең төменгі аппараттық талаптар:

- Процессор: 2 ядро, жиілігі 2500 МГц-тен бастап.
- Жедел жад: 4 ГБ.
- Дискідегі бос орын көлемі: Web Console деректері (/var/opt/kaspersky) сақталатын қалта үшін 40 ГБ қажет.

Құрылғыға әкімшілік серверді орнатқаннан кейін, осы құрылғыға Kaspersky Security Center Web Console бағдарламасын орнатуды ұсынамыз. Kaspersky Endpoint Security аппараттық құралдарына қойылатын талаптарды Kaspersky Endpoint Security for Linux анықтамасынан қараңыз.

Келесі операциялық жүйелердің бірі (**тек 64 разрядты нұсқалар**):

> Операциялық жүйеде процестер арасындағы байланыс үшін циклдік интерфейс қолжетімді болуы керек.

- Debian GNU/Linux 12 (Bookworm)
- Debian GNU/Linux 13 (Trixie)
- Ubuntu Server 22.04 LTS (Jammy Jellyfish)
- Ubuntu Server 24.04 LTS (Noble Numbat)
- Ubuntu Server 26.04 LTS (Resolute Raccoon), 64 разрядты
- CentOS Stream 9
- CentOS Stream 10

- Red Hat Enterprise Linux Server 7.x
- Red Hat Enterprise Linux Server 8.x
- Red Hat Enterprise Linux Server 9.x
- Red Hat Enterprise Linux Server 10.x
- SUSE Linux Enterprise Server 12 (барлық жаңартулар пакеттері)
- SUSE Linux Enterprise Server 15 (барлық жаңартулар пакеттері)
- Astra Linux Special Edition RUSB.10015-01 (кезекті жаңарту 1.6)
- Astra Linux Special Edition RUSB.10015-16 (1-орындау) (кезекті жаңарту 1.6)
- Astra Linux Special Edition RUSB.10015-01 (кезекті жаңарту 1.7)
- Astra Linux Special Edition RUSB.10015-17 (кезекті жаңарту 1.7.3)
- Astra Linux Special Edition RUSB.10015-01 (кезекті жаңарту 1.8)
- Astra Linux Special Edition RUSB.10015-03 (7.6 жаңартуы)
- Astra Linux Special Edition RUSB.10015-37 (кезекті жаңарту 7.7)
- Astra Linux Common Edition (кезекті жаңарту 2.12)
- Альт СП Сервер 10
- Альт СП жұмыс станциясы 10
- Oracle Linux 7
- Oracle Linux 8
- Oracle Linux 9
- Platform V SberLinux OS Server (SLO) 8.10.1
- Platform V SberLinux OS Server (SLO) 9.5.1
- Platform V SberLinux OS Server (SLO) 9.6 64 разрядты
- Platform V SberLinux OS Server (SLO) 9.7 нұсқасы, 64 разрядты
- РЕД ОС 7.3 Сервер
- РЕД ОС 7.3 Сертификатталған редакция
- РЕД ОС 8
- РОСА "КОБАЛЬТ" 7.9
- М ОС (Moscow Electronic School) 12 сервері

- Mostech Server
- MosOS 15.5 Arbat

Қолдау көрсетілетін виртуалдандыру платформалары туралы ақпарат алу үшін Kaspersky Security for Virtualization Light Agent онлайн анықтамасын қараңыз.

Клиент құрылғылары

Клиент құрылғысы Kaspersky Security Center Web Console серверімен жұмыс істеу үшін тек браузерді қажет етеді.

Экранның ең төменгі ажыратымдылығы – 1366x768 пиксель.

Құрылғының аппараттық және бағдарламалық жасақтамасына қойылатын талаптар Kaspersky Security Center Web Console серверімен жұмыс істеу үшін пайдаланылатын браузердің талаптарына сәйкес келеді.

Браузерлер:

- Google Chrome 149.0.7827.115 немесе одан кейінгі нұсқасы
- Microsoft Edge 149.0.4022.62 немесе одан кейінгі нұсқасы
- macOS жүйесіндегі Safari 18.6 (20621.3.11.11.3)
- Яндекс 26.4.4.799 браузері немесе одан кейінгі нұсқасы
- Mozilla Firefox Extended Support Release 140.11.0 немесе одан кейінгі нұсқасы

Желілік агентіне қойылатын талаптар

Ең төменгі аппараттық талаптар:

- Жиілігі 1 ГГц немесе одан жоғары процессор. 64 разрядты операциялық жүйемен жұмыс істегенде процессордың минималды жиілігі 1,4 ГГц құрайды.
- Жедел жад: 512 МБ.
- Дискідегі бос орын көлемі: 1 ГБ.

Linux операциялық жүйесі бар құрылғыларға қойылатын қолданбалық жасақтама талаптары: Perl тілі интерпретаторының 5.10 немесе одан жоғары нұсқасы орнатылуы керек.

Желілік агент. Қолдау көрсетілетін платформалар

Операциялық жүйелер. Microsoft Windows жұмыс станциялары	Microsoft Windows Embedded POSReady 2009, соңғы Service Pack-пен, 32 разрядты Microsoft Windows Embedded 7 Standard Service Pack 1, 32 разрядты/64 разрядты Microsoft Windows Embedded 8.1 Industry Pro, 32 разрядты/64 разрядты Microsoft Windows 10 Enterprise 2015 LTSB 32 разрядты/64 разрядты Microsoft Windows 10 Enterprise 2016 LTSB 32 разрядты/64 разрядты Microsoft Windows 10 IoT Enterprise 2015 LTSB 32 разрядты/64 разрядты Microsoft Windows 10 IoT Enterprise 2016 LTSB 32 разрядты/64 разрядты Microsoft Windows 10 Enterprise 2019 LTSC 32 разрядты / 64 разрядты Microsoft Windows 10 IoT Enterprise 1703, 1709, 1803, 1809-нұсқа 32 разрядты/64 разрядты Microsoft Windows 10 20H2, 21H2 IoT Enterprise 32 разрядты/64 разрядты Microsoft Windows 10 IoT Enterprise 32 разрядты/64 разрядты Microsoft Windows 10 IoT Enterprise 1909-нұсқа 32 разрядты/64 разрядты Microsoft Windows 10 IoT Enterprise LTSC 2021 32 разрядты/64 разрядты Microsoft Windows 10 IoT Enterprise 1607-нұсқа 32 разрядты/64 разрядты Microsoft Windows 10 TH1 (July 2015) Home/Pro/Pro for Workstations/Enterprise/Education, 32 разрядты/64 разрядты Microsoft Windows 10 TH2 (November 2015) Home/Pro/Pro for Workstations/Enterprise/Education, 32 разрядты/64 разрядты Microsoft Windows 10 RS1 (August 2016) Home/Pro/Pro for Workstations/Enterprise/Education, 32 разрядты/64 разрядты Microsoft Windows 10 RS2 (April 2017) Home/Pro/Pro for Workstations/Enterprise/Education, 32 разрядты/64 разрядты Microsoft Windows 10 RS3 (Fall Creators Update, v1709) Home/Pro/Pro for Workstations/Enterprise/Education 32 разрядты/64 разрядты Microsoft Windows 10 RS4 (April 2018 Update, 17134) Home/Pro/Pro for Workstations/Enterprise/Education, 32 разрядты/64 разрядты Microsoft Windows 10 RS5 (October 2018) Home/Pro/Pro for Workstations/Enterprise/Education, 32 разрядты/64 разрядты Microsoft Windows 10 RS6 (May 2019) Home/Pro/Pro for Workstations/Enterprise/Education, 64 разрядты Microsoft Windows 10 19H1, 19H2 Home/Pro/Pro for Workstations/Enterprise/Education, 32 разрядты/64 разрядты Microsoft Windows 10 20H1 (May 2020 Update) Home/Pro/Pro for Workstations/Enterprise/Education, 32 разрядты/64 разрядты Microsoft Windows 10 20H2 (October 2020 Update) Home/Pro/Pro for Workstations/Enterprise/Education, 32 разрядты/64 разрядты Microsoft Windows 10 21H1 (May 2021 Update) Home/Pro/Pro for Workstations/Enterprise/Education, 32 разрядты/64 разрядты Microsoft Windows 10 21H2 (October 2021 Update) Home/Pro/Pro for Workstations/Enterprise/Education, 32 разрядты/64 разрядты Microsoft Windows 10 22H2 (October 2023 Update) Home/Pro/Pro for Workstations/Enterprise/Education, 32 разрядты/64 разрядты Windows 11 Home/Pro/Pro for Workstations/Enterprise/Education ARM 64 разрядты Windows 11 Home/Pro/Pro for Workstations/Enterprise/Education 64 разрядты Microsoft Windows 11 IoT Enterprise, 25H2 нұсқасы, 64 разрядты Windows 11 22H2 Home/Pro/Pro for Workstations/Enterprise/Education 64 разрядты Windows 11 23H2 Home/Pro/Pro for Workstations/Enterprise/Education 64 разрядты Windows 11 24H2 Home/Pro/Pro for Workstations/Enterprise/Education 64 разрядты Windows 11 25H2 Home/Pro/Pro for Workstations/Enterprise/Education 64 разрядты Microsoft Windows 8.1 Pro/Enterprise 32 разрядты/64 разрядты Microsoft Windows 8 Pro/Enterprise 32 разрядты/64 разрядты Microsoft Windows 7 Professional/Enterprise/Ultimate/Home Basic/Premium Service Pack 1 және одан да жоғары 32 разрядты/64 разрядты Microsoft Windows XP Professional Service Pack 2 32 разрядты/64 разрядты (Желілік агенттің нұсқасы 10.5.1781 қолдау көрсетеді) Microsoft Windows XP Professional Service Pack 3 және одан жоғары 32 разрядты (Желілік агенттің 14.0.0.20023 нұсқасы қолдау көрсетеді, Windows XP жүйесіне арналған KB2868626 қауіпсіздік жаңартуын талап етеді) Microsoft Windows XP Professional for Embedded Systems Service Pack 3 32 разрядты (Желілік агенттің 14.0.0.20023 нұсқасы қолдау көрсетеді)

Операциялық жүйелер. Microsoft Windows серверлері	Microsoft Windows MultiPoint Server 2011 Standard/Premium 64 разрядты Microsoft Windows Server 2003 SP1 32 разрядты/64 разрядты (тек Техникалық қолдау қызметінен сұрауға болатын Желілік агенттің 10.5.1781 нұсқасына қолдау көрсетіледі) Windows Server 2003 SP2 Standard/Enterprise 32 разрядты/64 разрядты (тек желілік агенттің 10.5.1781 нұсқасы қолдау көрсетеді) Windows Server 2003 R2 Standard/Enterprise SP2 32 разрядты/64 разрядты (тек желілік агенттің 10.5.1781 нұсқасы қолдау көрсетеді) Microsoft Windows Server 2008 Foundation Service Pack 2 32 разрядты/64 разрядты Microsoft Windows Server 2008 Standard/Enterprise/Datacenter Service Pack 2 32 разрядты/64 разрядты Microsoft Windows Server 2008 R2 Datacenter/Enterprise/Foundation/Standard Service Pack 1 және одан да жоғары 64 разрядты Microsoft Windows Server 2012 Server Core/Datacenter/Essentials/Foundation/Standard 64 разрядты Microsoft Windows Server 2012 R2 Server Core/Datacenter/Essentials/Foundation/Standard 64 разрядты Windows Server 2016 Datacenter/Standard (Server Core орнату нұсқасы) (LTSB) 64 разрядты Microsoft Windows Server 2019 Standard/Datacenter/Core 64 разрядты Microsoft Windows Server 2019 RS5 Essentials/Standard 64 разрядты Microsoft Windows Server 2022 Standard/Datacenter/Core 64 разрядты Microsoft Windows Server 2025 Standard/Datacenter/Core 64 разрядты Microsoft Windows Server 2022 21H2 Standard/Datacenter 64 разрядты Microsoft Windows Storage Server 2019 64 разрядты Microsoft Windows Small Business Server 2011 Standard 64 разрядты Microsoft Windows Small Business Server 2011 Essentials 64 разрядты Microsoft Windows Small Business Server 2011 Premium Add-on 64 разрядты

Операциялық жүйелер. Linux	Debian GNU/Linux 10.x (Buster) 32 разрядты/64 разрядты Debian GNU/Linux 11.x (Bullseye) 32 разрядты/64 разрядты Debian GNU/Linux 12 (Bookworm) 32 разрядты/64 разрядты Debian GNU/Linux 12 (Bookworm) 64 разрядты Ubuntu Server 10.04 LTS (Lucid Lynx) 32 разрядты/64 разрядты Ubuntu Server 16.04 LTS (Xenial Xerus) 32 разрядты/64 разрядты Ubuntu Server 18.04 LTS (Bionic Beaver) 64 разрядты Ubuntu Server 20.04 LTS (Focal Fossa) 64 разрядты Ubuntu Server 22.04 LTS (Jammy Jellyfish) 64 разрядты Ubuntu Server 22.04 LTS ARM 64 разрядты Ubuntu Server 24.04 LTS (Noble Numbat), 64 разрядты Ubuntu Server 26.04 LTS (Resolute Raccoon), 64 разрядты Ubuntu Server 26.04 LTS ARM, 64 разрядты Ubuntu Desktop 10.04 LTS (Lucid Lynx) 32 разрядты/64 разрядты Ubuntu Desktop 16.04 LTS (Xenial Xerus) 32 разрядты/64 разрядты CentOS 5.2 32 разрядты/64 разрядты (тек Linux Legacy үшін Желілік агент қолдайды, оны Web Console интерфейсін пайдаланып немесе Kaspersky веб-сайтынан жүктеп алуға болады) CentOS 5.4 32 разрядты/64 разрядты (тек Linux Legacy үшін Желілік агент қолдайды, оны Web Console интерфейсін пайдаланып немесе Kaspersky веб-сайтынан жүктеп алуға болады) CentOS 6.4 32 разрядты/64 разрядты (тек Linux Legacy үшін Желілік агент қолдайды, оны Web Console интерфейсін пайдаланып немесе Kaspersky веб-сайтынан жүктеп алуға болады) CentOS 6.6 32 разрядты/64 разрядты (тек Linux Legacy үшін Желілік агент қолдайды, оны Web Console интерфейсін пайдаланып немесе Kaspersky веб-сайтынан жүктеп алуға болады) CentOS 7.2 және одан кейінгі, 64 разрядты CentOS Stream 8 64 разрядты CentOS Stream 9 64 разрядты CentOS Stream 9 ARM 64 разрядты CentOS Stream 10 64 разрядты Red Hat Enterprise Linux Server 6.x 32 разрядты/64 разрядты Red Hat Enterprise Linux Server 7.2 және одан кейінгі 64 разрядты Red Hat Enterprise Linux Server 8.x 64 разрядты Red Hat Enterprise Linux Server 9.x 64 разрядты Red Hat Enterprise Linux Server 10.x 64 разрядты SUSE Linux Enterprise Server 12.5 және одан кейінгі (барлық қызметтік пакет) 64 разрядты SUSE Linux Enterprise Server 15 (барлық жаңарту пакеттері) 64 разрядты SUSE Linux Enterprise Server 15 (барлық жаңарту пакеттері) ARM, 64 разрядты openSUSE Leap 15 64 разрядты EulerOS 2.0 SP10, 64 разрядты EulerOS 2.0 SP10 ARM 64 разрядты Astra Linux Special Edition RUSB.10015-01 (1.4 операциялық жаңартуы), 64 разрядты Astra Linux Special Edition RUSB.10015-01 (операциялық жаңарту 1.4), 64 разрядты (тек Linux Legacy үшін Желілік агентті қолдайды, оны Web Console интерфейсі арқылы немесе Kaspersky веб-сайтынан жүктеп алуға болады Astra Linux Special Edition RUSB.10015-01 (операциялық жаңарту 1.5) 64 разрядты Astra Linux Special Edition RUSB.10015-01 (кезекті жаңарту 1.6) 64 разрядты Astra Linux Special Edition RUSB.10015-16 (1-орындау) (кезекті жаңарту 1.6) 64 разрядты Astra Linux Special Edition RUSB.10015-17 (кезекті жаңарту 1.7.3) 64 разрядты Astra Linux Special Edition RUSB.10015-01 (кезекті жаңарту 1.7) 64 разрядты Astra Linux Special Edition RUSB.10015-01 (кезекті жаңарту 1.8) 64 разрядты Astra Linux Special Edition RUSB.10015-03 (7.6 жаңартуы) 64 разрядты Astra Linux Special Edition RUSB.10015-37 (кезекті жаңарту 7.7) 64 разрядты Astra Linux Special Edition RUSB.10152-02 (кезекті жаңарту 4.7) ARM 64 разрядты Astra Linux Common Edition (кезекті жаңарту 2.12) 64 разрядты Альт Жұмыс станциясы 11, 64 разрядты ALT Server 11 64 разрядты ALT Education 10.1 64 разрядты Альт Жұмыс станциясы 10.1, 64 разрядты

Альт Сервер 10.1, 64 разрядты

ALT Education 10.1, 64 разрядты

Альт СП Сервер 10, 32 разрядты/64 разрядты

Альт СП Сервер 10 ARM, 64 разрядты

Альт СП Жұмыс станциясы 10, 32 разрядты/64 разрядты

Альт СП Жұмыс станциялары 10 ARM, 64 разрядты

Альт 8 СП Сервер (ЛКНВ.11100-01) 32 разрядты/64 разрядты

Альт 8 СП Сервер (ЛКНВ.11100-02) 32 разрядты/64 разрядты

Альт 8 СП Сервер (ЛКНВ.11100-03) 32 разрядты/64 разрядты

Альт 8 СП Жұмыс станциясы (ЛКНВ.11100-01) 32 разрядты/64 разрядты

Альт 8 СП Жұмыс станциясы (ЛКНВ.11100-02) 32 разрядты/64 разрядты

Альт 8 СП Жұмыс станциясы (ЛКНВ.11100-03) 32 разрядты/64 разрядты

Oracle Linux 7 64 разрядты

Oracle Linux 8 64 разрядты

Oracle Linux 9 64 разрядты

Linux Mint 21.1 және одан жоғары 64 разрядты

Linux Mint 22.x 64 разрядты

AlterOS 7.5 немесе одан кейінгі нұсқа, 64 разрядты

AlterOS 2025 64 разрядты

ГосЛинукс IC6/7.17, 64 разрядты

ГосЛинукс IC6/7.2, 64 разрядты

SberOS 3.4.0 64 разрядты

SberOS 3.5.0 64 разрядты

SberOS 3.5.0, 64 разрядты

Platform V SberLinux OS Server (SLO) 8.10.1 64 разрядты

Platform V SberLinux OS Server (SLO) 9.1 64 разрядты

Platform V SberLinux OS Server (SLO) 9.5.1 64 разрядты

Platform V SberLinux OS Server (SLO) 9.6 64 разрядты

Platform V SberLinux OS Server (SLO) 9.7 нұсқасы, 64 разрядты

РЕД ОС 7.3 Сервер 64 разрядты

РЕД ОС 7.3 Сертификатталған редакция 64 разрядты

РЕД ОС 8 64 разрядты

RED OS 8 ARM 64 разрядты

ROSA Enterprise Linux Server 7.9 64 разрядты

ROSA Enterprise Linux Desktop 7.9, 64 разрядты

РОСА "КОБАЛЬТ" 7.9 64 разрядты

РОСА "ХРОМ" 12 64 разрядты

AlmaLinux 8 және одан да жоғары 64 разрядты

AlmaLinux 9 және одан да жоғары, 64 разрядты

Rocky Linux 8 және одан да жоғары, 64 разрядты

Rocky Linux 9 және одан да жоғары, 64 разрядты

Атлант, Alcyone құрастыру, 2022.02 нұсқасы, 64 разрядты

МСВСфера 9.2 Сервер 64 разрядты

МСВСфера 9.2 АРМ 64 разрядты

MSVSPHERE 9.4 SERVER 64 разрядты

MSVSPHERE 9.4 ARM 64 разрядты

СинтезМ Сервер 8.6 64 разрядты

СинтезМ Клиент 8.6 64 разрядты

OSnova 2.* 64 разрядты

ОСнова 3.* 64 разрядты

Kylin 10 64 разрядты

EMIAS 1.0 64 разрядты

Amazon Linux 2 64 разрядты

МосОС 15.5 Arbat, 64 разрядты

OS MES (Moscow Electronic School) 12 (компьютерлер мен ноутбуктер үшін) 64 разрядты

OS MES (Moscow Electronic School) 12 (интерактивті панельдер үшін) 64 разрядты

	M OC (Moscow Electronic School) 12 сервері, 64 разрядты Mostech 64 разрядты Mostech Server 64 разрядты Fedora Linux Server 41 64 разрядты Fedora Linux Workstation 41 64 разрядты
Операциялық жүйелер. macOS	Қолдау көрсетілетін операциялық жүйелер тізімін алу үшін Kaspersky Endpoint Security for Mac анықтамасын қараңыз.
Виртуализация платформалары	Қолдау көрсетілетін виртуалдандыру платформалары туралы ақпарат алу үшін Kaspersky Security for Virtualization Light Agent онлайн анықтамасын қараңыз.

Microsoft Windows Server 2008 R2 (сервер нұсқалары) және Microsoft Windows 7 (жұмыс үстелі нұсқалары) ескі Windows нұсқаларында Желілік агент келесі функцияларды қолдамайды:

- Жаңартуларды қайта аудару (тарату нүктелері пайдаланады)
- KSN прокси (тарату нүктелері пайдаланады)
- Осалдықты сканерлеу тапсырмасы

Microsoft Windows 10 ОЖ RS4 немесе RS5 нұсқалары басқаратын құрылғыларда Kaspersky Security Center бағдарламасы тізілім есебі қосылған қалталардағы кейбір осалдықтарды анықтамауы мүмкін.

Windows 7, Windows Server 2008, Windows Server 2008 R2 немесе Windows MultiPoint Server 2011 орнатылған құрылғыларда Желілік агентті орнату алдында Windows ОЖ үшін KB3063858 қауіпсіздік жаңартуы (Windows 7 үшін қауіпсіздік жаңартуы (KB3063858)), x64 негізіндегі жүйелерге арналған Windows 7 қауіпсіздік жаңартуы (KB3063858), Windows Server 2008 үшін қауіпсіздік жаңартуы (KB3063858), Windows Server 2008 x64 Edition үшін қауіпсіздік жаңартуы (KB3063858), Windows Server 2008 R2 x64 Edition үшін қауіпсіздік жаңартуы (KB3063858) орнатылғанына көз жеткізіңіз.

Microsoft Windows XP жүйесінде Желілік агент кейбір әрекеттерді дұрыс орындамауы мүмкін.

Windows XP үшін Желілік агентті тек Microsoft Windows XP жүйесінде орнатуға немесе жаңартуға болады. Microsoft Windows XP жүйесінің қолдау көрсетілетін редакциялары және оған сай келетін Желілік агент бағдарламасының нұсқалары қолдау көрсетілетін операциялық жүйелер тізімінде берілген. Microsoft Windows XP жүйесіне арналған Желілік агент бағдарламасының қажетті нұсқасын осы беттен жүктеп алуға болады.

Linux үшін Желілік агенттің Kaspersky Security Center Linux бағдарламасымен бірдей нұсқасын орнату ұсынылады.

Kaspersky Security Center Linux Желілік агенттің бірдей немесе одан жоғары нұсқасын толығымен қолдайды.

macOS үшін Желілік Агент осы операциялық жүйеге арналған Kaspersky қауіпсіздік бағдарламасымен бірге жеткізіледі.

Kaspersky үйлесімді бағдарламалары мен шешімдері

Kaspersky Security Center Linux қазіргі уақытта қолдау көрсетілетін барлық Kaspersky қолданбасы мен шешімін орталықтан орналастыруға және басқаруға қолдау көрсетеді. Қолданбалар мен шешімдердің нұсқаларын табу үшін Қолданба қолдауының өмірлік циклі веб-бетін қараңыз.

Қолдау көрсетілетін Kaspersky қолданбалары:

- Kaspersky Endpoint Security for Windows (файл серверлеріне қолдау көрсетеді)
- Kaspersky Endpoint Security for Linux (файл серверлеріне қолдау көрсетеді)
- Kaspersky Endpoint Security for Linux Elbrus Edition
- Kaspersky Endpoint Security for Mac
- Kaspersky Endpoint Security for Android
- Kaspersky Endpoint Security for Aurora
- Kaspersky Security for iOS
- Kaspersky Industrial CyberSecurity for Linux Nodes
- Kaspersky Industrial CyberSecurity for Nodes
- Kaspersky Industrial CyberSecurity for Networks
- Kaspersky Endpoint Agent
- Kaspersky Embedded Systems Security for Windows
- Kaspersky Embedded Systems Security for Linux
- Kaspersky Security for Virtualization Жеңіл агент
- KATA Sandbox (Kaspersky Anti Targeted Attack Platform компоненттерінің бірі)
- Kaspersky Thin Client
- Kaspersky NGFW
- Kaspersky Sandbox
- Kaspersky Password Manager for Business
- Kaspersky Vulnerability Management

Kaspersky Security Center Linux келесі шешімдерге кіреді:

- Kaspersky Endpoint Detection and Response Optimum
- Kaspersky Managed Detection and Response
- Kaspersky Security: Бизнеске арналған Кәсіби

Бағдарламалар мен шешімдердің нұсқалары туралы толық ақпарат алу үшін "Бағдарламалардың өмірлік циклі" бетін қараңыз.

Шектеулер тізімі

Kaspersky Industrial CyberSecurity for Networks үшін бірыңғай кіру (SSO) мүмкіндігіне қолдау көрсетілмейді.

Kaspersky Security Center Linux құрамдастарының үйлесімділігі туралы ақпарат

Төмендегі кестеден Kaspersky Security Center Linux құрамдастарының үйлесімділігі туралы ақпаратты табуға болады.

Kaspersky Security Center Linux құрамдастарының үйлесімділігі

Құрамдас	Келесімен үйлесімді
Kaspersky Security Center 16.3 Linux басқару сервері	• Келесі нұсқалардағы Kaspersky Security Center Web Console: 16.3, 16.2, 16.1 • Келесі нұсқалардағы Kaspersky Security Желілік агент: 16.3, 16.2, 16.1, 16, 15.4, 15.3, 15.2, 15.1, 15, 14*, 10.5**
Kaspersky Security Center 16.3 Web Console	Келесі нұсқалардағы Kaspersky Security Center Linux басқару сервері: 16.3, 16.2, 16.1, 16
Kaspersky Security Center 16.3 Linux негізгі басқару сервері	Қосалқы басқару серверлері: • Келесі нұсқалардағы Kaspersky Security Center Linux: 16.3, 16.2, 16.1, 16, 15.4, 15.3, 15.2, 15.1, 15 • Келесі нұсқалардағы Kaspersky Security Center Windows: 15.1
Kaspersky Security Center 16.3 Linux қосалқы басқару сервері	Негізгі Басқару серверлері: • Келесі нұсқалардағы Kaspersky Security Center Linux: 16.3, 16.2, 16.1, 16, 15.4, 15.3, 15.2, 15.1, 15 • Келесі нұсқалардағы Kaspersky Security Center Windows: 15.1
Kaspersky Security Center 16.3 Желілік агенті	Басқару серверлері: • Келесі нұсқалардағы Kaspersky Security Center Linux: 16.3, 16.2, 16.1, 16, 15.4, 15.3, 15.2, 15.1, 15 • Келесі нұсқалардағы Kaspersky Security Center Windows: 15.1
Kaspersky Security Center басқару сервері деректерінің сақтық көшірмесін жасау және қалпына келтіру	Деректердің сақтық көшірмесін жасауға және қалпына келтіруге Kaspersky Security Center Linux басқару серверінің келесі нұсқаларында қолдау көрсетіледі: 16.2, 16.1, 16, 15.4, 15.3, 15.2, 15.1, 15

*Бұл нұсқа Microsoft Windows XP Professional with Service Pack 3 нұсқасын қолдайды. Сіз бұл Желілік агент нұсқасын осы беттен жүктей аласыз.

**Бұл нұсқа Microsoft Windows XP Professional with Service Pack 2 нұсқасын қолдайды. Сіз бұл Желілік агент нұсқасын Техникалық қолдау қызметі арқылы сұрай аласыз.

Kaspersky Security Center басқару сервері мен Kaspersky Security Center Web Console соңғы нұсқасын пайдалану ұсынылады. Әйтпесе Kaspersky Security Center функцияларына шектеу қойылуы мүмкін. Сіз Kaspersky Security Center және Kaspersky Security Center Web Console Басқару серверін бір-бірінен тәуелсіз түрде орнатып, жаңарта аласыз. Бұл жағдайда, орнатылған Kaspersky Security Center Web Console қолданбасының нұсқасы сіз қосылатын Басқару сервері нұсқасымен үйлесімді екеніне көз жеткізіңіз:

Егер сізде Kaspersky Security Center Web Console бағдарламасының соңғы нұсқасы және Kaspersky Security Center бағдарламасының алдыңғы нұсқасы болса және домендік түпнұсқалық растама кезінде қате орын алса, қате мәтінінде стандартты хабарлама бар.

Kaspersky Security Center нұсқаларын салыстыру: Windows негізінде және Linux негізінде

Kaspersky Kaspersky Security Center бағдарламасын Windows және Linux платформаларына арналған жергілікті шешім ретінде ұсынады. Windows негізіндегі шешімде Windows құрылғысына басқару серверін орнатасыз және Linux негізіндегі шешімде Linux құрылғысына орнатуға арналған басқару серверінің нұсқасы бар. Бұл онлайн анықтамада Kaspersky Security Center туралы ақпарат берілген. Windows негізіндегі шешім туралы толық ақпарат алу үшін Kaspersky Security Center Windows онлайн анықтамасын қараңыз.

Төмендегі кесте Kaspersky Security Center бағдарламасының Windows негізіндегі шешімдер және Linux негізіндегі шешімдер ретінде негізгі мүмкіндіктерін салыстыруға жол ашады.

Windows негізіндегі және Linux негізіндегі Kaspersky Security Center бағдарламасының мүмкіндіктерін салыстыру

Функция немесе сипат	Kaspersky Security Center 15.1 Windows	Kaspersky Security Center 16.3 Linux
Басқару сервері		
Деректқорларды басқару жүйесінің (ДҚБЖ) орналасуы	Жергілікті инфрақұрылымда	Жергілікті инфрақұрылымда (Microsoft SQL-ге қолдау көрсетілмейді)
Басқару серверін орнатуға арналған операциялық жүйе	Windows	Linux
Басқару серверлерінің иерархиясы	✓	✓
Виртуалды басқару серверлеріне қолдау көрсету	✓	✓
Ақауларға төзімді Kaspersky Security Center кластерін орналастыру	✓ Тек бір сайтты кластер	✓ Kaspersky Security Center 16.2 Linux жүйесінен бастап, географиялық таратылған ақауларға төзімді кластер қолдау табады
Басқару серверінің статистикасын үшінші тарап бағдарламаларына жіберу үшін SNMP пайдалану	✓	✓
Орнату пакеттерін және басқа файлдарды жариялауға арналған веб-сервер	✓	✓
Басқару консолі		
Басқару консолінің түрі	MMC негізінде және веб-интерфейс	Веб-интерфейс

Функция немесе сипат	Kaspersky Security Center 15.1 Windows	Kaspersky Security Center 16.3 Linux
Веб-интерфейсі бар басқару консолін орнатуға арналған операциялық жүйе	Windows немесе Linux	Linux
Домендік түпнұсқалық растаманы пайдаланып, консольге кіру	✓	✓
Клиент құрылғыларын және басқару топтарын басқару		
Басқарылатын құрылғылардың максималды саны (бір басқару сервері үшін)	100 000 (Microsoft SQL Server көмегімен)	50 000 (PostgreSQL және Postgres Pro көмегімен)
Желіде сауалнама өткізу	✓	✓
Windows, macOS және Linux басқаратын құрылғыларды қорғау	✓	✓
Ұялы құрылғыларды қорғау	✓ Ұялы құрылғыларды негізгі басқару	✓ MDM және Kaspersky Secure Mobility Management функциясын пайдалану (лицензия бойынша)
Виртуалды машиналарды қорғауды басқару	✓	✓
Жария бұлтты инфрақұрылымды қорғау	✓	—
Клиент құрылғысының жұмыс үстеліне қашықтан қосылу	✓	✓
Деректерді шифрлау және қорғау	✓ Kaspersky Endpoint Security for Windows немесе Kaspersky Endpoint Security for Mac бар Windows негізіндегі басқарылатын құрылғыларда	✓ Kaspersky Endpoint Security for Windows немесе Kaspersky Endpoint Security for Mac бар Windows негізіндегі басқарылатын құрылғыларда
Басқару топтарындағы кластерлер мен сервер массивтеріне қолдау көрсету	✓	✓
Басқару топтары иерархиясы	✓	✓
Қосылым шлюзін тарату нүктесі ретінде демилитаризацияланған аймаққа қосу	✓ (Web Console үшін қолдау көрсетілмейді)	✓
Пайдаланушылармен жұмыс істеу		
Пайдаланушы есептік жазбаларын жасау, есептік жазбаларды бақылау	✓	✓
Kaspersky қолданбаларын басқару		
Бағдарламалар саясаты	✓	✓
Kaspersky бағдарламаларына арналған тапсырмалар	✓	✓
Kaspersky Security Network	✓	✓
KSN прокси-сервері	✓	✓
Kaspersky Private Security Network	✓	✓
Kaspersky бағдарламаларының лицензиялық кілттерін орталықтан тарату	✓	✓
Клиент құрылғыларын қашықтан диагностикалау	✓	✓
Kaspersky бағдарламаларын автоматты түрде жаңарту	✓	✓
Аномалияларды бейімделумен басқаруды қолдау	✓	✓
Құрылғылардың қауіпсіздігін басқару	✓	✓
Пайдаланушыға бағытталған қауіпсіздікті басқару	✓	✓

Функция немесе сипат	Kaspersky Security Center 15.1 Windows	Kaspersky Security Center 16.3 Linux
Жүйелерді басқару		
Клиент құрылғыларында операциялық жүйелерді орналастыру	✓	—
Үшінші тарап лицензиясын басқару	✓	2026 жылы жүзеге асырылады
Басқару серверін WSUS сервері ретінде пайдалану	✓	✓ (тек Windows жаңартуының енжар іздеу режимі)
Клиент құрылғыларындағы үшінші тарап бағдарламалары бағдарламаларын басқару		
Үшінші тарап қолданбаларының жаңартуларын орнату және үшінші тарап қолданбаларындағы осалдықтарды іздеу	✓	✓
Бағдарлама санаттарын импорттау және экспорттау	✓ (Web Console үшін қолдау көрсетілмейді)	2026 жылы жүзеге асырылады
Мониторинг, есеп беру және аудит		
Нысанды тексерумен жұмыс	✓	✓
Саясат тексерістерін салыстыру	✓	✓
Kaspersky Endpoint Detection and Response Optimum арқылы тіркелген дабылдарды көру және олармен жұмыс істеу	✓	✓
Басқарылатын құрылғыларда болған оқиғалар туралы хабарландырулар	✓	✓
Саясаттар мен тапсырмалар күйін бақылау	✓	✓
Интеграциялар		
Kaspersky Managed Detection and Response-пен біріктіру	✓	✓
SIEM жүйелерімен біріктіру	✓	✓
Дабылдарды біріктіру және Active directory, KASAP және Kaspersky TIP Sandbox арқылы жауап әрекеттерін орындау	—	✓ Kaspersky Security: Бизнеске арналған Кәсіби лицензиясында басқару серверін белсендіру, содан кейін басқарылатын қолданбаларға Kaspersky Security: Бизнеске арналған Кәсіби лицензия кілтін орналастыру керек

Kaspersky Next Expert View туралы

Kaspersky Security Center-ді жергілікті қолданба ретінде пайдалансаңыз, Kaspersky Security Center-ді, соның ішінде басқару серверін жергілікті құрылғыға орнатып, желінің қауіпсіздік жүйесін Microsoft Management Console негізіндегі басқару консолі (Kaspersky Security Center Windows-та ғана қолжетімді) немесе Kaspersky Security Center Web Console арқылы басқарасыз.

Оның орнына, сіз Kaspersky Security Center бағдарламасын бұлтты қызмет ретінде пайдалана аласыз. Бұл жағдайда, Kaspersky Security Center бағдарламасы сіз үшін Kaspersky мамандары тарапынан бұлтты ортада орнатылады және Kaspersky сізге Басқару серверіне қызмет ретінде қатысуға мүмкіндік береді. Kaspersky Next Expert View деп аталатын бұлтты қызметке негізделген Басқару консолі арқылы желі қауіпсіздігі жүйесін басқарасыз. Бұл консольде Kaspersky Security Center Web Console бағдарламасына ұқсас интерфейс бар.

Kaspersky Next Expert View интерфейсі мен құжаттамасы келесі тілдерде қолжетімді:

- Ағылшын тілі
- Француз тілі
- Неміс тілі
- Итальян тілі
- Жапон тілі
- Португал тілі (Бразилия)
- Орыс тілі
- Жеңілдетілген қытай тілі
- Испан тілі
- Испан тілі (Латын Америкасы)
- Дәстүрлі қытай тілі

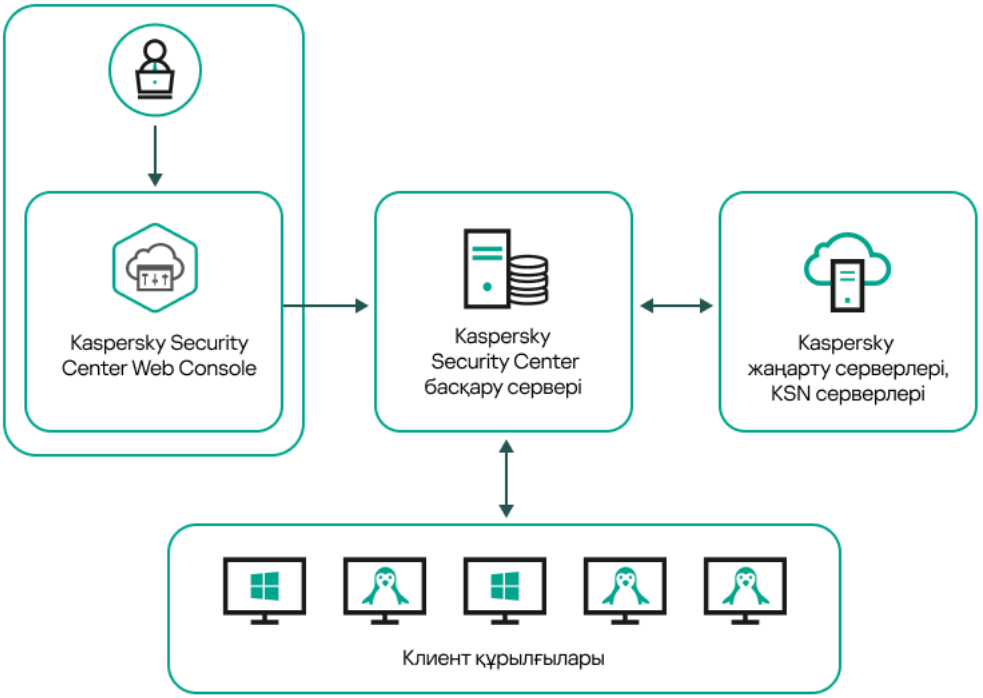
Kaspersky Next Expert View және оның мүмкіндіктері туралы көбірек ақпарат Kaspersky Next Expert View құжаттамасында және Kaspersky Endpoint Security for Business құжаттамасында қолжетімді.

Архитектура және негізгі ұғымдар

Бұл бөлімде қолданбаның архитектурасы және Kaspersky Security Center Linux қолданбасына қатысты негізгі ұғымдардың егжей-тегжейлі анықтамалары сипатталған.

Бағдарлама архитектурасы

Бұл бөлімде Kaspersky Security Center құрамдастарының және олардың өзара іс-қимылының сипаттамасы бар.



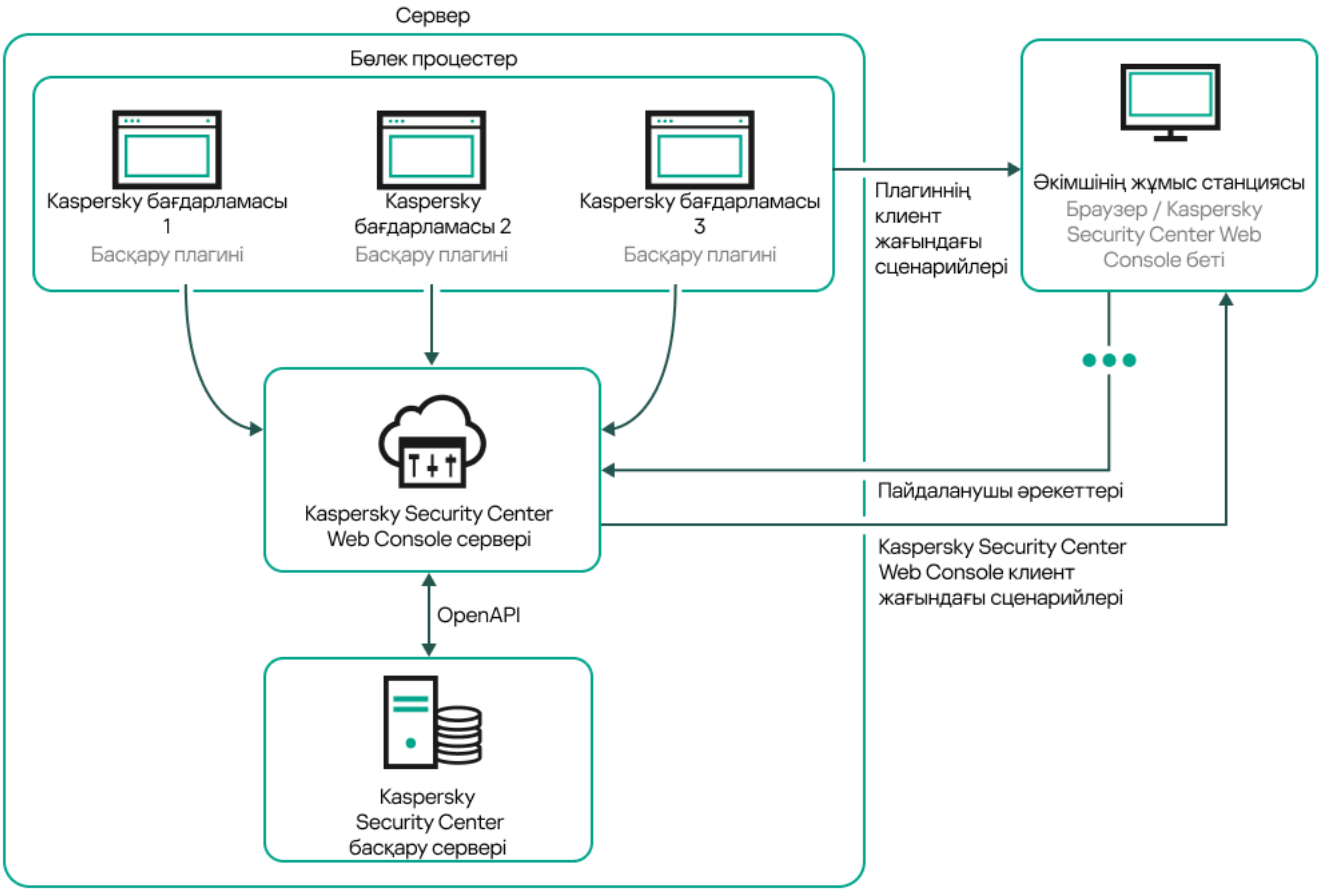
Kaspersky Security Center Linux бағдарламасы архитектурасы

Kaspersky Security Center Linux бағдарламасы келесі негізгі құрамдастарды қамтиды:

- **Kaspersky Security Center Web Console**. Бұл Kaspersky Security Center басқаратын ұйым-клиент желісін қорғау жүйесін құруға және басқаруға арналған веб-интерфейс.
- **Kaspersky Security Center Басқару сервері** (бұдан әрі *Сервер* деп те аталады). Ұйымның желісінде орнатылған бағдарламалар және оларды басқару туралы ақпаратты орталықтандырылған сақтау функцияларын жүзеге асырады.
- **Kaspersky жаңарту серверлері**. Kaspersky бағдарламаларына дерекқорлар мен модульдердің жаңартуларын жіберетін Kaspersky HTTP серверлері мен HTTPS серверлері.
- **KSN серверлері**. Серверлерде файлдардың, веб-ресурстардың және бағдарламалық жасақтаманың беделі туралы Kaspersky жедел білім базасы бар. Kaspersky Security Network Kaspersky бағдарламаларының қауіптерге реакциясының жоғары жылдамдығын қамтамасыз етеді, кейбір қорғаныс құрамдастарының тиімділігін арттырады, сондай-ақ жалған іске қосылудың ықтималдығын азайтады.
- **Клиент құрылғылары.** Ұйымның клиент құрылғыларын Kaspersky Security Center Linux қорғайды. Әрбір қорғалатын құрылғыда Kaspersky қауіпсіздік бағдарламаларының бірі орнатылуы керек.

Kaspersky Security Center Linux Басқару сервері мен Kaspersky Security Center Web Console бағдарламасын орналастыру схемасы

Келесі суретте Kaspersky Security Center Linux Басқару сервері мен Kaspersky Security Center Web Console бағдарламасын орналастыру схемасы келтірілген.



Kaspersky Security Center Linux Басқару сервері мен Kaspersky Security Center Web Console бағдарламасын орналастыру схемасы

Қорғалатын құрылғыларда орнатылған Kaspersky бағдарламаларын басқару плагиндерін (әр бағдарлама үшін бөлек плагин) орналастыру Kaspersky Security Center Web Console серверін орналастырумен бір мезгілде жүзеге асырылады.

Әкімші ретінде, сіз Kaspersky Security Center Web Console бағдарламасына өзіңіздің жұмыс станцияңыздың браузері арқылы қатынаса аласыз.

Сіз Kaspersky Security Center Web Console бағдарламасында белгілі бір әрекеттерді орындаған кезде, Kaspersky Security Center Web Console Server сервері Kaspersky Security Center Linux Басқару серверімен OpenAPI арқылы өзара әрекеттеседі. Kaspersky Security Center Web Console Server сервері Kaspersky Security Center Linux Басқару серверінен қажетті деректерді сұрайды және Kaspersky Security Center Web Console бағдарламасында сіздің әрекеттеріңіздің нәтижелерін көрсетеді.

Kaspersky Security Center Linux қолданатын порттар

Төмендегі кестелерде басқару сервері және клиент құрылғылары пайдаланатын әдепкі порттар көрсетілген. Қажет болса, осы әдепкі порттардың әрқайсысын өзгертуге болады.

Kaspersky Security Center Linux Басқару сервері пайдаланатын порттар

Порт нөмірі	Портты ашатын процесс атауы	Протокол	Портты тағайындау	Аймақ
8060	klcsweb	TCP	Клиент құрылғыларына жарияланған орнату пакеттерін беру	Орнату пакеттерін жариялау. Басқару серверінің сипаттар терезесіндегі **Веб-сервер** бөлімінде әдепкі порт нөмірін өзгертуге болады. Бұл порт міндетті емес. Қауіпсіздік мақсатында 8061 TCP портын пайдалану ұсынылады.
8061	klcsweb	TCP (TLS)	Клиент құрылғыларына жарияланған орнату пакеттерін беру	Орнату пакеттерін жариялау. Басқару серверінің сипаттар терезесіндегі **Веб-сервер** бөлімінде әдепкі порт нөмірін өзгертуге болады.
13000	klserver	TCP (TLS)	Желілік агенттерден және қосалқы Басқару серверлерінен қосылымдарды қабылдау; басты Серверден қосылымдарды қабылдау үшін қосалқы серверлерде де қолданылады (мысалы, егер қосалқы Сервер демилитаризацияланған аймақта болса)	Клиенттік құрылғыларды және бағынышты Басқару серверлерді басқару. Kaspersky Security Center Linux орнату кезінде байланыс порттарын конфигурациялауда желілік агенттерден келетін байланыстарды қабылдауға арналған әдепкі порт санын өзгертуге болады; басқару серверлерінің иерархиясын жасаған кезде, қосымша басқару серверлерінен келетін байланыстардың әдепкі портының санын өзгертуге болады.
13000	klserver	UDP	Желілік агенттерден құрылғыларды өшіру туралы ақпарат қабылдау	Клиент құрылғыларын басқару. Әдепкі порт нөмірін Желілік агент саясатының параметрлері терезесінде өзгерте аласыз.
13291	klserver	TCP (TLS)	Kaspersky Security Center Linux жұмысын автоматтандыру үшін klakaut утилитасын пайдалану	klakaut утилитасымен жұмыс істеу. klakaut утилитасы және оған арналған анықтамалық жүйе Kaspersky Security Center Linux орнату қалтасында орналасқан. Әдепкі бойынша порт жабық. Kaspersky Security Center Linux жұмысын автоматтандыру үшін klakaut утилитасын пайдаланғыңыз келсе, klscflag утилитасын пайдаланып, 13291 портын ашыңыз.
13299	klserver	TCP (TLS)	Есептік деректер және қатынасу диспетчерінен (IAM) басқару серверіне қосылымдар алу; басқару серверіне OpenAPI арқылы қосылымдар алу	Kaspersky Security Center Web Console пайдалану арқылы басқару серверін басқару; OpenAPI-мен жұмыс істеу. Әдепкі бойынша порт нөмірін Басқару сервері сипаттары терезесінде (**Жалпы** бөлімнің **Қосылу порттары** бөлікшесінде) немесе Басқару серверлерінің иерархиясын жасаған кезде өзгерте аласыз.

Порт нөмірі	Портты ашатын процесс атауы	Протокол	Портты тағайындау	Аймақ
14000	klserver	TCP	Желілік агенттерден қосылымдар қабылдау	Клиент құрылғыларын басқару. Сіз әдепкі бойынша порт нөмірін Kaspersky Security Center Linux орнатқанда қосылу порттарын конфигурациялау кезінде немесе клиент құрылғысын Басқару серверіне қолмен қосу кезінде өзгерте аласыз. Бұл порт қосымша беріледі және ол әдепкісінше жабық. Қауіпсіздік мақсатында 13000 TCP портын пайдалану ұсынылады.
13111 (құрылғыда KSN прокси-сервері қызметі іске қосылған болса ғана)	ksnproxy	TCP	Басқарылатын құрылғылардан KSN прокси-серверіне қатысты сұрауларды қабылдау	KSN прокси-сервері. Әдепкі бойынша порт мәндерін Басқару сервері сипаттары терезесінде өзгерте аласыз.
15111 (құрылғыда KSN прокси-сервері қызметі іске қосылған болса ғана)	ksnproxy	UDP	Басқарылатын құрылғылардан KSN прокси-серверіне қатысты сұрауларды қабылдау	KSN прокси-сервері. Әдепкі бойынша порт мәндерін Басқару сервері сипаттары терезесінде өзгерте аласыз.
17111 (құрылғыда KSN прокси-сервері қызметі іске қосылған болса ғана)	ksnproxy	HTTPS	Басқарылатын құрылғылардан KSN прокси-серверіне қатысты сұрауларды қабылдау	KSN прокси-сервері. Әдепкі бойынша порт мәндерін Басқару сервері сипаттары терезесінде өзгерте аласыз.
17000	klactprx	TCP (TLS)	Басқарылатын құрылғылардан бағдарламаларды белсендіру үшін қосылымдарды қабылдау	Басқарылатын құрылғыларға арналған белсендіру прокси-сервері. Әдепкі бойынша порт нөмірін Басқару сервері сипаттары терезесінде (**Жалпы** бөлімнің **Қосымша порттар** бөлікшесінде) өзгерте аласыз.
13292 (ұялы құрылғыларды басқарсаңыз ғана)	klserver	TCP (TLS)	Ұялы құрылғылардан қосылымдар қабылдау	Ұялы құрылғыларды басқару. Әдепкі бойынша порт нөмірін Басқару консоліндегі Басқару сервері сипаттары терезесінде немесе Kaspersky Security Center Web Console веб-консолінде өзгерте аласыз.
19170	klserver	HTTPS (TLS)	klsctunnel утилитасын пайдалану арқылы басқарылатын құрылғыларға қосылымдарды туннельмен жіберу	Kaspersky Security Center Web Console арқылы басқарылатын құрылғыларға қашықтан қосылу. Әдепкі порт нөмірін басқару сервері сипаттары терезесінде өзгертуге болады (**Жалпы** → **Қосылу порттары** → **RDP қосылымын туннельмен жіберу**).
4444	kliam	HTTPS	OpenID Connect протоколын пайдалану арқылы аутентификациялау	Браузер мен Есептік деректер және қатынасу диспетчері (IAM) арасында аутентификация токендерімен алмасу.
9050	kliam	HTTPS	IAM арқылы басқару серверіне қосылу	Kaspersky Security Center Web Console мен IAM арасында аутентификация токендерімен алмасу.

Егер сіз Басқару сервері мен дерекқорды әртүрлі құрылғыларға орнатқан болсаңыз, онда сіз дерекқор орналасқан құрылғыдағы қажетті порттарды (мысалы, MariaDB үшін 3306-порт) қолжетімді етуіңіз керек. Толығырақ ақпарат ДҚБЖ құжаттамасында көрсетілген.

Төмендегі кестеде iOS™ MDM серверінде қолданылатын порт көрсетілген (мобильдік құрылғыларды басқарсаңыз ғана).

iOS MDM сервері қолданатын порт

Порт нөмірі	Портты ашатын процесс атауы	Протокол	Портты тағайындау	Аймақ
443	kliosmdmservicesrv	TCP (TLS)	iOS мобильдік құрылғыларының қосылымдарын қабылдау	Ұялы құрылғыларды басқару. iOS MDM серверін орнату кезінде әдепкі бойынша порт нөмірін өзгерте аласыз.

Төмендегі кестеде Kaspersky Security Center Web Console Server пайдаланатын порт көрсетілген. Бұл, Басқару сервері орнатылған дәл сол құрылғы, не болмаса басқа құрылғы болуы мүмкін.

Kaspersky Security Center Web Console Server қолданатын порт

Порт нөмірі	Портты ашатын процесс атауы	Протокол	Портты тағайындау	Аймақ
8080	Node.js: серверлік JavaScript	TCP (TLS)	Браузерден қосылымдарды қабылдау және Kaspersky Security Center Web Console-іне жіберу	Kaspersky Security Center Web Console. Әдепкі порт нөмірін Kaspersky Security Center Web Console-ін орнату кезінде өзгерте аласыз. Kaspersky Security Center Web Console веб-консолін ALT Linux операциялық жүйесі бар құрылғыға орнатып жатсаңыз, онда 8080-порттан ерекшеленетін портты көрсету керек, себебі 8080-портты операциялық жүйе қолданады.

Төмендегі кестеде желілік агент орнатылған басқарылатын құрылғыларда қолданылатын порттар көрсетілген.

Желілік агент қолданатын порттар

Порт нөмірі	Портты ашатын процесс атауы	Протокол	Портты тағайындау	Аймақ
15000	klnagent	UDP	Басқару серверінен немесе тарату нүктесінен желілік агенттерге берілетін сигналдарды басқару	Клиент құрылғыларын басқару. Әдепкі порт нөмірін Желілік агент саясатының параметрлері терезесінде өзгерте аласыз.
15000	klnagent	UDP бойынша кеңінен тарататын таратылым	Дәл сол кеңінен тарататын домендегі басқа Желілік агенттер туралы деректер алу (бұдан әрі деректер Басқару серверіне жіберіледі)	Жаңартулар мен орнату пакеттерін жеткізу.
15001	klnagent	UDP	Тарату нүктелерінен көп мекенжайлы сұрауларды алу (қолданылса)	Тарату нүктесінен жаңартулар мен орнату пакеттерін алу. Әдепкі бойынша порт мәндерін тарату нүктесі сипаттары терезесінде өзгерте аласыз.
30522, 30523 (localhost интерфейсіндегі порттар)	klnagent	TCP	Қолданба жаңартуларын Желілік агенттен жергілікті орнатылған Kaspersky қолданбаларына FileTransferBridge компоненті арқылы тасымалдау	Дерекқор жаңартуларының көзі ретінде көрсетілген Басқару серверінен Kaspersky қолданбасының жаңартуларын алатын басқарылатын құрылғылар.

klnagent процесі мақсатты құрылғының операциялық жүйесі порттарының динамикалық ауқымынан бос порттарды да сұрай алатынын ескеріңіз. Операциялық жүйе бұл порттарды klnagent процесіне автоматты түрде тағайындайды, сондықтан klnagent процесі басқа бағдарламалық жасақтама пайдаланатын кейбір порттарды пайдалануы мүмкін. Егер klnagent процесі осы бағдарламалық жасақтамаға әсер етсе, бағдарламалық жасақтамадағы порт параметрлерін өзгертіңіз немесе осы бағдарламалық жасақтама пайдаланатын портты қоспау үшін операциялық жүйеңіздегі әдепкі бойынша порттың динамикалық ауқымын өзгертіңіз.

Kaspersky Security Center Linux қолданбасының үшінші тарап бағдарламалық құралымен үйлесімділігі туралы ұсыныстар тек анықтама үшін берілгенін және үшінші тарап бағдарламалық құралының жаңа нұсқаларына қолданылмауы мүмкін екенін ескеріңіз. Порттарды орнату бойынша сипатталған ұсыныстар техникалық қолдау қызметінің тәжірибесіне және ең жақсы тәжірибелерімізге негізделген.

Төмендегі кестеде тарату нүктесі рөлін атқаратын желілік агенті орнатылған басқарылатын құрылғыда қолданылатын порттар көрсетілген. Көрсетілген порттар желілік агенттер қолданатын порттарға қосымша ретінде тарату нүктесі құрылғыларында қолданылады (жоғарыдағы кестені қараңыз).

Тарату нүктесі ретінде жұмыс істейтін Желілік агент қолданатын порттар

Порт нөмірі	Портты ашатын процесс атауы	Протокол	Портты тағайындау	Аймақ
13000	klnagent	TCP (TLS)	Желілік агенттер мен қосылым шлюздерінен қосылымдарды қабылдау	Клиент құрылғыларын басқару, жаңартулар мен орнату пакеттерін жеткізу. Әдепкі бойынша порт мәндерін тарату нүктесі сипаттарында өзгерте аласыз.
13111 (құрылғыда KSN прокси-сервері қызметі іске қосылған болса ғана)	ksnproxy	TCP	Басқарылатын құрылғылардан KSN прокси-серверіне қатысты сұрауларды қабылдау	KSN прокси-сервері. Әдепкі бойынша порт мәндерін тарату нүктесі сипаттарында өзгерте аласыз.
15111 (құрылғыда KSN прокси-сервері қызметі іске қосылған болса ғана)	ksnproxy	UDP	Басқарылатын құрылғылардан KSN прокси-серверіне қатысты сұрауларды қабылдау	KSN прокси-сервері. Әдепкі бойынша порт мәндерін тарату нүктесі сипаттарында өзгерте аласыз.
17111 (құрылғыда KSN прокси-сервері қызметі іске қосылған болса ғана)	ksnproxy	HTTPS	Басқарылатын құрылғылардан KSN прокси-серверіне қатысты сұрауларды қабылдау	KSN прокси-сервері. Әдепкі бойынша порт мәндерін тарату нүктесі сипаттарында өзгерте аласыз.
13295 (тарату нүктесін push-сервер ретінде қолдансаңыз ғана)	klnagent	TCP (TLS)	Клиент құрылғыларынан қосылымдар қабылдау	Push-сервер. Әдепкі бойынша порт мәндерін тарату нүктесі сипаттарында өзгерте аласыз.
8060	klcsweb	TCP	Клиент құрылғыларына жарияланған орнату пакеттерін беру	Орнату пакеттерін жариялау. Басқару серверінің сипаттар терезесіндегі **Веб-сервер** бөлімінде әдепкі порт нөмірін өзгертуге болады.
8061	klcsweb	TCP (TLS)	Клиент құрылғыларына жарияланған орнату пакеттерін беру	Орнату пакеттерін жариялау. Басқару серверінің сипаттар терезесіндегі **Веб-сервер** бөлімінде әдепкі порт нөмірін өзгертуге болады.

Төмендегі кестеде домен контроллері құрылғысында пайдаланылатын порттар көрсетілген.

Домен контроллері құрылғысында пайдаланылатын порттар

Порт нөмірі	Протокол	Портты тағайындау	Аймақ
389	TCP немесе UDP арқылы LDAP	LDAP серверіне қосылу	Домен контроллері сауалнамасы
636	TLS арқылы LDAP	LDAP серверіне қосылу	Домен контроллері сауалнамасы

Төмендегі кестеде, Желілік агент орнатылмаған клиент құрылғыларында ашық болуы тиісті порт қамтылған.

Тағайындалмаған клиент құрылғысында пайдаланылатын порт

Порт нөмірі	Протокол	Портты тағайындау	Аймақ
22	SSH	SSH арқылы клиент құрылғысына қосылуда	Kaspersky қолданбаларын қашықтан орнату.

Kaspersky Security Center Web Console бағдарламасы қолданатын порттар

Төмендегі кестеде Kaspersky Security Center Web Console Server сервері (бұдан әрі жай ғана Kaspersky Security Center Web Console) орнатылған құрылғыда ашылатын порттар тізімі атап көрсетілген.

Порт нөмірі	Қызмет атауы	Протокол	Портты тағайындау	Аймақ
2001	Kaspersky Security Center Product Plugins Server	HTTPS	"Kaspersky Security Center Web Console Management Service" қызметінен сұрауларды қабылдау үшін басқару плагин процестері тарапынан қолданылатын API порты.	Басқару плагиндерінің node процестерін іске қосу.
1329, 2003	Kaspersky Security Center Web Console Management Service	HTTPS	Бір құрылғыда жұмыс істейтін "Kaspersky Security Center Web Console Management Service" қызметінен сұрауларды қабылдау үшін пайдаланылатын API порттары.	Kaspersky Security Center Web Console құрамдастарын жаңарту
2005	Kaspersky Security Center Web Console	HTTPS	Бір құрылғыда жұмыс істейтін "Kaspersky Security Center Web Console Management Service" қызметінен сұрауларды қабылдау үшін пайдаланылатын API порты.	Kaspersky Security Center Web Console бағдарламасының node процестерін іске қосу.
8200	—	HTTP	HashiCorp Vault арқылы сертификаттар жасау үшін қолданылатын API порты (толық ақпарат HashiCorp Vault веб-сайтында берілген).	Kaspersky Security Center Web Console веб-консолін орнату және Kaspersky Security Center Web Console құрамдастарын жаңарту
4222	Kaspersky Security Center Web Console NATS	HTTPS	Kaspersky Security Center Web Console процестері мен басқару плагиндері арасындағы байланыс үшін пайдаланылатын NATS негізіндегі Message Broker API порттары. 8222 порты NAT бақылау үшін пайдаланылады.	Kaspersky Security Center Web Console және басқару плагиндері арасындағы өзара іс қимыл
4444	Есептік деректер және қатынасу диспетчері (IAM)	HTTPS	OpenID Connect аутентификация протоколы пайдаланатын порт.	Kaspersky Security Center Web Console және Есептік деректер және қатынасу диспетчері (IAM) арасында аутентификация токендерімен алмасу.
9050	IAM	HTTPS	IAM пайдаланатын порт.	Kaspersky Security Center Web Console және IAM арасындағы өзара әрекет

Негізгі ұғымдар

Бұл бөлімде Kaspersky Security Center Linux бағдарламасына қатысты негізгі ұғымдардың егжей-тегжейлі анықтамалары бар.

Басқару сервері

Kaspersky Security Center Linux құрамдастары клиент құрылғыларында орнатылған Kaspersky бағдарламаларын қашықтан басқаруға мүмкіндік береді.

Басқару сервері құрамдасы орнатылған құрылғылар *Басқару серверлері* (бұдан әрі - *Серверлер*) деп аталады. Басқару серверлері рұқсатсыз қол жеткізудің кез келген түрінен, соның ішінде физикалық тұрғыдан қорғалуы тиіс.

Басқару сервері құрылғыға келесі атрибуттар жиынтығы бар қызмет ретінде орнатылады:

- `kladminserver_srv` атымен
- Операциялық жүйені іске қосу кезінде автоматты түрде іске қосу түрімен
- `ksc` есептік жазбасымен немесе Басқару серверін орнату кезінде жасалған таңдауларға сәйкес пайдаланушы есептік жазбасымен

Орнату параметрлерінің толық тізімін алу үшін келесі мақаланы қараңыз: Kaspersky Security Center Linux орнату.

Басқару сервері келесі функцияларды орындайды:

- Басқару топтары құрылымын сақтау
- Клиент құрылғыларының конфигурациясы туралы ақпаратты сақтау
- Бағдарламалардың дистрибутивтерінің қоймаларын ұйымдастыру
- Клиент құрылғыларына бағдарламаларды қашықтан орнату және бағдарламаларды жою
- Kaspersky дерекқорлары мен бағдарлама модульдерін жаңарту
- Клиент құрылғыларындағы саясат пен тапсырмаларды басқару
- Клиент құрылғыларында болған оқиғалар туралы ақпаратты сақтау
- Kaspersky бағдарламаларының жұмысы туралы есептерді қалыптастыру
- Клиент құрылғыларына лицензиялық кілттерді тарату, кілт туралы ақпаратты сақтау
- Тапсырмалардың орындалу барысы туралы хабарландырулар жіберу (мысалы, клиент құрылғысында вирустарды анықтау)

Бағдарлама интерфейсіндегі Басқару серверлерін атау ережесі

Kaspersky Security Center Web Console интерфейсінде Басқару серверлерінде келесі атаулар болуы мүмкін:

- Басқару сервері құрылғысының атауы, мысалы: "*құрылғы_атауы*" немесе "Басқару сервері: *құрылғы_атауы*".
- Басқару сервері құрылғысының IP мекенжайы, мысалы: "*IP_мекенжайы*" немесе "Басқару сервері: *IP_мекенжайы* ".
- Қосалқы Басқару серверлері мен виртуалды Басқару серверлерінің жалқы есімдері бар, оларды сіз виртуалды немесе қосалқы Басқару серверін негізгі Басқару серверіне қосу кезінде көрсетесіз.
- Егер сіз Linux басқаратын құрылғыға орнатылған Kaspersky Security Center Web Console бағдарламасын қолданып жатсаңыз, онда бағдарлама жауап файлдарында сенімді деп көрсетілген Басқару серверлерінің атауын көрсетеді.

Басқару серверіне Kaspersky Security Center Web Console көмегімен қосыла аласыз.

Басқару серверлерінің иерархиясы

Басқару серверлері иерархияны құра алады. Әрбір Басқару серверінде иерархияның әртүрлі деңгейлерінде бірнеше қосалқы Басқару серверлері (бұдан әрі - *қосалқы Серверлер*) болуы мүмкін. Қосалқы Серверлердің енгізу деңгейі шектелмейді. Бұл жағдайда, басты Серверді басқару топтарының құрамына барлық қосалқы Серверлердің клиент құрылғылары кіреді. Осылайша, компьютерлік желінің тәуелсіз аймақтарын әртүрлі Басқару серверлері басқара алады, ал оларды өз кезегінде басты Сервер басқарады.

Linux операциялық жүйесі бар Басқару сервері Сервер иерархиясында Басты сервер ретінде де, Қосалқы сервер ретінде де жұмыс істей алады. Linux операциялық жүйесі бар Басты сервер Linux және Windows операциялық жүйелері бар Қосалқы серверлерді басқара алады. Windows операциялық жүйесінде жұмыс істейтін негізгі сервер Linux операциялық жүйесінде жұмыс істейтін қосалқы серверді басқара алады.

Қосалқы Басқару серверлерінің жеке жағдайы *виртуалды Басқару серверлері* болып табылады.

Басқару серверлерінің иерархиясын келесі мақсаттар үшін қолдануға болады:

- Басқару серверіне түсетін жүктемені шектеу (желіде орнатылған бір Сервермен салыстырғанда).
- Желі ішіндегі трафикті қысқарту және қашықтағы кеңселермен жұмыс істеуді жеңілдету. Басты Сервер мен мысалы, басқа аймақтарда болуы мүмкін барлық желі құрылғылары арасында қосылым орнатудың қажеті жоқ. Желінің әр аймағында қосалқы Басқару серверлерін орнату, қосалқы Серверлердің басқару топтарында құрылғыларды тарату және қосалқы Серверлерге басты Сервермен жылдам байланыс арналары арқылы қосылуды қамтамасыз ету жеткілікті.
- Антивирустық қауіпсіздік әкімшілері арасындағы жауапкершілікті бөлу. Бұл ретте, ұйым желісінің вирусқа қарсы қауіпсіздігінің күйін орталықтандырылған басқару мен мониторингтеудің барлық мүмкіндіктері сақталады.
- Kaspersky Security Center Linux бағдарламасын қызмет өндірушілерімен пайдалану. Провайдерге Kaspersky Security Center Linux және Kaspersky Security Center Web Console орнату жеткілікті. Әртүрлі ұйымдардың көптеген клиент құрылғыларын басқару үшін провайдер Басқару серверлері иерархиясына (виртуалды Серверлерді қоса) қосалқы Басқару серверлерін қоса алады.

Басқару топтарының иерархиясына енгізілген әрбір құрылғыны тек бір Басқару серверіне қосуға болады. Құрылғылардың Басқару серверлеріне қосылуын өзіңіз тексеруіңіз керек. Ол үшін әртүрлі Серверлердің басқару топтарындағы желілік атрибуттар бойынша құрылғыларды іздеу функциясын пайдалануға болады.

Виртуалды Басқару сервері

Виртуалды Басқару сервері (бұдан әрі – *виртуалды Сервер*) — ұйым-клиенттің желісінің антивирустық қорғанысын басқаруға арналған Kaspersky Security Center Linux бағдарламасының құрамдасы.

Виртуалды Басқару сервері қосалқы Басқару серверінің жеке жағдайы болып табылады және физикалық Басқару серверімен салыстырғанда келесі негізгі шектеулерге ие:

- Виртуалды Басқару сервері тек негізгі Басқару серверінің құрамында ғана жұмыс істей алады.
- Виртуалды басқару сервері жұмыс істеген кезде негізгі Басқару серверінің негізгі дерекқорын пайдаланады. Деректерді сақтық көшірмелеу және қалпына келтіру тапсырмаларына, сондай-ақ жаңартуларды тексеру және жүктеу тапсырмаларына виртуалды Басқару серверінде қолдау көрсетілмейді.
- Виртуалды сервер үшін қосалқы Басқару серверлерін (соның ішінде виртуалды) құруға қолдау көрсетілмейді.

Сонымен қатар, виртуалды Басқару серверінде келесі шектеулер бар:

- Виртуалды Серверінің сипаттары терезесінде бөлімдер жиынтығы шектеулі.
- Виртуалды Сервер басқаратын клиент құрылғыларына Kaspersky бағдарламаларын қашықтан орнату мақсатында, виртуалды Сервермен байланысу үшін клиент құрылғыларының біріне Желілік агент орнатылуы қажет. Виртуалды Басқару серверіне алғаш қосылған кезде бұл құрылғы автоматты түрде тарату нүктесі ретінде тағайындалады және виртуалды Басқару сервері мен клиент құрылғыларының қосылым шлюзі рөлін атқарады.
- Виртуалды Басқару сервері желіде тарату нүктелері арқылы ғана сауалнама өткізе алады.
- Өнімділігі бұзылған виртуалды Серверді қайта іске қосу үшін Kaspersky Security Center Linux бағдарламасы негізгі Басқару серверін және барлық виртуалды Серверлерді қайта іске қосады.
- Виртуалды серверде жасалған пайдаланушыларға басқару серверінде рөлдерді тағайындау мүмкін емес.

Виртуалды Сервер әкімшісі осы виртуалды Сервердің шеңберінде барлық құқықтарға ие.

Веб-сервер

Kaspersky Security Center *Web Server* (бұдан әрі – *Веб-сервер*) – бұл Басқару серверінің құрамында орнатылатын Kaspersky Security Center құрамдасы. Веб-сервер жеке орнату пакеттерін, сондай-ақ ортақ қатынасы бар қалтадағы файлдарды желі арқылы беруге арналған.

Жасау кезінде, жеке орнату пакеті Веб-серверде автоматты түрде жарияланады. Автономды пакетті жүктеу сілтемесі, жасалған автономды орнату пакеттерінің тізімінде көрсетіледі. Қажет болса, автономды пакетті жариялауды болдырмауға немесе оны Веб-серверде қайта жариялауға болады.

Ортақ қатынасы бар қалта, құрылғылары Басқару сервері басқаратын барлық пайдаланушыларға қолжетімді ақпаратты орналастыру үшін пайдаланылады. Егер пайдаланушының ортақ қатынасы бар қалтаға тікелей қатынасу мүмкіндігі болмаса, оған Веб-сервер арқылы сол қалтадан ақпарат жіберуге болады.

Пайдаланушыларға Веб-сервер арқылы ортақ қатынасы бар қалтадан ақпарат беру үшін әкімші ортақ қатынасы бар қалтада салынған public қалтасын жасап, оған ақпаратты орналастыруы керек.

Пайдаланушыға ақпарат беру үшін сілтеме синтаксисі келесідей:

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

мұндағы

- `<Web Server name>` – Kaspersky Security Center Веб-серверінің атауы.
- `<HTTPS port>` – әкімші белгілеген Веб-сервер HTTPS порты. HTTPS портын Басқару сервері сипаттары терезесінің **Веб-сервер** бөлімінде белгілеуге болады. Әдепкі бойынша 8061-порт орнатылған.
- `<object>` – пайдаланушы үшін қатынасу мүмкіндігін ашуды қажет ететін салынған қалта немесе файл.

Әкімші қалыптастырылған сілтемені пайдаланушыға кез келген ыңғайлы тәсілмен, мысалы, электрондық пошта арқылы жібере алады.

Алынған сілтеме бойынша пайдаланушы өзіне арналған ақпаратты жергілікті құрылғыға жүктей алады.

Kaspersky Security Center Linux Web Server

Kaspersky Security Center Linux веб-сервері (бұдан әрі Веб-сервер) – Kaspersky Security Center Linux құрамдасы. Веб-сервер жеке орнату пакеттерін және ортақ қатынасы бар қалтадағы файлдарды жариялау үшін қолданылады.

Құрылған орнату пакеттері Веб-серверде автоматты түрде жарияланады және бірінші рет жүктегеннен кейін жойылады. Әкімші қалыптастырылған сілтемені пайдаланушыға кез келген ыңғайлы тәсілмен, мысалы, электрондық пошта арқылы жібере алады.

Алынған сілтеме арқылы, пайдаланушы ұялы құрылғыға арналған ақпаратты жүктей алады.

Веб-серверді конфигурациялау

Веб-Сервердің сипаттарында Веб-серверді дәл конфигурациялау үшін HTTP (8060) және HTTPS (8061) протоколдарының порттарын ауыстыруға болады. Сондай-ақ, порттарды ауыстырудан бөлек, HTTPS протоколы үшін серверлік сертификатты ауыстыруға және HTTP протоколы үшін веб-сервер FQDN атауын ауыстыруға болады.

Қосылым шлюзіндегі веб-сервер параметрлері

Бөлек веб-сервер қызметі тарату нүктесіне қосылым шлюзі режимінде ендіріледі, бұл Kaspersky Security Center Linux жүйесіне қосылған мобильдік құрылғыларда жұмыс істеуге мүмкіндік береді. Бұл қызмет қолданбаларды орнату пакеттерін және құрылғыны басқару профильдерін басқару серверіне тікелей қоспай-ақ құрылғыларға тасымалдауға жауапты. Қызмет қосылым шлюзінде HTTP/HTTPS файл сұрауларын өңдеген кезде, файлдар тасымалданады.

Қосылым шлюзіндегі веб-сервер қызметі желілік агент Linux-пен бірге орнатылады. Бұл функцияны пайдалану үшін веб-сервер ретінде пайдаланылатын қосылым шлюзі режимінде тарату нүктесі ретінде әрекет ететін құрылғыны тағайындау, содан кейін сәйкес параметрлерді көрсету керек. Қосылым шлюзінде веб-сервер параметрлерін конфигурациялау туралы толық ақпаратты Kaspersky Secure Mobility Management анықтамасынан қараңыз.

Желілік агент

Басқару сервері мен құрылғылар арасындағы өзара іс-қимылды *Желілік агент* – Kaspersky Security Center Linux құрамдасы қамтамасыз етеді. Желілік агент Kaspersky бағдарламаларының жұмысын басқару Kaspersky Security Center Linux көмегімен орындалатын барлық құрылғыларға орнатылуы қажет.

Желілік агент орнатылған құрылғы *басқарылатын құрылғы* немесе *құрылғы* деп аталады. Желілік агентке арналған орнату пакетін келесі дереккөздерден жүктеп алуға болады:

- Басқару сервері қоймасы (басқару сервері орнатылуы керек)
- Kaspersky веб-сайты

Linux жүйесіне арналған желілік агент құрылғыға келесі атрибуттар жиынтығы бар қызмет ретінде орнатылады:

- "Kaspersky желілік агенті" атауы
- Операциялық жүйені іске қосу кезінде автоматты түрде іске қосу түрімен
- Түбірлік есептік жазба көмегімен

Windows жүйесіне арналған желілік агент құрылғыға келесі атрибуттар жиынтығы бар қызмет ретінде орнатылады:

- "Kaspersky Security Center желілік агенті" атауы
- Операциялық жүйені іске қосу кезінде автоматты түрде іске қосу түрімен
- LocalSystem есептік жазбасы көмегімен

macOS жүйесіне арналған желілік агент құрылғыға келесі атрибуттар жиынтығы бар қызмет ретінде орнатылады:

- "com.kaspersky.klnagent.core" атауы
- Операциялық жүйені іске қосу кезінде автоматты түрде іске қосу түрімен
- Түбірлік есептік жазба көмегімен

Қызметтік процестердің атаулары:

- Linux үшін:
  - klnagent64.service (64 разрядты операциялық жүйе үшін);
  - klnagent.service (32 разрядты операциялық жүйе үшін).
- Windows үшін:
  - klnagent
- macOS үшін:
  - com.kaspersky.klnagent

Әдепкісінше желілік агент келесі орындарға орнатылады:

- Linux үшін:
  - 32 биттік жүйелер: /opt/kaspersky/klnagent/
  - 64 биттік жүйелер: /opt/kaspersky/klnagent64/
- Windows үшін:
  - 32 биттік жүйелер: C:\Program Files\Kaspersky Lab\NetworkAgent
  - 64 биттік жүйелер: C:\Program Files (x86)\Kaspersky Lab\NetworkAgent

- macOS үшін:
  - 64-биттік жүйелер: /Library/Application Support/Kaspersky Lab/klnagent/Binaries/klnagent

Windows құрылғыларының орнату пакеті параметрлерінде желілік агент орнату үшін басқа қалтаны көрсетуге болады. Дегенмен Linux құрылғыларында желілік агентті тек әдепкі каталогке орнатуға болады.

Желілік агенттің орнату қалтасында klmover және klnagchk утилиталары сияқты желілік агент жұмысын басқаруға және диагностикалауға арналған утилиталар да бар.

Басқару серверін орнату кезінде Желілік агенттің серверлік нұсқасы Басқару серверімен бірге автоматты түрде орнатылады. Басқару сервері бар құрылғыны басқарылатын басқа құрылғылар сияқты басқару үшін басқару сервері бар құрылғыға Linux жүйесіне арналған желілік агентті орнатыңыз. Бұл жағдайда Linux үшін Желілік агент орнатылады және Басқару серверімен бірге орнатылған Желілік агенттің сервер нұсқасына қарамастан тәуелсіз жұмыс істейді.

Желілік агент басқарылатын құрылғыларды Басқару серверімен синхрондайды. Синхрондау кезеңін (*мерзімді сигнал*) 10 000 басқарылатын құрылғыға 15 минутқа тең етіп белгілеу ұсынылады.

Басқару топтары

Басқару тобы (бұдан әрі *топ* деп те аталады) – бұл топтың құрылғыларын Kaspersky Security Center Linux-те біртұтас ретінде басқару мақсатында қандай да бір белгі бойынша біріктірілген басқарылатын құрылғылар жиынтығы.

Басқару тобындағы барлық басқарылатын құрылғылар үшін төмендегілер белгіленеді:

- Бағдарламалардың жұмысының бірыңғай параметрлері – топтық саясаттар көмегімен.
- Барлық бағдарламалардың бірыңғай жұмыс режимі – белгілі бір параметрлер жиынтығы бар топтық тапсырмаларды құру арқылы. Топтық тапсырмалар мысалдарына: жалпы орнату пакетін жасау және орнату, бағдарлама дерекқорлары мен модульдерін жаңарту, құрылғыны талап бойынша тексеру және тұрақты қорғаныста қосу кіреді.

Басқарылатын құрылғы тек бір басқару тобының құрамына кіре алады.

Басқару серверлері мен басқару топтары үшін кез келген тіркеме деңгейі бар иерархиялар жасауға болады. Иерархияның бір деңгейінде қосалқы және виртуалды Басқару серверлері, топтар және басқарылатын құрылғылар орналасуы мүмкін. Құрылғыларды физикалық түрде жылжытпай, бір топтан екінші топқа ауыстыруға болады. Мысалы, кәсіпорын қызметкері бухгалтер лауазымынан әзірлеуші лауазымына ауысса, сіз сол қызметкердің құрылғысын "Бухгалтерлер" басқару тобынан "Әзірлеушілер" басқару тобына ауыстыра аласыз. Осылайша әзірлеушілер үшін қажетті қолданба параметрлері құрылғыға автоматты түрде жіберіледі.

Басқарылатын құрылғы

Басқарылатын құрылғы — бұл желілік агент орнатылған, Linux, Windows немесе macOS операциялық жүйесі бар құрылғы. Сіз мұндай құрылғыларды, құрылғыларда орнатылған бағдарламаларға арналған тапсырмалар мен саясаттардың көмегімен басқара аласыз. Сондай-ақ, сіз басқарылатын құрылғыларға арналған есептерді құрастыра аласыз.

Сіз тарату нүктесі мен қосылым шлюзі функцияларын орындайтын басқарылатын құрылғыны конфигурациялай аласыз.

Құрылғы тек бір Басқару серверінің басқаруымен болуы мүмкін. Бір басқару сервері арқылы басқаруға болатын құрылғылар саны басқару сервері орналасқан құрылғы конфигурациясына және ДҚБЖ шектеулеріне байланысты.

Тағайындалмаған құрылғы

Тағайындалмаған құрылғы – бірден-бір басқару тобына қосылмаған желідегі құрылғы. Сіз тағайындалмаған құрылғылармен әрекеттерді орындай аласыз, мысалы, оларды басқару топтарына көшіре аласыз, оларға бағдарламалар орната аласыз.

Желіде жаңа құрылғы анықталған кезде, ол **Тағайындалмаған құрылғылар** басқару тобына орналастырылады. Құрылғыларды анықтаған сәтте басқару топтары бойынша автоматты түрде тарату ережелерін конфигурациялауға болады.

Әкімшінің жұмыс станциясы

Kaspersky Security Center Web Console Server сервері орнатылған құрылғылар *әкімшілердің жұмыс орындары* деп аталады. Осы құрылғылардан әкімшілер клиент құрылғыларында орнатылған Kaspersky бағдарламаларын қашықтан орталықтандырылған басқаруды жүзеге асыра алады.

Әкімшінің жұмыс станцияларының саны шектелмейді. Әрбір әкімші жұмыс станциясынан желідегі бірнеше Басқару серверлерінің басқару топтарын бірден басқаруға болады. Әкімшінің жұмыс станциясын кез келген иерархия деңгейіндегі Басқару серверіне (физикалық және виртуалды) қосуға болады.

Әкімшінің жұмыс станциясын клиент құрылғысы ретінде басқару тобы құрамына қосуға болады.

Кез келген Сервердің басқару топтарында бір құрылғы бір уақытта Басқару серверінің клиенті де, Басқару сервері де және әкімшінің жұмыс станциясы да бола алады.

Басқару веб-плагиндері

Басқару веб-плагиндері – Kaspersky Security Center Web Console көмегімен Kaspersky бағдарламалары тарапынан қашықтан басқару үшін қолданылатын арнайы құрамдас. Басқару веб-плагині *басқару плагині* деп те аталады. Басқару плагині Kaspersky Security Center Web Console бағдарламасы мен Kaspersky белгілі бір бағдарламасы арасындағы интерфейс болып табылады. Басқару плагині көмегімен бағдарлама үшін тапсырмалар мен саясаттарды конфигурациялауға болады.

Сіз басқару веб-плагиндерін Kaspersky Техникалық қолдау қызметі веб-сайтынан жүктеп ала аласыз.

Басқару плагині келесі мүмкіндіктерді ұсынады:

- Бағдарламаның тапсырмалары мен параметрлерін жасауға және өзгертуге арналған интерфейс.
- Kaspersky бағдарламалары мен құрылғыларды қашықтан орталықтандырылған түрде конфигурациялау үшін саясаттар мен саясаттар профильдерін жасауға арналған өзгертуге арналған интерфейс.

- Бағдарламалар қалыптастырған оқиғаларды беру.
- Бағдарламаның оқиғалары мен жедел деректерін, сондай-ақ клиент құрылғысынан алынған статистиканы көрсетуге арналған Kaspersky Security Center Web Console функциялары.

Саясаттар

Саясат – басқару тобы мен оның ішкі тобына қатысты қолданылатын Kaspersky бағдарламасының параметрлері жиынтығы. Kaspersky бағдарламаларының бірнешеуін басқару тобының құрылғыларына орната аласыз. Kaspersky Security Center бағдарламасы басқару тобындағы Kaspersky бағдарламасының әрқайсысы үшін бір саясаттан ұсынады. Саясат келесі мәртебелердің біріне ие:

Саясат күйі

Күй	Сипаттамасы
Белсенді	Бұл, құрылғыға қатысты қолданылатын ағымдағы саясат. Kaspersky бағдарламасы үшін әрбір басқару тобында тек бір саясат белсенді болуы мүмкін. Kaspersky бағдарламасының белсенді саясаты параметрлерінің мәндері құрылғыға қатысты қолданылады.
Белсенді емес	Қазіргі уақытта құрылғыға қатысты қолданылмайтын саясат.
Автономды пайдаланушылар үшін	Егер бұл нұсқа таңдалса, құрылғы ұйым желісінен шыққан кезде саясат күшіне енеді.

Саясаттар келесі ережелер бойынша әрекет етеді:

- Бір бағдарлама үшін түрлі мәндері бар бірнеше саясатты конфигурациялауға болады.
- Бір бағдарлама үшін тек бір саясат белсенді болуы мүмкін.
- Саясаттың еншілес саясаттары болуы мүмкін.

Сіз вирустық шабуыл сияқты төтенше жағдайларға дайындалу үшін саясатты қолдана аласыз. Мысалы, USB флеш-дискілері арқылы шабуыл орын алса, флеш-дискілерге қатынасуға тыйым салатын саясатты іске қосуға болады. Бұл жағдайда, ағымдағы белсенді саясат автоматты түрде белсенді емес болады.

Көптеген саясаттарды қолдамау үшін, мысалы, әртүрлі жағдайларда бірнеше параметрлерді ғана өзгерту қажет болғанда, сіз саясат профильдерін қолдана аласыз.

Саясат профилі – саясат параметрлерін алмастыратын аталған саясат параметрлері ішкі жиынтығы. Саясат профилі басқарылатын құрылғының тиімді параметрлерін қалыптастыруға әсер етеді. *Тиімді параметрлер* – қазіргі уақытта құрылғыға қатысты қолданылатын саясат параметрлері, саясат профилі параметрлері және жергілікті бағдарлама параметрлері жиынтығы.

Саясат профильдері келесі ережелер бойынша жұмыс істейді:

- Саясат профилі белгіленген белсендіру шарты туындаған кезде күшіне енеді.
- Саясат профильдері саясат параметрлерінен ерекшеленетін параметр мәндерін қамтиды.
- Саясат профилін белсендіру кезінде басқарылатын құрылғының тиімді параметрлері өзгереді.
- Саясатта ең көбі 100 профиль болуы мүмкін.

Саясат профильдері

Әртүрлі басқару топтары үшін бір саясаттың бірнеше көшірмесін жасау қажеттілігі туындауы мүмкін; осы саясаттардың параметрлерін орталықтан өзгерту қажеттілігі де туындауы ықтимал. Бұл көшірмелер бір немесе екі параметрде ерекшеленуі мүмкін. Мысалы, ұйымдағы барлық бухгалтерлер бірдей саясаттың басқаруымен жұмыс істейді, бірақ аға бухгалтерлерге USB флеш-дискілерін пайдалануға рұқсат етіледі, ал кіші бухгалтерлерге рұқсат етілмейді. Бұл жағдайда, басқару топтарының иерархиясы арқылы құрылғыларға саясаттарды қолдану ыңғайсыз болуы мүмкін.

Бір саясаттың бірнеше көшірмесін жасауды болдырмау үшін Kaspersky Security Center Linux *саясаттардың профильдерін* жасауға мүмкіндік береді. Саясат профильдері, бір басқару тобындағы құрылғылардың әртүрлі саясат параметрлері болуы үшін қажет.

Саясат профилі, саясат параметрлерінің аталған ішкі жиынтығы болып табылады. Параметрлердің осы ішкі жиынтығы құрылғыларға саясатпен бірге таралады және келесі шартты – *профильді белсендіру шартын* орындаған кезде саясатты толықтырады. Профильдер басқарылатын құрылғыда әрекет ететін "негізгі" саясаттан ерекшеленетін параметрлерді ғана қамтиды. Профильді белсендіру кезінде құрылғыда бастапқыда әрекет еткен "негізгі" саясат параметрлері өзгереді. Бұл параметрлер профильде көрсетілген мәндерді қабылдайды.

Тапсырмалар

Kaspersky Security Center Linux *тапсырмаларды* құру және іске қосу арқылы құрылғыларда орнатылған Kaspersky қауіпсіздік бағдарламаларының жұмысын басқарады. Тапсырмалардың көмегімен бағдарламаларды орнату, іске қосу және тоқтату, файлдарды сканерлеу, бағдарламалардың дерекқорлары мен модульдерін жаңарту, бағдарламалармен басқа әрекеттер орындалады.

Бағдарлама үшін басқару плагині орнатылған жағдайда ғана тапсырма жасай аласыз.

Тапсырмалар Басқару серверінде және құрылғыларда орындалуы мүмкін.

Басқару серверінде орындалатын тапсырмалар:

- Есептерді автоматты түрде жеткізу
- Жаңартуларды Басқару серверінің қоймасына жүктеп алу
- Басқару сервері деректерінің сақтық көшірмесін жасау
- Дерекқорларға қызмет көрсету

Құрылғыларда тапсырмалардың келесі түрлері орындалады:

- *Жергілікті тапсырмалар* – нақты құрылғыда орындалатын тапсырмалар.

  Жергілікті тапсырмаларды тек әкімші Kaspersky Security Center Web Console-інің құралдары арқылы ғана емес, қашықтағы құрылғының пайдаланушысы да өзгерте алады (мысалы, қауіпсіздік бағдарламасының интерфейсінде). Егер жергілікті тапсырманы басқарылатын құрылғыда әкімші де, пайдаланушы да бір уақытта өзгерткен болса, онда әкімші енгізген өзгерістер басым болып күшіне енеді.

- *Топтық тапсырмалар* – бұл аталған топтың барлық құрылғыларында орындалатын тапсырмалар.

  Егер тапсырманың сипаттарында басқаша көрсетілмесе, топтық тапсырма аталған топтың ішкі топтарына да таралады. Топтық тапсырмалар (міндетті емес) осы топқа және ішкі топтарға орналастырылған қосалқы және виртуалды Басқару серверлеріне қосылған құрылғыларда да жұмыс істейді.

- *Глобалдық тапсырмалар* – бұл басқару топтарына кіретіндігіне қарамастан, таңдалған құрылғыларда орындалатын тапсырмалар.

Әр бағдарлама үшін сіз топтық тапсырмалардың, глобалдық тапсырмалардың және жергілікті тапсырмалардың кез келген санын жасай аласыз.

Тапсырма параметрлеріне өзгертулер енгізуге, тапсырмалардың орындалуын бақылауға, тапсырмаларды көшіруге, экспорттауға және импорттауға, сондай-ақ жоюға болады.

Құрылғыдағы тапсырмаларды іске қосу тек осы тапсырмалар жасалған бағдарлама іске қосылған жағдайда ғана орындалады.

Тапсырмаларды орындау нәтижелері оқиғалардың жүйелік журналында және Kaspersky Security Center Linux оқиғалар журналында орталықтандырылған түрінде Басқару серверінде де, әр құрылғыда жергілікті түрінде де сақталады.

Тапсырмалар параметрлерінде құпия деректерді пайдаланбаңыз. Мысалы, домен әкімшісінің құпиясөзін көрсетпеуге тырысыңыз.

Тапсырманың әрекет ету ауқымы

Тапсырма ауқымы — тапсырма орындалатын құрылғылар жинағы. Тапсырма ауқымының келесі түрлері бар:

- *Жергілікті тапсырма* ауқымы – құрылғының өзі.
- *Басқару серверінің тапсырмасы* ауқымы – Басқару сервері.
- *Топтық тапсырма* ауқымы – топқа кіретін құрылғылардың тізбесі.

Глобалдық тапсырма жасаған кезде оның ауқымын анықтаудың келесі әдістерін қолдануға болады:

- Қажетті құрылғыларды қолмен көрсету.

  Құрылғының мекенжайы ретінде сіз IP мекенжайын (немесе IP аралығын) немесе DNS атауын пайдалана аласыз. Басқару серверімен анықталған желілік құрылғыларды таңдауға да болады.

- Құрылғылар тізімін қосылатын құрылғылар мекенжайлары тізбесін қамтитын TXT пішіміндегі файлдан құрылғылар тізімін импорттау (әр мекенжай бөлек жолда орналасуы тиіс).

  Егер құрылғылар тізімі файлдан импортталса немесе қолмен қалыптастырылса, ал құрылғылар атауы бойынша анықталса, онда тізімге ақпараты Басқару серверінің дерекқорына әлдеқашан қосылған құрылғылар ғана қосылуы мүмкін. Деректер, осы құрылғыларды қосу кезінде немесе құрылғыларды анықтау нәтижесінде дерекқорға енгізілуі тиіс.

- Құрылғы таңдауларын көрсету.

Уақыт өте келе, тапсырманың әрекет ету ауқымы, таңдауға кіретін құрылғылардың жиынтығы қалай өзгеретіндігіне байланысты өзгеріп отырады. Құрылғыны таңдауы құрылғы атрибуттары негізінде, соның ішінде құрылғыда орнатылған бағдарламалық жасақтама негізінде, сондай-ақ құрылғыға белгіленген тегтер негізінде құрылуы мүмкін. Құрылғыны таңдауы тапсырманың әрекет ету ауқымын белгілеудің ең икемді тәсілі болып саналады.

Құрылғы таңдаулары үшін тапсырмаларды кесте бойынша іске қосуды әрқашан Басқару сервері орындайды. Мұндай тапсырмалар Басқару серверімен байланысы жоқ құрылғыларда іске қосылмайды. Әрекет ету ауқымы басқа тәсілмен белгіленетін тапсырмалар құрылғыларда тікелей іске қосылады және құрылғы мен Басқару сервері арасындағы байланыстың болуына тәуелді емес.

Құрылғылар таңдауына арналған тапсырмалар құрылғының жергілікті уақыты бойынша емес, Басқару серверінің жергілікті уақыты бойынша іске қосылады. Әрекет ету ауқымы басқа тәсілмен белгіленетін тапсырмалар құрылғының жергілікті уақыты бойынша іске қосылады.

Саясат пен бағдарламаның жергілікті параметрлерінің өзара байланысы

Сіз саясаттардың көмегімен топтың құрамына кіретін барлық құрылғылар үшін бағдарламаның жұмыс параметрлерінің бірдей мәндерін орната аласыз.

Топтағы жеке құрылғылар үшін саясат белгілеген параметрлердің мәндерін бағдарламаның жергілікті параметрлері арқылы қайта анықтауға болады. Бұл жағдайда, сіз өзгертуге саясат тыйым салмаған параметрлердің мәндерін ғана орната аласыз (параметр құлыпталмаған).

Клиент құрылғысындағы бағдарлама қолданатын параметрдің мәні, саясаттағы параметрде құлыптың (🔒) болуымен анықталады:

- Егер параметрді өзгертуге тыйым салынса, барлық клиент құрылғылары бірдей саясатпен белгіленген мәнді пайдаланады.

- Егер тыйым салынбаған болса, онда әрбір клиент құрылғысында бағдарлама саясатта көрсетілгеннен гөрі жергілікті параметр мәнін пайдаланады. Бұл жағдайда, параметрдің мәні бағдарламаның жергілікті параметрлері арқылы өзгеруі мүмкін.

Осылайша, клиент құрылғысында тапсырманы орындау кезінде бағдарлама екі түрлі жолмен берілген параметрлерді қолданады:

- егер саясатта параметрді өзгертуге тыйым салынбаған болса, тапсырма параметрлері және бағдарламаның жергілікті параметрлері арқылы;

- егер саясатта параметрді өзгертуге тыйым салынған болса, топтың саясаты арқылы.

Бағдарламаның жергілікті параметрлері саясат параметрлеріне сәйкес саясатты бірінші рет қолданғаннан кейін өзгереді.

Тарату нүктесі

Тарату нүктесі (бұған дейін "жаңартулар агенті" деп аталып келген) — жаңартуларды тарату, бағдарламаларды қашықтан орнату, желідегі құрылғылар туралы ақпарат алу үшін қолданылатын Желілік агенті орнатылған құрылғы.

Тарату нүктесі ретінде пайдаланылатын құрылғыда орнатылған желілік агент мүмкіндіктері мен пайдалану жағдайлары операциялық жүйеге байланысты әртүрлі.

Тарату нүктесі келесі функцияларды орындауы мүмкін:

- Басқару серверінен алынған жаңартулар мен орнату пакеттерін топтың клиент құрылғыларына тарату (соның ішінде, UDP протоколы бойынша кеңінен тарататын таратылым арқылы). Жаңартулар Басқару серверінен де, Kaspersky жаңарту серверлерінен де алынуы мүмкін. Соңғы жағдайда, тарату нүктесі үшін жаңарту тапсырмасы жасалуы тиіс.

  Тарату нүктелері жаңартуларды таратуды тездетеді және Басқару серверінің ресурстарын босатуға мүмкіндік береді.

- Саясаттар мен топтық тапсырмаларды UDP протоколы бойынша кеңінен тарататын таратылым арқылы тарату.

- Басқару тобы құрылғылары үшін Басқару серверімен қосылым шлюзі рөлін орындау.

  Топтың басқарылатын құрылғылары мен Басқару сервері арасында тікелей қосылым жасау мүмкін болмаса, онда тарату нүктесін осы топтың Басқару серверімен қосылым шлюзі ретінде тағайындауға болады. Бұл жағдайда, басқарылатын құрылғылар қосылым шлюзіне, ол болса Басқару серверіне қосылады.

  Қосылым шлюзі ретінде жұмыс істейтін тарату нүктесінің болуы басқарылатын құрылғыларды Басқару серверіне тікелей қосуды жоққа шығармайды. Қосылым шлюзі қолжетімді болмаса, ал Басқару серверіне тікелей қосылу мүмкін болса, басқарылатын құрылғылар тікелей Серверге қосылады.

- Жаңа құрылғыларды анықтау және бұрыннан белгілі құрылғылар туралы ақпаратты жаңарту мақсатымен желіні сұрастыру. Тарату нүктесі Басқару серверімен бірдей құрылғыларды табу әдістерін қолдануы мүмкін.

- Kaspersky бағдарламаларын және басқа жеткізушілердің бағдарламалық жасақтамаларын қашықтан орнатуды, соның ішінде Желілік агентсіз клиенттік құрылғыларға орнатуды орындау.

  Бұл функция, Басқару сервері тікелей қатынаса алмайтын желілерде орналасқан клиент құрылғыларына Желілік агенттің орнату пакеттерін қашықтан жіберуге мүмкіндік береді.

- Kaspersky Security Network (KSN) желісінде қатысатын прокси-сервер рөлінде әрекет ету.

  Құрылғы KSN прокси-сервері рөлін орындауы үшін KSN прокси-серверін тарату нүктесі жағында қосуға болады. Бұл жағдайда, құрылғыда KSN прокси-сервері қызметі іске қосылады.

Файлдарды Басқару серверінен тарату нүктесіне жіберу HTTP протоколы арқылы немесе SSL қосылымының қолданылуы конфигурацияланған болса – HTTPS протоколы арқылы жүзеге асырылады. HTTP немесе HTTPS протоколын қолдану, SOAP протоколын қолданумен салыстырғанда трафикті қысқарту арқасында аса жоғары өнімділікті қамтамасыз етеді.

Желілік агенті орнатылған құрылғыларды, тарату нүктелері тарапынан әкімші өз қолымен немесе Басқару сервері автоматты түрде тағайындауы мүмкін. Көрсетілген басқару топтары үшін тарату нүктелерінің толық тізімі, тарату нүктелерінің тізімі бар есепте көрсетіледі.

Тарату нүктесінің әрекет ету аумағы, ол әкімші болып тағайындалған басқару тобы, сондай-ақ оның барлық тіркеме деңгейлеріндегі ішкі топтар болып саналады. Басқару топтарының иерархияларында бірнеше тарату нүктесі тағайындалған болса, басқарылатын құрылғының Желілік агенті иерархия бойынша ең жақын тарату нүктесіне қосылады.

Тарату нүктелерін Басқару сервері автоматты түрде тағайындайтын болса, онда Сервер тарату нүктелерін басқару топтары бойынша емес, кеңінен тарататын домендер бойынша тағайындайды. Бұл, кеңінен тарататын домендер белгілі болғаннан кейін орын алады. Желілік агент өзінің ішкі желісінің басқа да Желілік агенттерімен хабар алмасады және өзі туралы ақпарат пен басқа да Желілік агенттер туралы қысқаша ақпаратты Басқару серверіне жібереді. Осы ақпарат негізінде, Басқару сервері Желілік агенттерді кең тарататын домендер бойынша топтастыра алады. Кең тарататын домендер Басқару серверіне басқару топтарындағы Желілік агенттердің 70%-дан астамы сұрастырылғаннан кейін белгілі болады. Басқару сервері кеңінен тарататын домендерді екі сағат сайын сұрастырып тұрады. Тарату нүктелері кеңінен тарататын домендер бойынша тағайындалғаннан кейін, оларды басқару топтары бойынша қайтадан тағайындауға болмайды.

Әкімші тарату нүктелерін қолмен тағайындаса, оларды басқару топтарына немесе желілік орындарға тағайындауға болады.

Белсенді қосылым профилі бар Желілік агенттер кеңінен тарататын доменді анықтауға қатыспайды.

Kaspersky Security Center Linux әрбір Желілік агентке басқа мекенжайлармен қиылыспайтын көп мекенжайлы IP таратылымының бірегей мекенжайын белгілейді. Соның арқасында, мекенжайлардың қиылысуына байланысты желіге түсетін жүктеменің артуының алдын алуға болады. Бағдарламаның алдыңғы нұсқаларында тағайындалған көп мекенжайлы IP таратудың мекенжайлары өзгертілмейді.

Желінің бір аумағында немесе басқару тобында екі немесе одан да көп тарату нүктесі тағайындалса, олардың бірі белсенді тарату нүктесі болып, қалғандары резервтік болады. Белсенді тарату нүктесі жаңартулар мен орнату пакеттерін тікелей Басқару серверінен жүктеп алады, ал резервтік тарату нүктелері жаңартуларды алу үшін тек белсенді тарату нүктесіне жүгінеді. Бұл жағдайда, файлдар Басқару серверінен тек бір рет жүктеліп, одан кейін тарату нүктелері арасында бөлінеді. Белсенді тарату нүктесі қандай да бір себептермен қолжетімді емес болып қалса, резервтік тарату нүктелерінің бірі белсенді болып тағайындалады. Басқару сервері тарату нүктесін автоматты түрде резервтік деп тағайындайды.

Тарату нүктесі күйі (*Белсенді*/*Резервтік*) klnagchk утилитасы есебінде жалауша түрінде көрсетіледі.

Тарату нүктесінің жұмыс істеуі үшін дискіде кемінде 4 ГБ бос орын керек. Тарату нүктесінің дискісіндегі бос орын көлемі 2 ГБ-тан кем болса, Kaspersky Security Center Linux орталығы *Ескерту* маңыздылық деңгейіне ие қауіпсіздік мәселесін жасайды. Қауіпсіздік мәселесі құрылғы сипаттарында **Қауіпсіздік мәселелері** бөлімінде жарияланады.

Тарату нүктесі бар құрылғыда қашықтан орнату тапсырмалары жұмыс істеген кезде, қосымша бос диск кеңістігі қажет болады. Бос диск кеңістігі, орнатылатын орнату пакеттерінің барлығының өлшемінен үлкен болуы тиіс.

Тарату нүктесі бар құрылғыда жаңартуларды (патчтарды) орнату және осалдықты түзету тапсырмасы жұмыс істеген кезде, қосымша бос диск кеңістігі қажет болады. Бос дискі кеңістігі, орнатылатын патчтардың барлығының өлшемінен кемінде екі есе үлкен болуы тиіс.

Тарату нүктелері рөлін атқаратын құрылғылар рұқсатсыз қол жеткізудің кез келген түрінен, соның ішінде физикалық тұрғыдан қорғалуы тиіс.

Қосылым шлюзі

Қосылым шлюзі – ерекше режимде жұмыс істейтін Желілік агент. Қосылым шлюзі басқа Желілік агенттерінен қосылымдарды қабылдайды және оларды Сервермен орнатылған өзінің қосылымы арқылы Басқару серверіне туннельдейді. Әдеттегі Желілік агенттен айырмашылығы, қосылым шлюзі Басқару серверімен байланыс орнатпайды, тек Басқару серверінен қосылымдарды күтеді.

Қосылым шлюзі 10 000 құрылғыдан қосылымдарды қабылдай алады.

Қосылым шлюздерін пайдаланудың екі нұсқасы бар:

- Демилитаризацияланған аймаққа (DMZ) қосылым шлюзін орнату ұсынылады. Автономды құрылғыларда орнатылған басқа Желілік агенттер үшін қосылым шлюзі арқылы Басқару серверіне қосылуды арнайы конфигурациялау қажет.

  Қосылу шлюзі Желілік агенттерден Басқару серверіне берілетін деректерді өзгертпейді немесе өңдемейді. Қосылым шлюзі бұл деректерді буферге жазбайды, сондықтан Желілік агенттен деректерді қабылдай алмайды, содан кейін оларды Басқару серверіне жібере алмайды. Желілік агент Басқару серверіне қосылым шлюзі арқылы қосылуға тырысса, бірақ қосылым шлюзі Басқару серверіне қосыла алмаса, Желілік агент мұны қолжетімді емес Басқару сервері ретінде қабылдайды. Барлық деректер Желілік агентте қала береді (қосылым шлюзінде емес).

  Қосылым шлюзі басқа қосылым шлюзі арқылы Басқару серверіне қосыла алмайды. Бұл дегеніміз, Желілік агент бір уақытта қосылым шлюзі бола алмайды және Басқару серверіне қосылу үшін қосылым шлюзін қолдана алмайды.

  Барлық қосылым шлюздері Басқару сервері сипаттарындағы тарату нүктелерінің тізіміне енгізілген.

- Сондай-ақ, желідегі қосылым шлюздерін пайдалануға болады. Мысалы, автоматты түрде тағайындалатын тарату нүктелері өзінің әрекет ету ауқымында дәл солай қосылым шлюздеріне айналады. Алайда, ішкі желіде қосылым шлюздері айтарлықтай артықшылықтар бермейді. Олар Басқару сервері қабылдаған желілік қосылымдардың санын азайтады, бірақ кіріс деректерінің көлемін азайтпайды. Қосылым шлюздері болмаса да, барлық құрылғылар Басқару серверіне қосыла алады.

Виртуалды Басқару серверлері

Физикалық Басқару серверінің шеңберінде бірнеше виртуалды Басқару серверлерін құруға болады, олардың көпшілігі қосалқы Серверлерге ұқсас. Қатынасуды бақылау тізіміне (ACL) негізделген қатынасуды бөлу моделімен салыстырғанда, виртуалды Серверлер моделі анағұрлым функционалды болып келеді және оқшаулаудың үлкен дәрежесін ұсынады. Саясат пен тапсырма құрылғыларына тағайындауға арналған басқару топтарының құрылымынан басқа, әрбір виртуалды Басқару серверінің өзіндік тағайындалмаған құрылғылар тобы, өзіндік есептер жиынтығы, құрылғыларды таңдау және оқиғалар, орнату пакеттері, жылжыту ережелері және т.б. бар. Виртуалды Басқару серверлерінің функционалдығы, әртүрлі клиенттерді бір-бірінен барынша оқшаулау үшін провайдерлер (xSP) тарапынан, сондай-ақ күрделі құрылымы және көптеген әкімшілері бар ірі ұйымдар тарапынан қолданылуы мүмкін.

Виртуалды Серверлер көбінесе қосалқы Басқару серверлеріне ұқсас болып келеді, алайда олардың келесі айырмашылықтары бар:

- виртуалды Серверде көптеген жаһандық параметрлер мен өзіндік TCP порттары жоқ;
- виртуалды Серверде қосалқы Серверлер болуы мүмкін емес;
- виртуалды Серверде өзінің виртуалды Серверлері болуы мүмкін емес;

- физикалық Басқару серверінде, оның барлық виртуалды Серверлерінің басқарылатын құрылғыларынан (карантин элементтері, бағдарламалар тізімдемесі және т.б.) құрылғылар, топтар, оқиғалар мен нысандар көрінеді;

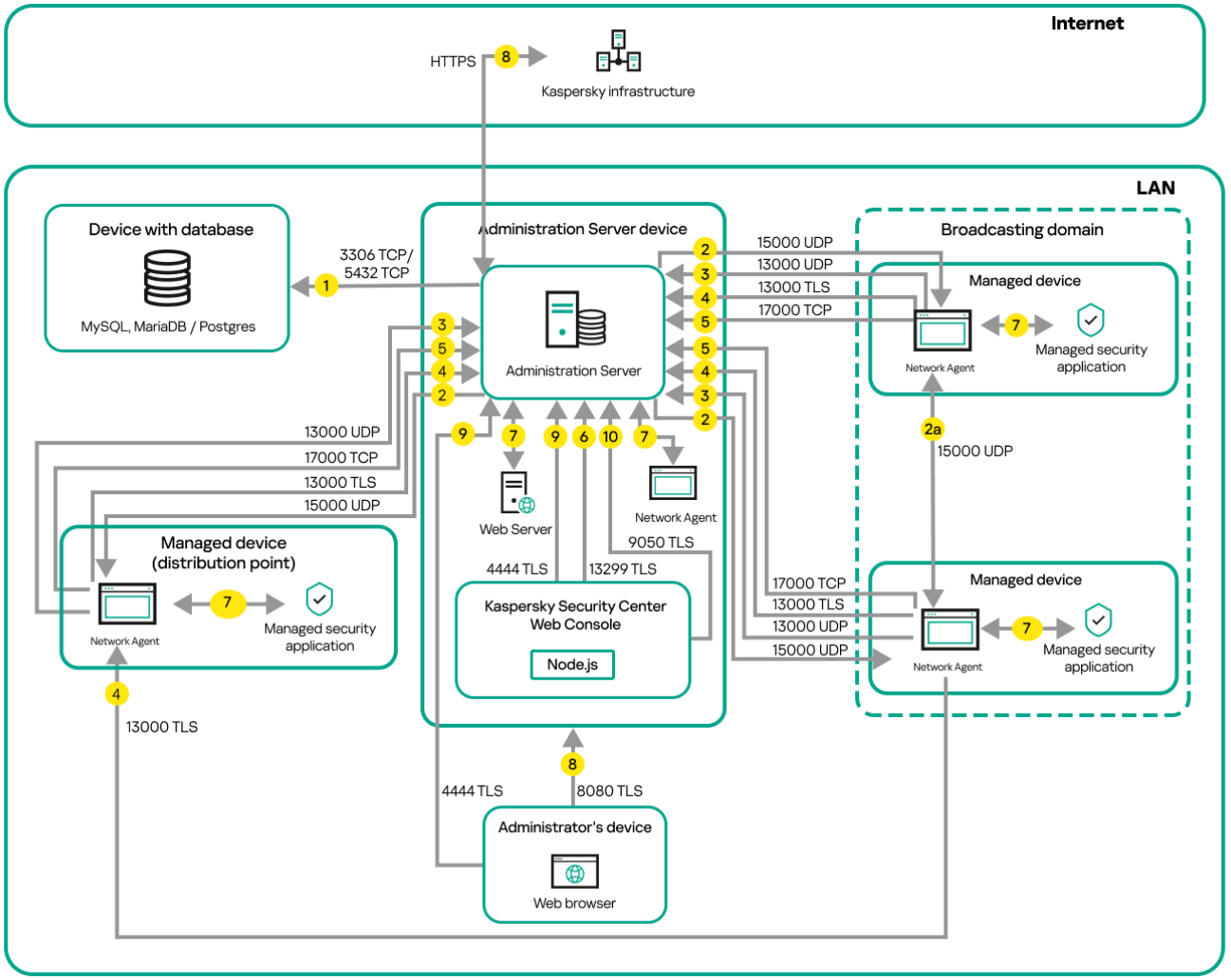
- виртуалды Сервер желіні тек оған қосылған тарату нүктелері арқылы сканерлей алады.

Деректер трафигі және порттарды пайдалану схемалары

Бұл бөлімде Kaspersky Security Center Linux құрамдастары, басқарылатын қауіпсіздік қолданбалары және әртүрлі конфигурацияларға арналған сыртқы серверлер арасындағы деректер трафигінің схемалары берілген. Схемаларда жергілікті құрылғыларда қолжетімді болуы тиісті порт нөмірлері бар.

Жергілікті желідегі (LAN) Басқару сервері және басқарылатын құрылғылар

Төмендегі суретте, Kaspersky Security Center бағдарламасы тек жергілікті желіде (LAN) орналастырылған болса, деректер трафигі көрсетілген.



Жергілікті желідегі (LAN) Басқару сервері және басқарылатын құрылғылар

Суретте әртүрлі басқарылатын құрылғылардың Басқару серверіне әртүрлі тәсілдермен қалай қосылатыны көрсетілген: тікелей немесе тарату нүктесі арқылы. Тарату нүктелері, жаңартуларды тарату кезінде және желідегі трафикті оңтайландыру кезінде Басқару серверіне түсетін жүктемені азайтады. Алайда, тарату нүктелері, басқарылатын құрылғылардың саны айтарлықтай көп болған кезде ғана керек. Басқарылатын құрылғылардың саны аз болса, барлық басқарылатын құрылғылар жаңартуларды тікелей Басқару серверінен ала алады.

Нұсқалар трафиктің бағытын көрсетеді: әрбір нұсқар қоңырауға "жауап беретін" құрылғыға қосылымды бастайтын құрылғыдан өткізілген. Деректерді беру үшін қолданылатын протоколдың атауы мен порт нөмірі көрсетілген. Әрбір нұсқар нөмірленген және тиісті деректер трафигі туралы келесі ақпаратты қамтиды:

1. Басқару сервері деректерді дерекқорға жібереді. Егер сіз Басқару сервері мен дерекқорды әртүрлі құрылғыларға орнатқан болсаңыз, онда сіз дерекқор орналасқан құрылғыдағы қажетті порттарды (мысалы, MySQL Server және MariaDB Server үшін 3306-порт немесе PostgreSQL Server немесе Postgres Pro Server үшін 5432-порт) қолжетімді етуіңіз қажет. Толығырақ ақпарат ДҚБЖ құжаттамасында көрсетілген.

2. Басқару серверімен байланысуға арналған сұраулар 15000 UDP порты арқылы барлық ұялы емес басқарылатын құрылғыларға жіберіледі.

   Желілік агенттер сұрауларды бір-біріне бір кеңінен таратылатын домен шегінде жібереді. Содан соң, деректер Басқару серверіне жіберіледі және кеңінен таратылатын доменнің шектерін анықтау үшін және тарату нүктелерін автоматты түрде тағайындау үшін қолданылады (бұл параметр қосулы болса).

   Басқару серверінің басқарылатын құрылғыларға тікелей қатынасы болмаса, Басқару серверінен осы құрылғыларға байланыс сұраулары тікелей жіберілмейді.

   2a. Мобильді емес басқарылатын құрылғылардағы желі агенттері бір кеңінен тарату доменіндегі басқа желі агенттері туралы деректермен алмасады (содан кейін деректер Басқару серверге жіберіледі).

3. Басқарылатын құрылғыларды өшіру туралы ақпарат Желілік агенттен Басқару серверіне 13000 UDP порты арқылы беріледі.

4. Басқару сервері қосылымдарды Желілік агенттерден және қосалқы Басқару серверлерінен 13000 TLS порты арқылы қабылдайды.

   Егер сіз Kaspersky Security Center бағдарламасының алдыңғы нұсқаларының бірін қолдансаңыз, онда сіздің желіңізде Басқару сервері 14000 TLS порты арқылы Желілік агенттерден қосылымдарды қабылдай алады. Kaspersky Security Center нұсқасы да 14000-порт бойынша Желілік агенттерді қосуды қолдайды, бірақ 13000 TLS портын пайдалану ұсынылады.

5. Басқарылатын құрылғылар (ұялы құрылғылардан басқа) 17000 TCP порты арқылы белсендіруді сұрайды. Құрылғының интернетке өзіндік қатынасы болса, мұның қажеті жоқ; бұл жағдайда, құрылғы деректерді Kaspersky серверлеріне тікелей интернет арқылы жібереді.

6. Kaspersky Security Center Web Console сервері деректерді бірдей құрылғыда немесе басқасында орнатылуы мүмкін Басқару серверіне 13299 TLS-порты арқылы жібереді.

   Есептік деректер және қатынасу диспетчері (IAM) құрамдасы басқару серверіне TLS 13299 порты арқылы қосылады.

7. Бір құрылғыдағы бағдарламалар жергілікті трафикпен алмасады (не Басқару серверінде, не басқарылатын құрылғыда). Сыртқы порттарды ашу қажет емес.

8. Басқару серверінен Kaspersky серверлеріне жіберілетін деректер (мысалы, KSN деректері, лицензиялар туралы ақпарат) және Kaspersky серверлерінен Басқару серверіне жіберілетін деректер (мысалы, бағдарламаларды жаңарту және антивирустық дерекқорларды жаңарту) HTTPS протоколы бойынша жіберіледі.

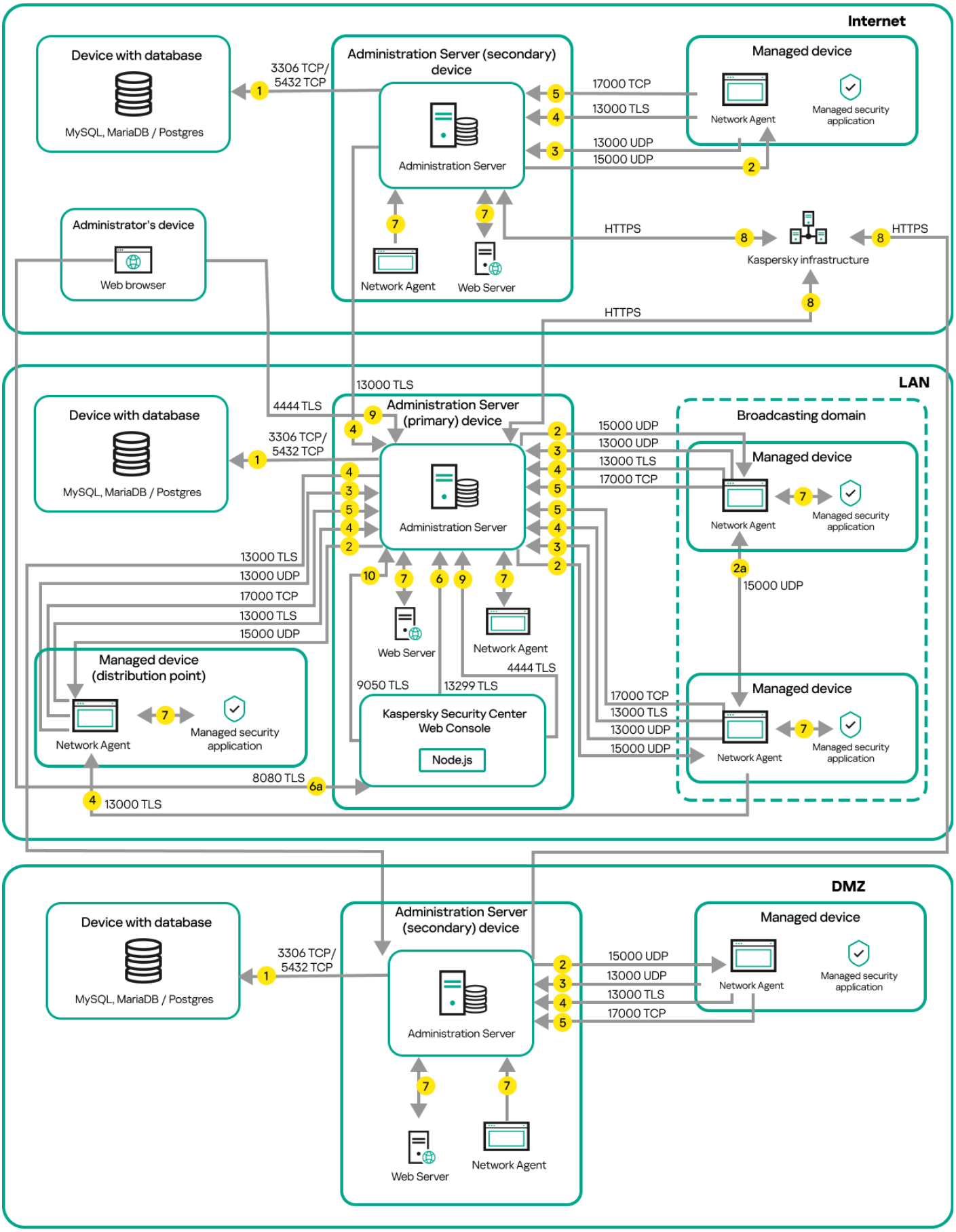
   Басқару серверіңізде интернетке қатысыңыздың болуын қаламасаңыз, осы деректерді қолмен басқаруыңыз керек.

9. Kaspersky Security Center Web Console Server мен браузер (Kaspersky Security Center Web Console-мен бірге қолданылады) басқару серверіне TLS 4444 порты арқылы OpenID Connect аутентификация протоколы көмегімен қосылады.

10. Kaspersky Security Center Web Console Server басқару серверіне TLS 9050 порты арқылы қосылады.

Жергілікті желідегі (LAN) негізгі Басқару сервері және екі қосалқы Басқару сервері

Суретте Басқару серверлерінің иерархиясы көрсетілген: негізгі Басқару сервері жергілікті желіде (LAN) орналасқан. Қосалқы Басқару сервері демилитаризацияланған аймақта (DMZ) орналасқан; басқа қосалқы Басқару сервері интернетте орналасқан.



Басқару серверлерінің иерархиясы: негізгі Басқару сервері және екі қосалқы Басқару сервері

Нұсқарлар трафиктің бағытын көрсетеді: әрбір нұсқар қоңырауға "жауап беретін" құрылғыға қосылымды бастайтын құрылғыдан өткізілген. Деректерді беру үшін қолданылатын протоколдың атауы мен порт нөмірі көрсетілген. Әрбір нұсқар нөмірленген және тиісті деректер трафигі туралы келесі ақпаратты қамтиды:

1. Басқару сервері деректерді дерекқорға жібереді. Егер сіз Басқару сервері мен дерекқорды әртүрлі құрылғыларға орнатқан болсаңыз, онда сіз дерекқор орналасқан құрылғыдағы қажетті порттарды (мысалы, MySQL Server және MariaDB Server үшін 3306-порт немесе PostgreSQL Server немесе Postgres Pro Server үшін 5432-порт) қолжетімді етуіңіз қажет. Толығырақ ақпарат ДҚБЖ құжаттамасында көрсетілген.

2. Басқару серверімен байланысуға арналған сұраулар 15000 UDP порты арқылы барлық ұялы емес басқарылатын құрылғыларға жіберіледі.

   Желілік агенттер сұрауларды бір-біріне бір кеңінен тарататын домен шегінде жібереді. Содан соң, деректер Басқару серверіне жіберіледі және кеңінен тарататын доменнің шектерін анықтау үшін және тарату нүктелерін автоматты түрде тағайындау үшін қолданылады (бұл параметр қосулы болса).

   Басқару серверінің басқарылатын құрылғыларға тікелей қатынасы болмаса, Басқару серверінен осы құрылғыларға байланыс сұраулары тікелей жіберілмейді.

3. Басқарылатын құрылғыларды өшіру туралы ақпарат Желілік агенттен Басқару серверіне 13000 UDP порты арқылы беріледі.

4. Басқару сервері қосылымдарды Желілік агенттерден және қосалқы Басқару серверлерінен 13000 TLS порты арқылы қабылдайды.

   Егер сіз Kaspersky Security Center бағдарламасының алдыңғы нұсқаларының бірін қолдансаңыз, онда сіздің желіңізде Басқару сервері 14000 TLS порты арқылы Желілік агенттерден қосылымдарды қабылдай алады. Kaspersky Security Center Linux нұсқасы да 14000-порт бойынша Желілік агенттерді қосуды қолдайды, бірақ 13000 TLS портын пайдалану ұсынылады.

5. Басқарылатын құрылғылар (ұялы құрылғылардан басқа) 17000 TCP порты арқылы белсендіруді сұрайды. Құрылғының интернетке өзіндік қатынасы болса, мұның қажеті жоқ; бұл жағдайда, құрылғы деректерді Kaspersky серверлеріне тікелей интернет арқылы жібереді.

6. Kaspersky Security Center Web Console сервері деректерді бірдей құрылғыда немесе басқасында орнатылуы мүмкін Басқару серверіне 13299 TLS-порты арқылы жібереді.

   Есептік деректер және қатынасу диспетчері (IAM) құрамдасы басқару серверіне TLS 13299 порты арқылы қосылады.

   6а. Жеке әкімші құрылғысында орнатылған браузерден алынған деректер TLS 8080 порты арқылы Kaspersky Security Center Web Console Server серверіне жіберіледі. Kaspersky Security Center Web Console Server серверін Басқару сервері орнатылған құрылғыға немесе басқа құрылғыға орнатуға болады.

7. Бір құрылғыдағы бағдарламалар жергілікті трафикпен алмасады (не Басқару серверінде, не басқарылатын құрылғыда). Сыртқы порттарды ашу қажет емес.

8. Басқару серверінен Kaspersky серверлеріне жіберілетін деректер (мысалы, KSN деректері, лицензиялар туралы ақпарат) және Kaspersky серверлерінен Басқару серверіне жіберілетін деректер (мысалы, бағдарламаларды жаңарту және антивирустық дерекқорларды жаңарту) HTTPS протоколы бойынша жіберіледі.

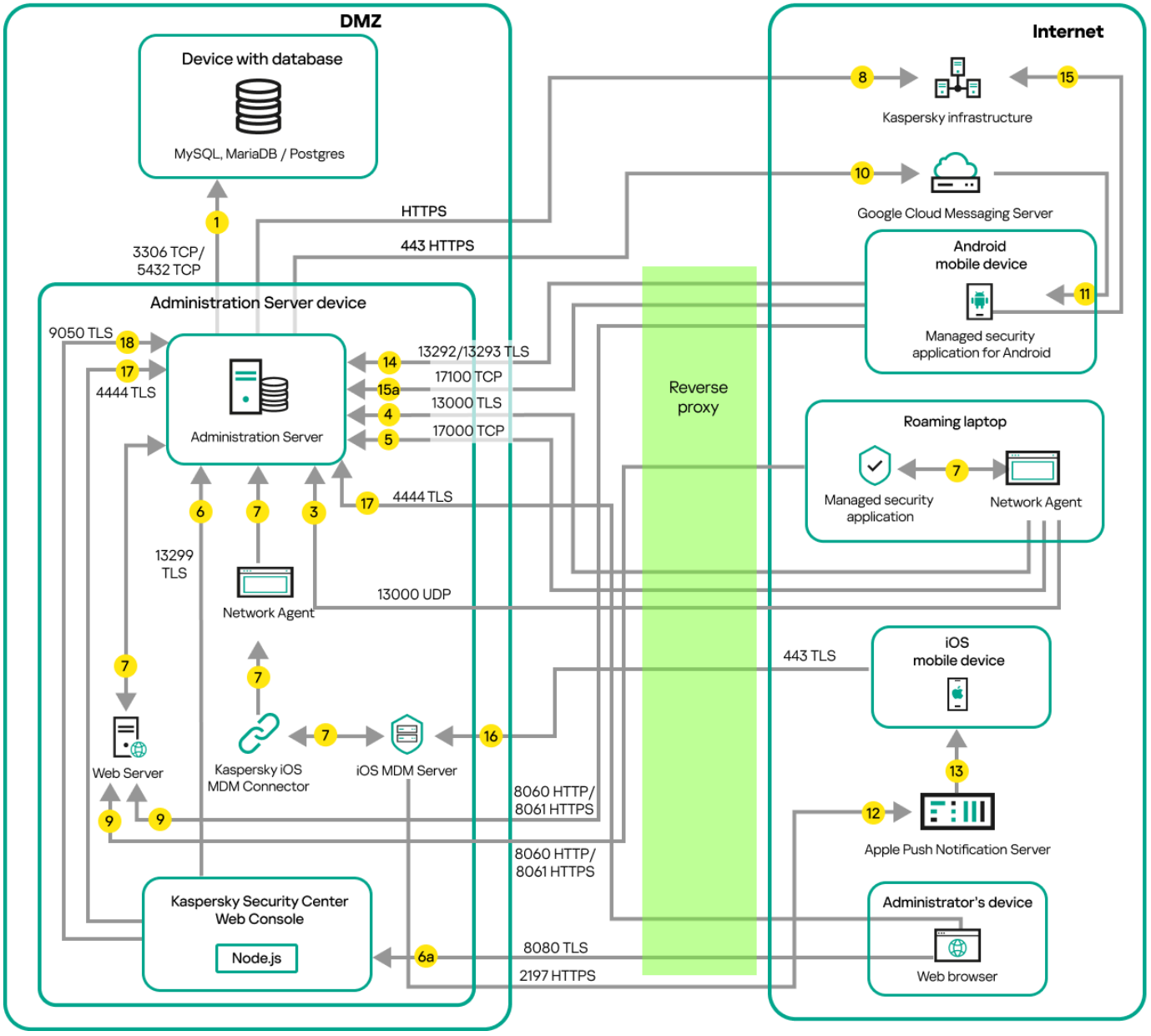
   Басқару серверіңізде интернетке қатысыңыздың болуын қаламасаңыз, осы деректерді қолмен басқаруыңыз керек.

9. Kaspersky Security Center Web Console Server мен браузер (Kaspersky Security Center Web Console-мен бірге қолданылады) басқару серверіне TLS 4444 порты арқылы OpenID Connect аутентификация протоколы көмегімен қосылады.

10. Kaspersky Security Center Web Console Server басқару серверіне TLS 9050 порты арқылы қосылады.

Жергілікті желі (LAN) ішіндегі басқару сервері, интернеттегі басқарылатын құрылғылар; кері прокси-серверді пайдалану

Төмендегі суретте, Басқару сервері жергілікті желі (LAN) ішінде, ал басқарылатын құрылғылар интернетте болатын деректер трафигі көрсетілген. Төмендегі сурет сіз таңдаған кері прокси-серверді пайдаланады. Қосымша ақпарат алу үшін осы бағдарламаның құжаттамасын қараңыз.



Жергілікті желідегі басқару сервері; басқарылатын құрылғылар басқару серверіне кері прокси-сервер арқылы қосылады

Бұл орналастыру схемасы, ұялы құрылғылар тікелей Басқару серверіне қосылғанын қаламасаңыз және қосылым шлюзін демилитаризацияланған аймақта (DMZ) тағайындауды қаламасаңыз, ұсынылады.

Нұсқалар трафиктің бағытын көрсетеді: әрбір нұсқар қоңырауға "жауап беретін" құрылғыға қосылымды бастайтын құрылғыдан өткізілген. Деректерді беру үшін қолданылатын протоколдың атауы мен порт нөмірі көрсетілген. Әрбір нұсқар нөмірленген және тиісті деректер трафигі туралы келесі ақпаратты қамтиды:

1. Басқару сервері деректерді дерекқорға жібереді. Егер сіз Басқару сервері мен дерекқорды әртүрлі құрылғыларға орнатқан болсаңыз, онда сіз дерекқор орналасқан құрылғыдағы қажетті порттарды (мысалы, MySQL Server және MariaDB Server үшін 3306-порт немесе PostgreSQL Server немесе Postgres Pro Server үшін 5432-порт) қолжетімді етуіңіз қажет. Толығырақ ақпарат ДҚБЖ құжаттамасында көрсетілген.

2. Басқару серверімен байланысуға арналған сұраулар 15000 UDP порты арқылы барлық ұялы емес басқарылатын құрылғыларға жіберіледі.

   Желілік агенттер сұрауларды бір-біріне бір кеңінен тарататын домен шегінде жібереді. Содан соң, деректер Басқару серверіне жіберіледі және кеңінен тарататын доменнің шектерін анықтау үшін және тарату нүктелерін автоматты түрде тағайындау үшін қолданылады (бұл параметр қосулы болса).

   Басқару серверінің басқарылатын құрылғыларға тікелей қатынасы болмаса, Басқару серверінен осы құрылғыларға байланыс сұраулары тікелей жіберілмейді.

3. Басқарылатын құрылғыларды өшіру туралы ақпарат Желілік агенттен Басқару серверіне 13000 UDP порты арқылы беріледі.

4. Басқару сервері қосылымдарды Желілік агенттерден және қосалқы Басқару серверлерінен 13000 TLS порты арқылы қабылдайды.

   Егер сіз Kaspersky Security Center бағдарламасының алдыңғы нұсқаларының бірін қолдансаңыз, онда сіздің желіңізде Басқару сервері 14000 TLS порты арқылы Желілік агенттерден қосылымдарды қабылдай алады. Kaspersky Security Center Linux нұсқасы да 14000-порт бойынша Желілік агенттерді қосуды қолдайды, бірақ 13000 TLS портын пайдалану ұсынылады.

5. Басқарылатын құрылғылар (ұялы құрылғылардан басқа) 17000 TCP порты арқылы белсендіруді сұрайды. Құрылғының интернетке өзіндік қатынасы болса, мұның қажеті жоқ; бұл жағдайда, құрылғы деректерді Kaspersky серверлеріне тікелей интернет арқылы жібереді.

6. Kaspersky Security Center Web Console сервері деректерді бірдей құрылғыда немесе басқасында орнатылуы мүмкін Басқару серверіне 13299 TLS-порты арқылы жібереді.

   Есептік деректер және қатынасу диспетчері (IAM) құрамдасы басқару серверіне TLS 13299 порты арқылы қосылады.

   6а. Жеке әкімші құрылғысында орнатылған браузерден алынған деректер TLS 8080 порты арқылы Kaspersky Security Center Web Console Server серверіне жіберіледі. Kaspersky Security Center Web Console Server серверін Басқару сервері орнатылған құрылғыға немесе басқа құрылғыға орнатуға болады.

7. Бір құрылғыдағы бағдарламалар жергілікті трафикпен алмасады (не Басқару серверінде, не басқарылатын құрылғыда). Сыртқы порттарды ашу қажет емес.

8. Басқару серверінен Kaspersky серверлеріне жіберілетін деректер (мысалы, KSN деректері, лицензиялар туралы ақпарат) және Kaspersky серверлерінен Басқару серверіне жіберілетін деректер (мысалы, бағдарламаларды жаңарту және антивирустық дерекқорларды жаңарту) HTTPS протоколы бойынша жіберіледі.

   Басқару серверіңізде интернетке қатысыңыздың болуын қаламасаңыз, осы деректерді қолмен басқаруыңыз керек.

9. Басқарылатын құрылғылардан, соның ішінде ұялы құрылғылардан пакеттерге арналған сұраулар Басқару сервері орнатылған құрылғыда орналасқан Веб-серверге жіберіледі.

10. Тек Android ұялы құрылғылары үшін: Басқару серверінен алынған деректер Google қызметтеріне беріледі. Бұл қосылым Android ұялы құрылғыларына, Басқару серверіне қосылуы қажет екендігі туралы хабарлау үшін қолданылады. Содан соң, push хабарландырулары ұялы құрылғыларға жіберіледі.

11. Тек Android ұялы құрылғылары үшін: Google серверлерінен келетін push хабарландырулары ұялы құрылғыға жіберіледі. Бұл қосылым ұялы құрылғыларға, Басқару серверіне қосылуы қажет екендігі туралы хабарлау үшін қолданылады.

12. Тек iOS мобильдік құрылғылары үшін: iOS MDM серверінен алынған деректер Apple Push Notification серверлеріне жіберіледі. Содан соң, push хабарландырулары ұялы құрылғыларға жіберіледі.

13. Тек iOS ұялы құрылғылары үшін: Apple серверлерінен келетін push хабарландырулары ұялы құрылғыға жіберіледі. Бұл қосылым мобильдік құрылғыларға iOS MDM серверіне қосылуы қажет екені туралы хабарлау үшін қолданылады.

14. Тек мобильдік құрылғылар үшін: басқарылатын қолданба деректерді басқару серверіне 13292/13293 TLS порты арқылы тікелей немесе кері прокси-сервер көмегімен жібереді.

15. Тек ұялы құрылғылар үшін: ұялы құрылғыдан алынған деректер Kaspersky инфрақұрылымына беріледі.

    Мобильдік құрылғыда интернетке кіру рұқсаты болмаса, деректер басқару серверіне 17100 порты арқылы тасымалданады және басқару сервері оларды Kaspersky инфрақұрылымына жібереді; алайда бұл сценарий өте сирек қолданылады.

16. Тек iOS ұялы құрылғылары үшін: ұялы құрылғылардан алынған деректер 443 TLS порты арқылы Басқару сервері немесе қосылым шлюзі орнатылған құрылғыда орналасқан iOS MDM серверіне жіберіледі.

17. Kaspersky Security Center Web Console Server мен браузер (Kaspersky Security Center Web Console-мен бірге қолданылады) басқару серверіне TLS 4444 порты арқылы OpenID Connect аутентификация протоколы көмегімен қосылады.

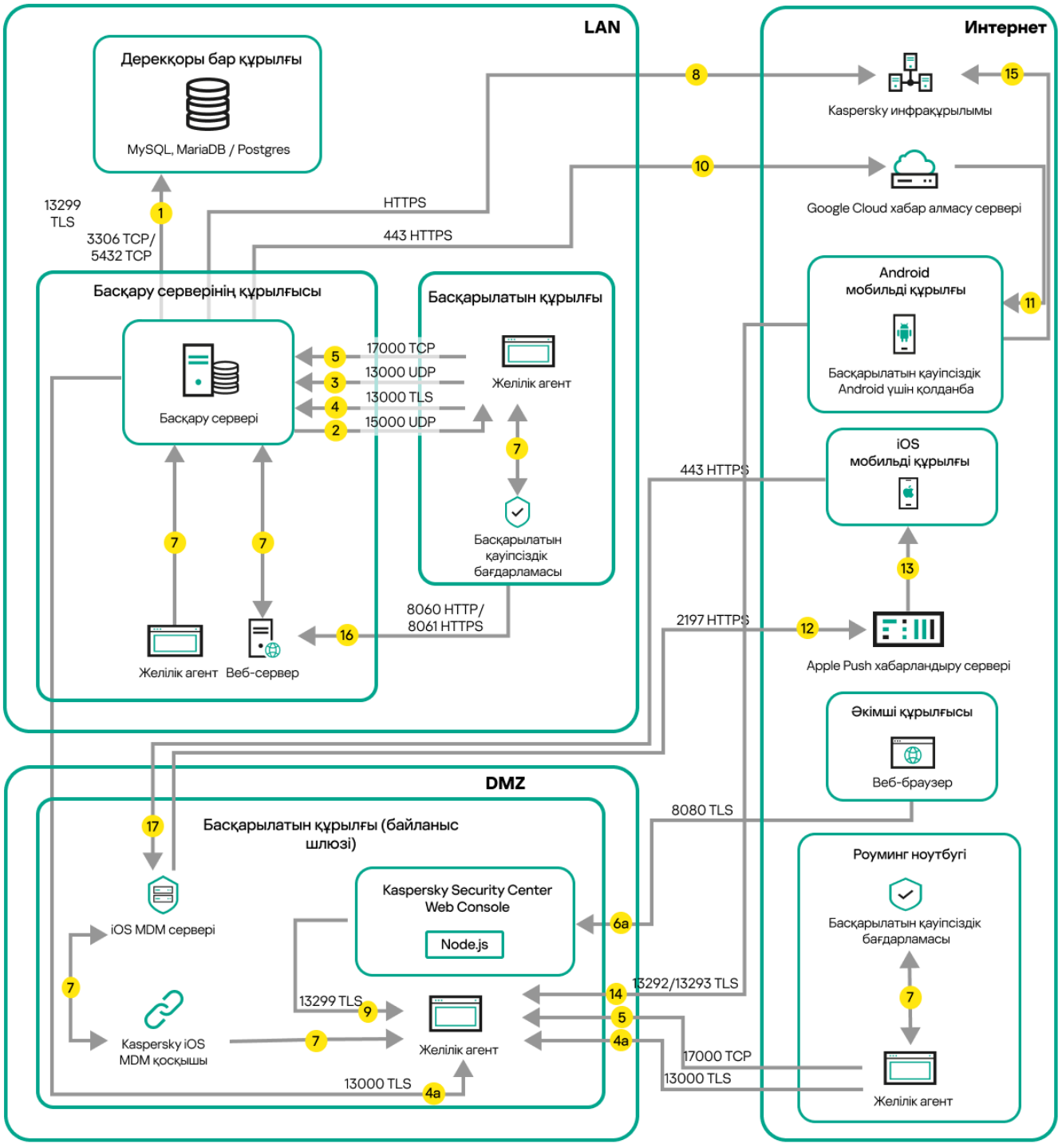
18. Kaspersky Security Center Web Console Server басқару серверіне TLS 9050 порты арқылы қосылады.

Жергілікті желі (LAN) ішіндегі Басқару сервері, интернеттегі басқарылатын құрылғылар; қосылым шлюзін қолдану

Төмендегі суретте, Басқару сервері жергілікті желі (LAN) ішінде, ал басқарылатын құрылғылар интернетте болатын деректер трафигі көрсетілген. Қосылым шлюзі қолданылуда.

Бұл орналастыру схемасы, басқарылатын құрылғылардың тікелей Басқару серверіне қосылғанын қаламасаңыз және кері прокси-сервер немесе корпоративтік брандмауэрді қолданғыңыз келмесе, ұсынылады.

Бұл орналастыру схемасы үшін Identity and Access Manager (IAM) қамтамасыз еткен домен аутентификациясына (бір рет кіру) қолдау көрсетілмейді.



Басқару серверіне қосылым шлюзі арқылы қосылған басқарылатын ұялы құрылғылар

Бұл суретте басқарылатын құрылғылар демилитаризацияланған аймақта (DMZ) орналасқан қосылым шлюзі арқылы Басқару серверіне қосылған. Кері прокси-сервер немесе корпоративтік желілік экран пайдаланылмайды.

Нұсқалар трафиктің бағытын көрсетеді: әрбір нұсқар қоңырауға "жауап беретін" құрылғыға қосылымды бастайтын құрылғыдан өткізілген. Деректерді беру үшін қолданылатын протоколдың атауы мен порт нөмірі көрсетілген. Әрбір нұсқар нөмірленген және тиісті деректер трафигі туралы келесі ақпаратты қамтиды:

1. Басқару сервері деректерді дерекқорға жібереді. Егер сіз Басқару сервері мен дерекқорды әртүрлі құрылғыларға орнатқан болсаңыз, онда сіз дерекқор орналасқан құрылғыдағы қажетті порттарды (мысалы, MySQL Server және MariaDB Server үшін 3306-порт немесе PostgreSQL Server немесе Postgres Pro Server үшін 5432-порт) қолжетімді етуіңіз қажет. Толығырақ ақпарат ДҚБЖ құжаттамасында көрсетілген.

2. Басқару серверімен байланысуға арналған сұраулар 15000 UDP порты арқылы барлық ұялы емес басқарылатын құрылғыларға жіберіледі.

   Желілік агенттер сұрауларды бір-біріне бір кеңінен тарататын домен шегінде жібереді. Содан соң, деректер Басқару серверіне жіберіледі және кеңінен тарататын доменнің шектерін анықтау үшін және тарату нүктелерін автоматты түрде тағайындау үшін қолданылады (бұл параметр қосулы болса).

   Басқару серверінің басқарылатын құрылғыларға тікелей қатынасы болмаса, Басқару серверінен осы құрылғыларға байланыс сұраулары тікелей жіберілмейді.

3. Басқарылатын құрылғыларды өшіру туралы ақпарат Желілік агенттен Басқару серверіне 13000 UDP порты арқылы беріледі.

4. Басқару сервері қосылымдарды Желілік агенттерден және қосалқы Басқару серверлерінен 13000 TLS порты арқылы қабылдайды.

   Егер сіз Kaspersky Security Center бағдарламасының алдыңғы нұсқаларының бірін қолдансаңыз, онда сіздің желіңізде Басқару сервері 14000 TLS порты арқылы Желілік агенттерден қосылымдарды қабылдай алады. Kaspersky Security Center Linux нұсқасы да 14000-порт бойынша Желілік агенттерді қосуды қолдайды, бірақ 13000 TLS портын пайдалану ұсынылады.

   4а. Демилитаризацияланған аймақтағы қосылым шлюзі 13000 TLS порты арқылы Басқару серверінен қосылымды қабылдайды. Демилитаризацияланған аймақтағы қосылым шлюзі Басқару сервері порттарына кіре алмайтындықтан, Басқару сервері қосылым шлюзімен тұрақты сигнал байланысын жасайды және қолдайды. Сигнал қосылымы деректерді беру үшін пайдаланылмайды; ол тек желіге шақыру жіберу үшін қолданылады. Қосылым шлюзі Серверге қосылуы қажет болғанда, ол Серверге осы сигнал қосылымы арқылы хабарлайды, содан кейін Сервер деректерді беру үшін қажетті қосылым жасайды.

   Сыртқы құрылғылар қосылым шлюзіне 13000 TLS порты арқылы да қосылады.

5. Басқарылатын құрылғылар (ұялы құрылғылардан басқа) 17000 TCP порты арқылы белсендіруді сұрайды. Құрылғының интернетке өзіндік қатынасы болса, мұның қажеті жоқ; бұл жағдайда, құрылғы деректерді Kaspersky серверлеріне тікелей интернет арқылы жібереді.

6. Kaspersky Security Center Web Console сервері деректерді бірдей құрылғыда немесе басқасында орнатылуы мүмкін Басқару серверіне 13299 TLS-порты арқылы жібереді.

   6а. Жеке әкімші құрылғысында орнатылған браузерден алынған деректер TLS 8080 порты арқылы Kaspersky Security Center Web Console Server серверіне жіберіледі. Kaspersky Security Center Web Console Server серверін Басқару сервері орнатылған құрылғыға немесе басқа құрылғыға орнатуға болады.

7. Бір құрылғыдағы бағдарламалар жергілікті трафикпен алмасады (не Басқару серверінде, не басқарылатын құрылғыда). Сыртқы порттарды ашу қажет емес.

8. Басқару серверінен Kaspersky серверлеріне жіберілетін деректер (мысалы, KSN деректері, лицензиялар туралы ақпарат) және Kaspersky серверлерінен Басқару серверіне жіберілетін деректер (мысалы, бағдарламаларды жаңарту және антивирустық дерекқорларды жаңарту) HTTPS протоколы бойынша жіберіледі.

   Басқару серверіңізде интернетке қатысыңыздың болуын қаламасаңыз, осы деректерді қолмен басқаруыңыз керек.

9. Басқарылатын құрылғылардан, соның ішінде ұялы құрылғылардан пакеттерге арналған сұраулар Басқару сервері орнатылған құрылғыда орналасқан Веб-серверге жіберіледі.

10. Тек Android ұялы құрылғылары үшін: Басқару серверінен алынған деректер Google қызметтеріне беріледі. Бұл қосылым Android ұялы құрылғыларына, Басқару серверіне қосылуы қажет екендігі туралы хабарлау үшін қолданылады. Содан соң, push хабарландырулары ұялы құрылғыларға жіберіледі.

11. Тек Android ұялы құрылғылары үшін: Google серверлерінен келетін push хабарландырулары ұялы құрылғыға жіберіледі. Бұл қосылым ұялы құрылғыларға, Басқару серверіне қосылуы қажет екендігі туралы хабарлау үшін қолданылады.

12. Тек iOS мобильдік құрылғылары үшін: iOS MDM серверінен алынған деректер Apple Push Notification серверлеріне жіберіледі. Содан соң, push хабарландырулары ұялы құрылғыларға жіберіледі.

13. Тек iOS ұялы құрылғылары үшін: Apple серверлерінен келетін push хабарландырулары ұялы құрылғыға жіберіледі. Бұл қосылым мобильдік құрылғыларға iOS MDM серверіне қосылуы қажет екені туралы хабарлау үшін қолданылады.

14. Тек мобильдік құрылғылар үшін: басқарылатын қолданба деректерді басқару серверіне 13292/13293 TLS порты арқылы тікелей немесе кері прокси-сервер көмегімен жібереді.

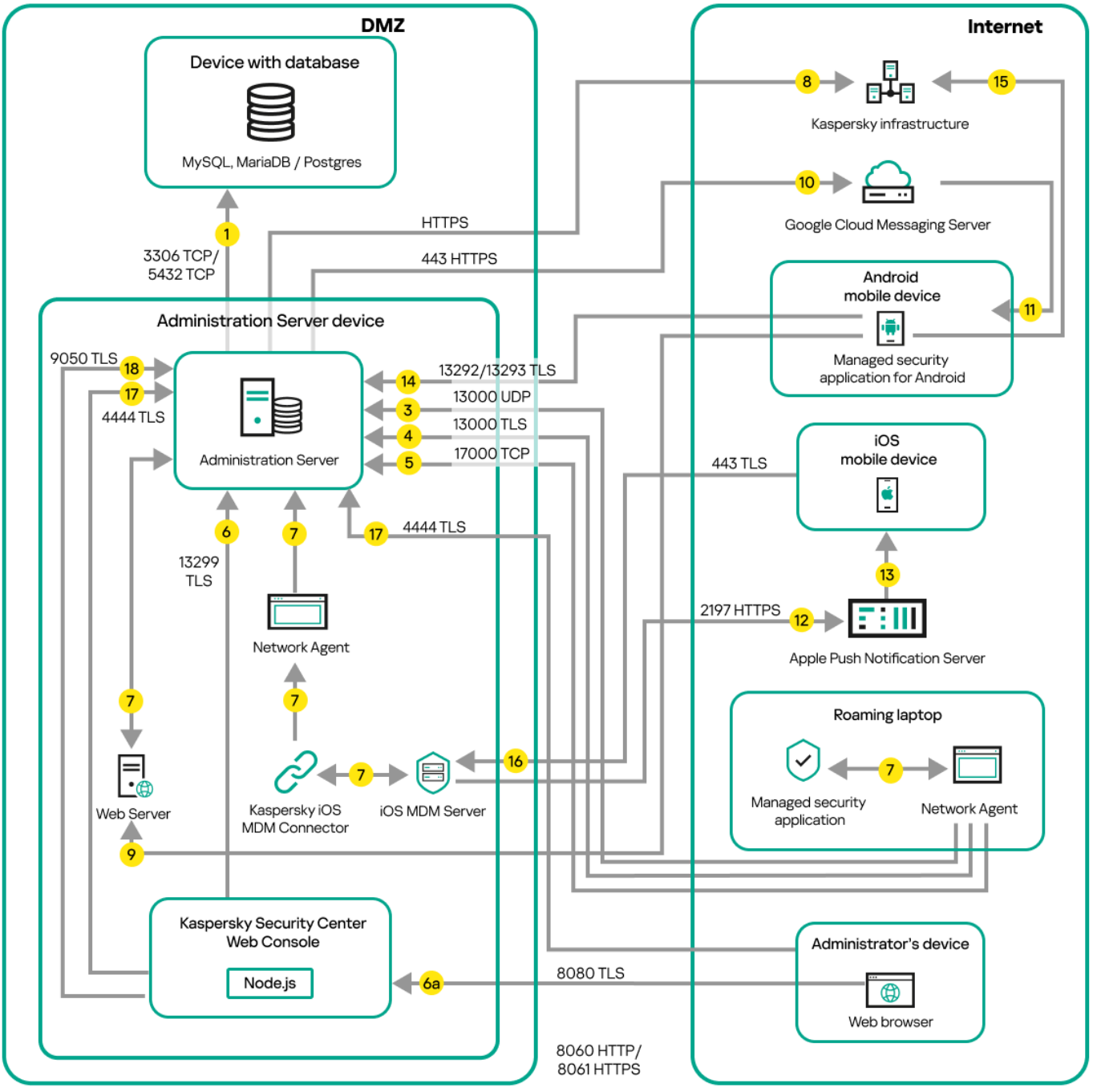
15. Тек ұялы құрылғылар үшін: ұялы құрылғыдан алынған деректер Kaspersky инфрақұрылымына беріледі.

    Мобильдік құрылғыда интернетке кіру рұқсаты болмаса, деректер басқару серверіне 17100 порты арқылы тасымалданады және басқару сервері оларды Kaspersky инфрақұрылымына жібереді; алайда бұл сценарий өте сирек қолданылады.

16. Тек iOS ұялы құрылғылары үшін: ұялы құрылғылардан алынған деректер 443 TLS порты арқылы Басқару сервері немесе қосылым шлюзі орнатылған құрылғыда орналасқан iOS MDM серверіне жіберіледі.

Демилитаризацияланған аймақтың (DMZ) ішіндегі Басқару сервері, интернеттегі басқарылатын құрылғылар

Төмендегі суретте Басқару сервері демилитаризацияланған аймақта, басқарылатын құрылғылар интернетте орналасқан деректер трафигі көрсетілген.



Демилитаризацияланған аймақтағы Басқару сервері, интернеттегі басқарылатын ұялы құрылғылары

Бұл суретте қосылым шлюзі пайдаланылмайды: ұялы құрылғылар Басқару серверіне тікелей қосылады.

Нұсқалар трафиктің бағытын көрсетеді: әрбір нұсқар қоңырауға "жауап беретін" құрылғыға қосылымды бастайтын құрылғыдан өткізілген. Деректерді беру үшін қолданылатын протоколдың атауы мен порт нөмірі көрсетілген. Әрбір нұсқар нөмірленген және тиісті деректер трафигі туралы келесі ақпаратты қамтиды:

1. Басқару сервері деректерді дерекқорға жібереді. Егер сіз Басқару сервері мен дерекқорды әртүрлі құрылғыларға орнатқан болсаңыз, онда сіз дерекқор орналасқан құрылғыдағы қажетті порттарды (мысалы, MySQL Server және MariaDB Server үшін 3306-порт немесе PostgreSQL Server немесе Postgres Pro Server үшін 5432-порт) қолжетімді етуіңіз қажет. Толығырақ ақпарат ДҚБЖ құжаттамасында көрсетілген.

2. Басқару серверімен байланысуға арналған сұраулар 15000 UDP порты арқылы барлық ұялы емес басқарылатын құрылғыларға жіберіледі.

   Желілік агенттер сұрауларды бір-біріне бір кеңінен тарататын домен шегінде жібереді. Содан соң, деректер Басқару серверіне жіберіледі және кеңінен тарататын доменнің шектерін анықтау үшін және тарату нүктелерін автоматты түрде тағайындау үшін қолданылады (бұл параметр қосулы болса).

   Басқару серверінің басқарылатын құрылғыларға тікелей қатынасы болмаса, Басқару серверінен осы құрылғыларға байланыс сұраулары тікелей жіберілмейді.

3. Басқарылатын құрылғыларды өшіру туралы ақпарат Желілік агенттен Басқару серверіне 13000 UDP порты арқылы беріледі.

4. Басқару сервері қосылымдарды Желілік агенттерден және қосалқы Басқару серверлерінен 13000 TLS порты арқылы қабылдайды.

   Егер сіз Kaspersky Security Center бағдарламасының алдыңғы нұсқаларының бірін қолдансаңыз, онда сіздің желіңізде Басқару сервері 14000 TLS порты арқылы Желілік агенттерден қосылымдарды қабылдай алады. Kaspersky Security Center Linux нұсқасы да 14000-порт бойынша Желілік агенттерді қосуды қолдайды, бірақ 13000 TLS портын пайдалану ұсынылады.

5. Басқарылатын құрылғылар (ұялы құрылғылардан басқа) 17000 TCP порты арқылы белсендіруді сұрайды. Құрылғының интернетке өзіндік қатынасы болса, мұның қажеті жоқ; бұл жағдайда, құрылғы деректерді Kaspersky серверлеріне тікелей интернет арқылы жібереді.

6. Kaspersky Security Center Web Console сервері деректерді бірдей құрылғыда немесе басқасында орнатылуы мүмкін Басқару серверіне 13299 TLS-порты арқылы жібереді.

   Есептік деректер және қатынасу диспетчері (IAM) құрамдасы басқару серверіне TLS 13299 порты арқылы қосылады.

   6а. Жеке әкімші құрылғысында орнатылған браузерден алынған деректер TLS 8080 порты арқылы Kaspersky Security Center Web Console Server серверіне жіберіледі. Kaspersky Security Center Web Console Server серверін Басқару сервері орнатылған құрылғыға немесе басқа құрылғыға орнатуға болады.

7. Бір құрылғыдағы бағдарламалар жергілікті трафикпен алмасады (не Басқару серверінде, не басқарылатын құрылғыда). Сыртқы порттарды ашу қажет емес.

8. Басқару серверінен Kaspersky серверлеріне жіберілетін деректер (мысалы, KSN деректері, лицензиялар туралы ақпарат) және Kaspersky серверлерінен Басқару серверіне жіберілетін деректер (мысалы, бағдарламаларды жаңарту және антивирустық дерекқорларды жаңарту) HTTPS протоколы бойынша жіберіледі.

   Басқару серверіңізде интернетке қатысыңыздың болуын қаламасаңыз, осы деректерді қолмен басқаруыңыз керек.

9. Басқарылатын құрылғылардан пакеттерге арналған сұраулар Басқару сервері орнатылған құрылғыда орналасқан Веб-серверге жіберіледі.

10. Тек Android ұялы құрылғылары үшін: Басқару серверінен алынған деректер Google қызметтеріне беріледі. Бұл қосылым Android ұялы құрылғыларына, Басқару серверіне қосылуы қажет екендігі туралы хабарлау үшін қолданылады. Содан соң, push хабарландырулары ұялы құрылғыларға жіберіледі. FCM қызметі 443 HTTPS портында да жұмыс істейді.

11. Тек Android ұялы құрылғылары үшін: Google серверлерінен келетін push хабарландырулары ұялы құрылғыға жіберіледі. Бұл қосылым ұялы құрылғыларға, Басқару серверіне қосылуы қажет екендігі туралы хабарлау үшін қолданылады.

12. Тек iOS мобильдік құрылғылары үшін: iOS MDM серверінен алынған деректер Apple Push Notification серверлеріне жіберіледі. Содан соң, push хабарландырулары ұялы құрылғыларға жіберіледі.

13. Тек iOS ұялы құрылғылары үшін: Apple серверлерінен келетін push хабарландырулары ұялы құрылғыға жіберіледі. Бұл қосылым мобильдік құрылғыларға iOS MDM серверіне қосылуы қажет екені туралы хабарлау үшін қолданылады.

14. Тек мобильдік құрылғылар үшін: басқарылатын қолданба деректерді басқару серверіне 13292/13293 TLS порты арқылы тікелей немесе кері прокси-сервер көмегімен жібереді.

15. Тек ұялы құрылғылар үшін: ұялы құрылғыдан алынған деректер Kaspersky инфрақұрылымына беріледі.

    Мобильдік құрылғыда интернетке кіру рұқсаты болмаса, деректер басқару серверіне 17100 порты арқылы тасымалданады және басқару сервері оларды Kaspersky инфрақұрылымына жібереді; алайда бұл сценарий өте сирек қолданылады.

16. Тек iOS ұялы құрылғылары үшін: ұялы құрылғылардан алынған деректер 443 TLS порты арқылы Басқару сервері немесе қосылым шлюзі орнатылған құрылғыда орналасқан iOS MDM серверіне жіберіледі.

17. Kaspersky Security Center Web Console Server мен браузер (Kaspersky Security Center Web Console-мен бірге қолданылады) басқару серверіне TLS 4444 порты арқылы OpenID Connect аутентификация протоколы көмегімен қосылады.

18. Kaspersky Security Center Web Console Server басқару серверіне TLS 9050 порты арқылы қосылады.

Kaspersky Security Center Linux құрамдастары мен қауіпсіздік қолданбаларының өзара әрекеттесуі: қосымша мәліметтер

Бұл бөлімде Kaspersky Security Center Linux құрамындағы құрамдастар мен басқарылатын қауіпсіздік қолданбалары арасындағы өзара әрекеттесу схемалары берілген. Схемаларда, қолжетімді болуы керек порт нөмірлері және порттарды ашатын процестердің атауы көрсетіледі.

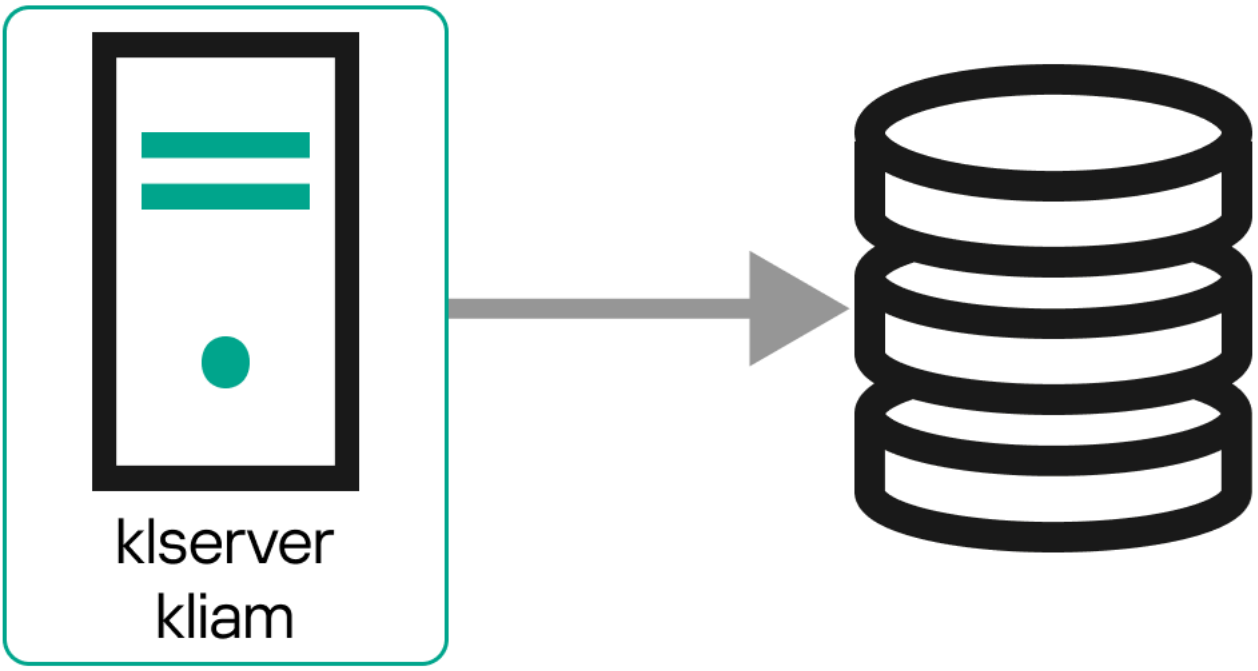
Өзара әрекеттесу схемаларындағы шартты белгілер

Төмендегі кестеде, схемаларда қолданылған шартты белгілер келтірілген.

Белгіше	Мән
	Басқару сервері
	Қосалқы Басқару сервері
	ДҚБЖ
	Желілік агент және Kaspersky Endpoint Security отбасының қолданбасы (немесе Kaspersky Security Center Linux басқара алатын басқа қауіпсіздік қолданбасы) орнатылған клиент құрылғысы
	Қосылым шлюзі
	Тарату нүктесі
	Пайдаланушының құрылғысындағы браузер
	Құрылғыда іске қосылған және кез келген портты ашатын процесс
	Порт және оның нөмірі
	TCP трафигі (меңзер бағыты трафик бағытын білдіреді)
	TCP трафигі (меңзер бағыты трафик бағытын білдіреді)
	ДҚБЖ тасымалдау
	Демилитаризацияланған аймақ шекаралары

Басқару сервері және ДҚБЖ

Басқару серверінің және Есептік деректер және қатынасу диспетчері (IAM) деректері бір ДҚБЖ ішінде бөлек дерекқорларға сақталады.



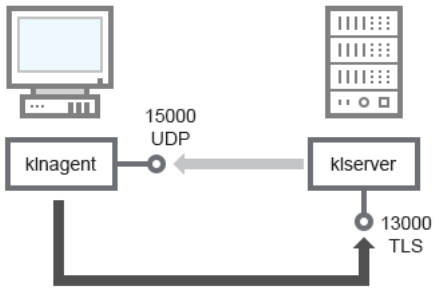
Басқару сервері, есептік деректер және қатынасу диспетчері және ДҚБЖ

Егер сіз Басқару сервері мен дерекқорды әртүрлі құрылғыларға орнатқан болсаңыз, онда сіз дерекқор орналасқан құрылғыдағы қажетті порттарды (мысалы, MariaDB үшін 3306-порт) қолжетімді етуіңіз керек. Толығырақ ақпарат ДҚБЖ құжаттамасында көрсетілген.
Пайдаланушы IAM-ды ДҚБЖ-ға қосу портын Kaspersky Security Center Linux орнату кезінде көрсетеді.

Басқару сервері серверді жойған немесе басқа құрылғыға жылжытқан кезде Басқару серверінің дерекқорларын және IAM дерекқорын автоматты түрде жоймайды. Қажет болса, дерекқорларды қолмен жою керек.

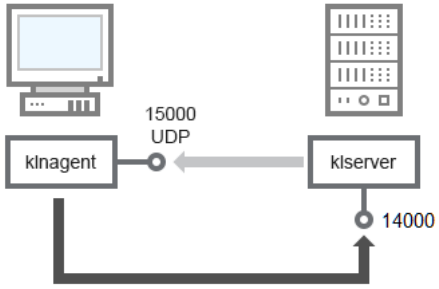
Басқару сервері және клиент құрылғысы: Қауіпсіздік бағдарламасын басқару

Басқару сервері 13000 TLS порты бойынша Желілік агенттерден қосылымдарды қабылдайды (төмендегі суретті қараңыз).



Басқару сервері және клиент құрылғысы: қауіпсіздік бағдарламасын басқару, 13000-порт арқылы қосылу (ұсынылады)

Егер сіз Kaspersky Security Center Linux бағдарламасының алдыңғы нұсқаларының бірін қолданған болсаңыз, онда сіздің желіңізде Басқару сервері 14000 қорғалмаған порты арқылы Желілік агенттерден қосылымдарды қабылдай алады (төмендегі суретті қараңыз). Kaspersky Security Center Linux нұсқасы да 14000-порт бойынша Желілік агенттерді қосуды қолдайды, бірақ 13000 қорғалған портын пайдалану ұсынылады.



Басқару сервері және клиент құрылғысы: қауіпсіздік бағдарламасын басқару, 14000-порт арқылы қосылу (төмен қорғаныс)

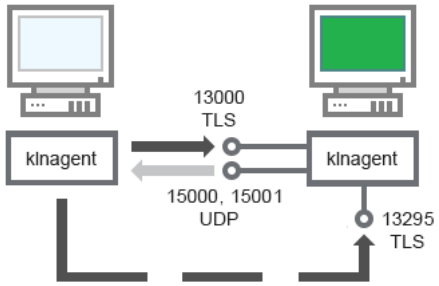
Схемаларға түсініктемелер алу үшін төмендегі кестені қараңыз.

Басқару сервері және клиент құрылғысы: Қауіпсіздік бағдарламасын басқару (трафик)

Құрылғы	Порт нөмірі	Портты ашатын процесс атауы	Протокол	Портты тағайындау
Желілік агент	15000	klnagent	UDP	Желілік агенттерге арналған көп мекенжайлы таратылым
Басқару сервері	13000	klserver	TCP (TLS)	Желілік агенттерден қосылымдар қабылдау
Басқару сервері	14000	klserver	TCP	Желілік агенттерден қосылымдар қабылдау

Тарату нүктесін пайдаланып клиент құрылғысындағы бағдарламалық жасақтаманы жаңарту

Клиент құрылғысы тарату нүктесіне 13000-порт арқылы, ал сіз тарату нүктесін push сервері ретінде пайдалансаңыз, 13295-порт арқылы қосылады; тарату нүктесі 15000-порт арқылы Желілік агенттерге көп мекенжайлы таратылым жібереді (төмендегі суретті қараңыз). Жаңартулар мен орнату пакеттері тарату нүктесінен 15001 порты арқылы алынады.



Тарату нүктесін пайдаланып клиент құрылғысындағы бағдарламалық жасақтаманы жаңарту

Схемаға түсініктемелер алу үшін төмендегі кестені қараңыз.

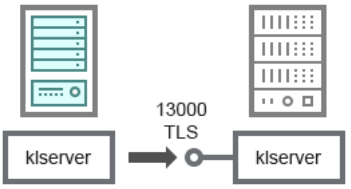
Тарату нүктесі арқылы бағдарламалық жасақтаманы жаңарту (трафик)

Құрылғы	Порт нөмірі	Портты ашатын процесс атауы	Протокол	Портты тағайындау
Желілік агент	15000	klnagent	UDP	Желілік агенттерге арналған көп мекенжайлы таратылым
Желілік агент	15001	klnagent	UDP	Тарату нүктесінен жаңартулар мен орнату пакеттерін алу
Тарату нүктесі	13000	klnagent	TCP (TLS)	Желілік агенттерден қосылымдар қабылдау
Тарату нүктесі	13295	klnagent	TCP (TLS)	Клиент құрылғыларынан (push-серверден) қосылымдарды қабылдау

Басқару серверлерінің иерархиясы: негізгі Басқару сервері және қосалқы Басқару сервері

Схемада (төмендегі суретті қараңыз), 13000-порт иерархияға біріктірілген Басқару серверлерінің өзара әрекеттесуі үшін қалай қолданылатынын көрсетеді.

Алдағыда, Серверлерді иерархияға біріктіргеннен кейін, сіз екі Серверді де негізгі Басқару серверіне қосылған Kaspersky Security Center Web Console консолі арқылы басқара аласыз. Осылайша, тек басты Сервердің 13299-порты қолжетімді болуы керек.



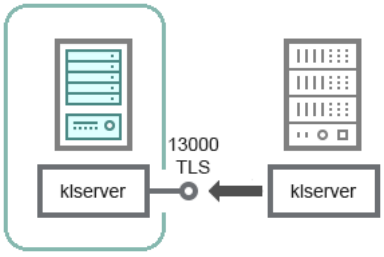
Басқару серверлерінің иерархиясы: негізгі Басқару сервері және қосалқы Басқару сервері

Схемаға түсініктемелер алу үшін төмендегі кестені қараңыз.

Басқару серверлерінің иерархиясы (трафик)

Құрылғы	Порт нөмірі	Портты ашатын процесс атауы	Протокол	Портты тағайындау
Негізгі Басқару сервері	13000	klserver	TCP (TLS)	Қосалқы Басқару серверлерінен қосылымдарды қабылдау

Демилитаризацияланған аймақта қосалқы Сервері бар Басқару серверлері иерархиясы



Демилитаризацияланған аймақта қосалқы Сервері бар Басқару серверлері иерархиясы

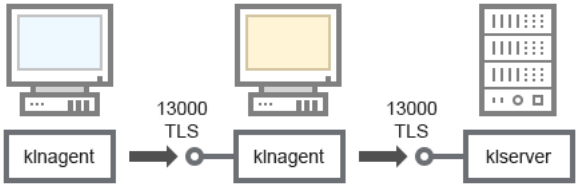
Схемада Басқару серверлерінің иерархиясы көрсетілген, онда демилитаризацияланған аймақтағы қосалқы Сервер басты Серверден қосылымды қабылдайды (схемаға түсініктемелер алу үшін төмендегі кестені қараңыз). Серверлерді иерархияға біріктіру кезінде екі Сервердің 13299-порты қолжетімді болуы керек. Kaspersky Security Center Web Console қолданбасы Басқару серверіне 13299-порт арқылы қосылады.

Алдағыда, Серверлерді иерархияға біріктіргеннен кейін, сіз екі Серверді де негізгі Басқару серверіне қосылған Kaspersky Security Center Web Console консолі арқылы басқара аласыз. Осылайша, тек басты Сервердің 13299-порты қолжетімді болуы керек.

Демилитаризацияланған аймақта қосалқы Сервері бар Басқару серверлері иерархиясы (трафик)

Құрылғы	Порт нөмірі	Портты ашатын процесс атауы	Протокол	Портты тағайындау
Қосалқы Басқару сервері	13000	klserver	TCP (TLS)	Негізгі Басқару серверінен қосылымдарды қабылдау

Басқару сервері, желі сегментіндегі қосылымдар шлюзі және клиент құрылғысы



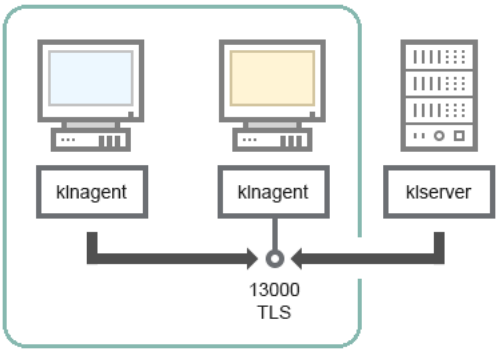
Басқару сервері, желі сегментіндегі қосылымдар шлюзі және клиент құрылғысы

Схемаға түсініктемелер алу үшін төмендегі кестені қараңыз.

Басқару сервері, желі сегментіндегі қосылымдар шлюзі және клиент құрылғысы (трафик)

Құрылғы	Порт нөмірі	Портты ашатын процесс атауы	Протокол	Портты тағайындау
Басқару сервері	13000	klserver	TCP (TLS)	Желілік агенттерден қосылымдар қабылдау
Желілік агент	13000	klnagent	TCP (TLS)	Желілік агенттерден қосылымдар қабылдау

Басқару сервері және демилитаризацияланған аймағы екі құрылғы: қосылымдар шлюзі және клиент құрылғысы



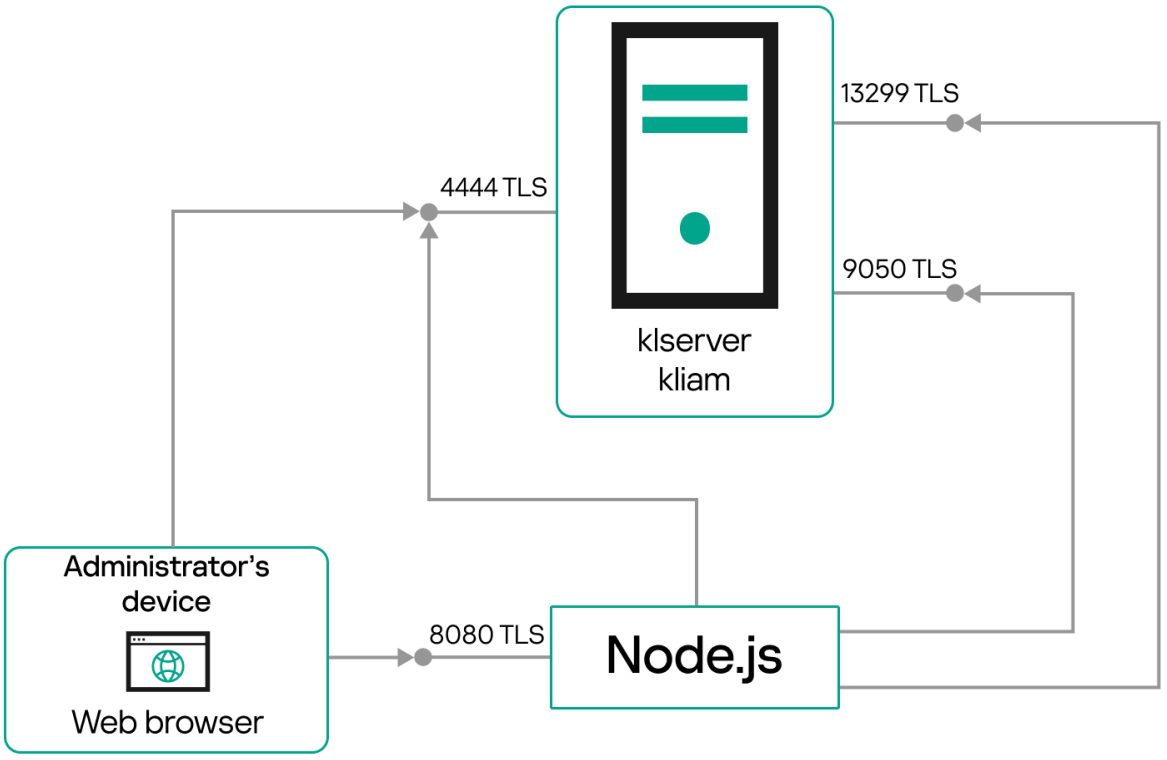
Демилитаризацияланған аймақтағы Басқару сервері, қосылымдар шлюзі және клиент құрылғысы

Схемаға түсініктемелер алу үшін төмендегі кестені қараңыз.

Басқару сервері, желі сегментіндегі қосылымдар шлюзі және клиент құрылғысы (трафик)

Құрылғы	Порт нөмірі	Портты ашатын процесс атауы	Протокол	Портты тағайындау
Желілік агент	13000	klnagent	TCP (TLS)	Желілік агенттерден қосылымдар қабылдау

Басқару сервері және Kaspersky Security Center Web Console



Басқару сервері және Kaspersky Security Center Web Console

Схемаға түсініктемелер алу үшін төмендегі кестені қараңыз.

Басқару сервері және Kaspersky Security Center Web Console (трафик)

Құрылғы	Порт нөмірі	Портты ашатын процесс атауы	Протокол	Портты тағайындау
Басқару сервері	13299	klserver	TCP (TLS)	Kaspersky Security Center Web Console мен Есептік деректер және қатынасу диспетчерінен (IAM) OpenAPI арқылы басқару серверіне қосылуды қабылдау
Kaspersky Security Center Web Console сервері немесе Басқару сервері	8080	Node.js: серверлік JavaScript	TCP (TLS)	Kaspersky Security Center Web Console серверінен қосылымдар алу
Басқару сервері	4444	kliam	TCP (TLS)	OpenID Connect аутентификация протоколы арқылы Kaspersky Security Center Web Console Server серверінен және браузерден (Kaspersky Security Center Web Console-мен бірге пайдаланылады) IAM бар басқару серверіне қосылуды қабылдау
Басқару сервері	9050	kliam	TCP (TLS)	Kaspersky Security Center Web Console серверінен IAM-ге қосылуды қабылдау

Kaspersky Security Center Web Console серверін Басқару сервері орнатылған құрылғыға немесе басқа құрылғыға орнатуға болады.

Жұмысқа кірісу

Осы сценарийді орындап, Kaspersky Security Center Linux Басқару сервері мен Kaspersky Security Center Web Console бағдарламасын орнатыңыз, бағдарламаны жылдам іске қосу шебері арқылы Басқару серверін бастапқы конфигурациялауды орындаңыз, сондай-ақ қорғанысты орналастыру шебері арқылы басқарылатын құрылғыларға Kaspersky бағдарламаларын орнатыңыз.

Алдын ала талаптар

Бизнес үшін Kaspersky Endpoint Security үшін лицензиялық кілт (белсендіру коды) немесе Kaspersky қауіпсіздік бағдарламалары үшін лицензия кілттері (белсендіру кодтары) бар болу керек.

Алдымен Kaspersky Security Center Linux-ті қолданып көргіңіз келсе, Kaspersky веб-сайтынан 30 күндік сынақ нұсқасын ала аласыз.

Кезеңдер

Негізгі орнату сценарийі келесі кезеңдерден тұрады:

1. **Ұйымның қорғаныс құрылымын таңдау**

   Kaspersky Security Center Linux құрамдастарымен танысыңыз. Желі конфигурациясы мен байланыс арналарының өткізу қабілеттілігіне сүйене отырып, Басқару серверлерінің қанша санын пайдалану керектігін және егер сіз таратылған желімен жұмыс жасасаңыз, оларды кеңселерге қалай орналастыру керектігін анықтаңыз.

   Ұйымыңызда Басқару сервері иерархиясы қолданылады ма екенін анықтаңыз. Бұл үшін барлық клиент құрылғыларына бір Басқару серверімен қызмет көрсету мүмкін бе және мақсатқа сай келеді ме, әлде Басқару серверлерінің иерархиясын құру қажет пе екенін түсіну керек. Сондай-ақ, сізге желісін қорғағыңыз келетін кәсіпорынның ұйымдық құрылымымен сәйкес келетін Басқару серверлерінің иерархиясын құру қажет болуы мүмкін.

2. **Пайдаланушы сертификаттарын пайдалануға дайындық**

   Ұйымыңыздың жалпыға ортақ кілт инфрақұрылымы (PKI) сізден белгілі бір сенімді сертификаттау орталығы (CA) шығарған пайдаланушы сертификаттарын пайдалануды талап етсе, осы сертификаттарды дайындаңыз және олардың барлық талаптарға сай екеніне көз жеткізіңіз.

3. **Дерекқорды басқару жүйесін (ДҚБЖ) орнату**

   Kaspersky Security Center Linux қолданатын ДҚБЖ орнатыңыз немесе қолданыстағы ДҚБЖ пайдаланыңыз.

   Сіз ДҚБЖ қолданатын платформалардың бірін таңдай аласыз. Таңдалған ДҚБЖ жүйесін қалай орнату керектігі туралы мәліметтер оның құжаттамасында келтірілген.

   Егер Linux негізіндегі операциялық жүйеңіздің дистрибутивінде қолдау көрсетілетін ДҚБЖ болмаса, ДҚБЖ жүйесін үшінші тарап пакеттер қоймасынан орнатуға болады. Егер үшінші тарап қоймаларынан дистрибутивтерді орнатуға тыйым салынса, ДҚБЖ жүйесін бөлек құрылғыға орнатуға болады.

Егер сіз PostgreSQL немесе Postgres Pro ДҚБЖ орнатуды шешсеңіз, суперпайдаланушының құпиясөзін енгізгеніңізге көз жеткізіңіз. Егер құпиясөз көрсетілмесе, Басқару сервері дерекқорға қосылмауы мүмкін.

MariaDB, PostgreSQL немесе Postgres Pro орнатсаңыз, онда ДҚБЖ дұрыс жұмыс істеуін қамтамасыз ету үшін ұсынылатын параметрлерді қолданыңыз.

Орнатқаннан кейін ДҚБЖ түрін өзгерткіңіз келсе, Kaspersky Security Center Linux жүйесін қайта орнатуыңыз қажет. Қайта орнатқаннан кейін импорттау үшін тапсырмалар мен саясаттарды экспорттай аласыз. Келесі мақалаларды қараңыз: Тапсырманы экспорттау, Саясатты экспорттау.

4 Порттарды конфигурациялау

Сіз таңдаған қорғаныс құрылымына сәйкес құрамдастардың өзара әрекеттесуі үшін қажетті порттардың ашық екеніне көз жеткізіңіз.

Егер интернеттен Басқару серверіне қатынас ұсыну қажет болса, порттар мен қосылым параметрлерін желі конфигурациясына қарай конфигурациялаңыз.

5 Kaspersky Security Center Linux орнату

Басқару сервері ретінде пайдаланатын Linux операциялық жүйесі бар құрылғыны таңдаңыз; құрылғының аппараттық және бағдарламалық жасақтамасы талаптарға сәйкес келетініне көз жеткізіңіз және құрылғыға Kaspersky Security Center Linux орнатыңыз. Басқару сервері құрамдасымен бірге автоматты түрде Желілік агенттің серверлік нұсқасы орнатылады.

6 Kaspersky Security Center Web Console және басқару веб-плагиндерін орнату

Әкімшінің жұмыс станциясы ретінде пайдаланатын Linux операциялық жүйесі бар құрылғыны таңдаңыз; құрылғының аппараттық және бағдарламалық жасақтамасы талаптарға сәйкес келетініне көз жеткізіңіз және осы құрылғыға Kaspersky Security Center Web Console-ін орнатыңыз. Kaspersky Security Center Web Console-ін Басқару серверімен бірге бір құрылғыда орнатуға болады.

Kaspersky Endpoint Security for Linux веб-басқару плагинін жүктеп алыңыз және оны Kaspersky Security Center Web Console бағдарламасы орнатылған құрылғыға орнатыңыз.

7 Басқару сервері бар құрылғыда Kaspersky Endpoint Security for Linux және Желілік агентін орнату

Әдепкі бойынша, бағдарлама Басқару сервері бар құрылғыны басқарылатын құрылғы ретінде пайдаланбайды. Басқару серверін вирустардан және басқа қауіптерден қорғау, сондай-ақ осы құрылғыны басқару үшін Kaspersky Endpoint Security for Linux бағдарламасын және Linux үшін Желілік агент Басқару сервері бар құрылғыға орнату ұсынылады. Бұл жағдайда Linux үшін Желілік агент орнатылады және Басқару серверімен бірге орнатылған Желілік агенттің сервер нұсқасына қарамастан тәуелсіз жұмыс істейді.

8 Бастапқы конфигурациялауды орындау

Басқару серверін орнату аяқталғаннан кейін, Басқару серверіне алғаш рет қосылған кезде Бағдарламаны жылдам іске қосу шебері автоматты түрде іске қосылады. Сіздің талаптарыңызға сәйкес Басқару серверін бастапқы конфигурациялауды орындаңыз. Бағдарламаны жылдам іске қосу кезеңінде, шебер қорғанысты орналастыру үшін қажетті әдепкі бойынша параметрі бар саясат пен тапсырманы жасайды. Бұл параметрлер сіздің ұйымыңыздың қажеттіліктері үшін оңтайлы болмауы мүмкін. Қажет болса, саясаттар мен тапсырмалар параметрлерін өзгерте аласыз.

9 Желілік құрылғыларды табу

Құрылғыны қолмен табу үшін желіге сауалнама жүргізіңіз. Нәтижесінде, Kaspersky Security Center Linux Басқару сервері желіде тіркелген барлық құрылғылардың мекенжайлары мен атауларын алады. Алдағыда, Kaspersky Security Center Linux көмегімен табылған құрылғыларға Kaspersky және басқа өндірушілердің бағдарламаларын орната аласыз. Kaspersky Security Center Linux құрылғыларды анықтауды үнемі іске қосады, сондықтан желіде жаңа құрылғылар пайда болса, олар автоматты түрде анықталады.

10 Құрылғыларды басқару топтарына біріктіру

Кейбір жағдайларда қорғанысты желі құрылғыларында оңтайлы түрде орналастыру үшін құрылғыларды ұйымның ұйымдық құрылымын ескере отырып, басқару топтарына бөлу қажет болуы мүмкін. Құрылғыларды топтар бойынша тарату немесе құрылғыларды қолмен тарату үшін жылжыту ережелерін жасауға болады. Басқару топтары үшін топтық тапсырмаларды тағайындауға, саясаттардың әрекет ету ауқымын анықтауға және тарату нүктелерін тағайындауға болады.

Барлық басқарылатын құрылғылар тиісті басқару топтары бойынша таратылғанына және желіңізде тағайындалмаған құрылғылардың қалмағанына көз жеткіңіз.

11 Тарату нүктелерін тағайындау

Басқару топтары үшін тарату нүктелері автоматты түрде тағайындалады, бірақ қажет болса, оларды қолмен тағайындауға болады. Тарату нүктелерін Басқару серверіне жүктемені азайту үшін үлкен желілерде, сондай-ақ Басқару серверіне өткізу қабілеті төмен арналармен біріктірілген құрылғыларға немесе құрылғылар тобына қатынасуды ұсыну үшін таратылған құрылымы бар желілерде пайдалану ұсынылады.

12 Желідегі құрылғыларға Желілік агент пен қауіпсіздік бағдарламаларын орнату

Ұйымның желісінде қорғанысты орналастыру Желілік агент пен қауіпсіздік бағдарламаларын Басқару сервері құрылғыларды анықтау процесінде тапқан құрылғыларға орнатуды қамтиды.

Бағдарламаны қашықтан орнатуды орындау үшін қорғанысты орналастыру шеберін іске қосыңыз.

Қауіпсіздік бағдарламалары құрылғыларды вирустардан және басқа қауіп төндіретін бағдарламалардан қорғайды. Желілік агент құрылғының Басқару серверімен байланысын қамтамасыз етеді. Желілік агенттің параметрлері әдепкі бойынша автоматты түрде конфигурацияланады.

Желідегі құрылғыларға Желілік агент пен қауіпсіздік бағдарламаларын орнатпас бұрын, бұл құрылғылардың қолжетімді (қосулы) екеніне көз жеткізіңіз.

13 Лицензиялық кілттерді клиент құрылғыларына тарату

Осы құрылғыларда басқарылатын қауіпсіздік бағдарламаларын белсендіру үшін лицензиялық кілттерді клиент құрылғыларына таратыңыз.

14 Kaspersky бағдарламаларының саясаттарын конфигурациялау

Әртүрлі құрылғыларда бағдарламалардың әртүрлі параметрлері қолданылуы үшін, құрылғы қауіпсіздігін басқару немесе пайдаланушыға бағытталған қауіпсіздікті басқару нұсқаларын пайдалануға болады. Құрылғылардың қауіпсіздігін басқару саясаттар мен тапсырмалар арқылы іске асырылады. Тапсырмаларды тек белгілі бір шарттарға сәйкес келетін құрылғыларда орындауға болады. Құрылғы таңдаулары шарттарын жасау үшін құрылғы таңдаулары мен тегтер қолданылады.

15 Желі қорғанысы күйінің мониторингі

Сіз ақпараттық тақтадағы веб-виджеттер арқылы желі жұмысын бақылауды ұйымдастыра аласыз, Kaspersky бағдарламалары туралы есептер жасай аласыз, басқарылатын құрылғылардағы бағдарламалардан алынған оқиғаларды таңдауды конфигурациялап, көре аласыз және хабарландырулар тізімін көре аласыз.

Қорғаныстықүшейтунұсқаулығы

Kaspersky Security Center Linux бағдарламасы ұйымның желісін қорғау жүйесін басқару және қызмет көрсету жөніндегі негізгі тапсырмаларды орталықтандырылған шешуге арналған. Қолданба әкімшіге ұйым желісінің қауіпсіздік деңгейі туралы егжей-тегжейлі ақпаратқа қол жеткізуге мүмкіндік береді. Kaspersky Security Center Linux, Kaspersky қолданбаларына негізделген барлық қорғаныс құрамдастарын конфигурациялауға мүмкіндік береді.

Kaspersky Security Center Linux Басқару сервері клиент құрылғыларының қорғанысын басқаруға толық қатынасу мүмкіндігіне ие және ұйымның қорғаныс жүйесінің маңызды құрамдас бөлігі болып табылады. Сондықтан, Басқару сервері үшін күшейтілген қорғаныс шаралары қажет.

Конфигурациялау алдында Басқару сервері деректерінің сақтық көшірмесін жасау тапсырмасын немесе klbackup утилитасын пайдаланып, Kaspersky Security Center Linux басқару серверінің сақтық көшірмесін жасаңыз және оны қауіпсіз жерде сақтаңыз.

Қорғаныстықүшейтунұсқаулығы, бұзылу қаупін азайту үшін Kaspersky Security Center Linux және оның құрамдастарын конфигурациялаудың ұсыныстары мен ерекшеліктерін сипаттайды.

Қорғаныстықүшейтунұсқаулығы келесі ақпаратты қамтиды:

- Басқару серверін орналастыру схемасын таңдау
- Басқару серверіне қауіпсіз қосылымды конфигурациялау
- Басқару серверімен жұмыс істеу үшін есептік жазбаларды конфигурациялау
- Басқару серверін қорғауды басқару
- Клиент құрылғыларын қорғауды басқару
- Басқарылатын қолданбалар қорғанысын конфигурациялау
- Басқару серверіне техникалық қызмет көрсету
- Үшінші тарап жүйелеріне ақпарат беру
- Үшінші тарап ақпараттық жүйелерінің қауіпсіздігі бойынша ұсыныстар

Қорғаныстықүшейтудің тексеру тізімі

Басқару серверін орналастыру

- Басқару серверін арнайы физикалық немесе виртуалды серверге орнатыңыз.
- Басқа қызметтерді іске қосу үшін арнайы серверді пайдаланбаңыз.

- Басқару серверін (бұдан әрі – сервер) мына жерге орнатпаңыз:
  - Домен контроллері
  - Терминал сервері
  - Пайдаланушы құрылғысы

Қосылым қауіпсіздігі

- Серверге қажетті порттардан басқа барлық порттар мен протоколдарда сервер құрылғысына кіруді шектеу үшін желіаралық қалқанды теңшеңіз. Сервер құрылғысына тек сенімді құрылғылардан кіруге рұқсат беріңіз.
- Kaspersky Security Center Web Console (Web Console деп те аталады) веб-консолін серверге қосу мақсатында, пайдаланылатын сервер порттары үшін IP мекенжайларының рұқсат етілген тізімін конфигурациялаңыз.
- Web Console арқылы тек сенімді құрылғылардан кіруге рұқсат беру үшін желілік экранды конфигурациялаңыз.
- Серверде TLS протоколының 1.2 немесе одан жоғары нұсқасын конфигурациялаңыз.
- Сервер ДҚБЖ орнатылған құрылғыға кіруді шектеу үшін желілік экранды конфигурациялаңыз.
- Сервер мен ДҚБЖ (MySQL немесе PostgreSQL) арасында SSL аутентификациясын конфигурациялаңыз.

Есептік жазбалар және авторизация

- Серверге кіру үшін екі факторлы аутентификацияны (TOTP, RFC 6238) конфигурациялаңыз.
- Серверге Web Console арқылы қосылған сол құрылғыда аутентификация қолданбасын орнатпаңыз.
- Сервер құрылғысына токенмен, смарт картамен немесе басқа әдіспен кіру үшін көп факторлы аутентификацияны (MFA) пайдаланыңыз.
- Сервер құрылғысы үшін арнайы басқару тобын жасаңыз және ол үшін арнайы қауіпсіздік саясатын жасаңыз.
- Бас әкімші рөлі бар пайдаланушылар санын шектеңіз.
- Пайдаланушылар мен топтардың рөлдері негізінде сервер мүмкіндіктеріне кіру құқықтарын конфигурациялаңыз.
- Жеке пайдаланушы есептік жазбасы үшін қолданбаларды қашықтан орнатуға рұқсат беріңіз.
- Сервердегі барлық пайдаланушының тұрақты аудитін жүргізіңіз.

Басқару серверін қорғауды басқару

- Сервер құрылғысында қауіпсіздік қолданбасын орнату:
  - Физикалық сервер үшін – Kaspersky Endpoint Security
  - Виртуалды сервер үшін – Kaspersky Security for Virtualization
- Серверді қорғау үшін бөлек саясат жасаңыз және қолданыңыз (басқарылатын құрылғылардың қауіпсіздік саясатынан басқа).
- Серверді қорғау үшін бөлек құпиясөз жасаңыз және қолданыңыз (басқа басқарылатын құрылғылардың құпия сөзінен өзгеше).
- Қауіпсіздік бағдарламасында барлық қолжетімді қорғаныс модульдерін қосыңыз (Kaspersky Security Center Linux жүйесімен жұмыс істеу үшін ұсынылатын ең аз қауіпсіздік параметрлері туралы ақпаратты Kaspersky Endpoint Security for Linux онлайн анықтамалығынан қараңыз).

Басқарылатын қолданбаларға арналған саясаттар мен тапсырмаларды конфигурациялау

- Келесі қолданбалар үшін барлық басқарылатын құрылғыға немесе басқарылатын жаңа құрылғылар тобына саясаттарды жасаңыз және қолданыңыз:
  - Желілік агент
  - Kaspersky Endpoint Security for Windows/Linux/macOS
  - Kaspersky Endpoint Agent (немесе басқа Kaspersky қолданбалары)
- Kaspersky қолданбалары қорғанысын өшіруге немесе жоюға қарсы құпиясөз қорғанысын қосыңыз.
- Басқарылатын құрылғыларда осы параметрлердің қайта тағайындалуын болдырмау үшін саясат параметрлерін құлыптау («құлыпты» жабыңыз).
- Барлық құрылғының жоспарланған толық сканерлеу тапсырмасын жасаңыз.
- Kaspersky Security Network (KSN) пайдалануды қосыңыз және соңғы KSN мәлімдемесін қабылдаңыз.
- Құрылғыларды табуды конфигурациялаңыз және жаңадан табылған құрылғылар үшін әдепкі басқару тобын көрсетіңіз.
- Басқару топтары арасында құрылғыларды жылжыту үшін автоматты ережелерді пайдалануға шектеу қойыңыз.
- Тарату нүктелерін рұқсатсыз кіруден қорғаңыз.
- Шағын желілерде немесе маңыздылығы жоғары желілерде тарату нүктелерін автоматты түрде тағайындамаңыз.

Басқару серверіне техникалық қызмет көрсету

- Келесі тапсырмаларды жоймаңыз немесе өшірмеңіз:
  - Сақтық көшірме
  - Басқару серверіне техникалық қызмет көрсету
- ОЖ және үшінші тараптың бағдарламалық жасақтама жаңартуларын жүйелі түрде орнатыңыз.

Оқиғаларды үшінші тарап жүйелеріне беру

- Қауіпсіздік оқиғаларының бақылау және есеп беру мүмкіндігін конфигурациялаңыз.
- Оқиғаны SIEM жүйесіне экспорттауды конфигурациялаңыз.
- Сервер хабарландыруларын келесілер үшін конфигурациялаңыз:
  - Аудит оқиғалары
  - Критикалық оқиғалар
  - Ақауларға төзімді оқиғалар мен ескертулер

Үшінші тарап ақпараттық жүйелерінің қауіпсіздігі бойынша ұсыныстар

- Қолданылатын операциялық жүйелерге, ДҚБЖ мен гипервизорларға CIS Benchmarks қауіпсіздік ұсыныстарын қолданыңыз.
- Astra Linux үшін тиісті Red Book нұсқасындағы қауіпсіздік ұсыныстарын орындаңыз.
- RED ОЖ үшін ресми RED ОЖ құжаттамасында берілген ұсыныстарды орындаңыз.

Басқару серверін орналастыру

Басқару сервері архитектурасы

Жалпы алғанда, басқарудың орталықтандырылған архитектурасын таңдауға қорғалатын құрылғылардың орналасуы, іргелес желілерден қатынасу, дерекқорларды жаңарту схемалары және басқа параметрлер әсер етеді.

Архитектураны дамытудың бастапқы кезеңінде Kaspersky Security Center Linux құрамдастарымен және олардың бір-бірімен өзара әрекеттесуімен, сондай-ақ деректер трафигі және портты пайдалану схемаларымен танысуды ұсынамыз.

Осы ақпарат негізінде мыналарды анықтайтын архитектураны қалыптастыру қажет:

- Басқару серверінің орналасуы және желіге қосылуы
- Әкімшілердің жұмыс станцияларын ұйымдастыру және Басқару серверіне қосылу тәсілдері
- Желілік агент және қорғау бағдарламасын орнату тәсілі
- Тарату нүктелерін пайдалану
- Виртуалды Басқару серверлерін қолдану
- Басқару серверлерінің иерархиясын қолдану
- Антивирустық дерекқорларды жаңарту схемасы
- Басқа ақпарат ағындары

Басқару сервері үшін құрылғыны таңдау

Басқару серверін инфрақұрылымдағы арнайы серверге орнату ұсынылады. Серверде үшінші тарап бағдарламалық жасақтамасы болмаса, бұл Kaspersky Security Center Linux талаптарын ескере отырып және үшінші тарап бағдарламалық жасақтамасының талаптарына тәуелді болмай, қауіпсіздік параметрлерін конфигурациялауға мүмкіндік береді.

Басқару серверін физикалық серверде де, виртуалды машинада да орналастыруға болады. Таңдалған құрылғы аппараттық және бағдарламалық талаптарға сәйкес келетініне көз жеткізіңіз.

Басқару серверін домен контроллеріне, терминал серверіне немесе пайдаланушы құрылғысына орнатуды шектеу

Басқару серверін домен контроллеріне, терминал серверіне немесе пайдаланушы құрылғысына орнату мүлдем ұсынылмайды.

Желінің өзекті құрылғыларын функционалдық бөлуді көздеу ұсынылады. Бұл, құрылғы істен шыққанда немесе бұзылған кезде әртүрлі жүйелердің жұмыс істеу қабілетін сақтауға мүмкіндік береді. Сонымен қатар, бұл тәсілдеме әр құрылғы үшін әртүрлі қауіпсіздік саясатын жүзеге асыруға мүмкіндік береді.

Басқару серверін орнату және іске қосу үшін есептік жазбалар

Басқару серверді орналастыру кезінде артықшылығы жоқ екі есептік жазба жасау керек. Басқару серверге енгізілген қызметтер осы артықшылықсыз есептік жазбаларда жұмыс істейді. Есептік жазбаларға құқықтар мен рұқсаттар беру кезінде ең аз артықшылықтар қағидатын ұстаныңыз. kladmins тобына қажетсіз есептік жазбаларды қоспаңыз.

Сондай-ақ ішкі ДҚБЖ есептік жазбасын жасау қажет. Басқару сервер таңдалған ДҚБЖ-ға қол жеткізу үшін осы ішкі ДҚБЖ есептік жазбасын пайдаланады.

Қажетті есептік жазбалар жиынтығы және олардың құқықтары таңдалған ДҚБЖ және Басқару серверінің дерекқорын құру тәсіліне байланысты.

Қосылым қауіпсіздігі

TLS пайдалану

Басқару серверіне қауіпсіз емес қосылымдарға тыйым салу ұсынылады. Мысалы, Басқару серверін конфигурациялау кезінде HTTP протоколы арқылы Басқару серверіне қосылымдарды қоспау ұсынылады.

Басқару серверінің кейбір HTTP порттары әдепкі бойынша жабық екенін ескеріңіз. Қалған портты Kaspersky Security Center веб-сервері (8060) пайдаланады. Бұл портты Басқару сервері бар құрылғының желілік экран параметрлері арқылы шектеуге болады.

Қатаң TLS параметрлері

TLS 1.2 немесе одан жоғары нұсқасын пайдалану және қауіпсіз емес шифрлау алгоритмдерін пайдалануды шектеу немесе өшіру ұсынылады.

Басқару сервері пайдаланатын шифрлау протоколдарын (TLS) конфигурациялауға болады. Бұл ретте, Басқару серверінің белгілі бір нұсқасын шығару кезінде деректерді қауіпсіз тасымалдауды қамтамасыз ету үшін әдепкі бойынша шифрлау протоколының параметрлері конфигурацияланатынын есте сақтаңыз.

Басқару сервері дерекқорына қатынасуды шектеу

Басқару сервері дерекқорына қатынасуды шектеу ұсынылады. Мысалы, Басқару сервері бар құрылғыдан ғана қатынасуға рұқсат бере аласыз. Бұл белгілі осалдықтар арқылы Деректерді басқару серверінің дерекқорын бұзу ықтималдығын азайтады.

Параметрлерді пайдаланылатын дерекқордың пайдалану нұсқаулығына сәйкес конфигурациялауға, сондай-ақ желілік экрандарда жабық порттарды көздеуге болады.

Сыртқы ДҚБЖ-мен өзара әрекет қауіпсіздігі

Басқару серверін (сыртқы ДҚБЖ) орнату кезінде ДҚБЖ бөлек құрылғыға орнатылса, осы ДҚБЖ-мен қауіпсіз өзара әрекет жасау және аутентификация үшін параметрлерді конфигурациялау ұсынылады. SSL аутентификациясын конфигурациялау туралы қосымша ақпаратты PostgreSQL серверінің аутентификациясы және Сценарий: MySQL серверінің аутентификациясы бөлімдерінен қараңыз.

Басқару серверіне қосылуға арналған рұқсат етілген IP мекенжайлары тізімін конфигурациялау

Әдепкісінше Kaspersky Security Center Linux пайдаланушылары Kaspersky Security Center Linux жүйесіне Kaspersky Security Center Web Console немесе OpenAPI қолданбалары орнатылған кез келген құрылғыдан кіре алады. Басқару серверін, пайдаланушылар оған тек рұқсат етілген IP мекенжайлары бар құрылғылардан қосыла алатындай етіп конфигурациялауға болады. Мысалы, қаскүнем рұқсат тізімінде жоқ құрылғыға орнатылған Kaspersky Security Center Web Console Server арқылы Kaspersky Security Center Linux жүйесіне қосылуға әрекеттенген кезде, ол Kaspersky Security Center Linux жүйесіне кіре алмайды.

Kaspersky Security Center Web Console-ге қосылу үшін IP мекенжайларының рұқсат тізімін конфигурациялау

Әдепкісінше Kaspersky Security Center Linux пайдаланушылары Kaspersky Security Center Web Console-ге кез келген құрылғыдан қосыла алады. Kaspersky Security Center Web Console бар құрылғыда пайдаланушылар Kaspersky Security Center Web Console-ге тек рұқсат етілген IP мекенжайлары арқылы қосыла алуы үшін, желілік экранды (операциялық жүйеге немесе үшінші тарапқа орнатылған) конфигурациялау керек.

Сауалнама кезінде домен контроллеріне қосылу қауіпсіздігі

Домен контроллеріне сауалнама жүргізу үшін басқару сервері немесе Linux тарату нүктесі осы доменге LDAPS арқылы қосылуға әрекеттенеді. Әдепкісінше қосылу кезінде сертификатты растау қажет болмайды. Сертификатты растау процесін енгізу үшін `KLNAG_LDAP_TLS_REQCERT` жалаушасын 1-ге орнатыңыз. Сондай-ақ `KLNAG_LDAP_SSL_CACERT` жалауын пайдалану арқылы сертификаттар тізбегіне кіру үшін сертификат орталығына (CA) апаратын арнаулы жолды көрсетуге болады.

Есептік жазбалар және авторизация

Төмендегі қадамдарды орындамай тұрып, Басқару сервері деректерінің сақтық көшірмесін жасау тапсырмасын немесе klbackup утилитасын пайдаланып, Kaspersky Security Center Linux басқару серверінің сақтық көшірмесін жасаңыз және оны қауіпсіз жерде сақтаңыз.

Басқару серверімен екі факторлы аутентификацияны пайдалану

Kaspersky Security Center Linux бағдарламасы Kaspersky Security Center Web Console веб-консоліне кірген уақытта RFC 6238 стандартына (TOTP: уақытқа негізделген бір реттік құпиясөз алгоритмі) негізделген екі факторлы аутентификация мүмкіндігін қолданады.

Kaspersky Security Center Web Console веб-консоліне кірген сайын пайдаланушы атыңызды, құпиясөзіңізді және қосымша бір реттік қауіпсіздік кодын енгізесіз. Бір реттік қауіпсіздік кодын алу үшін, сіз өзіңіздің компьютеріңізге немесе ұялы құрылғыға аутентификация қолданбасын орнатуыңыз керек.

RFC 6238 стандартын қолдайтын бағдарламалық және аппараттық аутентификаторлар (токендер) бар. Мысалы, бағдарламалық аутентификаторларға Google Authenticator, Microsoft Authenticator, FreeOTP кіреді.

Басқару серверіне қосылатын сол құрылғыда аутентификация қолданбасын орнату мүлдем ұсынылмайды. Мысалы, ұялы құрылғыға аутентификация қолданбасын орнатуға болады.

Екі факторлы операциялық жүйе түпнұсқалық растамасын пайдалану

Екі факторлы аутентификацияны пайдалану арқылы кешенді қорғауды қамтамасыз ету үшін тек Басқару серверін ғана емес, сонымен қатар ол орнатылған құрылғыны да қорғау қажет.

Басқару сервері орнатылған құрылғыға (SSH, RDP немесе басқа протоколдар арқылы) қосылған кезде, токен, смарт карталар немесе басқа аутентификация әдісімен көп факторлы аутентификацияны (MFA) пайдалануды ұсынамыз.

Әкімші құпиясөзін сақтауға тыйым салу

Сондай-ақ, Kaspersky Security Center Web Console веб-консолі арқылы Басқару серверімен жұмыс істегенде, пайдаланушы құрылғысындағы браузерде әкімші құпиясөзін сақтау ұсынылмайды.

Ішкі пайдаланушы авторизациясы

Әдепкі бойынша Басқару серверінің ішкі пайдаланушы есептік жазбасының құпиясөзі келесі талаптарға сай болуы керек:

- Құпиясөздің ұзындығы 8-ден 256 таңбаға дейін болуы керек.
- Құпиясөзде төмендегі тізімдегі кемінде үш топтың таңбалары болуы керек:
  - Бас әріптер (A-Z)
  - Кіші әріптер (a-z)
  - Сандар (0-9)

- Арнайы таңбалар (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)

- Құпиясөзде бос орындар, Юникод таңбалары немесе "." таңбасы "@" алдында тұрған кезде "." және "@" тіркесімі болмауы тиіс.

Әдепкі бойынша, енгізу әрекеттерінің максималды саны 10-ға тең. Құпиясөзді енгізу әрекеттерінің санын өзгерте аласыз.

Kaspersky Security Center Linux пайдаланушысы құпиясөзді шектеулі рет енгізе алады. Осыдан кейін, пайдаланушы есептік жазбасы бір сағатқа бұғатталады.

Ішкі пайдаланушы есептік жазбасының құпиясөзін өзгерту опцияларын конфигурациялау

Ішкі пайдаланушы есептік жазбасының құпиясөзін өзгерту үшін келесі опцияларды конфигурациялауды ұсынамыз:

- Құпиясөзді ауыстыру кезеңі
- Құпиясөзді өзгерту қажеттігі туралы алдын ала көрсетілетін ескерту уақыты
- **Пайдаланушы бірінші кірген кезде құпиясөзді өзгертуі керек** опциясының мәні

Есептік жазбаны рұқсатсыз өзгертуден қорғау

Басқару серверінің ішкі пайдаланушы есептік жазбасын рұқсатсыз өзгертуден қорғау үшін қосымша опцияны қосуды ұсынамыз. Бұл қорғаныс әрбір ішкі пайдаланушы үшін бөлек конфигурациялануы керек.

Басқару сервері бар құрылғы үшін бөлек басқару тобы

Басқару сервері үшін бөлінген басқару тобын жасау ұсынылады. Бұл топқа арнайы кіру құқықтарын беріңіз және ол үшін қауіпсіздік саясатын жасаңыз.

Басқару серверінің қорғау деңгейін әдейі төмендетпеу үшін осы басқару тобын басқара алатын есептік жазбалар тізімін шектеу ұсынылады.

Бас әкімші рөлін тағайындауды шектеу

kladduser утилитасы көмегімен жасалған пайдаланушыға басқару серверінің немесе виртуалды басқару серверінің қол жеткізуді басқару тізімінде (ACL) негізгі әкімші рөлі тағайындалады. Бас әкімші рөлін көп пайдаланушыға тағайындамаған жөн.

Қолданба функцияларына қатынасу құқықтарын конфигурациялау

Kaspersky Security Center Linux жүйесінің әртүрлі функцияларына пайдаланушылар мен пайдаланушы топтарының қол жеткізу құқықтарының икемді параметрі мүмкіндігін пайдалану ұсынылады.

Рөлдер негізінде қатынасуды басқару арқасында алдын ала конфигурацияланған құқықтар жиынтығы бар осы типтік пайдаланушы рөлдерін жасауға және пайдаланушыларға олардың қызметтік міндеттеріне қарай рөлдер тағайындауға болады.

Қатынасуды басқарудың рөлдік моделінің негізгі артықшылықтары:

- басқарудың қарапайымдылығы;
- рөлдер иерархиясы;
- ең аз артықшылық қағидаты;
- міндеттерді бөлу.

Сіз кірістірілген рөлдерді пайдалана аласыз және оларды лауазымдар негізінде нақты қызметкерлерге тағайындай аласыз немесе әбден жаңа рөлдерді жасай аласыз.

Рөлдерді конфигурациялау кезінде құрылғыны қорғау күйін өзгертуге және үшінші тарап бағдарламалық жасақтамасын қашықтан орнатуға қатысты артықшылықтарға ерекше назар аударыңыз:

- Басқару топтарын басқару.
- Басқару серверіне қатысты әрекеттер.
- Қашықтан орнату.
- Оқиғаларды сақтау және хабарландыруларды жіберу параметрлерін өзгерту.

  Бұл артықшылық, оқиға орын алған кезде Басқару сервері бар құрылғыда скриптті немесе орындалатын модульді іске қосатын хабарландыруларды конфигурациялауға мүмкіндік береді.

Қолданбаларды қашықтан орнату үшін бөлек есептік жазба

Қатынасу құқықтарын негізгі шектеуден басқа, барлық есептік жазбалар үшін ("Бас әкімші" немесе басқа мамандандырылған есептік жазбадан басқа) қолданбаларды қашықтан орнату мүмкіндігін шектеу ұсынылады.

Қолданбаларды қашықтан орнату үшін бөлек есептік жазбаны пайдалану ұсынылады. Бөлек есептік жазбаға рөл немесе рұқсаттар тағайындауға болады.

Барлық пайдаланушы мен пайдаланушы әрекеттерінің тұрақты аудиті

Басқару сервері орнатылған құрылғыдағы барлық пайдаланушылардың тұрақты аудитін жүргізу ұсынылады. Бұл, құрылғының ықтимал бұзылуымен байланысты қауіпсіздік қатерлерінің кейбір түрлеріне жауап беруге мүмкіндік береді.

Сондай-ақ басқару серверіне қосу және ажырату, басқару серверіне қатемен қосу және нысандарды өзгерту (тексеруді басқаруға қолдау көрсететін нысандар үшін) сияқты пайдаланушылардың әрекеттерін бақылауға болады.

Басқару серверін қорғауды басқару

Басқару серверін қорғау бағдарламасын таңдау

Басқару сервері орнатылған құрылғыны қорғауға арналған қолданбаны таңдау Басқару серверін орналастыру түріне және жалпы қорғау стратегиясына байланысты.

Басқару серверін бөлінген құрылғыда қолданатын болсаңыз, құрылғыны Басқару серверімен қорғау үшін Kaspersky Endpoint Security бағдарламасын таңдау ұсынылады. Бұл құрылғыны қорғау үшін барлық қолжетімді технологияларды, соның ішінде әрекет талдауы модульдерін пайдалануға мүмкіндік береді.

Басқару сервері инфрақұрылымда бұрыннан бар және бұған дейін басқа тапсырмаларды орындау үшін пайдаланылған құрылғыда орнатылған болса, келесі қорғау қолданбалары ұсынылады:

- Kaspersky Industrial Cyber Security for Nodes. Бұл бағдарламаны өнеркәсіптік желіге кіретін құрылғыларға орнату ұсынылады. Kaspersky Industrial Cyber Security for Nodes – әртүрлі өнеркәсіптік бағдарламалық жасақтама өндірушілерімен үйлесімділік сертификаттары бар бағдарлама.

- Ұсынылатын қауіпсіздік бағдарламалары. Басқару сервері басқа бағдарламалық жасақтамасы бар құрылғыда орнатылған болса, сіз бағдарламалық жасақтама өндірушісінің антивирустық бағдарламаларды пайдалану бойынша ұсыныстарын оқып шығуыңыз керек (қорғау бағдарламасын таңдау бойынша ұсыныстар бұрыннан бар болуы мүмкін және сенімді аймақты конфигурациялау қажет болуы мүмкін).

Бағдарламаны қорғау үшін бөлек қауіпсіздік саясатын жасау

Басқару серверінің қорғау қолданбалары үшін бөлек қауіпсіздік саясатын жасау қажет. Бұл саясат клиент құрылғыларының қауіпсіздік саясатынан өзгеше болуы керек. Бұл тәсілдеме басқа құрылғылардың қорғау деңгейіне әсер етпестен, Басқару серверіне барынша сәйкес келетін қауіпсіздік параметрлерін орнатуға мүмкіндік береді.

Басқару сервері бар құрылғыны бөлек басқару тобына тағайындау арқылы құрылғыларды топтарға бөлу ұсынылады, ол үшін арнайы қауіпсіздік саясатын жасауға болады.

Қорғаныс модульдері

Басқару серверімен бір құрылғыда орнатылған үшінші тарап бағдарламалық жасақтамасының өндірушісінен ерекше ұсыныстар болмаса, барлық қолжетімді қорғаныс модульдерін іске қосу және конфигурациялау ұсынылады (олардың жұмысын белгілі бір уақыт аралығында тексергеннен кейін).

Басқару сервері арқылы құрылғының желілік экранын конфигурациялау

Басқару сервері бар құрылғыда желілік экранды әкімшілер Басқару серверіне Kaspersky Security Center Web Console консолі арқылы қосыла алатын құрылғылардың санын шектейтіндей етіп конфигурациялау ұсынылады.

Kaspersky Security Center Web Console ішінен байланысты қабылдау үшін Басқару сервер әдепкі бойынша 13299 портын пайдаланады. Басқару серверін осы порт арқылы басқаруға болатын құрылғылардың санын шектеу ұсынылады.

Клиент құрылғыларын қорғауды басқару

Орнату пакеттеріне лицензиялық кілттерді қосуды шектеу

Орнату пакеттері, Packages қалтасына салынған Басқару серверінің ортақ қатынас бар қалтасында сақталады. Орнату пакетіне лицензия кілтін қоссаңыз, лицензия кілті осы қалтадағы оқу құқығы бар барлық пайдаланушыларға қолжетімді болады (тікелей немесе Басқару серверге ендірілген веб-сервер арқылы).

Лицензиялық кілттің бұзылуын болдырмау үшін орнату пакеттеріне лицензиялық кілттерді қоспау ұсынылады.

Лицензиялық кілттерді басқарылатын құрылғыларға автоматты түрде таратуды пайдалануды, Басқарылатын бағдарлама үшін лицензиялық кілтті қосу тапсырмасы арқылы орналастыруды, сондай-ақ құрылғыларға белсендіру кодын немесе кілт файлын қолмен қосуды ұсынамыз.

Басқару топтары арасында құрылғыларды автоматты түрде жылжыту ережелері

Басқару топтары арасында құрылғыларды автоматты түрде жылжыту үшін ережелерді пайдалануды шектеу ұсынылады.

Автоматты түрде жылжыту ережелерін пайдалану, құрылғыға жылжытуға дейінгіден көбірек артықшылықтар беретін саясаттар таратуға әкелуі мүмкін.

Клиент құрылғысын басқа басқару тобына жылжыту, оған саясат параметрлерінің таралуына әкелуі мүмкін. Бұл саясат параметрлері қонақ ретіндегі және сенімсіз құрылғыларға тарату үшін қажет болмауы мүмкін.

Бұл ұсыныс құрылғыларды басқару топтары бойынша бастапқы таратуға қолданылмайды.

Тарату нүктелері мен қосылым шлюздері бар құрылғыларға арналған қауіпсіздік талаптары

Желілік агент орнатылған құрылғыларды тарату нүктесі ретінде пайдалануға және келесі функцияларды орындауға болады:

- Басқару серверінен алынған жаңартулар мен орнату пакеттерін топтағы клиент құрылғыларына тарату.
- Клиент құрылғыларында үшінші тарап бағдарламаларын және Kaspersky бағдарламаларын қашықтан орнату.
- Жаңа құрылғыларды анықтау және бұрыннан белгілі құрылғылар туралы ақпаратты жаңарту мақсатымен желіні сұрастыру. Тарату нүктесі Басқару серверімен бірдей құрылғыларды табу әдістерін қолдануы мүмкін.

Ұйымның желісінде тарату нүктелерін орналастыру мыналар үшін қолданылады:

- Басқару серверіне түсетін жүктемені азайту;
- трафикті оңтайландыру;
- Басқару серверіне желінің жетуі қиын бөліктеріндегі құрылғыларға қатынасу мүмкіндік беру.

Қолжетімді мүмкіндіктерді ескере отырып, рұқсат етілмеген қатынасудың кез келген түрінен тарату нүктелері ретінде әрекет ететін құрылғыларды, соның ішінде физикалық түрде қорғау ұсынылады.

Тарату нүктелерін автоматты түрде тағайындауды шектеу

Басқаруды жеңілдету және желінің жұмыс істеу қабілетін сақтау үшін тарату нүктелерін автоматты түрде тағайындауды пайдалануды ұсынамыз. Дегенмен, өнеркәсіптік және шағын желілерде тарату нүктелерін автоматты түрде тағайындаудан аулақ болу ұсынылады, өйткені тарату нүктелеріне, мысалы, операциялық жүйе құралдарының көмегімен мәжбүрлеп қашықтан орнату тапсырмаларын орындау үшін пайдаланылатын есептік жазбалардың құпия мәліметін беруге болады.

Өнеркәсіптік және шағын желілерде тарату нүктелерін қолмен тағайындауға болады.

Қажет болса, Тарату нүктелерінің әрекетіндегі есепті де қарап шығуға болады.

Kaspersky Security Center Linux пайдаланушыларының құрылғыларына арналған қауіпсіздік талаптары

Kaspersky Security Center Linux пайдаланушыларының құрылғыларына арнайы қауіпсіздік талаптары қолданылуы керек. Бұл құрылғыларды кез келген рұқсатсыз кіруден (соның ішінде физикалық) қорғауды ұсынамыз.

Kaspersky Security Center Linux пайдаланушы құрылғыларына мыналар кіреді:

- Kaspersky Security Center Linux пайдаланушылары браузер арқылы Kaspersky Security Center Web Console-ге қосылатын құрылғылар.
- OpenAPI арқылы басқару серверімен әрекеттесетін қолданбалардан Kaspersky Security Center Linux жүйесіне қосылған құрылғылар.

Kaspersky Security Center Web Console орнатылған құрылғыларға арналған қауіпсіздік талаптары

Kaspersky Security Center Web Console орнатылған құрылғылар Kaspersky Security Center Linux жүйесін басқару үшін пайдаланылады, сондықтан бұл құрылғылардың қауіпсіздігіне арнайы талаптар қолданылуы керек. Бұл құрылғыларды кез келген рұқсатсыз кіруден (соның ішінде физикалық) қорғауды ұсынамыз.

Басқарылатын қолданбалар қорғанысын конфигурациялау

Басқарылатын қолданба саясаттары

Kaspersky Security Center Linux (желілік агент, Kaspersky Endpoint Security for Windows, Kaspersky Endpoint Security for Linux, Kaspersky Endpoint Agent және т.б.) пайдаланылатын қолданбалары мен құрамдастарының әр түрі үшін саясат жасауға кеңес береміз. Бұл топтық саясат барлық басқарылатын құрылғыларға (түбірлік басқару тобына) немесе конфигурацияланған жылжыту ережелеріне сәйкес жаңа басқарылатын құрылғылар автоматты түрде кіретін бөлек топқа қолданылуы керек.

Қорғанысты өшіру және қолданбаны жою үшін құпиясөзді орнату

Қаскүнемдер Kaspersky қауіпсіздік қолданбаларын өшірмеуі немесе жоймауы үшін, құпия сөзбен қорғауды қосу ұсынылады. Құпиясөзбен қорғауға қолдау көрсететін платформаларда, мысалы, Kaspersky Endpoint Security, желілік агент және басқа Kaspersky қолданбалары үшін құпиясөз орнатуға болады. Құпия сөзбен қорғауды қосқаннан кейін бұл параметрлерді "құлыппен" жабу арқылы құлыптау ұсынылады.

Клиенттік құрылғыны Басқару серверге қолмен қосу үшін құпия сөзді көрсету (klmover утилитасы)

klmover утилитасы клиенттік құрылғыны Басқару серверге қолмен қосуға мүмкіндік береді. klmover утилитасы Желілік агентті орнату қалтасында орналасқан.

Зиянкестер құрылғыларды Басқару серверіңіздің басқаруынан шығаруына жол бермеу үшін klmover утилитасын іске қосқан кезде құпия сөзбен қорғауды міндетті түрде қосу ұсынылады. Құпиясөз қорғанысын қосу үшін Желілік агент саясаты параметрлерінде **Жою құпиясөзін пайдалану** опциясын таңдаңыз.

klmover утилитасына жергілікті әкімші құқықтары қажет.

Енді Kaspersky Security Center Linux басқармайтын құпиясөзбен қорғалған құрылғыда орнатылған желілік агенттің құпиясөзін жоғалтып алсаңыз немесе ұмытып қалсаңыз, klmover утилитасын немесе пәрмен жолын пайдаланып, желілік агентті жоя алмайсыз. Бұл жағдайда құпиясөзбен қорғалған желілік агент орнатылған құрылғыда операциялық жүйені қайта орнату қажет.

Windows құрылғыларында **Жою құпиясөзін пайдалану** опциясы қосылса, Cleaner құралы (cleaner.exe) үшін құпиясөз қорғанысы да қосылады.

Kaspersky Security Network қолдану

Басқарылатын қолданбалардың барлық саясаттарында және Басқару серверінің сипаттарында Kaspersky Security Network (KSN) пайдалану және ағымдағы KSN мәлімдемесін қабылдау ұсынылады. Басқару серверін жаңарту кезінде сіз жаңартылған KSN мәлімдемесін де қабылдай аласыз. Бұлттық қызметтерді пайдалануға заңнамамен немесе өзге де нормативтік актілермен тыйым салынған жағдайларда, KSN қызметін қоса алмайсыз.

Басқарылатын құрылғыларды жүйелі түрде тексеру

Барлық құрылғылар топтары үшін құрылғыларды толықтай тексеруді кезең-кезең іске қосатын тапсырманы жасау ұсынылады.

Жаңа құрылғыларды табу

Құрылғыны табу параметрлерін дұрыс конфигурациялау: домен контроллерлерімен интеграцияны орнату және жаңа құрылғыларды табу үшін IP мекенжайлары ауқымдарын көрсету ұсынылады.

Қауіпсіздік мақсатында, сіз барлық жаңа құрылғыларды қамтитын әдепкі бойынша басқару тобын және осы топқа қолданылатын әдепкі бойынша саясаттарды пайдалана аласыз.

Басқару серверіне техникалық қызмет көрсету

Басқару сервері деректерін сақтық көшірмелеу

Деректердің сақтық көшірмесі Басқару сервері деректерін жоғалтпай қалпына келтіруге мүмкіндік береді.

Әдепкі бойынша, сақтық көшірмелеу тапсырмасы Kaspersky Security Center орнатылғаннан кейін автоматты түрде жасалады және сақтық көшірмелерді тиісті директорияда сақтай отырып, мерзімді түрде орындалады.

Пайдаланушы сақтық көшірмелеу тапсырмасының параметрлерін өзгерте алады:

- резервтік көшірмелеу жиілігін арттыру;
- көшірмелерді сақтау үшін ерекше директорияны анықтау;
- сақтық көшірме құпиясөзін өзгерту.

Сақтық көшірмелерді әдепкі бойынша директориядан басқа директориядан сақтаған кезде, осы директорияның ACL шегін шектеу ұсынылады. Басқару серверінің есептік жазбалары мен Басқару серверінің дерекқоры серверінің осы директорияда жазуға қатынасу рұқсаты болуы керек.

Басқару серверіне техникалық қызмет көрсету

Басқару серверіне қызмет көрсету арқасында дерекқор көлемін қысқартуға, бағдарлама жұмысының өнімділігі мен сенімділігін арттыруға болады. Басқару серверіне аптасына бір реттен сиретпей техникалық қызмет көрсету ұсынылады.

Басқару серверіне техникалық қызмет көрсету тиісті тапсырманың көмегімен орындалады. Басқару серверіне техникалық қызмет көрсету барысында бағдарлама келесі әрекеттерді орындайды:

- дерекқордың индекстерін қайта құрады;
- дерекқордың статистикасын жаңартады;
- дерекқорды қысады (қажет болса).

Басқару сервері бар құрылғыдағы операциялық жүйені және үшінші тарап бағдарламалық жасақтамасын жаңарту

Басқару сервері бар құрылғыда операциялық жүйе мен үшінші тарап бағдарламалық жасақтамасының жаңартуларын жүйелі түрде орнату ұсынылады.

Клиент құрылғыларына Басқару серверіне тұрақты қосылым қажет емес, сондықтан жаңартуларды орнатқаннан кейін құрылғыны Басқару серверімен қауіпсіз қайта жүктеуге болады. Басқару сервері әрекетсіз тұрғанда клиент құрылғыларында тіркелген барлық оқиғалар, қосылым қалпына келтірілгеннен кейін оған жіберіледі.

Оқиғаларды үшінші тарап жүйелеріне беру

Бақылау және есеп беру

Қауіпсіздік мәселелеріне дер кезінде жауап беру үшін бақылау және есеп беру функцияларын конфигурациялауға болады.

Оқиғаларды SIEM жүйелеріне экспорттау

Елеулі нұқсан келтірілмей тұрып, мәселелерді мүмкіндігінше тез анықтау үшін оқиғаларды SIEM жүйесіне жіберуді пайдалану ұсынылады.

Аудит оқиғалары туралы электрондық пошта арқылы хабарландыру

Kaspersky Security Center Linux бағдарламасы, басқарылатын бағдарламаларға орнатылған Kaspersky Басқару сервері мен бағдарламаларының жұмысы барысында орын алған оқиғалар туралы ақпаратты алуға мүмкіндік береді. Орын алған төтенше жағдайларға дер кезінде жауап беру үшін Басқару серверін ол жариялайтын аудит оқиғалары, критикалық оқиғалар, функционалдық ақаулар және ескертулер туралы хабарландыруларды жіберуге конфигурациялау ұсынылады.

Аудит оқиғалары жүйеішілік болғандықтан, олар сирек тіркеледі және мұндай оқиғалар туралы хабарландырулардың саны пошта жіберілімі үшін әбден қолайлы.

Үшінші тарап ақпараттық жүйелерінің қауіпсіздігі бойынша ұсыныстар

CIS Benchmarks қауіпсіздік бойынша ұсыныстары

Басқару сервері және Желілік агент қолдайтын операциялық жүйелердің, виртуализация платформаларының немесе дерекқор серверлерінің нұсқаларын пайдаланған кезде, бұл ақпараттық жүйелерді дәл конфигурациялау үшін Center for Internet Security (CIS) ақпаратты қорғау әдістерін, егер олар бар болса, пайдалану ұсынылады.

Center for Internet Security (CIS) – ақпараттық технологиялар саласындағы қауіпсіздікті арттырумен айналысатын коммерциялық емес ұйым. Атап айтқанда, CIS ұйымы CIS Controls және CIS Benchmarks сияқты қауіпсіздік стандарттарын әзірлейді және таратады. Бұл стандарттар ақпараттық жүйелердің қауіпсіздігін қамтамасыз ету бойынша ұсыныстар мен тәжірибелердің жиынтығы болып табылады.

CIS МД порталында Басқару сервері және Желілік агент қолдау көрсететін келесі ақпараттық жүйелердің нұсқалары үшін ұсыныстар бар:

- Келесі отбасылардың операциялық жүйелері:
  - Жұмыс станцияларына арналған Windows
  - Серверлерге арналған Windows
  - Debian
  - Ubuntu
  - CentOS

    - Oracle Linux
    - Red Hat Enterprise Linux
    - SUSE Linux Enterprise Server
    - macOS
- VMware виртуализация платформалары
- Дерекқор серверлері:
    - Microsoft SQL Server
    - MySQL
    - MariaDB
    - PostgreSQL

Astra Linux операциялық жүйесі үшін қауіпсіздік ұсыныстары

Astra Linux операциялық жүйесін пайдаланған кезде Astra Linux сәйкес нұсқасы үшін Red Book атты кітапта сипатталған қауіпсіздік ұсыныстарын ұстану керек.

РЕД ОС операциялық жүйесі үшін қауіпсіздік ұсыныстары

RED OS операциялық жүйесін пайдаланған кезде, RED OS ресми құжаттамасында сипатталған әкімші нұсқаулығындағы қауіпсіздік ұсыныстарын орындау керек.

Kaspersky қауіпсіздік қолданбаларын пайдалануға қатысты ұсыныстар

Kaspersky Endpoint Security for Windows бағдарламасында KLAdmin құпиясөзін пайдалану

KLAdmin есептік жазбасы — Kaspersky Endpoint Security for Windows қолданбасына шексіз кіру рұқсаты бар әкімші есептік жазбасы. KLAdmin есептік жазбасы, қолданбаны жоюды қоса алғанда, Kaspersky Endpoint Security for Windows қолданбасында құпиясөзбен қорғалған кез келген әрекетті орындауға құқылы. KLAdmin есептік жазбасының құқықтарын қайтарып алу мүмкін емес. KLAdmin есептік жазбасы үшін құпиясөзді Kaspersky Endpoint Security for Windows саясат сипаттарында орнатуға болады. Kaspersky Endpoint Security for Windows әкімшісі KLAdmin есептік жазбасына арналған құпиясөзді қауіпсіз пайдалануға толықтай жауапты. Ұйымыңыздың жеке құпиясөз саясаты болса, сол саясаттағы нұсқауларды орындаңыз. Құпиясөз неғұрлым ұзын және күрделі болса, соғұрлым ол қауіпсіз болады.

Ұйымыңызды KLAdmin құпиясөзін ұрлаудан қорғау үшін мына қадамдарды орындаңыз:

- **Жалпы талаптар.**

  Есептік жазба атын немесе атының бір бөлігін құпиясөз ретінде пайдаланбаңыз.

- **Құпиясөздің минималды ұзындығына қойылатын талаптар.**

  Кемінде 10 таңбадан тұратын құпиясөз жасаңыз.

- **Бірнеше таңба түрін пайдалану талаптары.**

  Әртүрлі санаттағы таңбаларды қамтитын күрделі құпиясөз орнатыңыз: кіші және бас әріптер, сандар және арнайы таңбалар.

- **Құпиясөздің жарамдылық мерзіміне қойылатын талаптар.**

  Құпиясөздің минималды жарамдылық мерзімін 90 күнге орнатыңыз. Жаңа құпиясөз соңғы 24 құпиясөздің ешқайсысымен бірдей болмауы керек.

Сценарий: MySQL Server серверінің аутентификациясы

MySQL серверінің аутентификациясы үшін TLS сертификатын пайдалану ұсынылады. Сенімді сертификаттау орталығының (CA) сертификатын немесе өздігінен қол қойылған сертификатты қолдана аласыз.

Басқару сервер MySQL үшін бір жақты және екі жақты SSL аутентификациясына қолдау көрсетеді.

Бір жақты SSL аутентификациясын қосу

MySQL үшін бір жақты SSL аутентификациясын орнату мақсатында мына қадамдарды орындаңыз:

1. **MySQL сервері үшін өздігінен қол қойылған TLS сертификатын жасау.**

   Келесі пәрменді орындаңыз:

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

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

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

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

2. **Сервер жалаушасының файлын жасау**

   Klscflag утилитасын пайдаланып, KLSRV_MYSQL_OPT_SSL_CA сервері жалаушасын жасаңыз және оның мәндері ретінде сертификатқа жолды көрсетіңіз: Klscflag утилитасы Басқару сервер орнатылған каталогте орналасқан. Әдепкі бойынша жол - /opt/kaspersky/ksc64/sbin.

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

3. **Дерекқорды конфигурациялаңыз**

   my.cnf файлында сертификаттарды көрсетіңіз. Мәтіндік редакторда my.cnf файлын ашыңыз және [mysqld] бөліміне келесі жолдарды қосыңыз:

```
[mysqld]

ssl-ca=".../mysqlcerts/ca-cert.pem"

ssl-cert=".../mysqlcerts/server-cert.pem"

ssl-key=".../mysqlcerts/server-key.pem"
```

Екі жақты SSL аутентификациясын қосу

MySQL үшін екі жақты SSL аутентификациясын орнату мақсатында мына қадамдарды орындаңыз:

1. **Сервер жалауша файлдарын жасау**

   Klscflag утилитасын пайдаланып, сервер жалаушаларын жасаңыз және олардың мәндері ретінде сертификат файлдарына жолды көрсетіңіз:

   ```
   klscflag -fset -pv klserver -n KLSRV_MYSQL_OPT_SSL_CA -v <жолы: ca-cert.pem> -t s

   klscflag -fset -pv klserver -n KLSRV_MYSQL_OPT_SSL_CERT -v <жолы: server-cert.pem> -t
   s

   klscflag -fset -pv klserver -n KLSRV_MYSQL_OPT_SSL_KEY -v <жолы: server-key.pem> -t s
   ```

   Klscflag утилитасы Басқару сервер орнатылған каталогте орналасқан. Әдепкі бойынша жол - /opt/kaspersky/ksc64/sbin.

2. **Құпия сөйлемді көрсетіңіз (міндетті емес)**

   Егер server-key.pem кодты сөйлемді қажет етсе, KLSRV_MARIADB_OPT_TLS_PASPHRASE жалаушасын жасаңыз және кодты сөйлемді оның мәні ретінде көрсетіңіз:

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

3. **Дерекқорды конфигурациялаңыз**

   my.cnf файлында сертификаттарды көрсетіңіз. Мәтіндік редакторда my.cnf файлын ашыңыз және [mysqld] бөліміне келесі жолдарды қосыңыз:

   ```
   [mysqld]

   ssl-ca=".../mysqlcerts/ca-cert.pem"

   ssl-cert=".../mysqlcerts/server-cert.pem"

   ssl-key=".../mysqlcerts/server-key.pem"
   ```

Сценарий: PostgreSQL Server серверінің аутентификациясы

PostgreSQL серверінің аутентификациясы үшін TLS сертификатын пайдалану ұсынылады. Сенімді сертификаттау орталығының (CA) сертификатын немесе өздігінен қол қойылған сертификатты қолдана аласыз.

Басқару сервер PostgreSQL үшін бір жақты және екі жақты SSL аутентификациясына қолдау көрсетеді.

PostgreSQL серверінің аутентификациясы кезең-кезеңімен жүзеге асырылады:

1. **PostgreSQL сервері үшін сертификат жасау**

Келесі пәрмендерді орындаңыз:

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

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

2. **Басқару сервері үшін сертификат жасау**

Келесі пәрмендерді орындаңыз. CN мәні Басқару сервер атынан PostgreSQL-ге қосылатын пайдаланушының атына сәйкес болуы керек. Әдепкі пайдаланушы аты - postgres.

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

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

3. **Клиент сертификатының аутентификациясын конфигурациялау**

pg_hba.conf келесідей өзгертіңіз:

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

pg_hba.conf ішінде `host` деп басталатын жазба жоқ екеніне көз жеткізіңіз.

4. **PostgreSQL сертификатын көрсету**

Бір жақты SSL аутентификациясы

postgresql.conf файлын келесідей өзгертіңіз (.crt және .key файлдарына дұрыс жолды көрсетіңіз):

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

Екі жақты SSL аутентификациясы

postgresql.conf файлын келесідей өзгертіңіз (.crt және .key файлдарына дұрыс жолды көрсетіңіз):

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

5. **PostgreSQL демонын қайта іске қосу**

Келесі пәрменді орындаңыз:

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

6. **Басқару сервері үшін сервер жалаушасын көрсету**

Бір жақты SSL аутентификациясы

Klscflag утилитасын пайдаланып, KLSRV_POSTGRES_OPT_SSL_CA сервері жалаушасын жасаңыз және оның мәндері ретінде сертификатқа жолды көрсетіңіз:

Пәрмен жолын іске қосыңыз және ағымдағы каталогты klscflag утилитасы бар каталогке өзгертіңіз. Klscflag утилитасы Басқару сервер орнатылған каталогте орналасқан. Әдепкі бойынша жол - /opt/kaspersky/ksc64/sbin.

Келесі пәрменді орындаңыз:

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

Екі жақты SSL аутентификациясы

Klscflag утилитасын пайдаланып, сервер жалаушаларын жасаңыз және олардың мәндері ретінде сертификат файлдарына жолды көрсетіңіз.

Пәрмен жолын іске қосыңыз және ағымдағы каталогты klscflag утилитасы бар каталогке өзгертіңіз. Klscflag утилитасы Басқару сервер орнатылған каталогте орналасқан. Әдепкі бойынша жол - /opt/kaspersky/ksc64/sbin.

Келесі пәрмендерді орындаңыз:

```
klscflag -fset -pv klserver -n KLSRV_POSTGRES_OPT_SSL_CA -v <жолы: psql.crt> -t s
klscflag -fset -pv klserver -n KLSRV_POSTGRES_OPT_SSL_CERT -v <жолы: postgres.crt> -t s
klscflag -fset -pv klserver -n KLSRV_POSTGRES_OPT_SSL_KEY -v <жолы: postgres.key> -t s
```

Егер `postgres.key` кодты сөйлемді қажет етсе, KLSRV_POSTGRES_OPT_TLS_PASPHRASE жалаушасын жасаңыз және кодты сөйлемді оның мәні ретінде көрсетіңіз:

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

7. **Басқару сервері қызметін қайта іске қосу**

Орналастыруға дайындық

Бұл бөлімде ұйым қажеттіліктеріне сай Kaspersky Security Center Linux орналастыру, Kaspersky Security Center Linux конфигурациялау және ДҚБЖ конфигурациялау опциясын таңдау әдісі сипатталған.

Келесі шарттарға сәйкес ұйым желісінде Kaspersky Security Center Linux құрамдастарын орналастырудың бірнеше опциясы бар:

- Құрылғылардың жалпы санын
- Ұйымдық немесе географиялық оқшауланған бөлімшелердің (кеңселер, филиалдар) болуы
- Тар арналармен байланған оқшауланған желілердің болуы
- Интернеттен Басқару серверіне қатынасу қажеттілігі

Бір басқару сервері 50 000-ға дейін құрылғыға қызмет көрсете алады (ДҚБЖ ретінде PostgreSQL немесе Postgres Pro көмегімен). Егер ұйымның желісіндегі құрылғылардың жалпы саны 50 000-нан асса, орталықтандырылған басқаруды жеңілдету үшін иерархияға біріктірілген бірнеше Басқару серверлерін ұйымның желісіне орналастыру керек.

Егер ұйымның құрамында өз әкімшілері бар үлкен географиялық қашықтағы кеңселер (филиалдар) болса, осы кеңселерде Басқару серверлерін орналастырған жөн. Болмаса бұл кеңселерді өткізу қабілеті төмен арналар арқылы байланысқан ажыратылған арналар ретінде көру керек. "Стандартты конфигурация: өзіндік әкімшілері бар бірнеше үлкен кеңсе" мақаласын қараңыз.

Егер тар арналармен байланысқан оқшауланған желілер болса, мұндай желілердегі трафикті үнемдеу үшін бір немесе бірнеше Желілік агентті тарату нүктелері етіп тағайындау керек (тарату нүктелерінің санын есептеу үшін кестені қараңыз). Бұл жағдайда, оқшауланған желінің барлық құрылғылары осындай "жергілікті жаңарту орталықтарынан" жаңартулар алады. Нақты тарату нүктелері жаңартуларды әкімші серверінен (әдепкі сценарий) және интернеттегі Kaspersky серверлерінен жүктеп ала алады ("Стандартты конфигурация: қашықтағы көптеген шағын кеңселер" мақаласын қараңыз).

"Kaspersky Security Center Linux типтік конфигурациялары" бөлімінде Kaspersky Security Center Linux типтік конфигурацияларының егжей-тегжейлі сипаттамасы берілген. Орналастыруды жоспарлау кезінде, ұйымның құрылымына байланысты, ең қолайлы типтік конфигурацияны таңдау керек.

Орналастыруды жоспарлау кезеңінде Басқару серверіне X.509 арнайы сертификатын белгілеу қажеттілігін ескеру қажет. Басқару серверіне X.509 арнайы сертификатын белгілеу келесі жағдайларда орынды болуы мүмкін (толық емес тізім):

- SSL трафигін SSL termination proxy арқылы инспекциялау үшін немесе Reverse Proxy қолдану үшін;
- ұйымның жалпыға ортақ кілті (PKI) инфрақұрылымымен біріктіру үшін;
- сертификат өрістерінің қажетті мәндерін белгілеу үшін;
- сертификаттың қажетті криптографиялық беріктігін қамтамасыз ету үшін.

Kaspersky Security Center Linux конфигурациясын таңдау

Бұл бөлімде ұйымның желісінде Kaspersky Security Center Linux құрамдастарын орналастырудың келесі типтік конфигурациялары сипатталған:

- Бір кеңсе
- Өзіндік әкімшілері бар бірнеше ірі географиялық бөлінген кеңселер
- Көптеген шағын географиялық бөлінген кеңселер

Типтік конфигурация: бір кеңсе

Ұйымның желісінде бір немесе бірнеше Басқару сервері орналастырылуы мүмкін. Серверлер саны қолжетімді аппараттық жасақтаманың болуына байланысты, сондай-ақ басқарылатын құрылғылардың жалпы санына байланысты таңдалуы мүмкін.

Бір Басқару сервер 50 000-нан аспайтын құрылғыға қызмет көрсете алады (PostgreSQL немесе Postgres Pro көмегімен ДҚБЖ ретінде). Таяу болашақта басқарылатын құрылғылардың санын көбейту мүмкіндігін ескеру қажет: бір Басқару серверіне біршама аз құрылғыларды қосу қажет болуы мүмкін.

Басқару серверлері ішкі желіде де, демилитаризацияланған аймақта да орналастырылуы мүмкін, бұл интернеттен Басқару серверлеріне қатынасу қажет пе екендігіне байланысты.

Егер бірнеше Сервер болса, оларды иерархияға біріктіру ұсынылады. Басқару серверлерінің иерархиясының болуы саясат пен тапсырмалардың қайталануын болдырмауға, барлық басқарылатын құрылғылардың көпшілігімен олардың барлығы бір Басқару серверімен басқарылатындай жұмыс істеуге (яғни құрылғыларды іздеуге, құрылғы таңдауларын жасауға, есептер жасауға) мүмкіндік береді.

Типтік конфигурация: өзіндік әкімшілері бар бірнеше үлкен кеңсе

Бірнеше ірі қашықтағы кеңсе болған кезде, әр кеңседе Басқару серверлерін орналастыру мүмкіндігі туралы ойлану керек. Клиент құрылғыларының санына және қолжетімді аппараттық жасақтамаға байланысты әр кеңседе бір немесе бірнеше Басқару серверінен. Бұл жағдайда, кеңселердің әрбірі "Типтік конфигурация: бір кеңсе" ретінде қарастырылуы мүмкін. Басқаруды жеңілдету үшін барлық Басқару серверлері иерархияға, бәлкім, көп деңгейлі иерархияға біріктірілуі керек.

Егер кеңселер арасында құрылғылармен (ноутбуктермен) бірге орын ауыстыратын қызметкерлер болса, Желілік агент саясатында Желілік агентті қосу профильдері жасалуы керек.

Типтік конфигурация: қашықтағы көптеген шағын кеңселер

Бұл типтік конфигурация бір бас кеңсені және интернет арқылы бас кеңсеге хабарласа алатын көптеген шағын қашықтағы кеңселерді ұсынады. Қашықтағы кеңселердің әрқайсысы Network Address Translation (бұдан әрі - NAT) артында орналасқан, яғни бір қашықтағы кеңседен екіншісіне қосылу мүмкін емес, кеңселер бір-бірінен оқшауланған.

Бас кеңседе Басқару серверін орналастыру керек, ал қалған кеңселерде бір немесе бірнеше тарату нүктесін тағайындау керек. Кеңселер арасындағы байланыс интернет арқылы жүзеге асырылатындықтан, тарату нүктелері үшін *Жаңартуларды тарату орындарының қоймаларына жүктеп алу* тапсырмасын, тарату нүктелері жаңартуларды Басқару серверінен емес, тікелей Kaspersky серверлерінен, жергілікті немесе желілік қалталардан жүктеп алатындай етіп жасаған жөн.

Егер қашықтағы кеңседе құрылғылардың бір бөлігі Басқару серверіне тікелей қатынаса алмаса (мысалы, Басқару серверіне интернет арқылы қатынасады, бірақ интернетке құрылғылардың барлығы бірдей қатынаса алмайды), онда тарату нүктелерін шлюз режиміне ауыстыру керек. Бұл жағдайда, қашықтағы кеңседегі құрылғылардағы Желілік агенттер Басқару серверіне тікелей емес, шлюз арқылы қосылады (синхрондау мақсатында).

Көп жағдайда басқару сервері қашықтағы кеңседегі желіге сауалнама жүргізе алмайтындықтан, бұл функцияны орындауды тарату нүктелерінің біріне жүктеген жөн.

Басқару сервері қашықтағы кеңседе NAT артында орналасқан басқарылатын құрылғыларға 15000 UDP портына хабарландыру жібере алмайды. Бұл мәселені шешу үшін тарату нүктелері болып табылатын құрылғылардың сипаттарында Басқару серверіне тұрақты қосылым режимін қосуға болады (**Басқару серверімен байланысты үзбеу** жалаушасы). Егер тарату нүктелерінің жалпы саны 300-ден аспаса, бұл режим қолжетімді болады. Басқарылатын құрылғы мен Басқару сервері арасындағы тұрақты байланысты қамтамасыз ету үшін push серверлерін пайдаланыңыз. Мәліметтер алу үшін келесі мақаланы қараңыз: Push серверін қосу.

Ұйымның қорғаныс құрылымын таңдау

Ұйымның қорғаныс құрылымын таңдау келесі факторларды анықтайды:

- Ұйым желісінің топологиясы.
- Ұйымдық құрылым.

- Желіні қорғауға жауапты қызметкерлердің саны және олардың арасындағы міндеттерді бөлу.
- Қорғанысты басқару құрамдастарын орнатуға бөлінуі мүмкін аппараттық ресурстар.
- Ұйымның желісіндегі қорғаныс құрамдастарының жұмысына бөлінуі мүмкін байланыс арналарының өткізу қабілеті.
- Ұйым желісіндегі маңызды басқару операцияларын орындаудың рұқсат етілген уақыты. Маңызды басқару операцияларына, мысалы, антивирустық дерекқордың жаңартуларын тарату және клиент құрылғыларына арналған саясатты өзгерту кіреді.

Қорғаныс құрылымын таңдағанда, алдымен орталықтандырылған қорғаныс жүйесін басқаруға болатын қолжетімді желілік және аппараттық ресурстарды анықтау ұсынылады.

Желілік және аппараттық инфрақұрылымды талдау үшін келесі әрекеттер тәртібі ұсынылады:

1. Қорғаныс орналастырылатын желінің келесі параметрлерін анықтау:
   - желі сегменттері саны;
   - желінің жеке сегменттері арасындағы байланыс арналарының жылдамдығы;
   - желі сегменттерінің әрқайсысында басқарылатын құрылғылар саны;
   - қорғаныстың жұмыс істеуі үшін бөлінуі мүмкін әрбір байланыс арнасының өткізу қабілеттілігі.
2. Барлық басқарылатын құрылғылар үшін өзекті басқару операцияларының рұқсат етілген орындалу уақытын анықтау.
3. 1 және 2 тармақтарындағы ақпаратты, сондай-ақ басқару серверін жүктемелік тестілеу деректерін талдау. Жүргізілген талдау негізінде келесі сұрақтарға жауап беріңіз:
   - Барлық клиенттерге бір Басқару серверімен қызмет көрсету мүмкін бе немесе Басқару серверлері иерархиясы қажет пе?
   - 2-тармақта анықталған уақыт ішінде барлық клиенттерге қызмет көрсету үшін Басқару серверінің қандай аппараттық конфигурациясы қажет?
   - Байланыс арналарына түсетін жүктемені азайту үшін тарату нүктелерін пайдалану қажет пе?

Аталған сұрақтарға жауап бергеннен кейін, сіз ұйымның рұқсат етілген қорғаныс құрылымдарының жиынтығын жасай аласыз.

Ұйымның желісінде келесі типтік қорғаныс құрылымдарының бірін пайдалануға болады:

- Бір Басқару сервері. Барлық клиент құрылғылары бір Басқару серверіне қосылған. Тарату нүктесінің рөлін Басқару сервері атқарады.
- Тарату нүктелері бар бір Басқару сервері. Барлық клиент құрылғылары бір Басқару серверіне қосылған. Желіде тарату нүктелерінің рөлін атқаратын клиент құрылғылары көрсетілген.

- Басқару серверлерінің иерархиясы. Желінің әрбір сегменті үшін Басқару серверінің жалпы иерархиясына қосылған бөлек Басқару сервері бөлектелген. Тарату нүктесінің рөлін негізгі Басқару сервері атқарады.

- Тарату нүктелері бар Басқару серверлерінің иерархиясы. Желінің әрбір сегменті үшін Басқару серверінің жалпы иерархиясына қосылған бөлек Басқару сервері бөлектелген. Желіде тарату нүктелерінің рөлін атқаратын клиент құрылғылары көрсетілген.

Қорғаныс жүйесін орналастырудың типтік тәсілдері

Бұл бөлімде Kaspersky Security Center көмегімен ұйымның желісінде қорғаныс жүйесін орналастырудың типтік тәсілдері сипатталған.

Жүйені барлық түрлердің рұқсатсыз қатынасуынан қорғауды қамтамасыз ету қажет. Бағдарламаны құрылғыға орнатпас бұрын, операциялық жүйеге арналған барлық қолжетімді қауіпсіздік жаңартуларын орнатып, Басқару серверлері мен тарату нүктелерін физикалық қорғауды қамтамасыз ету ұсынылады.

Келесі орналастыру схемаларын қолдана отырып, Kaspersky Security Center көмегімен ұйымның желісінде қорғаныс жүйесін орналастыруға болады:

- Kaspersky Security Center және Kaspersky Security Center Web Console арқылы қорғау жүйесін орналастыру.

  Kaspersky бағдарламаларын клиент құрылғыларына орнату және клиент құрылғыларын Басқару серверіне қосу Kaspersky Security Center көмегімен автоматты түрде жүзеге асырылады.

- Kaspersky Security Center бағдарламасында құрылған жеке орнату пакеттері арқылы қорғаныс жүйесін қолмен орналастыру.

  Kaspersky бағдарламаларын клиент құрылғыларына және әкімшінің жұмыс станциясына орнату қолмен жүргізіледі, клиент құрылғыларын Басқару серверіне қосу параметрлері Желілік агентті орнату кезінде белгіленеді.

  Бұл орналастыру нұсқасын қашықтан орнату мүмкін болмаған жағдайда қолдану ұсынылады.

Kaspersky Security Center Microsoft Active Directory® топтық саясаттарды пайдаланып орналастыруға қолдау көрсетпейді.

ДҚБЖ таңдау

Төмендегі кестеде ДҚБЖ рұқсат етілген нұсқалары және оларды ұсынымдары мен қолдану шектеулері аталған.

ДҚБЖ ұсынымдар және шектеулер

ДҚБЖ	Ұсынымдар және шектеулер
MySQL (қолдау көрсетілетін нұсқаларды қараңыз)	20 000-нан аз құрылғылар үшін бір Басқару серверін пайдалануды жоспарласаңыз, осы ДҚБЖ пайдаланыңыз.
MariaDB (қолдау көрсетілетін нұсқаларды қараңыз)	20 000-нан аз құрылғылар үшін бір Басқару серверін пайдалануды жоспарласаңыз, осы ДҚБЖ пайдаланыңыз.

PostgreSQL, Postgres Pro (қолдау көрсетілетін нұсқаларды қараңыз)	50 000-нан аз құрылғылар үшін бір Басқару серверін пайдалануды жоспарласаңыз, осы ДҚБЖ пайдаланыңыз.
Tantor (қолдау көрсетілетін нұсқаларды қараңыз)	50 000-нан аз құрылғылар үшін бір Басқару серверін пайдалануды жоспарласаңыз, осы ДҚБЖ пайдаланыңыз. Tantor-ға ДҚБЖ тек Astra Linux Special Edition RUSB.10015-01 арнайы шығарылымында (1.8 операциялық жаңарту) қолдау көрсетіледі.

Таңдалған ДҚБЖ жүйесін қалай орнату керектігі туралы мәліметтер оның құжаттамасында келтірілген.

Қолданбалық жасақтаманы түгендеу тапсырмасын өшіру және Басқару сервердің қолданбаларды іске қосу туралы хабарландыруларын өшіру (Kaspersky Endpoint Security саясатының параметрлерінде) ұсынылады.

Егер сіз PostgreSQL немесе Postgres Pro ДҚБЖ орнатуды шешсеңіз, суперпайдаланушының құпиясөзін енгізгеніңізге көз жеткізіңіз. Егер құпиясөз көрсетілмесе, Басқару сервері дерекқорға қосылмауы мүмкін.

MySQL, MariaDB, PostgreSQL немесе Postgres Pro орнатсаңыз, ДҚБЖ дұрыс жұмыс істеуін қамтамасыз ету үшін ұсынылатын параметрлерді қолданыңыз.

PostgreSQL, MariaDB немесе MySQL ДҚБЖ пайдалансаңыз, **Оқиғалар** қойындысы таңдалған клиент құрылғысы үшін оқиғалардың толық тізімін көрсетпеуі мүмкін. Бұл, ДҚБЖ оқиғалардың өте көп санын сақтаған кезде орын алады. Келесі әрекеттердің бірін орындау арқылы көрсетілетін оқиғалар санын көбейтуге болады:

- Керек емес оқиғаларды жою.
- Керек емес оқиғаларды сақтау мерзімін қысқарту.

Құрылғы үшін Басқару серверінде тіркелген оқиғалардың толық тізімін көру үшін Есептерді пайдаланыңыз.

Басқару серверіне интернеттен қатынасуды ұсыну

Кейбір жағдайларда интернеттен Басқару серверіне қатынасу мүмкіндігін ұсыну қажет:

- Kaspersky дерекқорларын, бағдарламалық модульдерін және бағдарламаларын үнемі жаңарту.
- Үшінші тарап бағдарламаларын жаңарту

  Әдепкі бойынша, Басқару сервері Microsoft бағдарламасының жаңартуларын басқарылатын құрылғыларға орнату үшін интернет байланысын қажет етпейді. Мысалы, басқарылатын құрылғылар Microsoft бағдарламасының жаңартуларын тікелей Microsoft жаңарту серверлерінен немесе ұйымыңыздың желісінде орналастырылған Microsoft Windows Server Update Services (WSUS) қызметтері бар Windows Server серверінен жүктей алады. Басқару сервері келесі жағдайларда интернетке қосылуы керек:

  - Басқару серверін WSUS сервері ретінде пайдаланған кезде.
  - Microsoft бағдарламаларынан басқа үшінші тарап бағдарламаларының жаңартуларын орнату үшін.
- Үшінші тарап бағдарламаларында осалдықтарды түзету

Басқару серверін интернетке қосу келесі тапсырмаларды орындау үшін қажет:

- Microsoft бағдарламалық жасақтама осалдықтарының ұсынылған түзетулер тізімін жасау. Тізімді Kaspersky мамандары қалыптастырады және үнемі жаңартып отырады.
- Microsoft қолданбаларынан басқа үшінші тарап қолданбаларындағы осалдықтарды түзету.

- Автономды пайдаланушылардың құрылғыларын (ноутбуктарын) басқару үшін.
- Қашықтағы кеңселердегі құрылғыларды басқару үшін.
- Қашықтағы кеңселерде орналасқан негізгі немесе қосалқы Басқару серверлерімен өзара әрекеттесу кезінде.
- ұялы құрылғыларды басқару үшін

Бұл бөлімде интернеттен Басқару серверіне қатынасуды қамтамасыз етудің типтік тәсілдері қарастырылған. Интернеттен Басқару серверіне қатынасуды қамтамасыз етудің барлық жағдайларында Басқару серверіне арнайы сертификат белгілеу қажет болуы мүмкін.

Интернеттен қатынасу: жергілікті желідегі Басқару сервері

Басқару сервері ұйымның ішкі желісінде орналасса, сіз 13000 TCP Басқару серверінің портын "Port Forwarding" механизмі арқылы сырттан қолжетімді ете аласыз.

Интернеттен қатынасу: Демилитаризацияланған аймақтағы Басқару сервері

Басқару сервері ұйым желісінің демилитаризацияланған аймағында орналасса, онда ол ұйымның ішкі желісіне қатынаса алмайды. Соның салдарынан, келесі шектеулер қойылады:

- Басқару сервері жаңа құрылғыларды өз бетінше анықтай алмайды.
- Басқару сервері ұйымның ішкі желісінің құрылғыларына мәжбүрлеп орнату арқылы Желілік агентті бастапқы орналастыруды орындай алмайды.

  Мәселе тек Желілік агентті бастапқы орнату туралы. Желілік агент нұсқасының кейінгі жаңартуларын немесе қауіпсіздік бағдарламасын орнатуды Басқару сервері жүзеге асыра алады.

Kaspersky Security Center Linux жүйесі Microsoft Windows топтық саясаттарын пайдаланып орналастыруға қолдау көрсетпейтінін ескеріңіз.

Ұйымыңыздың желісінде орналасқан тарату нүктелерін пайдалануға болады. Бастапқы орналастыруды Желілік агенті жоқ құрылғыларда орындау үшін алдымен Желілік агентті құрылғылардың біріне орнатып, сол құрылғыны тарату нүктесіне тағайындау керек. Нәтижесінде, Желілік агентті басқа құрылғыларға бастапқы орнатуды осы тарату нүктесі арқылы Басқару сервері жүзеге асырады.

Хабарландыруларды ұйымның ішкі желісінде орналасқан басқарылатын құрылғыларға 15000 UDP портына сәтті жіберу үшін кәсіпорынның бүкіл желісін тарату нүктелерімен қамту керек. Тағайындалған тарату нүктелерінің сипаттарында **Басқару серверімен байланысты үзбеу** жалаушасын қойыңыз. Нәтижесінде, Басқару сервері тарату нүктелерімен тұрақты байланысады, ал тарату нүктелері хабарландыруларды ұйымның ішкі желісінде орналастырылған құрылғыларға 15000 UDP портына жібере алады (бұл IPv4 желісі немесе IPv6 желісі болуы мүмкін).

Орнату

Бұл бөлімде Kaspersky Security Center Linux және Kaspersky Security Center Web Console бағдарламаларын орнату жолы сипатталған.

Kaspersky Security Center Linux нұсқасымен жұмыс істеу үшін MariaDB x64 серверінің конфигурациясы

MariaDB x64 серверін Kaspersky Security Center-мен жұмыс істеу мақсатында сәтті конфигурациялау үшін осы мақалада көрсетілген сервер параметрлерін қоспағанда, әдепкі сервер параметрлерін пайдалану керек.

my.cnf файлы үшін ұсынылатын параметрлер

ДҚБЖ параметрі туралы толық ақпаратты есептік жазбаны конфигурациялау процедурасынан қараңыз. ДҚБЖ туралы ақпарат алу үшін ДҚБЖ орнату процедурасын қараңыз.

my.cnf файлын конфигурациялау үшін:

1. Мәтіндік редактор көмегімен my.cnf файлын ашыңыз.

2. my.cnf файлының [mysqld] бөліміне келесі жолдарды енгізіңіз:

```
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=< нақты мәні KAV дерекқорының күтілетін өлшемінің 80%-ынан
кем болмауы керек >
innodb_thread_concurrency=20
innodb_flush_log_at_trx_commit=0
innodb_lock_wait_timeout=300
max_allowed_packet=32M
max_connections=151
max_prepared_stmt_count=12800
table_open_cache=60000
table_open_cache_instances=4
table_definition_cache=60000
sql_mode="STRICT_TRANS_TABLES,NO_AUTO_CREATE_USER,NO_ENGINE_SUBSTITUTION"
```

`innodb_buffer_pool_size` мәні KAV дерекқорының күтілетін өлшемінің 80 пайызынан кем болмауы тиіс. Сервер іске қосылғанда көрсетілген жадтың бөлінетінің ескеріңіз. Егер дерекқор өлшемі көрсетілген буфер өлшемінен аз болса, тек қажетті жад бөлінеді. MariaDB 10.4.3 немесе одан бұрынғы нұсқасын пайдалансаңыз, нақты бөлінген жад көрсетілген буфер өлшемінен шамамен 10 пайызға үлкен.

`innodb_flush_log_at_trx_commit=0` параметрінің мәнін қолдану ұсынылады, себебі "1" немесе "2" мәндері MariaDB жұмыс жылдамдығына теріс әсерін тигізеді. `innodb_file_per_table` параметрінің `1` мәніне орнатылғанын тексеріңіз.

MariaDB 10.1 үшін [mysqld] бөліміне қосымша ретінде келесі жолақтарды енгізіңіз:

```
innodb_file_format='Barracuda'
innodb_default_row_format=dynamic
innodb_large_prefix=1
```

MariaDB 10.6 үшін [mysqld] бөліміне қосымша ретінде келесі жолақтарды енгізіңіз:

```
optimizer_prune_level=0
optimizer_search_depth=8
```

Әдепкі бойынша оптимизатордың `join_cache_incremental`, `join_cache_hashed` және `join_cache_bka` конфигурациялары қосулы. Егер бұл баптаулар қосылмаған болса, оларды қосу керек.

Оптимизатор баптауларының қосулы ма екенін тексеру үшін:

1. MariaDB клиент консолінде келесі пәрменді іске қосыңыз:

   ```
   SELECT @@optimizer_switch;
   ```

2. Шықпасы келесі жолдарды қамтитынына көз жеткізіңіз:

   ```
   join_cache_incremental=on
   join_cache_hashed=on
   join_cache_bka=on
   ```

   Бұл жолдар бар болып, `on` мәндерін қамтыса, онда оптимизатор баптаулары қосулы.

   Бұл жолдар жоқ болса немесе `off` мәндері ие болса, келесі әрекеттерді орындаңыз:

   a. Мәтіндік редактор көмегімен my.cnf файлын ашыңыз.

   b. my.cnf файлға келесі жолдарды қосыңыз:

   ```
   optimizer_switch='join_cache_incremental=on'
   optimizer_switch='join_cache_hashed=on'
   optimizer_switch='join_cache_bka=on'
   ```

`join_cache_incremental`, `join_cache_hash` және `join_cache_bka` баптаулары қосулы.

Жүктеме кезінде тұрақтылықты қамтамасыз ету үшін MariaDB systemd қызметі үшін ашуға болатын файлдардың (файл сипаттамаларының) әдепкі шегін арттырыңыз.

Файл сипаттамаларының шегін арттыру үшін:

1. Келесі пәрменді орындаңыз:

   ```
   sudo systemctl edit mariadb.service
   ```

2. `[Service]` бөлімінің `LimitNOFILE` параметрінде файл дескрипторларының шегін көрсетіңіз:

   ```
   LimitNOFILE=1048576
   ```

3. Параметрлердің дұрыстығына көз жеткізу үшін келесі пәрменді іске қосыңыз:

   ```
   sudo systemd-analyze verify mariadb.service
   ```

4. systemd процесін қайта бастау үшін келесі пәрменді іске қосыңыз:

   ```
   sudo systemctl daemon-reload
   ```

5. MariaDB қызметін қайта іске қосу үшін келесі пәрменді орындаңыз:

   ```
   sudo systemctl restart mariadb.service
   ```

   Файл дескрипторларының шегі енді ұлғайтылды.

Kaspersky Security Center Linux бағдарламасымен жұмыс істеу үшін PostgreSQL немесе Postgres Pro серверін конфигурациялау

Kaspersky Security Center Linux жүйесімен жұмыс істеу үшін PostgreSQL немесе Postgres Pro серверін сәтті конфигурациялау үшін осы мақалада көрсетілген сервер параметрлерін қоспағанда, әдепкі сервер параметрлерін пайдалану керек.

Kaspersky Security Center Linux бағдарламасы PostgreSQL және Postgres Pro ДҚБЖ қолдайды. Егер сіз осы ДҚБЖ-нің біреуін қолдансаңыз, ДҚБЖ жүйесі мен Kaspersky Security Center Linux бағдарламасының жұмысын оңтайландыру үшін ДҚБЖ серверінің параметрлерін конфигурациялау мүмкіндігін қарастырыңыз.

Конфигурация файлының әдепкі бойынша жолы: `/etc/postgresql/< НҰСҚА >/main/postgresql.conf`

Linux ALT операциялық жүйесінде әдепкі жол - `/var/lib/pgsql/data/postgresql.conf`

PostgreSQL және Postgres Pro үшін ұсынылатын параметрлер:

- `max_connections = 151`

  Postgres ДҚБЖ кластерін пайдалансаңыз, барлық ДҚБЖ сервері үшін, сондай-ақ кластер конфигурациясында `max_connections` параметрін көрсетіңіз.

- `shared_buffers` = N

  N = ДҚБЖ үшін болжамды ЖЖҚ өлшемінің 25%-ы. Егер ДҚБЖ Басқару серверінің жанындағы құрылғыға орнатылған болса, есептеу құрылғының жалпы ЖЖҚ-на емес, ДҚБЖ үшін бөлінген ЖЖҚ-ға негізделуі керек.

  Егер жедел жад 1 ГБ-тан аз болса, онда әдепкі бойынша мәнді қалдырыңыз.

- `temp_buffers = 24MB`

- `work_mem = 16MB`

- `maintenance_work_mem = 128MB`

- `max_stack_depth` = стектің максималды өлшемі (осы КБ мәнін алу үшін '`ulimit -s`' пәрменін орындаңыз) минус 1 МБ

- `max_parallel_workers_per_gather = 0`

- `standard_conforming_strings` = on

Postgres Pro 15.7 немесе Postgres Pro 15.7.1 пайдалансаңыз, `enable_compound_index_stats` опциясын өшіріңіз:

```
enable_compound_index_stats = off
```

Конфигурацияны қолданыңыз немесе конфигурация файлын жаңартқаннан кейін ДҚБЖ серверін қайта іске қосыңыз.

PostgreSQL және Postgres Pro серверінің параметрлері, сондай-ақ осы параметрлерді қалай көрсету керектігі туралы толық ақпаратты ДҚБЖ бойынша тиісті құжаттамадан қараңыз.

PostgreSQL және Postgres Pro үшін есептік жазбаларды жасау және конфигурациялау туралы қосымша ақпаратты келесі бөлімінен қараңыз: PostgreSQL және Postgres Pro жүйелерімен жұмыс істеу үшін есептік жазбаларды конфигурациялау.

Жоғары қолжетімділіктегі ДҚБЖ кластерін қалай конфигурациялау керектігі туралы толық ақпарат алу үшін келесі мақаланы қараңыз: Kaspersky Security Center Linux жүйесімен жұмыс істеу үшін жоғары қолжетімділіктегі ДҚБЖ кластерін дайындау.

Kaspersky Security Center Linux нұсқасымен жұмыс істеу үшін MySQL x64 серверінің конфигурациясы

MySQL x64 серверін Kaspersky Security Center-мен пайдалану мақсатында сәтті конфигурациялау үшін осы мақалада көрсетілген сервер параметрлерін қоспағанда, әдепкі сервер параметрлерін пайдалану керек.

Kaspersky Security Center үшін MySQL серверін қолдансаңыз, InnoDB және MEMORY қоймасы қолдауын, сондай-ақ UTF-8 және UCS-2 кодтамасы қолдауын қосыңыз.

my.cnf файлы үшін ұсынылатын параметрлер

ДҚБЖ параметрі туралы толық ақпаратты есептік жазбаны конфигурациялау процедурасынан қараңыз. ДҚБЖ туралы ақпарат алу үшін ДҚБЖ орнату процедурасын қараңыз.

my.cnf файлын конфигурациялау үшін:

1. Мәтіндік редактор көмегімен my.cnf файлын ашыңыз.
2. my.cnf файлының `[mysqld]` бөліміне келесі жолдарды қосыңыз:

```
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=< нақты мәні KAV дерекқорының күтілетін өлшемінің 80%-ынан
кем болмауы керек >
innodb_thread_concurrency=20
innodb_flush_log_at_trx_commit=0 (көп жағдайда сервер шағын транзакцияларды
пайдаланады)
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
```

`innodb_buffer_pool_size` ішінде көрсетілген жад сервер іске қосылғанда бөлінетін ескеріңіз. Егер дерекқор өлшемі көрсетілген буфер өлшемінен аз болса, тек қажетті жад бөлінеді. Бөлінген жадтың нақты өлшемі көрсетілген буфер өлшемінен шамамен 10 пайызға үлкен. Қосымша ақпарат алу үшін MySQL құжаттамасын қараңыз.

`innodb_flush_log_at_trx_commit = 0` параметрінің мәнін қолдану ұсынылады, себебі "1" немесе "2" мәндері MySQL жұмыс жылдамдығына теріс әсерін тигізеді. `innodb_file_per_table` параметрінің `1` мәніне орнатылғанын тексеріңіз.

Жоғары қолжетімділікті ДҚБЖ кластерін Kaspersky Security Center Linux жүйесімен жұмыс істеуге дайындау

Kaspersky Security Center Linux келесі жоғары қолжетімділік кластерлерін қолдайды:

- Platform V Pangolin
- Postgres Pro кіріктірілген жоғары деңгейдегі қолжетімділік
- Patroni (қосымша HAProxy жүктеме теңгергішімен)

Репликация түрі синхронды күйге орнатылуы керек.

Егер сіз PostgreSQL үшін Patroni үлгісінің 3.3.1 немесе одан бұрынғы нұсқасын пайдалансаңыз, `synchronous_standby_names` параметрі дұрыс қолданылғанына көз жеткізіңіз. Синхронды репликацияның пайдаланылғанын тексеру үшін, басты түйінде келесі сұранысты орындаңыз:

```
SELECT application_name, client_addr, client_hostname, client_port, sync_state
FROM pg_stat_replication;
```

Егер кез келген торап үшін `sync_state` бағанында `sync` немесе `potential` мәндерінен басқа мәндер көрсетілсе, кластер қолдау көрсетілмейтін асинхронды репликацияны пайдаланады. Бұл мәселені шешу үшін келесі әрекеттердің кез келгенін орындаңыз:

- Patroni бағдарламасын 3.3.2 немесе одан жаңа нұсқасына жаңартыңыз.
- Patroni конфигурация файлында, `bootstrap` бөлімінің `dcs` кіші бөлімін орнатыңыз және `true` параметріне `synchronous_mode` белгілеңіз:

  `bootstrap:`

  `dcs:`

  `<...>`

  `synchronous_mode: true`

Ұсынылатын ең аз жоғары қолжетімділік ДҚБЖ кластерінің конфигурациясы кемінде үш түйінді қамтуы керек.

Platform V Pangolin ДҚБЖ жоғары деңгейдегі қолжетімділік кластерін Kaspersky Security Center Linux жүйесімен жұмыс істеуге дайындау үшін:

1. Kaspersky Security Center Linux-пен жұмыс істеу үшін PostgreSQL немесе Postgres Pro серверін конфигурациялау.

2. Егер сіз Басқару серверінің кластер түйіндерінің мекенжайларын автоматты түрде табуын қаласаңыз, сондықтан орнату бағдарламасы кезінде тек негізгі кластер түйінінің немесе көшірме кластер түйінінің DNS атауын немесе IP мекенжайын көрсету қажет болса, келесі қадамдарды орындаңыз:

   a. Конфигурация файлын /etc/pangolin-manager/postgres.yml (егер Platform V Pangolin пайдалансаңыз) немесе /etc/postgresql/<VERSION>/main/postgresql.conf (егер Postgres Pro кірістірілген жоғары деңгейдегі қолжетімділік кластерін пайдалансаңыз) барлық жоғары деңгейдегі қолжетімділік кластер түйіндерінде ДҚБЖ конфигурациясының конфигурация файлын `postgresql` бөліміне келесі сызықты қосу арқылы өзгертіңіз:

   `log_hostname=1`

   Басқа конфигурация файлының параметрлері үшін PostgreSQL және Postgres Pro үшін ұсынылған параметр мәндерін пайдалануға болады.

   b. Барлық ДҚБЖ жоғары деңгейдегі қолжетімділік кластері түйіндеріндегі ДҚБЖ кластерлік қызметі.

   c. Дерекқор пайдаланушысының `pg_read_all_stats` артықшылығы бар екеніне көз жеткізіңіз. Бұл артықшылықты келесі пәрменді іске қосу арқылы беруге болады:

   `GRANT pg_read_all_stats TO "%1";`

   Бұл жерде `%1` — дерекқор пайдаланушысының аты.

   Пайдаланушы аты `KLSRV_UNATT_DBMS_LOGIN` параметрінде басқару серверін орнатқан кезде көрсетіледі.

   d. IAM дерекқоры үшін жүктеме теңгергішін конфигурациялаңыз. Таңдаған жүктеме теңгергішінің құжаттамасын қараңыз.

Platform V Pangolin ДҚБЖ жоғары деңгейдегі қолжетімділік кластері Kaspersky Security Center Linux жүйесімен жұмыс істеуге дайын.

Kaspersky Security Center Linux орнату

Бұл бөлімде Kaspersky Security Center Linux орнату тәсілі сипатталған.

Орнатпай тұрып, келесі әрекеттерді орындауыңыз қажет:

- Kaspersky Security Center Linux үшін ДҚБЖ-ны орнатыңыз. Қолдау көрсетілетін ДҚБЖ-ның бірін таңдай аласыз. Таңдалған ДҚБЖ жүйесін қалай орнату керектігі туралы мәліметтер оның құжаттамасында келтірілген.

  Егер Linux негізіндегі операциялық жүйеңіздің дистрибутивінде қолдау көрсетілетін ДҚБЖ болмаса, ДҚБЖ жүйесін үшінші тарап пакеттер қоймасынан орнатуға болады.

ДҚБЖ орнатқаннан кейін, сәйкес нұсқауды орындаңыз:

- Kaspersky Security Center Linux бағдарламасымен жұмыс істеу үшін PostgreSQL немесе Postgres Pro серверін конфигурациялау

  PostgreSQL және Postgres Pro жүйесімен жұмыс істеу үшін ДҚБЖ есептік жазбасын конфигурациялау

  Егер сіз Басқару серверінің кластер түйіндерінің мекенжайларын автоматты түрде табуын қаласаңыз, сондықтан орнату кезінде тек негізгі түйіннің немесе көшірме түйінінің DNS атауын немесе IP мекенжайын көрсету қажет болса, келесі мақаладағы нұсқаулықтың 2-қадамын орындағаныңызға көз жеткізіңіз: Kaspersky Security Center Linux бағдарламасымен жұмыс істеу үшін жоғары қолжетімділіктегі ДҚБЖ кластерін дайындау.

- Kaspersky Security Center Linux нұсқасымен жұмыс істеу үшін MariaDB x64 серверінің конфигурациясы

  MySQL және MariaDB-мен жұмыс істеу үшін ДҚБЖ есептік жазбасын конфигурациялау

- Kaspersky Security Center Linux нұсқасымен жұмыс істеу үшін MySQL x64 серверінің конфигурациясы

  MySQL және MariaDB-мен жұмыс істеу үшін ДҚБЖ есептік жазбасын конфигурациялау

- Kaspersky Security Center Linux орнатқыңыз келетін құрылғыда қолдау көрсетілетін Linux дистрибутивтерінің бірі жұмыс істейтініне көз жеткізіңіз.

  > RED OS 7.3.4 не одан кейінгі немесе MSVSPHERE 9.2 не одан кейінгі операциялық жүйені пайдалансаңыз, басқару серверінің дұрыс жұмыс істеуіне арналған libxcrypt-compat пакетін орнатыңыз.

- Желіде DNS серверінің қолжетімді екеніне көз жеткізіңіз.

- Kaspersky веб-сайтынан орнату файлын жүктеп алыңыз. Құрылғыда орнатылған Linux дистрибутивіне сәйкес орнату файлын таңдаңыз — sc64_[нұсқа_нөмірі]_amd64.deb немесе ksc64-[нұсқа_нөмірі].x86_64.rpm.

> Kaspersky Security Center Linux жүйесін орнату үшін төмендегі нұсқауларда көрсетілген пәрмендерді root құқықтары бар есептік жазба астында орындауыңыз керек.

Kaspersky Security Center Linux орнату үшін:

1. "kladmins" тобын және артықшылықсыз "ksc" және "ksciam" есептік жазбаларын жасаңыз. Есептік жазбалар "kladmins" тобының мүшесі болуы керек. Ол үшін келесі пәрмендерді ретімен орындаңыз:

   ```
   adduser ksc
   ```

   ```
   groupadd kladmins
   ```

   ```
   gpasswd -a ksc kladmins
   ```

   ```
   usermod -g kladmins ksc
   ```

   ```
   adduser ksciam
   ```

   ```
   gpasswd -a ksciam kladmins
   ```

   ```
   usermod -g kladmins ksciam
   ```

2. ДҚБЖ серверінде IAM үшін дерекқор жасаңыз. Дерекқор атауы Kaspersky Security Center Linux бағдарламасымен жұмыс істеу үшін орнатылған дерекқордан басқаша болуы керек. Басқару сервері серверді жою немесе басқа құрылғыға жылжыту кезінде IAM дерекқорын автоматты түрде өшірмейді, дерекқорды қолмен өшіру керек.

   - PostgreSQL үшін келесі пәрменді іске қосыңыз:

     ```
     sudo -i -u postgres psql -U postgres -c "CREATE DATABASE <iam_db_name>;"
     ```

   - MariaDB үшін келесі пәрменді іске қосыңыз:

     ```
     sudo mysql -u root -p -e "CREATE DATABASE <iam_db_name>;"
     ```

3. Жоғары деңгейдегі қолжетімділік ДҚБЖ кластерін пайдалансаңыз, келесі қадамдарды орындаңыз:

   a. 'ksc' пайдаланушысына `pg_read_all_stats` артықшылығын беріңіз:

      ```
      GRANT pg_read_all_stats TO "ksc";
      ```

   b. Конфигурация файлын /etc/pangolin-manager/postgres.yml (егер Platform V Pangolin пайдалансаңыз) немесе /etc/postgresql/main/postgresql.conf (егер Postgres Pro кірістірілген жоғары деңгейдегі қолжетімділік кластерін пайдалансаңыз) барлық жоғары деңгейдегі қолжетімділік кластер түйіндерінде ДҚБЖ конфигурациясының конфигурация файлын өзгертіңіз. Кластерді Kaspersky Security Center Linux жүйесіне қосу кезінде негізгі түйіннің DNS атауын немесе IP мекенжайын немесе көшірме түйінін ғана көрсетсеңіз, `postgresql` бөліміне келесі жолды қосыңыз:

      ```
      log_hostname: '1'
      ```

   c. /etc/pangolin-manager/postgres.yml конфигурация файлын өңдегеннен кейін, ДҚБЖ кластері қызметін барлық жоғары деңгейдегі қолжетімділік ДҚБЖ кластер түйіндерінде (төрелік түйіннен басқа) келесідей қайта іске қосыңыз:

      ```
      systemctl restart pangolin-manager.service
      ```

      Немесе

      ```
      systemctl restart postgresql-<version>
      ```

4. Қажет болса, басқару сервері қызметтерінің функциясы үшін қолданылатын есептік жазбаларға ашуға болатын (файл дескрипторлары) файлдардың әдепкі шегін арттырыңыз. Ол үшін /etc/security/limits.conf файлын ашып, жұмсақ және қатты файл дескрипторының шектеулерін төмендегідей көрсетіңіз:

   ```
   ksc  soft  nofile  <max_number_of_opened_files>
   ```

   ```
   ksc  hard  nofile  <max_number_of_opened_files>
   ```

   Әдепкісінше файл дескрипторларының шектері орнату кезінде көрсетіледі. Жұмсақ файл шегі — 32 768 файл, қатты файл шегі — 131 072 файл.

5. Kaspersky Security Center Linux орнатуды іске қосыңыз. Linux дистрибутивіңізге байланысты келесі пәрмендердің бірін орындаңыз:

```
sudo apt-get install /<path>/ksc64_<version_number>_amd64.deb
```

```
sudo yum install /<path>/ksc64-<version_number>.x86_64.rpm
```

6. Kaspersky Security Center Linux конфигурациясын іске қосыңыз:

```
/opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl
```

7. Лицензиялық келісімді және Құпиялылық саясатын оқыңыз. Мәтін пәрмен жолы терезесінде көрсетіледі. Мәтіннің келесі бөлігін көру үшін бос орын пернесін басыңыз. Сұрау көрсетілген кезде келесі мәндерді енгізіңіз:

   a. Лицензиялық келісімнің шарттарын түсініп, қабылдасаңыз, `y` енгізіңіз. Лицензиялық келісімнің шарттарын қабылдамасаңыз, `n` енгізіңіз. Kaspersky Security Center Linux бағдарламасын пайдалану үшін Лицензиялық келісімнің шарттарын қабылдау керек.

   b. Құпиялық саясатының шарттарын түсінсеңіз және қабылдасаңыз және деректеріңіз Құпиялылық саясатына сәйкес өңделетініне және жіберілетініне (соның ішінде үшінші елдерге) келіссеңіз `y` енгізіңіз. Құпиялық саясатының шарттарын қабылдамасаңыз, `n` енгізіңіз. Kaspersky Security Center Linux жүйесін пайдалану үшін Құпиялық саясатының шарттарын қабылдауыңыз керек.

8. Сұрау көрсетілген кезде келесі параметрлерді енгізіңіз:

   a. Басқару серверінің орнату режимі ретінде **Стандарт** таңдаңыз.

   b. Басқару серверінің DNS атын немесе статикалық IP мекенжайын енгізіңіз. Бұл мекенжайды басқа құрылғылар Басқару серверіне қосылу үшін пайдаланады.

   c. Басқару сервері SSL портының нөмірін енгізіңіз. Әдепкі бойынша порт нөмірі – 13000.

   d. Басқаруды жоспарлап отырған құрылғылардың шамамен санын есептеңіз:

      - 1-100 басқарылатын құрылғыңыз болса, 1 санын енгізіңіз.
      - 101-1000 басқарылатын құрылғыңыз болса, 2 санын енгізіңіз.
      - 1000-нан көп басқарылатын құрылғыңыз болса, 3 санын енгізіңіз.

      Бұл параметр желі жүктемесін оңтайландыру үшін тапсырманың автоматты түрде рандомизацияланған кешігуі үшін пайдаланылады. Төмендегі тізімде кідіріс есептелетін аралық көрсетілген:

      - 1-100 басқарылатын құрылғы, 1 мәні. Кідіріс қолданылмайды.
      - 101-1000 басқарылатын құрылғы, 2 мәні. Кідіріс 5 минут.
      - 1000-нан көп басқарылатын құрылғы, 3 мәні. Кідіріс 10 минут.

   e. Қызметтер үшін қауіпсіздік тобының атын енгізіңіз. Әдепкісінше `kladmins` тобы пайдаланылады.

f. Басқару сервері қызметін іске қосу үшін есептік жазбаның атауын енгізіңіз. Есептік жазба көрсетілген қауіпсіздік тобының мүшесі болуы керек. Әдепкісінше `ksc` есептік жазбасы пайдаланылады.

g. Басқа қызметтерді іске қосу үшін есептік жазбаның атауын енгізіңіз. Есептік жазба көрсетілген қауіпсіздік тобының мүшесі болуы керек. Әдепкісінше `ksc` есептік жазбасы пайдаланылады.

h. Kaspersky Security Center Linux бағдарламасымен жұмыс істеу үшін орнатылған ДҚБЖ таңдаңыз:

- MySQL немесе MariaDB орнатқан болсаңыз, 1 енгізіңіз.
- PostgreSQL немесе Postgres Pro SQL орнатқан болсаңыз, 2 енгізіңіз.

i. Басқару серверінің ДҚБЖ орнатылған құрылғысының DNS атауын немесе IP мекенжайын енгізіңіз. Жергілікті ДҚБЖ орнату үшін әдепкі бойынша – 127.0.0.1.

Жоғары қолжетімді ақауларға төзімді кластерді пайдалану үшін келесі әрекеттердің бірін орындаңыз:

- Барлық түйіндердің DNS атауларын немесе IP мекенжайларын және порттарын келесі пішімде енгізіңіз:

```
<fqdn1>:<port>,<fqdn2>:<port>,<...><fqdnX>:<port>;
```

- Тек негізгі түйіннің немесе реплика түйінінің DNS атауын немесе IP мекенжайын көрсетіңіз.

j. Дерекқор портының нөмірін енгізіңіз. Бұл порт Басқару серверімен байланысу үшін пайдаланылады. Егер сіз 8.h қадамында барлық жоғары қолжетімді кластер түйіндерінің DNS атауларын немесе IP мекенжайларын және порттарын енгізсеңіз, бұл қадам өткізіп жіберіледі.

Әдепкі бойынша келесі порттар пайдаланылады:

- MySQL немесе MariaDB үшін `3306` порты.
- PostgreSQL немесе Postgres Pro үшін `5432` порты.

k. Дерекқор атауын енгізіңіз.

l. Дерекқорға қатынасу үшін пайдаланылатын дерекқордың әкімші есептік жазбасының атауын енгізіңіз.

m. Дерекқорға қатынасу үшін пайдаланылатын дерекқордың әкімші есептік жазбасының құпия сөзін енгізіңіз.

n. Егер сіз PostgreSQL немесе Postgres Pro орнатқан болсаңыз, Басқару сервері пайдаланатын дерекқор схемасын көрсете аласыз. Ол үшін схема атауын көрсетіңіз.

> Схема атауы регистрге сезімтал: тек кіші әріптерді пайдалану керек.

Егер сіз арнайы схеманы пайдаланғыңыз келмесе, ENTER пернесін басыңыз, сонда әдепкі схема қолданылады.

o. IAM серверінің FQDN атауын енгізіңіз. Бұл айнымалыны көрсетпесеңіз, басқару сервері орнатылған құрылғының DNS атауы пайдаланылады.

8a-қадамда енгізген Басқару серверінің DNS атауын көрсетуіңіз керек.

p. IAM қызметін іске қосу үшін есептік жазба атауын енгізіңіз. Есептік жазба көрсетілген қауіпсіздік тобының мүшесі болуы керек. Әдепкісінше ksciam есептік жазбасы пайдаланылады.

q. IAM қызметімен жұмыс істеу үшін орнатылған ДҚБЖ таңдаңыз:

- MySQL немесе MariaDB орнатқан болсаңыз, 1 енгізіңіз.
- PostgreSQL немесе Postgres Pro SQL орнатқан болсаңыз, 2 енгізіңіз.

r. IAM қызметі пайдаланатын IAM ДҚБЖ мекенжайын енгізіңіз.

Жоғары қолжетімді кластерді пайдалану үшін келесі әрекеттердің бірін орындаңыз:

- Барлық түйіндердің DNS атауларын немесе IP мекенжайларын және порттарын келесі пішімде енгізіңіз:

```
<fqdn1>:<port>,<fqdn2>:<port>,<...><fqdnX>:<port>;
```

- Жүктеме теңгергішінің тек DNS атауын немесе IP мекенжайын көрсетіңіз.

s. IAM ДҚБЖ порт нөмірін енгізіңіз. Бұл порт IAM қызметімен байланысу үшін пайдаланылады. Егер сіз 8.p қадамында барлық жоғары қолжетімді кластер түйіндерінің DNS атауларын немесе IP мекенжайларын және порттарын енгізсеңіз, бұл қадам өткізіп жіберіледі.

Әдепкі бойынша келесі порттар пайдаланылады:

- MySQL немесе MariaDB үшін 3306 порты
- PostgreSQL немесе Postgres Pro үшін 5432 порты

t. IAM қызметі пайдаланатын IAM дерекқор атауын енгізіңіз. IAM қызметі пайдаланатын дерекқордың атауы басқару сервері пайдаланатын дерекқордан өзгеше болуы керек.

u. IAM дерекқорына кіру үшін пайдаланылатын дерекқор есептік жазбасының атауын енгізіңіз.

v. IAM дерекқорына кіру үшін пайдаланылатын дерекқор есептік жазбасының құпиясөзін енгізіңіз.

Қызметтердің қосылуын және автоматты түрде іске қосылуын күтіңіз:

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

w. Егер сіз PostgreSQL немесе Postgres Pro орнатқан болсаңыз, IAM пайдаланатын дерекқор схемасын көрсете аласыз. Ол үшін схема атауын көрсетіңіз.

Егер сіз арнайы схеманы пайдаланғыңыз келмесе, ENTER пернесін басыңыз, сонда жалпы схема қолданылады.

Схема атауы регистрге сезімтал: тек кіші әріптерді пайдалану керек.
Резервтелген IAM схемаларының атауларын көрсетпеңіз: client, iam, ksc, locker, pat, scope, voltron.

x. Басқару серверінің әкімшісінің рөлін орындайтын есептік жазбаны жасаңыз. Пайдаланушының аты мен құпиясөзін енгізіңіз.

Құпиясөз келесі ережелерге сәйкес келуі керек:

- Пайдаланушының құпиясөзі 8 таңбадан кем немесе 256 таңбадан аспауы керек.
- Құпиясөзде төмендегі тізімдегі кемінде үш топтың таңбалары болуы керек:
  - Бас әріптер (A-Z)
  - Кіші әріптер (a-z)
  - Сандар (0-9)
  - Арнайы таңбалар (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)

Егер Сіз бұл қадамды өткізіп жіберсеңіз, кейінірек жаңа пайдаланушы жасау үшін келесі пәрменді пайдалана аласыз:

```
/opt/kaspersky/ksc64/sbin/kladduser -n kscadmin -p <password>
```

Пайдаланушы қосылды және Kaspersky Security Center Linux орнатылды.

Желілік агентті орнату

Басқару сервері бар құрылғыны басқарылатын басқа құрылғылар сияқты басқару үшін басқару сервері бар құрылғыға Linux жүйесіне арналған желілік агентті орнатыңыз. Бұл жағдайда Linux үшін Желілік агент орнатылады және Басқару серверімен бірге орнатылған Желілік агенттің сервер нұсқасына қарамастан тәуелсіз жұмыс істейді.

Қызметтерді тексеру

Қызметтің іске қосылғанын тексеру үшін келесі пәрмендерді пайдаланыңыз:

- `systemctl status klnagent_srv.service`
- `systemctl status kladminserver_srv.service`
- `systemctl status klactprx_srv.service`
- `systemctl status klwebsrv_srv.service`
- `systemctl status kliam_srv.service`

Kaspersky Security Center Linux бағдарламасын тыныш режимде орнату

Орнатуды дыбыссыз режимде, яғни пайдаланушының араласуынсыз іске қосу үшін жауап файлын пайдаланып, Kaspersky Security Center Linux жүйесін Linux құрылғыларына орнатуға болады. Жауап файлында орнату параметрлерінің реттелетін жиынтықтығы бар: айнымалылар және олардың тиісті мәндері.

Орнату алдында:

- Kaspersky Security Center Linux үшін ДҚБЖ-ны орнатыңыз. Қолдау көрсетілетін ДҚБЖ-ның бірін таңдай аласыз. Таңдалған ДҚБЖ жүйесін қалай орнату керектігі туралы мәліметтер оның құжаттамасында келтірілген.

  Егер Linux негізіндегі операциялық жүйеңіздің дистрибутивінде қолдау көрсетілетін ДҚБЖ болмаса, ДҚБЖ жүйесін үшінші тарап пакеттер қоймасынан орнатуға болады.

  ДҚБЖ орнатқаннан кейін, сәйкес нұсқауды орындаңыз:

  - Kaspersky Security Center Linux бағдарламасымен жұмыс істеу үшін PostgreSQL немесе Postgres Pro серверін конфигурациялау

    PostgreSQL және Postgres Pro жүйесімен жұмыс істеу үшін ДҚБЖ есептік жазбасын конфигурациялау

    Егер сіз Басқару серверінің кластер түйіндерінің мекенжайларын автоматты түрде табуын қаласаңыз, сондықтан орнату кезінде тек негізгі түйіннің немесе көшірме түйінінің DNS атауын немесе IP мекенжайын көрсету қажет болса, келесі мақаладағы нұсқаулықтың 2-қадамын орындағаныңызға көз жеткізіңіз: Kaspersky Security Center Linux бағдарламасымен жұмыс істеу үшін жоғары қолжетімділіктегі ДҚБЖ кластерін дайындау.

  - Kaspersky Security Center Linux нұсқасымен жұмыс істеу үшін MariaDB x64 серверінің конфигурациясы

    MySQL және MariaDB-мен жұмыс істеу үшін ДҚБЖ есептік жазбасын конфигурациялау

  - Kaspersky Security Center Linux нұсқасымен жұмыс істеу үшін MySQL x64 серверінің конфигурациясы

    MySQL және MariaDB-мен жұмыс істеу үшін ДҚБЖ есептік жазбасын конфигурациялау

- ДҚБЖ орнатылған құрылғыңызда келесідей аталатын ДҚБЖ пайдаланушы есептік жазбалары жоқ екеніне көз жеткізіңіз:

  - client
  - iam
  - ksc
  - locker
  - pat
  - scope
  - voltron

- Kaspersky Security Center Linux орнатқыңыз келетін құрылғыда қолдау көрсетілетін Linux дистрибутивтерінің бірі жұмыс істейтініне көз жеткізіңіз.

  RED OS 7.3.4 не одан кейінгі немесе MSVSPHERE 9.2 не одан кейінгі операциялық жүйені пайдалансаңыз, басқару серверінің дұрыс жұмыс істеуіне арналған libxcrypt-compat пакетін орнатыңыз.

- Kaspersky веб-сайтынан орнату файлын жүктеп алыңыз. Құрылғыда орнатылған Linux дистрибутивіне сәйкес орнату файлын таңдаңыз — sc64_[нұсқа_нөмірі]_amd64.deb немесе ksc64-[нұсқа_нөмірі].x86_64.rpm.

Kaspersky Security Center Linux бағдарламасын тыныш режимде орнату үшін:

1. Лицензиялық келісімді оқып шығыңыз. Лицензиялық келісімнің шарттарын түсініп, қабылдаған жағдайда ғана төмендегі қадамдарды орындаңыз.

2. "kladmins" тобын және "kladmins" тобының мүшелері болуы керек артықшылықсыз "ksc" және "ksciam" есептік жазбаларын жасаңыз. Ол үшін root-құқықтары бар есептік жазба астында келесі пәрмендерді кезекпен орындаңыз:

   `adduser ksc`

   `groupadd kladmins`

   `gpasswd -a ksc kladmins`

   `usermod -g kladmins ksc`

   `adduser ksciam`

   `gpasswd -a ksciam kladmins`

   `usermod -g kladmins ksciam`

3. ДҚБЖ серверінде IAM үшін дерекқор жасаңыз. Дерекқор атауы Kaspersky Security Center Linux бағдарламасымен жұмыс істеу үшін орнатылған дерекқордан басқаша болуы керек. Басқару сервері серверді жою немесе басқа құрылғыға жылжыту кезінде IAM дерекқорын автоматты түрде өшірмейді, дерекқорды қолмен өшіру керек.

   - PostgreSQL үшін келесі пәрменді іске қосыңыз:

     ```
     sudo -i -u postgres psql -U postgres -c "CREATE DATABASE <iam_db_name>;"
     ```

   - MariaDB үшін келесі пәрменді іске қосыңыз:

     ```
     sudo mysql -u root -p -e "CREATE DATABASE <iam_db_name>;"
     ```

4. Жауап файлын (TXT пішімінде) жасаңыз және жауап файлына `VARIABLE_NAME=variable_value` пішіміндегі айнымалылар тізімінің әрбірін бөлек жолға қосыңыз. Жауап файлы төмендегі кестеде көрсетілген айнымалыларды қамтуы керек.

5. Түбірлік немесе пайдаланушы ортасындағы `KLAUTOANSWERS` ортасының жауап файлының толық атауын, соның ішінде жолды қамтитын айнымалы мәнін, мысалы, келесі пәрменді пайдалану арқылы орнатыңыз:

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

6. Kaspersky Security Center Linux орнатуды дыбыссыз режимде бастаңыз және Linux дистрибутивіңізге байланысты келесі пәрмендердің бірін орындаңыз:

   Түбірлік ортада:

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

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

   Пайдаланушы ортасында:

   ```
   sudo -E apt-get install /<path>/ksc64_[version_number]_amd64.deb -y
   ```

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

7. Kaspersky Security Center Web Console-імен жұмыс істеу үшін есептік жазбаны жасаңыз. Ол үшін келесі пәрменді root құқықтары бар есептік жазбамен келесі пәрменді орындаңыз:

   `/opt/kaspersky/ksc64/sbin/kladduser -n kscadmin -p <password>`, мұнда құпиясөз кемінде 8 таңбадан тұруы керек.

8. Kaspersky Security Center Web Console веб-консолін орнатыңыз

Интерактивті емес режимде Kaspersky Security Center Linux орнату параметрлері ретінде пайдаланылатын жауап файлының айнымалылары

Айнымалының атауы	Міндетті	Сипаттамасы	Ықтимал мәндер
EULA_ACCEPTED	Иә	Лицензиялық келісімнің шарттарын түсінетініңізді және қабылдайтыныңызды растайды.	1
PP_ACCEPTED	Иә	Құпиялық саясатының шарттарын түсінетініңізді және қабылдайтыныңызды растайды.	1
KLSRV_UNATT_SERVERADDRESS	Иә	Басқару серверінің DNS атауы немесе статикалық IP мекенжайы.	Құрылғының DNS атауы немесе IP мекенжайы.
KLSRV_UNATT_PORT_SRV	Жоқ	Басқару серверінің порт нөмірі. Қосымша әдепкі мән — 14000.	Порт нөмірі
KLSRV_UNATT_PORT_SRV_SSL	Жоқ	Басқару сервері SSL портының нөмірі. Қосымша әдепкі мән — 13000.	Порт нөмірі
KLSRV_UNATT_PORT_KLOAPI	Жоқ	OpenAPI-мен жұмыс істеуге арналған порт нөмірі. Сондай-ақ бұл порт Kaspersky Security Center Web Console-ден қосылымдарды қабылдау үшін пайдаланылады. Сондай-ақ әдепкі мән — 13299.	Порт нөмірі
KLSRV_UNATT_PORT_GUI	Жоқ	klakaut утилитасымен жұмыс істеуге арналған порт нөмірі. Қосымша әдепкі мән — 13291. klakaut утилитасы және оған арналған анықтамалық жүйе Kaspersky Security Center Linux орнату қалтасында орналасқан. Әдепкі бойынша порт жабық. Kaspersky Security Center Linux жұмысын автоматтандыру үшін klakaut утилитасын пайдаланғыңыз келсе, klscflag утилитасын пайдаланып, 13291 портын ашыңыз.	Порт нөмірі

KLSRV_UNATT_NETRANGETYPE	Жоқ	Басқаруды жоспарлап отырған құрылғылардың шамамен саны. Бұл параметр желі жүктемесін оңтайландыру үшін пайдаланылады. Қосымша әдепкі мән — 1.	1-100 басқарылатын құрылғы үшін 1 101-1000 басқарылатын құрылғы үшін 2 1000-нан көп басқарылатын құрылғы үшін 3
KLSRV_UNATT_DBMS_TYPE	Иә	Дерекқорды басқару жүйесінің түрі: MySQL (MariaDB) немесе Postgres.	mysql немесе postgres
KLSRV_UNATT_DBMS_INSTANCE	Иә	Дерекқор серверінің IP мекенжайы. PostgreSQL, Postgres Pro кірістірілген жоғары деңгейдегі қолжетімділік кластерін немесе Platform V Pangolin ДҚБЖ кластерін пайдалану үшін DNS атауларын немесе IP мекенжайларын және барлық түйіннің порттарын келесі форматта енгізіңіз: <fqdn1>:<port>,<fqdn2>:<port>,<...><fqdnX>:<port>; Сонымен қатар, Platform V Pangolin ДҚБЖ кластерін пайдаланғыңыз келсе, ДҚБЖ мекенжайын көрсету кезінде тек DNS атауын немесе негізгі түйіннің IP мекенжайын не көшірме түйінін көрсете аласыз.	IP мекенжайы
KLSRV_UNATT_DBMS_PORT	Иә	Дерекқор серверінің порты. MySQL (MariaDB) үшін әдепкі мән – 3306; Postgres үшін – 5432.	3306 немесе 5432
KLSRV_UNATT_DB_NAME	Иә	Дерекқор атауы. Дерекқордың атауы KLSRV_UNATT_DB_IAM_NAME айнымалысында көрсетілген IAM дерекқор атауынан өзгеше болуы керек.	kav
KLSRV_UNATT_DBMS_LOGIN	Иә	Дерекқорға кіру рұқсаты бар пайдаланушының аты.	
KLSRV_UNATT_DBMS_PASSWORD	Иә	Дерекқорға рұқсаты бар пайдаланушының құпиясөзі.	
KLSRV_UNATT_DBMS_SCHEMA	Жоқ	Пайдаланушы ДҚБЖ схемасы. Егер сіз пайдаланушы схеманы көрсетпесеңіз, Басқару сервері әдепкі схеманы пайдаланады. Схема атауы регистрге сезімтал: тек кіші әріптерді пайдалану керек. Пайдаланушы схеманы тек PostgreSQL немесе Postgres Pro ДҚБЖ ретінде пайдаланылған жағдайда ғана көрсете аласыз. Әйтпесе, айнымалы еленбейді.	database_schema
KLSRV_UNATT_IAM_ADDRESS	Иә	Пайдаланушы браузерлері OpenIDConnect арқылы осы мекенжайға қайта бағытталады. IAM серверінің FQDN атауын енгізіңіз. Сіз KLSRV_UNATT_SERVERADDRESS параметрінде көрсетілген Басқару серверінің DNS атауын пайдалануыңыз керек.	FQDN
KLSRV_UNATT_KLIAMUSER	Иә	IAM қызметін іске қосуға арналған есептік жазбаның атауы. Есептік жазба KLSRV_UNATT_KLADMINSGROUP айнымалысында көрсетілген қауіпсіздік тобының мүшесі болуы тиіс.	ksciam

KLSRV_UNATT_DBMS_IAM_TYPE	Иә	IAM дерекқорын басқару жүйесінің түрі: MySQL (MariaDB) немесе Postgres.	mysql Немесе postgres
KLSRV_UNATT_DBMS_IAM_INSTANCE	Иә	IAM дерекқор серверінің мекенжайы. PostgreSQL, Postgres Pro кірістірілген жоғары деңгейдегі қолжетімділік кластерін немесе Platform V Pangolin ДҚБЖ кластерін пайдалану үшін DNS атауларын немесе IP мекенжайларын және барлық түйіннің порттарын келесі форматта енгізіңіз: <fqdn1>:<port>,<fqdn2>:<port>,<...><fqdnX>:<port>; Сонымен қатар, Platform V Pangolin ДҚБЖ кластерін пайдаланғыңыз келсе, ДҚБЖ мекенжайын көрсету кезінде тек DNS атауын немесе негізгі түйіннің IP мекенжайын не көшірме түйінін көрсете аласыз.	IP мекенжайы
KLSRV_UNATT_DBMS_IAM_PORT	Иә	IAM дерекқоры серверінің порты. MySQL (MariaDB) үшін әдепкі мән – 3306; Postgres үшін – 5432.	3306 Немесе 5432
KLSRV_UNATT_DBMS_IAM_LOGIN	Иә	IAM дерекқорына кіру рұқсаты бар пайдаланушының аты. IAM дерекқор түрі MySQL (MariaDB) болса және келесі параметрлердің екеуі де болса: • gtid_mode=ON • gtid_purged=ON|AUTO көрсетілген пайдаланушыда келесі ДҚБЖ артықшылықтарының біреуі бар екеніне көз жеткізіңіз: • RELOAD • FLUSH_TABLES	
KLSRV_UNATT_DBMS_IAM_PASSWORD	Иә	IAM дерекқорына кіру рұқсаты бар пайдаланушының құпиясөзі.	
KLSRV_UNATT_DBMS_IAM_SCHEMA	Жоқ	Пайдаланушы ДҚБЖ схемасы. Егер сіз пайдаланушы схеманы көрсетпесеңіз, IAM жалпыға қолжетімді схеманы пайдаланады. Пайдаланушы схеманы тек PostgreSQL немесе Postgres Pro ДҚБЖ ретінде пайдаланылған жағдайда ғана көрсете аласыз. Әйтпесе, айнымалы еленбейді. Схема атауы регистрге сезімтал: тек кіші әріптерді пайдалану керек. Резервтелген IAM схемаларының атауларын көрсетпеңіз: client, iam, ksc, locker, pat, scope, voltron.	database_schema
KLSRV_UNATT_DB_IAM_NAME	Иә	IAM дрекқорының атауы. IAM дерекқорының атауы KLSRV_UNATT_DB_NAME айнымалысында көрсетілген дерекқор атауынан өзгеше болуы керек. Қолмен жасалған бос дерекқорды көрсетіңіз.	iamdb
KLSRV_UNATT_KLADMINSGROUP	Иә	Қызметтер үшін қауіпсіздік тобының атауы.	kladmins

KLSRV_UNATT_KLSRVUSER	Иә	Басқару сервері қызметін іске қосу үшін есептік жазбаның атауы. Есептік жазба KLSRV_UNATT_KLADMINSGROUP айнымалысында көрсетілген қауіпсіздік тобының мүшесі болуы тиіс.	ksc
KLSRV_UNATT_KLSVCUSER	Иә	Басқа қызметтерді іске қосу үшін есептік жазбаның атауы. Есептік жазба KLSRV_UNATT_KLADMINSGROUP айнымалысында көрсетілген қауіпсіздік тобының мүшесі болуы тиіс.	ksc
Басқару сервері Kaspersky Security Center Linux ақауларға төзімді кластері ретінде орналастырылатын болса, жауап файлы келесі қосымша айнымалыларды қамтуы керек:			
KLFOC_UNATT_EXT_RESOURCE_MANAGEMENT	Жоқ	Ақауларға төзімді кластердің конфигурациясы. Егер параметр жауап файлында көрсетілмесе, әдепкі мән қолданылады. Ықтимал мәндер: 0 – түйіндері бір деректерді өңдеу орталығында орналасқан ақауларға төзімді кластер (әдепкі мән). 2 – түйіндері әртүрлі деректерді өңдеу орталықтарында орналасқан географиялық бөлінген ақауларға төзімді кластер.	0 немесе 2
KLFOC_UNATT_NODE	Иә	Түйін нөмірі (1 немесе 2).	1 немесе 2
KLFOC_UNATT_STATE_SHARE_MOUNT_PATH	Иә	Күйдің ортақ қалтасының қосылым нүктесі.	
KLFOC_UNATT_DATA_SHARE_MOUNT_PATH	Иә	Деректердің ортақ қалтасының қосылым нүктесі.	
KLFOC_UNATT_CONN_MODE	Иә	Ақауларғы төзімді кластердің қосылым режимі.	VirtualAdapter Немесе ExternalLoadBalancer
Егер KLFOC_UNATT_CONN_MODE айнымалысы VirtualAdapter мәніне орнатылса, жауап файлы келесі қосымша айнымалыларды қамтуы керек:			
KLFOC_UNATT_CONN_MODE_VA_NAME	Иә	Виртуалды желілік адаптердің атауы.	
KLFOC_UNATT_CONN_MODE_VA_IPV4	Осы айнымалылардың бірі қажет	Виртуалды желілік адаптердің IP мекенжайы.	IP мекенжайы
KLFOC_UNATT_CONN_MODE_VA_IPV6		Виртуалды желілік адаптердің IPv6 мекенжайы.	IPv6 мекенжайы

Тұйық бағдарламалық орта режимінде Astra Linux-ке Kaspersky Security Center Linux орнату

Бұл бөлім Kaspersky Security Center Linux жүйесін Astra Linux Special Edition операциялық жүйесі бар құрылғыға орнату жолын сипаттайды.

Орнату алдында:

- ДҚБЖ орнатыңыз.
- kaspersky_astra_pub_key.gpg бағдарламасының кілтін жүктеп алыңыз.
- Kaspersky веб-сайтынан ksc64_[нұсқа_нөмірі]_amd64.deb орнату файлын жүктеп алыңыз.

root артықшылықтары бар есептік жазба ретінде осы нұсқаулықта берілген пәрмендерді жоғары тұтастық деңгейімен және нөлдік құпиялылықпен орындаңыз.

Kaspersky Security Center Linux жүйесін Astra Linux Special Edition (кезекті жаңарту 1.7.2) және Astra Linux Special Edition (кезекті жаңарту 1.6) орнатылған құрылғыға орнату үшін:

1. `/etc/digsig/digsig_initramfs.conf` файлын ашыңыз және келесі параметрлерді көрсетіңіз:

   ```
   DIGSIG_ELF_MODE=1
   ```

2. Пәрмен жолында үйлесімділік пакетін орнату үшін келесі пәрменді енгізіңіз:

   ```
   apt install astra-digsig-oldkeys
   ```

3. Бағдарлама кілті үшін директория жасаңыз:

   ```
   mkdir -p /etc/digsig/keys/legacy/kaspersky/
   ```

4. Алдыңғы қадамда жасалған директорияға бағдарлама кілтін салыңыз:

   ```
   cp kaspersky_astra_pub_key.gpg /etc/digsig/keys/legacy/kaspersky/
   ```

5. Барлық жүйе ядролары үшін RAM файлдық жүйесінің бастапқы кескінін жаңартыңыз:

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

   Жүйені қайта жүктеңіз.

6. "kladmins" тобын және артықшылықсыз "ksc" және "ksciam" есептік жазбаларын жасаңыз. Есептік жазбалар "kladmins" тобының мүшесі болуы керек. Ол үшін келесі пәрмендерді ретімен орындаңыз:

   ```
   # adduser ksc
   # groupadd kladmins
   # gpasswd -a ksc kladmins
   # usermod -g kladmins ksc
   # adduser ksciam
   # gpasswd -a ksciam kladmins
   # usermod -g kladmins ksciam
   ```

7. Kaspersky Security Center Linux орнатуды іске қосыңыз:

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

8. Kaspersky Security Center Linux конфигурациясын іске қосыңыз:

   ```
   # /opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl
   ```

9. Лицензиялық келісімді және Құпиялылық саясатын оқыңыз. Мәтін пәрмен жолы терезесінде көрсетіледі. Мәтіннің келесі бөлігін көру үшін бос орын пернесін басыңыз. Сұрау көрсетілген кезде келесі мәндерді енгізіңіз:

    a. Лицензиялық келісімнің шарттарын түсініп, қабылдасаңыз, y енгізіңіз. Лицензиялық келісімнің шарттарын қабылдамасаңыз, n енгізіңіз. Kaspersky Security Center Linux бағдарламасын пайдалану үшін Лицензиялық келісімнің шарттарын қабылдау керек.

    b. Құпиялық саясатының шарттарын түсінсеңіз және қабылдасаңыз және деректеріңіз Құпиялылық саясатына сәйкес өңделетініне және жіберілетініне (соның ішінде үшінші елдерге) келіссеңіз y енгізіңіз. Құпиялық саясатының шарттарын қабылдамасаңыз, n енгізіңіз. Kaspersky Security Center Linux жүйесін пайдалану үшін Құпиялық саясатының шарттарын қабылдауыңыз керек.

10. Сұрау көрсетілген кезде келесі параметрлерді енгізіңіз:

    a. Басқару серверінің DNS атын немесе статикалық IP мекенжайын енгізіңіз.

    b. Басқару сервері портының нөмірі енгізіңіз. Әдепкі бойынша порт нөмірі – 14000.

    c. Басқару сервері SSL портының нөмірін енгізіңіз. Әдепкі бойынша порт нөмірі – 13000.

    d. Басқаруды жоспарлап отырған құрылғылардың шамамен санын есептеңіз:

        - 1-100 басқарылатын құрылғыңыз болса, 1 санын енгізіңіз.
        - 101-1000 басқарылатын құрылғыңыз болса, 2 санын енгізіңіз.
        - 1000-нан көп басқарылатын құрылғыңыз болса, 3 санын енгізіңіз.

        Бұл параметр желі жүктемесін оңтайландыру үшін тапсырманың автоматты түрде рандомизацияланған кешігуі үшін пайдаланылады. Төмендегі тізімде кідіріс есептелетін аралық көрсетілген:

        - 1-100 басқарылатын құрылғы, 1 мәні. Кідіріс қолданылмайды.
        - 101-1000 басқарылатын құрылғы, 2 мәні. Кідіріс 5 минут.
        - 1000-нан көп басқарылатын құрылғы, 3 мәні. Кідіріс 10 минут.

    e. Қызметтер үшін қауіпсіздік тобының атын енгізіңіз. Әдепкі бойынша kladmins тобы пайдаланылады.

    f. Басқару сервері қызметін іске қосу үшін есептік жазбаның атауын енгізіңіз. Есептік жазба көрсетілген қауіпсіздік тобының мүшесі болуы керек. Әдепкі бойынша ksc есептік жазба пайдаланылады.

    g. Басқа қызметтерді іске қосу үшін есептік жазбаның атауын енгізіңіз. Есептік жазба көрсетілген қауіпсіздік тобының мүшесі болуы керек. Әдепкі бойынша ksc есептік жазба пайдаланылады.

    h. Kaspersky Security Center Linux бағдарламасымен жұмыс істеу үшін орнатылған ДҚБЖ таңдаңыз:

        - MySQL немесе MariaDB орнатқан болсаңыз, 1 енгізіңіз.
        - PostgreSQL немесе Postgres Pro SQL орнатқан болсаңыз, 2 енгізіңіз.

    i. Дерекқор орнатылған құрылғының IP мекенжайын енгізіңіз.

j. Дерекқор портының нөмірін енгізіңіз. Бұл порт Басқару серверімен байланысу үшін пайдаланылады. Әдепкі бойынша келесі порттар пайдаланылады:

   - MySQL немесе MariaDB үшін 3306 порты.
   - PostgreSQL немесе Postgres Pro үшін 5432 порты.

k. Дерекқор атауын енгізіңіз.

l. Дерекқорға қатынасу үшін пайдаланылатын дерекқордың әкімші есептік жазбасының атауын енгізіңіз.

m. Дерекқорға қатынасу үшін пайдаланылатын дерекқордың әкімші есептік жазбасының құпия сөзін енгізіңіз.

n. IAM серверінің FQDN атауын енгізіңіз.

   10a-қадамда енгізген Басқару серверінің DNS атауын көрсетуіңіз керек.

o. kliam қызметін іске қосу үшін есептік жазбаның атауын енгізіңіз. Есептік жазба көрсетілген қауіпсіздік тобының мүшесі болуы керек.

p. IAM қызметімен жұмыс істеу үшін орнатылған ДҚБЖ таңдаңыз:

   - MySQL немесе MariaDB орнатқан болсаңыз, 1 енгізіңіз.
   - PostgreSQL немесе Postgres Pro SQL орнатқан болсаңыз, 2 енгізіңіз.

q. IAM қызметі пайдаланатын ДҚБЖ мекенжайын енгізіңіз.

r. Дерекқор портының нөмірін енгізіңіз. Бұл порт IAM қызметімен байланысу үшін пайдаланылады. Әдепкі бойынша келесі порттар пайдаланылады:

   - MySQL немесе MariaDB үшін 3306 порты.
   - PostgreSQL немесе Postgres Pro үшін 5432 порты.

s. IAM қызметі пайдаланатын дерекқор атауын енгізіңіз. IAM қызметі пайдаланатын дерекқордың атауы басқару сервері пайдаланатын дерекқордан өзгеше болуы керек.

t. IAM дерекқорына кіру үшін пайдаланылатын дерекқор түбірінің есептік жазба атауын енгізіңіз.

u. IAM дерекқорына кіру үшін пайдаланылатын дерекқор түбірінің есептік жазба құпиясөзін енгізіңіз.

   Қызметтердің қосылуын және автоматты түрде іске қосылуын күтіңіз:

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

v. Басқару серверінің әкімшісінің рөлін орындайтын есептік жазбаны жасаңыз. Пайдаланушының аты мен құпиясөзін енгізіңіз.

Құпиясөз келесі ережелерге сәйкес келуі керек:

- Пайдаланушы құпиясөзі кемінде 8 таңбадан тұруы, бірақ 256 таңбадан аспауы керек.
- Құпиясөзде төмендегі тізімдегі кемінде үш топтың таңбалары болуы керек:
  - Бас әріптер (A-Z)
  - Кіші әріптер (a-z)
  - Сандар (0-9)
  - Арнайы таңбалар (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)

Kaspersky Security Center Linux орнатылды және пайдаланушы қосылды.

Қызметтерді тексеру

Қызметтің іске қосылғанын тексеру үшін келесі пәрмендерді пайдаланыңыз:

- `# systemctl status klnagent_srv.service`
- `# systemctl status kladminserver_srv.service`
- `# systemctl status klactprx_srv.service`
- `# systemctl status klwebsrv_srv.service`
- `# systemctl status kliam_srv.service`

Kaspersky Security Center Web Console орнату

Бұл бөлімде Kaspersky Security Center Web Console Server серверін (бұдан әрі Kaspersky Security Center Web Console деп те аталады) қалай Linux операциялық жүйелері бар құрылғыларға орнатуға болатыны сипатталған. Алдымен ДҚБЖ және Kaspersky Security Center Linux басқару серверін орнату қажет.

Astra Linux жүйесінде Kaspersky Security Center Web Console консолін жабық бастапқы режимде орнатып жатсаңыз, Astra Linux нұсқауларын орындаңыз.

Құрылғыңызда орнатылған Linux дистрибутивіне сәйкес келетін келесі орнату файлдарының бірін пайдаланыңыз:

- Debian үшін: ksc-web-console-<құрастыру нөмірі>.x86_64.deb
- RPM негізіндегі операциялық жүйелер үшін: ksc-web-console-<құрастыру нөмірі>.x86_64.rpm

Орнату файлын Kaspersky сайтынан жүктеу арқылы аласыз.

Kaspersky Security Center Web Console орнату үшін:

1. Kaspersky Security Center Web Console орнатқыңыз келетін құрылғыда қолдау көрсетілетін Linux дистрибутивтерінің бірі жұмыс істейтініне көз жеткізіңіз.

2. Лицензиялық келісімді оқып шығыңыз. Kaspersky Security Center Linux дистрибутиві құрамына Лицензиялық келісім мәтіні бар TXT файлы кірмесе, бұл файлды Kaspersky сайтынан жүктеп алуға болады. Егер сіз Лицензиялық келісімнің шарттарымен келіспесеңіз, бағдарламаны орнатпаңыз.

3. Kaspersky Security Center Web Console веб-консолін Басқару сервері қосу параметрлері бар жауаптар файлын жасаңыз: `/etc/ksc-web-console-setup.json`

   Параметрлердің ең аз жинағын қамтитын жауап файлының мысалы

   Жауап файлының параметрлер жинағы Kaspersky Security Center Web Console қосылатын басқару серверінің нұсқасына байланысты:

   - Басқару серверінің 16 және одан жоғары нұсқасы

     Басқару серверінің 16 немесе одан кейінгі нұсқасына кіруге арналған параметрлердің минималды жинағы бар жауап файлының мысалы:

     ```
     {
         "address": "ksc-web-console.example.com",
         "port": 8080,
         "trusted":  {
             "Administration Server v16": {
                 "iamHost": "ksc16.example.com",
                 "iamOAuthPort": 4444,
                 "iamProxyPort": 9050,
                 "iamCertPath": "/var/opt/kaspersky/klnagent_srv/iam/main_certificate.pem",
                 "iamPATPath": "/var/opt/kaspersky/klnagent_srv/iam/initial_token.txt",
                 "kscPort": 13299,
                 "kscCertPath": "/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer"
             }
         },
         "certDomain":"ksc-web-console.example.com",
         "acceptEula": true
     }
     ```

   - Басқару серверінің 15.4 немесе одан кейінгі нұсқасы

     Басқару серверінің 1.4 немесе одан кейінгі нұсқасына кіруге арналған параметрлердің минималды жинағы бар жауап файлының мысалы:

     ```
     {
         "address": "ksc-web-console.example.com",
         "port": 8080,
         "trusted":  {
              "Administration Server v15.4": {
                  "kscHost": "ksc.example.com",
                  "kscPort": 13299,
                  "kscCertPath": "/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer"
              }
         },
         "certDomain":"ksc-web-console.example.com",
         "acceptEula": true
     }
     ```

   Kaspersky Security Center Web Console-ді басқару серверімен бір құрылғыға немесе басқа құрылғыға орнатуға болады. Егер Kaspersky Security Center Web Console басқа құрылғыға орнатылған болса, Kaspersky Security Center Web Console-ның веб-мекенжайы (көрсетілген `address`) және Басқару серверінің веб-мекенжайы (көрсетілген `iamHost` немесе `kscHost`) ерекшеленеді. Егер Kaspersky Security Center Web Console Басқару серверімен бір құрылғыда орнатылған болса, бұл параметрлердің мәндері бірдей болады.

Басқару серверін орнату бағдарламасы кезінде көрсетілген IAM мекенжайына `iamHost` мәні сәйкес келуі керек. Көрсетілген IAM мекенжайын алу үшін Басқару сервері орнатылған құрылғыда келесі пәрменді орындаңыз:

```
grep "iam_address:" /var/opt/kaspersky/klnagent_srv/iam/iam_config.yaml
```

Толық ақпарат алу үшін Kaspersky Security Center Web Console орнату параметрлері мақаласын қараңыз.

Сенімді серверлер тізіміне әртүрлі нұсқалардың бірнеше басқару серверін қосуға болады. Бұл жағдайда серверлер әртүрлі аутентификация әдістерін қолдануы мүмкін.

1024-тен жоғары порт нөмірлерін көрсету ұсынылады. Kaspersky Security Center Web Console 1024-тен төмен порттарда жұмыс істегенін қаласаңыз, орнатудан кейін сізде setcup утилитасы бар екеніне көз жеткізіп, келесі пәрменді орындауыңыз керек:

```
sudo setcap 'cap_net_bind_service=+ep' /var/opt/kaspersky/ksc-web-console/node
```

setcap утилитасы болмаса, оны орнатуға болады. **Пәрмендерді көру үшін осы сілтемені басыңыз**.

Debian және Ubuntu операциялық жүйелері үшін келесі пәрмендердің бірін іске қосыңыз:

- `sudo apt-get install libcap2-bin`
- `sudo apt install libcap2-bin`

SUSE Linux Enterprise Server және Red Hat Enterprise Linux үшін пәрменді іске қосыңыз:

- `sudo zypper install libcap-progs`

Kaspersky Security Center Web Console веб-консолін ALT Linux операциялық жүйесі бар құрылғыға орнату кезінде, онда 8080-порттан ерекшеленетін портты көрсету керек, себебі 8080-портты операциялық жүйе қолданады.

Kaspersky Security Center Web Console бағдарламасын бірдей .rpm орнату файлының көмегімен жаңарту мүмкін емес. Егер сіз жауаптар файлының параметрлерін өзгерткіңіз келсе және осы файлды бағдарламаны қайта орнату үшін пайдаланғыңыз келсе, алдымен бағдарламаны жойып, содан кейін оны жаңа жауаптар файлымен қайта орнатуыңыз керек.

4. root артықшылықты есептік жазбаның астында Linux дистрибутивіңізге байланысты .deb немесе .rpm кеңейтімі бар орнату файлын іске қосу үшін пәрмен жолын пайдаланыңыз.

   - .deb файлынан Kaspersky Security Center Web Console алдыңғы нұсқасын орнату немесе жаңарту үшін келесі пәрменді іске қосыңыз:
     ```
     sudo apt-get install ksc-web-console-<құрастыру нөмірі>.x86_64.deb
     ```
   - Kaspersky Security Center Web Console-ін .RPM файлынан орнату үшін келесі пәрмендердің біреуін орындаңыз:
     ```
     sudo yum install ksc-web-console-<құрастыру нөмірі>.x86_64.rpm
     ```
     Немесе
     ```
     sudo alien -i ksc-web-console-<құрастыру нөмірі>.x86_64.rpm
     ```

- Kaspersky Security Center Web Console алдыңғы нұсқасын жаңарту үшін келесі пәрмендердің бірін орындаңыз:

  - RPM операциялық жүйелері бар құрылғылар үшін:
    ```
    sudo yum install ksc-web-console-<құрастыру нөмірі>.x86_64.rpm
    ```

  - Debian операциялық жүйелері бар құрылғылар үшін:
    ```
    sudo apt-get install ksc-web-console-<құрастыру нөмірі>.x86_64.deb
    ```

  Орнату файлын ашу басталады. Орнату аяқталғанша күте тұрыңыз. Kaspersky Security Center Web Console келесі директорияға орнатылады: /var/opt/kaspersky/ksc-web-console.

5. Келесі пәрменді орындау арқылы Kaspersky Security Center Web Console барлық қызметтерін қайта іске қосыңыз:
   ```
   sudo systemctl restart KSC*
   ```

   Орнату аяқталғаннан кейін, сіз Kaspersky Security Center Web Console веб-консолін ашып, жүйеге кіру үшін браузерді пайдалана аласыз.

Егер Басқару серверінің жалпы сертификаты сақтық көшірмеден басқа сертификатпен ауыстырылса немесе klsetsrvcert утилитасын пайдалану арқылы ауыстырылса, оны алып тастап, Kaspersky Security Center Web Console веб-консолін қайта орнатуыңыз керек. Әйтпесе, Web Console веб-консоліне кіру шектеледі.
Қайта орнатқаннан кейін Web Console-ге кіре алмасаңыз, IAM серверінің конфигурациясын тексеріңіз.

Kaspersky Security Center Web Console веб-консолін орнату параметрлері

Linux операциялық жүйелері бар құрылғыларға Kaspersky Security Center Web Console серверін орнату үшін Kaspersky Security Center Web Console веб-консолін Басқару серверіне қосу параметрлерін қамтитын жауаптар файлын (.json файл) жасау қажет. Бұл файлды ksc-web-console-setup.json деп атап, оны келесі /etc/ksc-web-console-setup.json каталогіне орналастыруыңыз керек.

Жауап файлының параметрлер жинағы Kaspersky Security Center Web Console қосылатын басқару серверінің нұсқасына байланысты.

- Басқару серверінің 16 және одан жоғары нұсқасы

  Басқару серверінің 16 немесе одан кейінгі нұсқасы Kaspersky Security Center Web Console-де бір рет кіру (SSO) арқылы домен аутентификациясын қамтамасыз ететін Есептік деректер және қатынасу диспетчері (IAM) бар. Kaspersky Security Center Web Console Басқару серверіне қосылу үшін жауап файлында IAM құрамдас бөлігімен өзара әрекет параметрлері болуы керек, тіпті Бірыңғай кіру (SSO) қолданбасаңыз да.

  Басқару серверінің 16 немесе одан кейінгі нұсқасына қосылатын Web Console орнатуға арналған жауап файлының мысалы. Бұл мысалда Web Console және Басқару сервері әртүрлі құрылғыларда орнатылған:

```
{
    "address": "ksc-web-console.example.com",
    "port": 8080,
    "defaultLangId": 1049,
    "enableLog": true,
    "trusted":  {
        "Administration Server v16": {
    "iamHost": "ksc16.example.com",
    "iamOAuthPort": 4444,
    "iamProxyPort": 9050,
    "iamCertPath": "/var/opt/kaspersky/klnagent_srv/iam/main_certificate.pem",
    "iamPATPath": "/var/opt/kaspersky/klnagent_srv/iam/initial_token.txt",
```

```
    "kscPort": 13299,
    "kscCertPath": "/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer"
        }
    },
    "acceptEula": true,
    "certPath": "/root/server.crt",
    "keyPath": "/root/key-without-passphrase.pem",
    "webConsoleAccount": "Group1:User1",
    "managementServiceAccount": "Group1:User2",
    "serviceWebConsoleAccount": "Group1:User3",
    "pluginAccount": "Group1:User4",
    "natsMessageQueueAccount": "Group1:User6"
}
```

- Басқару серверінің 15.4 немесе одан кейінгі нұсқасы

  Басқару серверінің 15.4 немесе одан бұрынғы нұсқасы тек ішкі пайдаланушының немесе домен пайдаланушысының аты мен құпиясөзін көрсету арқылы аутентификациялауға қолдау көрсетеді.

  Басқару серверінің 15.4 немесе одан бұрынғы нұсқасына қосылатын Web Console орнатуға арналған жауап файлының мысалы:

```
{
    "address": "ksc-web-console.example.com",
    "port": 8080,
    "defaultLangId": 1049,
    "enableLog": true,
    "trusted":  {
        "Administration Server v15.4": {
    "kscHost": "ksc.example.com",
    "kscPort": 13299,
    "kscCertPath": "/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer"
        }
    },
    "acceptEula": true,
    "certPath": "/root/server.crt",
    "keyPath": "/root/key-without-passphrase.pem",
    "webConsoleAccount": "Group1:User1",
    "managementServiceAccount": "Group1:User2",
    "serviceWebConsoleAccount": "Group1:User3",
    "pluginAccount": "Group1:User4",
    "natsMessageQueueAccount": "Group1:User6"
}
```

`webConsoleAccount`, `managementServiceAccount`, `serviceWebConsoleAccount`, `pluginAccount`, `natsMessageQueueAccount`, `certPath` және `keyPath` параметрлері міндетті емес. Жауап файлында бұл параметрлерді өткізіп жіберуге болады.

Арнаулы сертификат пайдаланғыңыз келсе, `certPath` және `keyPath` параметрлерінің екеуін де көрсетіңіз. Параметрлерді көрсетпесеңіз немесе тек біреуін көрсетсеңіз, веб-браузер қосылымыңыз құпия емес екенін хабарлайуды жалғастырады.

Қауіпсіздік себептеріне байланысты `webConsoleAccount`, `managementServiceAccount`, `serviceWebConsoleAccount`, `pluginAccount` және `natsMessageQueueAccount` параметрлерін көрсетуге кеңес бермейміз.
Осы параметрлерді көрсетуді шешсеңіз, арнаулы пайдаланушының есептік жазбалары бірдей қауіпсіздік тобына тиесілі екенін тексеріңіз. Бұл параметрлер көрсетілмесе, Kaspersky Security Center Web Console орнатушысы әдепкі қауіпсіздік тобын жасайды, содан кейін осы топта әдепкі атаулары бар пайдаланушы есептік жазбаларын жасайды.
`webConsoleAccount`, `managementServiceAccount`, `serviceWebConsoleAccount`, `pluginAccount` және `natsMessageQueueAccount` параметрлерін бір-бірінен бөлек пайдаланбау керек: бұл параметрлердің барлығы үшін мәндерді көрсетіңіз немесе ешқайсысы үшін көрсетпеңіз.

Kaspersky Security Center Web Console-ді басқару серверімен бір құрылғыға немесе басқа құрылғыға орнатуға болады. Егер Kaspersky Security Center Web Console басқа құрылғыға орнатылған болса, Kaspersky Security Center Web Console-ның веб-мекенжайы (көрсетілген `address`) және Басқару серверінің веб-мекенжайы (көрсетілген `iamHost` немесе `kscHost`) ерекшеленеді. Егер Kaspersky Security Center Web Console Басқару серверімен бір құрылғыда орнатылған болса, бұл параметрлердің мәндері бірдей болады.

Басқару серверін орнату бағдарламасы кезінде көрсетілген IAM мекенжайына `iamHost` мәні сәйкес келуі керек. Көрсетілген IAM мекенжайын алу үшін Басқару сервері хостында келесі пәрменді орындаңыз:

```
grep "iam_address:" /var/opt/kaspersky/klnagent_srv/iam/iam_config.yaml
```

1024-тен жоғары порт нөмірлерін көрсету ұсынылады. Kaspersky Security Center Web Console-дің 1024-тен төмен порттарда жұмыс істеуін қаласаңыз, келесі пәрменді орындауыңыз керек:

```
sudo setcap 'cap_net_bind_service=+ep' /var/opt/kaspersky/ksc-web-console/node
```

setcap утилитасы болмаса, оны орнатуға болады. **Пәрмендерді көру үшін осы сілтемені басыңыз**.

Debian және Ubuntu операциялық жүйелері үшін келесі пәрмендердің бірін іске қосыңыз:

- `sudo apt-get install libcap2-bin`
- `sudo apt install libcap2-bin`

SUSE Linux Enterprise Server және Red Hat Enterprise Linux үшін пәрменді іске қосыңыз:

- `sudo zypper install libcap-progs`

Kaspersky Security Center Web Console веб-консолін ALT Linux операциялық жүйесі бар құрылғыға орнату кезінде, онда 8080-порттан ерекшеленетін портты көрсету керек, себебі 8080-портты операциялық жүйе қолданады.

Төмендегі кестеде, жауап файлында көрсетуге болатын параметрлер сипатталған.

Linux операциялық жүйелері бар құрылғыларда Kaspersky Security Center Web Console веб-консолін орнату параметрлері

Параметр	Сипаттамасы	Қолжетімді мәндері
`address`	Kaspersky Security Center Web Console орнатылған құрылғының мекенжайы (FQDN немесе хост атауы) (міндетті). Kaspersky Security Center Web Console-ді Kaspersky Security Center Server серверіне орнатсаңыз, Kaspersky Security Center Linux жүйесін орнату кезінде көрсеткен мекенжайды пайдаланыңыз. Kaspersky Security Center Web Console-ді басқа құрылғыға орнатсаңыз, Kaspersky Security Center Web Console Server-ге қосылу үшін веб-браузер пайдаланатын құрылғының IP мекенжайын (FQDN немесе хост атауы) көрсетіңіз.	Жол мәні. Мысалы: `"ksc.example.com"`
`port`	Веб-браузерлерден қосылымдарды алу үшін Kaspersky Security Center Web Console пайдаланатын порт (міндетті).	Сандық мән. Ұсынылған мән: 8080 (Linux ALT операц қоспағанда).

Параметр	Сипаттамасы	Қолжетімді мәндері
`defaultLangId`	Пайдаланушы интерфейсі тілі (әдепкі бойынша `1033`). Қажет болса, Kaspersky Security Center Web Console интерфейсінің тілін өзгертуге болады.	Тілдің сандық коды: • Неміс тілі: `1031` • Ағылшын тілі: `1033` • Испан тілі: `1034` • Испан тілі (Мексика): `2058` • Француз тілі: `1036` • Итальян тілі: `1040` • Жапон тілі: `1041` • Қазақ тілі: `1087` • Поляк тілі: `1045` • Португал тілі (Бразилия): `1046` • Орыс тілі: `1049` • Түрік тілі: `1055` • Жеңілдетілген қытай тілі: `2052` • Дәстүрлі қытай тілі: `1028` Егер мән көрсетілмесе, ағылшын тілі қол US).
`enableLog`	Kaspersky Security Center Web Console трасса журналын қосу немесе қоспау. Параметрдің әдепкі мәнін тек Kaspersky техникалық қолдау қызметінің маманы сұраған жағдайда ғана өзгертуді ұсынамыз.	Логикалық мән: • `true` — журналға жазу қосылды. • `false` — журналға жазу өшірілді (әд таңдалған).

Параметр	Сипаттамасы	Қолжетімді мәндері
`trusted`	Kaspersky Security Center Web Console қосыла алатын сенімді басқару серверлерінің мекенжайларының тізімі. Сенімді серверлер тізіміне әртүрлі нұсқалардың бірнеше басқару серверін қосуға болады. Басқару серверінің 16 және одан кейінгі нұсқасы: • Кіру терезесінде көрсетілетін басқару серверінің атауы. • `iamHost` – IAM құрамдасын (Kaspersky Security Center Linux 16-нұсқасынан бастап) қамтитын және Kaspersky Security Center Web Console қосылатын басқару серверінің мекенжайы (FQDN немесе хост атауы). Басқару серверін орнату бағдарламасы кезінде көрсетілген IAM мекенжайына `iamHost` мәні сәйкес келуі керек. Көрсетілген IAM мекенжайын алу үшін Басқару сервері хостында келесі пәрменді орындаңыз: `grep "iam_address:" /var/opt/kaspersky/klnagent_srv/iam/iam_config.yaml` • `iamOAuthPort` – OpenID Connect аутентификация протоколы арқылы аутентификация токендерін алмастыру үшін пайдаланылатын порт (әдепкі мәні – 4444). Бұл порт Kaspersky Security Center Web Console Server мен басқару сервері арасындағы, сондай-ақ браузер (Kaspersky Security Center Web Console-мен пайдаланылады) мен басқару сервері арасындағы байланыс үшін де пайдаланылады. • `iamProxyPort` – Kaspersky Security Center Web Console Server-ді басқару серверіне қосу үшін пайдаланылатын порт (әдепкі мән — 9050). • `iamCertPath` – IAM сертификатының жолы. IAM сертификаты басқару серверін бірінші рет іске қосқанда автоматты түрде жасалады. Сертификат басқару сервері орнатылған құрылғыда орналасқан. Сертификаттың әдепкі жолы: /var/opt/kaspersky/klnagent_srv/iam/main_certificate.pem. Өздігінен қол қойылған IAM сертификаты автоматты түрде бұрылады. • `iamPATPath` – IAM жүйесінде Kaspersky Security Center Web Console-ді OAuth клиенті ретінде тіркеу үшін пайдаланылатын токен жолы. Бұл файл басқару серверін бірінші рет іске қосқанда автоматты түрде жасалады. Токен басқару сервері орнатылған құрылғыда орналасқан. Токеннің әдепкі жолы: var/opt/kaspersky/klnagent_srv/iam/initial_token.txt. Токен шексіз уақыт жарамды және бұруды қажет етпейді. • `kscPort` – Kaspersky Security Center Web Console-ді OpenAPI арқылы басқару серверіне қосу үшін пайдаланылатын порт (әдепкі мән — 13299). • `kscCertPath` – басқару сервері сертификатының жолы. Сертификат басқару сервері орнатылған құрылғыда орналасқан. Сертификаттың әдепкі жолы: /var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer. Басқару серверінің 15.2 және одан кейінгі нұсқасы: • Кіру терезесінде көрсетілетін басқару серверінің атауы. • `kscHost` – Kaspersky Security Center Web Console қосылатын басқару серверінің мекенжайы (FQDN немесе хост атауы). • `kscPort` – басқару серверіне қосылу үшін Kaspersky Security Center Web Console Server пайдаланатын OpenAPI порты (әдепкі мәні — 13299). • `kscCertPath` – басқару сервері сертификатының жолы. Сертификат басқару сервері орнатылған құрылғыда орналасқан. Сертификаттың әдепкі жолы: /var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer. Kaspersky Security Center Веб-Консолін Басқару сервер құрылғысынан басқа құрылғыға орнатқан кезде, Басқару серверінің сертификат файлын (`kscCertPath` арқылы көрсетілген), IAM сертификат файлын (`iamCertPath` арқылы көрсетілген) және токен файлын (`iamPATPath` арқылы көрсетілген) Басқару сервері орнатылған құрылғыдан сыртқы құрылғыға көшіріңіз. Web Console орнату бағдарламасының жауап файлында бұл файлдардың жергілікті жолын көрсетіңіз.	JSON файлының келесі форматтағы бөл `"trusted": { "Administration Server v16": { "iamHost": "ksc-iam.example.com", "iamOAuthPort": 4444, "iamProxyPort": 9050, "iamCertPath": "/var/opt/kaspersky/klnagent_srv/iam/main_c "iamPATPath": "/var/opt/kaspersky/klnagent_srv/iam/initia "kscPort": 13299, "kscCertPath": "/var/opt/kaspersky/klnagent_srv/1093/cert/ }, "Administration Server v15.4": { "kscHost": "ksc.example.com", "kscPort": 13299, "kscCertPath": "/var/opt/kaspersky/klnagent_srv/1093/cert/ } }`  `Administration Server v16` және `Administration Server v15.4` орны Басқару сервері атауларын көрсете ала

Параметр	Сипаттамасы	Қолжетімді мәндері
`acceptEula`	Лицензиялық келісімнің шарттарын қабылдайсыз ба. Лицензиялық келісімнің шарттары бар файл орнату файлымен бірге жүктеледі.	Логикалық мән: • `true` – мен осы Түпкі пайдаланушы лицензиялық келісімінің шарттары м талаптарын толық оқып шыққанымд және қабылдайтынымды растаймын • `false` – Мен Лицензиялық келісімн қабылдамаймын (әдепкі бойынша та Егер мәні көрсетілмесе, Kaspersky Secu Web Console орнату бағдарламасы Лиц келісімді көрсетеді және Лицензиялық к шарттарын қабылдауға келісесіз бе деп
`certDomain`	Жаңа өздігінен қол қойылған сертификат жасағыңыз келсе, веб-браузерді Kaspersky Security Center Web Console-ге қосатын FQDN көрсету мақсатында осы параметрді пайдаланыңыз.	Жол мәні.
`certPath`	Инфрақұрылымыңызда сенімді және арнаулы сертификаттарға қойылатын талаптарға сай келетін Kaspersky Security Center Web Console арнаулы сертификатының жолын көрсету үшін параметрді пайдаланыңыз. Бір сертификат немесе сертификат тізбегі үшін тек бір жеке кілтті (`keyPath`) көрсетуге болады.	Жол мәні. Шифрланған сертификаттарға Kaspersk Center Web Console қолдау көрсетпейд Kaspersky Security Center Web Console құрылғыда PEM форматындағы сертифи жолын көрсетіңіз. Мысалы: `/root/server.crt`
`keyPath`	`certPath` параметрінде көрсетілген Kaspersky Security Center Web Console арнаулы сертификатымен байланысты жеке кілт жолын көрсету үшін параметрді пайдаланыңыз.	Жол мәні. Жеке кілті бар файл шифрланбауы кере Kaspersky Security Center Web Console құрылғыда PEM форматындағы кілт фай көрсетіңіз. Мысалы: `/root/key-without-passph`
`webConsoleAccount`	Kaspersky Security Center Web Console қызметі іске қосылған есептік жазбаның атауы.	Келесі форматтағы жол мәні: `"< топ ат < пайдаланушы аты >"`. Мысалы: `"Group1:User1"`. Егер мән көрсетілмесе, Kaspersky Secu Web Console орнатушысы әдепкі бойын `user_management_%uid%` есептік жазб
`managementServiceAccount`	Kaspersky Security Center Web Console Management Service қызметі іске қосылған есептік жазбаның атауы.	Келесі форматтағы жол мәні: `"< топ ат < пайдаланушы аты >"`. Мысалы: `"Group1:User2"`. Егер мән көрсетілмесе, Kaspersky Secu Web Console орнатушысы әдепкі бойын `user_nodejs_%uid%` есептік жазбасын
`serviceWebConsoleAccount`	Kaspersky Security Center Web Console қызметі іске қосылған есептік жазбаның атауы.	Келесі форматтағы жол мәні: `"< топ ат < пайдаланушы аты >"`. Мысалы: `"Group1:User3"`. Егер мән көрсетілмесе, Kaspersky Secu Web Console орнатушысы әдепкі бойын `user_svc_nodejs_%uid%` есептік жазб
`pluginAccount`	Kaspersky Security Center Product Plugins қызметі іске қосылған есептік жазбаның атауы.	Келесі форматтағы жол мәні: `"< топ ат < пайдаланушы аты >"`. Мысалы: `"Group1:User4"`. Егер мән көрсетілмесе, Kaspersky Secu Web Console орнатушысы әдепкі бойын `user_web_plugin_%uid%` есептік жазб
`natsMessageQueueAccount`	Kaspersky Security Center Web Console NATS қызметі іске қосылған есептік жазбаның атауы.	Келесі форматтағы жол мәні: `"< топ ат < пайдаланушы аты >"`. Мысалы: `"Group1:User6"`. Егер мән көрсетілмесе, Kaspersky Secu Web Console орнатушысы әдепкі бойын `user_message_queue_%uid%` есептік ж жасайды.

Тұйық бағдарламалық орта режимінде Astra Linux-ке Kaspersky Security Center Web Console орнату

Бұл бөлімде Kaspersky Security Center Web Console Server серверін (бұдан әрі Kaspersky Security Center Web Console деп те аталады) қалай Astra Linux Special Edition операциялық жүйесі бар құрылғыларға орнатуға болатыны сипатталған. Алдымен ДҚБЖ және Kaspersky Security Center Linux басқару серверін орнату қажет.

Kaspersky Security Center Web Console орнату үшін:

1. Kaspersky Security Center Web Console орнатқыңыз келетін құрылғыда қолдау көрсетілетін Linux дистрибутивтерінің бірі жұмыс істейтініне көз жеткізіңіз.

2. Лицензиялық келісімді оқып шығыңыз. Kaspersky Security Center Linux дистрибутиві құрамына Лицензиялық келісім мәтіні бар TXT файлы кірмесе, бұл файлды Kaspersky сайтынан жүктеп алуға болады. Егер сіз Лицензиялық келісімнің шарттарымен келіспесеңіз, бағдарламаны орнатпаңыз.

3. Kaspersky Security Center Web Console веб-консолін Басқару сервері қосу параметрлері бар жауаптар файлын жасаңыз: `/etc/ksc-web-console-setup.json`

   Параметрлердің ең аз жинағын қамтитын жауап файлының мысалы

   Жауап файлының параметрлер жинағы Kaspersky Security Center Web Console қосылатын басқару серверінің нұсқасына байланысты:

   - Басқару серверінің 16 және одан жоғары нұсқасы

     Басқару серверінің 16 немесе одан кейінгі нұсқасына кіруге арналған параметрлердің минималды жинағы бар жауап файлының мысалы:

```
{
    "address": "ksc-web-console.example.com",
    "port": 8080,
    "trusted":  {
        "Administration Server v16": {
            "iamHost": "ksc16.example.com",
            "iamOAuthPort": 4444,
            "iamProxyPort": 9050,
            "iamCertPath": "/var/opt/kaspersky/klnagent_srv/iam/main_certificate.pem",
            "iamPATPath": "/var/opt/kaspersky/klnagent_srv/iam/initial_token.txt",
            "kscPort": 13299,
            "kscCertPath": "/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer"
        }
    },
    "certDomain":"ksc-web-console.example.com",
    "acceptEula": true
}
```

- Басқару серверінің 15.4 немесе одан кейінгі нұсқасы

  Басқару серверінің 1.4 немесе одан кейінгі нұсқасына кіруге арналған параметрлердің минималды жинағы бар жауап файлының мысалы:

```
{
    "address": "ksc-web-console.example.com",
    "port": 8080,
    "trusted":  {
         "Administration Server v15.4": {
             "kscHost": "ksc.example.com",
             "kscPort": 13299,
             "kscCertPath": "/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer"
         }
    },
    "certDomain":"ksc-web-console.example.com",
    "acceptEula": true
}
```

Kaspersky Security Center Web Console-ді басқару серверімен бір құрылғыға немесе басқа құрылғыға орнатуға болады. Егер Kaspersky Security Center Web Console басқа құрылғыға орнатылған болса, Kaspersky Security Center Web Console-ның веб-мекенжайы (көрсетілген `address`) және Басқару серверінің веб-мекенжайы (көрсетілген `iamHost` немесе `kscHost`) ерекшеленеді. Егер Kaspersky Security Center Web Console Басқару серверімен бір құрылғыда орнатылған болса, бұл параметрлердің мәндері бірдей болады.

Басқару серверін орнату бағдарламасы кезінде көрсетілген IAM мекенжайына `iamHost` мәні сәйкес келуі керек. Көрсетілген IAM мекенжайын алу үшін Басқару сервері орнатылған құрылғыда келесі пәрменді орындаңыз:

```
grep "iam_address:" /var/opt/kaspersky/klnagent_srv/iam/iam_config.yaml
```

Толық ақпарат алу үшін Kaspersky Security Center Web Console орнату параметрлері мақаласын қараңыз.

Сенімді серверлер тізіміне әртүрлі нұсқалардың бірнеше басқару серверін қосуға болады. Бұл жағдайда серверлер әртүрлі аутентификация әдістерін қолдануы мүмкін.

4. `/etc/digsig/digsig_initramfs.conf` файлын ашыңыз және келесі параметрлерді көрсетіңіз:

```
DIGSIG_ELF_MODE=1
```

5. Пәрмен жолында үйлесімділік пакетін орнату үшін келесі пәрменді енгізіңіз:

```
apt install astra-digsig-oldkeys
```

6. Бағдарлама кілті үшін директория жасаңыз:

```
mkdir -p /etc/digsig/keys/legacy/kaspersky/
```

7. `/opt/kaspersky/ksc64/share/kaspersky_astra_pub_key.gpg` бағдарлама кілтін алдыңғы қадамда жасалған каталогқа орналастырыңыз:

```
cp kaspersky_astra_pub_key.gpg /etc/digsig/keys/legacy/kaspersky/
```

Егер Kaspersky Security Center Linux жеткізілім жинағында kaspersky_astra_pub_key.gpg кілті болмаса, бұл кілтті https://media.kaspersky.com/utilities/CorporateUtilities/kaspersky_astra_pub_key.gpg сілтемесінен жүктеп алуға болады.

8. Дискілердің жедел жадын жаңартыңыз:

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

Жүйені қайта жүктеңіз.

9. root құқықтары бар тіркелгіде орнату файлын іске қосу үшін пәрмен жолын пайдаланыңыз. Орнату файлын Kaspersky сайтынан жүктеу арқылы аласыз.

- Kaspersky Security Center Web Console алдыңғы нұсқасын орнату немесе жаңарту үшін келесі пәрменді іске қосыңыз:

```
sudo apt-get install ksc-web-console-<құрастыру_нөмірі>.x86_64.deb
```

- Kaspersky Security Center Web Console алдыңғы нұсқасын жаңарту үшін келесі пәрмендердің бірін орындаңыз:

```
sudo apt-get install ksc-web-console-<құрастыру_нөмірі>.x86_64.deb
```

Орнату файлын ашу басталады. Орнату аяқталғанша күте тұрыңыз. Kaspersky Security Center Web Console келесі директорияға орнатылады: `/var/opt/kaspersky/ksc-web-console`.

10. Келесі пәрменді орындау арқылы Kaspersky Security Center Web Console барлық қызметтерін қайта іске қосыңыз:

```
sudo systemctl restart KSC*
```

Орнату аяқталғаннан кейін, сіз Kaspersky Security Center Web Console веб-консолін ашып, жүйеге кіру үшін браузерді пайдалана аласыз.

Kaspersky Security Center Linux жүйесін скриптпен орнату

`ksc_fast_install.py` скрипті сізге Kaspersky Security Center Linux жүйесін орналастыруға және оның компоненттерін: Басқару сервері мен Web Console веб-консолін, соның ішінде ДҚБЖ және қажетті қолдау пакеттерін бастапқы орнатуға мүмкіндік береді.

Скрипт параметр файлынан параметрлерді оқиды. Параметрлердің әдепкі мәндері пайдаланылады. Қажет болса, басты бетті өзгертуге болады.

Скрипт қалай жұмыс істейді

Іске қосылған кезде скрипт:

- Шарттардың орындалғанын тексереді:
  - Сізде скриптті орындау үшін қажетті құқықтар бар.
  - Скрипт операциялық жүйемен және ДҚБЖ-мен үйлесімді.
  - EULA және Құпиялық саясаты қабылданады.

    Егер оларды параметр файлында қабылдамасаңыз, сценарийді іске қосқаннан кейін оларды қабылдау ұсынылады.
  - Басқару серверлері мен Web Console веб-консоліне қойылатын аппараттық талаптар

    Талаптар Өлшеу нұсқаулығында анықталған.
- ДҚБЖ орнатады (егер әлі орнатылмаған болса) және оның параметрлерін конфигурациялайды
- Kaspersky Security Center дерекқорларын жасайды, ОЖ есептік деректерін конфигурациялайды
- Басқару серверін, Web Console веб-консолін орнатады
- Web Console веб-консоліне кіру үшін логин мен құпиясөзді ұсынады.

  Пәрмен жолы терминалын жаппас бұрын, есептік деректерін кез келген ыңғайлы жолмен сақтаңыз. Есептік деректерді жоғалтсаңыз, келесі пәрменді орындау арқылы жаңа пайдаланушы есептік жазбасын қосуыңыз керек: `/opt/kaspersky/ksc64/sbin/kladduser -n <пайдаланушы>`

Егер бір немесе бірнеше шарт маған сәйкес келмесе немесе қате орын алса, скрипт тоқтатылады және тиісті хабарландыру көрсетіледі.

> Скрипт жүйені нығайту әрекеттерін қамтымайды. Kaspersky Security Center жүйесін бұзу қаупін азайту үшін Қауіпсіздікті күшейту жөніндегі нұсқаулықтың ұсыныстарын қарастырыңыз.
> Сценарийге негізделген орнату әдісі Kaspersky Security Center Linux орнатылмаған құрылғыда Kaspersky Security Center Linux 16.3 және одан кейінгі нұсқаларын өрістету үшін қолданылады.
> Сценарийді іске қосу үшін Python 3.6 және одан кейінгі нұсқалары қажет.

Өрістету ағымдағы құрылғыда Kaspersky Security Center Linux орнатылмаған жағдайда ғана мүмкін.

Сценарийді Kaspersky Security Center Linux жаңа нұсқасына жаңарту үшін немесе Kaspersky Security Center Linux орын басу кластері өрістетілген болса пайдалануға болмайды.

`ksc_fast_install.py` орнату бағдарламасы кестеде сипатталған ДҚБЖ бар операциялық жүйе нұсқаларында Kaspersky Security Center Linux жүйесін орнатуды қолдайды.

Операциялық жүйенің нұсқасы	ДҚБЖ
Ubuntu Server 26.04 LTS (Noble Numbat)	PostgreSQL 18
РЕД ОС 8	PostgreSQL 16

Astra Linux Special Edition RUSB.10015-01 (1.8.5 нұсқасы)	PostgreSQL 15
CentOS Stream 10	PostgreSQL 18

Арнайы дерекқор схемасы скриптпен қолдау көрсетілмейді.

Скрипт арқылы орналастыруды қалай орындау керек

Алдын ала талаптар

Бастамас бұрын, келесі әрекеттерді орындағаныңызға көз жеткізіңіз:

- Операциялық жүйені келесі командалардың бірін орындау арқылы жаңартыңыз: `dnf update` немесе `apt update`
- Пәрменді орындау арқылы супер пайдаланушы құқықтарын алыңыз: `sudo -i`
- Скриптті іске қосуға рұқсат ету үшін келесі команданы орындаңыз: `chmod +x ./ksc_fast_install.py`
- Операциялық жүйеңіздің репозиторийінде қолдау көрсетілетін ДҚБЖ орналасқанына көз жеткізіңіз: `sudo apt policy postgresql`

Скриптті іске қосу арқылы Kaspersky Security Center Linux жүйесін орналастыру үшін:

1. Kaspersky веб-сайтынан келесіні жүктеп алыңыз:
   - Басқару сервері және Web Console веб-консоліне арналған .deb немесе .rpm дистрибутивтері.
   - "KSC орнату сценарийі" мұрағаты.

     > Сценарийді пайдаланған кезде операциялық жүйенің пакеттік менеджеріне үйлесімді Басқару сервері мен Web Console дистрибутивтерін таңдаңыз.

     Мұрағатта келесі файлдар бар:
     - `ksc_fast_install.py` скрипт файлы.
     - Параметр файлы.

       Әдепкі файл атауы - `params.txt`. Файлдың атауын өзгерткіңіз келсе, пәрмен жолы терминалында скриптті іске қосқан кезде жаңа атауды `--params` параметрі арқылы көрсеткеніңізге көз жеткізіңіз:
     - Басқару серверіне арналған EULA және Құпиялық саясаты бар файл.
     - Kaspersky Security Center Web Console үшін EULA файлы.
     - EULA үшін хэш қосындылары бар файлдар.
2. Жүктелген файлдардың барлығын бір жергілікті каталогқа орналастырыңыз.
3. Қажет болса, параметр файлын конфигурациялаңыз.

Параметр файлының мысалын оның параметрлерінің сипаттамасымен бірге көру үшін мына жерді басыңыз

```
# Required parameters:

#klfi_server_eula_accepted=N

#klfi_nwc_eula_accepted=N

#klfi_pp_accepted=N

# Optional parameters:

#klfi_klserver_db=KAV

#klfi_klserver_dbuser=klserver

#klfi_klserver_address=

#klfi_kliam_db=KAV_IAM

#klfi_kliam_dbuser=kliam

#klfi_kliam_address=

#klfi_sys_group_kladmin=kladmins

#klfi_sys_user_klserver=klsrvuser

#klfi_sys_user_kliam=kliamuser

#klfi_sys_user_svc=klsvcuser

#klfi_nwc_port=8080

#klfi_display_name=

#klfi_netsize=M
```

`klfi_server_eula_accepted=N`, `klfi_nwc_eula_accepted=N` және `klfi_pp_accepted=N` параметрлер міндетті және әрқашан параметр файлында болады. Басқа параметрлер міндетті емес.

Міндетті параметрлер үшін:

- Егер сіз әдепкі мән жолын түсіндірместен өзгертсеңіз, сізден EULA және Құпиялық саясатын қабылдау сұралады.
- Егер сіз басқа мәнді көрсетсеңіз `Y` немесе `N`, егер сіз жолға түсініктеме бермесеңіз де, сізден EULA және Құпиялылық саясатын қабылдау сұралады.
- Егер сіз әдепкі параметрді өзгертпестен жолды түсіндірмесіз қалдырсаңыз `N` мәні болса, скрипт жұмыс істемейді.
- Егер сіз жолды түсіндірмеден алып тастап, орнатсаңыз `Y` мәні болса, скрипт сізге нұсқау бермейді.

Параметр және оның әдепкі мәні	Параметр сипаттамасы және басқа мүмкін мәндер (бар болса)
`klfi_server_eula_accepted=N`	Басқару серверге арналған соңғы пайдаланушы лицензиялық келісімі. Ықтимал мәндер: • `Y` – EULA қабылданды. • `N` – EULA қабылданбады.
`klfi_nwc_eula_accepted=N`	Kaspersky Security Center Web Console үшін Түпкі пайдаланушының лицензиялық келісімі. Ықтимал мәндер: • `Y` – EULA қабылданды. • `N` – EULA қабылданбады.
`klfi_pp_accepted=N`	Құпиялық саясаты. Ықтимал мәндер: • `Y` – Құпиялық саясаты қабылданды. • `N` – Құпиялық саясаты қабылданбайды.
`klfi_klserver_db=KAV`	Басқару сервері дерекқорының атауын көрсетіңіз. Дерекқордың атауы `klfi_kliam_db` айнымалысында көрсетілген IAM дерекқор атауынан өзгеше болуы керек.
`klfi_kliam_db=KAV_IAM`	IAM дрекқорының атауы. Атауы көрсетілген Басқару сервері дерекқорының атауынан өзгеше болуы керек `klfi_klserver_db` параметр.
`klfi_klserver_dbuser=klserver`	Басқару сервері дерекқорын құру тәсілі:
`klfi_kliam_dbuser=kliam`	IAM дерекқоры пайдаланушысының аты-жөні.
`klfi_klserver_address=FQDN`	Басқару серверінің FQDN немесе ағымдағы құрылғы атауы. Егер параметр мәні көрсетілмесе, скрипт автоматты түрде FQDN немесе скрипт іске қосылған құрылғының атауын анықтайды. Егер скрипт мәндерді анықтай алмаса, орнату бағдарламасы қатемен аяқталады.
`klfi_kliam_address=FQDN`	IAM серверінің FQDN немесе ағымдағы құрылғы атауы. Егер параметр мәні көрсетілмесе, скрипт автоматты түрде FQDN немесе скрипт іске қосылған құрылғының атауын анықтайды. Егер скрипт мәндерді анықтай алмаса, орнату бағдарламасы қатемен аяқталады.
`klfi_sys_group_kladmin=kladmins`	Қызметтер үшін қауіпсіздік тобының атауы.
`klfi_sys_user_klserver=klsrvuser`	Басқару сервері қызметін іске қосу үшін есептік жазбаның атауы.
`klfi_sys_user_kliam=kliamuser`	IAM қызметін іске қосуға арналған есептік жазбаның атауы.
`klfi_sys_user_svc=klsvcuser`	Басқа қызметтерді іске қосу үшін есептік жазбаның атауы.
`klfi_nwc_port=8080`	Kaspersky Security Center Web Console-іне қосылуға арналған порт.
`klfi_display_name=FQDN`	Кіру терезесінде көрсетілетін басқару серверінің атауы.

`klfi_netsize=M`	Басқаруды жоспарлап отырған құрылғылардың шамамен саны. Әрбір бағалау Kaspersky қолданбаларын іске қосу үшін қажетті ресурстарды ескереді. Есептеу Басқару серверінің, Желілік агенттің, Kaspersky Security Center Web Console-дың және Kaspersky Endpoint Security for Linux қолданбаларын бір құрылғыда бір уақытта жұмыс істеуін қамтиды. Басқару серверінің сақтық көшірмелеріне арналған сақтау орны бұл есептеулерге кірмейді. Сақтық көшірмелерді бөлек құрылғыда сақтау үшін сыртқы файл ресурсын бекіту нүктесі ретінде пайдаланыңыз немесе сақтық көшірме орнын ескеру үшін қолжетімді диск кеңістігін арттырыңыз. Операциялық жүйені орнату үшін қосымша 4–6 ГБ жедел жад пен 20 ГБ бос диск кеңістігін бөлуді ұсынамыз. Желі өлшемі бойынша аппараттық ресурстарды бағалау: • `S` –1-ден 1000-ға дейін басқарылатын құрылғылар. • Орталық процессор – 8 ядро • Жедел жад — 16 ГБ • Бос дискілік кеңістік `/var` каталог – 70 ГБ, 300 IOPS немесе одан жоғары • `M` –1001-ден 10000-ға дейін басқарылатын құрылғылар. • Орталық процессор – 12 ядро • Жедел жад — 24 ГБ • Бос дискілік кеңістік `/var` каталог – 340 ГБ, 300 IOPS немесе одан жоғары • `L` – 10001-ден 30000-ға дейін басқарылатын құрылғылар. • CPU – 20 ядро • Жедел жад — 40 ГБ • Бос дискілік кеңістік `/var` каталог – 490 ГБ, 300 IOPS немесе одан жоғары • `XL` – 30001-ден 50000-ға дейін басқарылатын құрылғылар. • CPU – 28 ядро • Жедел жад — 54 ГБ • Бос дискілік кеңістік `/var` каталог – 640 ГБ, 300 IOPS немесе одан жоғары

Параметр файлының жолдарына түсініктеме беріледі. Егер сіз мәндерді конфигурациялағыңыз келсе, түсініктемені алып тастағыңыз келетін жолдың басындағы # белгісін алып тастаңыз.

`klfi_server_eula_accepted`, `klfi_nwc_eula_accepted` және `klfi_pp_accepted` параметрлер міндетті болып табылады және олардың `N` әдепкі мәні. Егер сіз скриптті параметр файлындағы осы мәндерді өзгертпей іске қоссаңыз, сізден EULA және Құпиялылық саясатын қабылдау сұралады.

4. Скриптті іске қосыңыз.

Скрипт орындалғаннан кейін Kaspersky Security Center Linux компоненттерін сәтті орналастыру туралы хабарлама, сондай-ақ Web Console веб-консоліне кіру үшін логин мен құпиясөз көрсетіледі.

Егер скрипт негізіндегі орнату шарттары орындалмаса, белгісіз параметрлер параметр файлында көрсетілсе немесе параметр бірнеше рет қайталанса, скрипт қатені қайтарады және сәйкес хабарлама көрсетіледі.

Егер сценарий ресурстарды анықтау кезеңінде жедел жадтың жеткіліксіздігін қате анықтаса, орнату кезеңіне динамикалық жедел жадты пайдалануды сөндіріңіз.

Егер Kaspersky Security Center Linux компоненттерін немесе ДҚБЖ орнату кезінде қате орын алса, орнату бағдарламасы өзгертулерді кері қайтарады, содан кейін тоқтайды.

Орнату кері қайтару ақауы

Егер Kaspersky Security Center Linux компоненттерін немесе ДҚБЖ орнату кезінде қате орын алса, кері қайтару скрипт арқылы автоматты түрде орындалады. Қате орын алғанға дейін орнатылған компонент немесе ДҚБЖ жойылады.

Операциялық жүйе пакеттерін жаңарту және қолдау пакеттерін орнату кері қайтарылмайды.

Егер сіз скриптті қолмен тоқтатсаңыз, сәтті аяқталған қадамдар кері қайтарылмайды. Қажет болса, скриптті қайта іске қосуға болады, сонда орнату үзілген қадамнан жалғасады.

Орнатуды жалғастыру үшін, скриптті `rollback` параметрі бар пәрмен жолы терминалында іске қосу керек:
`python3 ksc_fast_install.py rollback`

Ақауларға төзімді Kaspersky Security Center Linux кластерін орналастыру

Ақауларға төзімді Kaspersky Security Center Linux кластері Kaspersky Security Center Linux бағдарламасының жоғары қолжетімділігін қамтамасыз етеді және апат болған жағдайда басқару серверінің босқа тұрып қалуын азайтады. Ақауларға төзімді кластер екі компьютерде орнатылған екі бірдей Kaspersky Security Center Linux данасына негізделген. Даналардың бірі белсенді түйін ретінде, екіншісі пассивті түйін ретінде жұмыс істейді. Белсенді түйін клиент құрылғыларын қорғауды басқарады, ал пассивті белсенді түйін істен шыққан жағдайда – белсенді түйіннің барлық функцияларын қабылдауға дайын. Апат болған кезде пассивті түйін белсенді болады, ал белсенді түйін пассивті болады.

Kaspersky Security Center Linux ақауларға төзімді кластері екі конфигурацияны қолдайды:

- Түйіндері бір деректерді өңдеу орталығында орналасқан ақауларға төзімді кластер.
- Түйіндері әртүрлі деректерді өңдеу орталықтарында орналасқан географиялық бөлінген ақауларға төзімді кластер.

Ақауларға төзімді Kaspersky Security Center Linux кластерінде барлық Kaspersky Security Center Linux қызметтері автоматты түрде басқарылады. Қызметтерді қолмен қайта іске қосуға тырыспаңыз.

Ақауларды жою үшін жүйе журналы мүмкіндігін пайдаланыңыз.

Ауысу шарты

Істен шығуға төзімді кластер клиент құрылғыларын қорғауды басқаруды белсенді түйіннен пассивті түйінге ауыстырады, егер белсенді түйінде келесі оқиғалардың кез келгені орын алса:

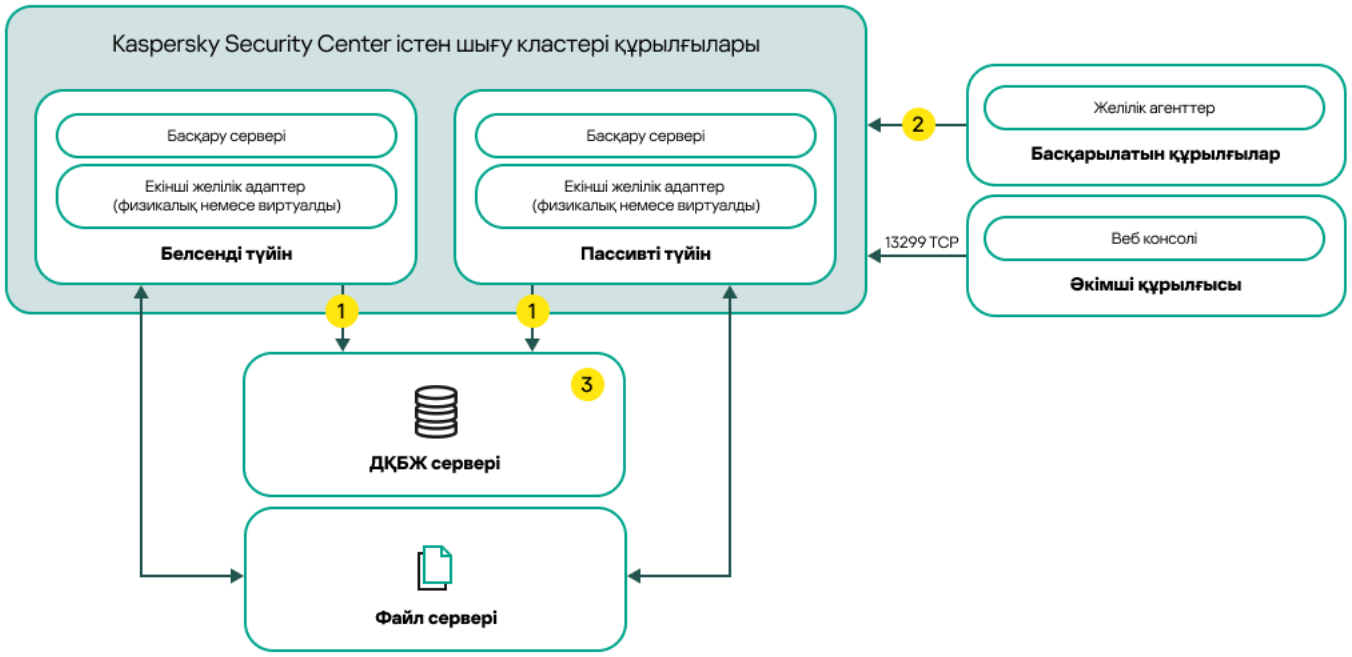
- Белсенді түйін бағдарламалық немесе аппараттық ақауға байланысты сынған.
- Техникалық жұмыстарды жүргізу үшін белсенді түйін уақытша тоқтатылды.
- Kaspersky Security Center Linux қызметтерінің (немесе процестерінің) кем дегенде біреуі сәтсіз аяқталды немесе кездейсоқ тоқтатылды. Kaspersky Security Center Linux қызметтері келесідей: klnagent_klfoc, kladminserver_klfoc, klactprx_klfoc, klwebsrv_klfoc.
- Белсенді түйін мен файл серверіндегі сақтау орны арасындағы желілік байланыс үзілді немесе тоқтатылды (тек бір деректерді өңдеу орталығында орналасқан кластер үшін).

Ақауларға төзімді Kaspersky Security Center Linux кластері. Орналастыру схемалары

Kaspersky Security Center Linux ақауларға төзімді кластерін орналастыру үшін келесі схемалардың бірін таңдауға болады:

- Kaspersky Security Center Linux ақауларға төзімді кластері бір деректерді өңдеу орталығында орналастырылған:
  - Қосымша желілік адаптерді және арнайы құрылғыға орнатылған ДҚБЖ пайдаланатын схема.
  - Үшінші тараптың жүктеме теңестіргішін және арнайы құрылғыға орнатылған ДҚБЖ пайдаланатын схема.
- Географиялық таратылған Kaspersky Security Center Linux ақауларға төзімді кластері бірнеше деректерді өңдеу орталықтарында орналастырылған.

Қосымша желілік адаптерді және арнайы құрылғыға орнатылған ДҚБЖ пайдаланатын схема.



Қосымша желілік адаптерді және арнайы құрылғыға орнатылған ДҚБЖ пайдаланатын схема.

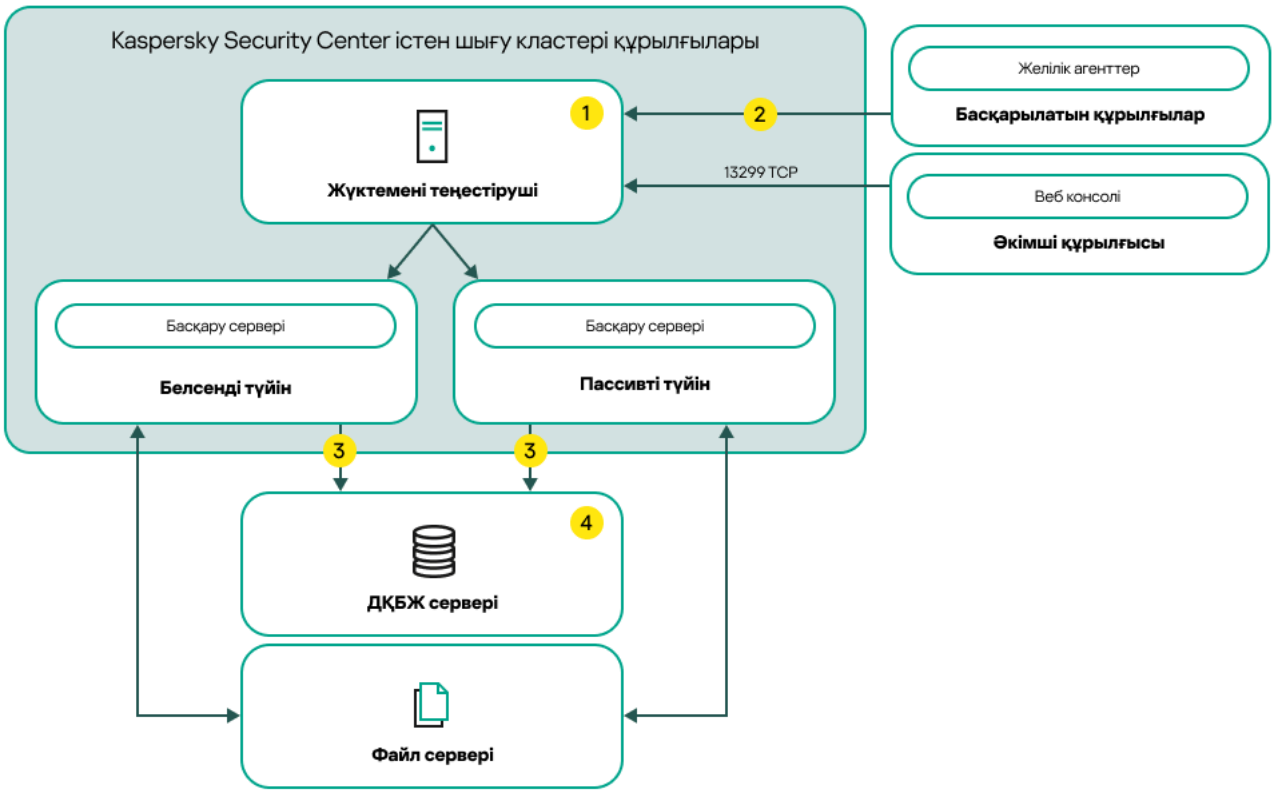
Схеманың шартты белгілері:

1 Басқару сервері деректерді дерекқорға жібереді. MySQL сервері үшін 3306 порты немесе PostgreSQL не Postgres Pro үшін 5432 порты сияқты дерекқор орналасқан құрылғыда қажетті порттарды ашыңыз. Толығырақ ақпарат ДҚБЖ құжаттамасында көрсетілген.

2 Басқарылатын құрылғыларға қосылу үшін басқару сервері бар құрылғыларда келесі порттарды ашыңыз: TCP 13000, UDP 13000 және TCP 17000.

3 Дерекқорды басқару жүйесі (ДҚБЖ) бар құрылғы. MariaDB Galera Cluster-ді ДҚБЖ ретінде пайдалансаңыз, бұл мақсат үшін арнайы құрылғы қажет емес. Әрбір түйінге MariaDB Galera кластерін орнатыңыз.

Үшінші тараптың жүктеме теңестіргішін және арнайы құрылғыға орнатылған ДҚБЖ пайдаланатын схема.



Үшінші тараптың жүктеме теңестіргішін және арнайы құрылғыға орнатылған ДҚБЖ пайдаланатын схема.

Схеманың шартты белгілері:

1 Жүктемені теңдестіру құрылғысында барлық басқару сервері портын ашыңыз: TCP 13000, UDP 13000, TCP 13299 және TCP 17000.

> Автоматтандыру үшін klakaut утилитасын пайдаланғыңыз келсе, TCP 13291 портын да ашуыңыз керек.

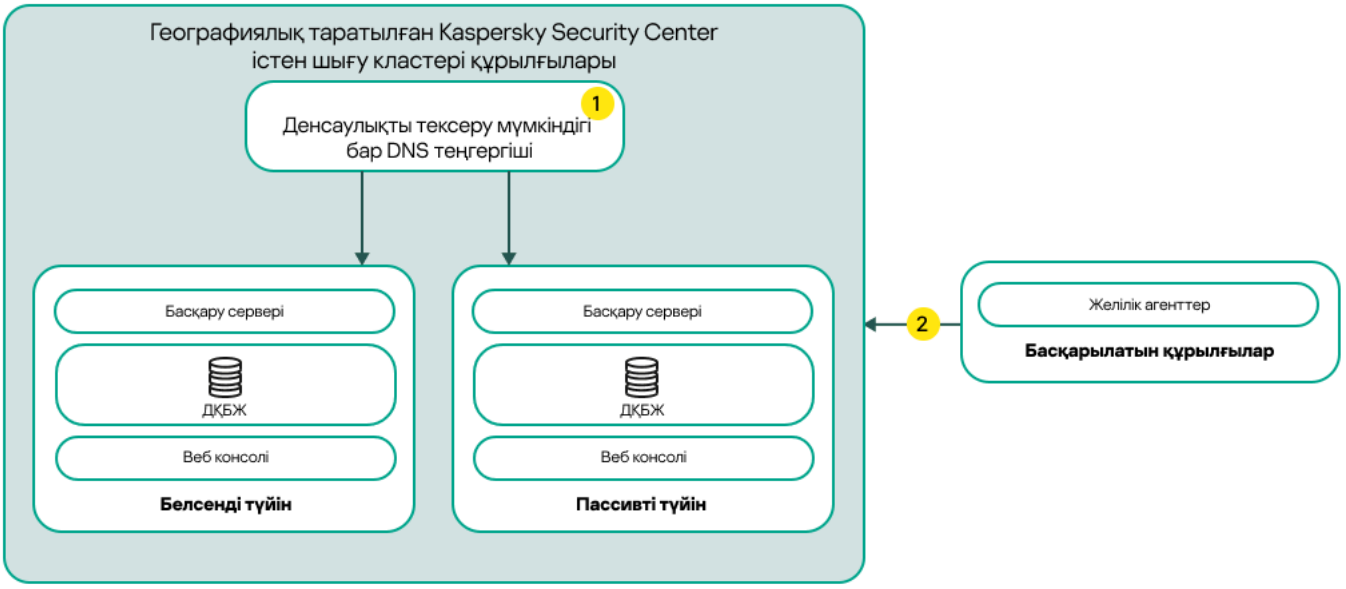
2 Басқарылатын құрылғыларға қосылу үшін басқару сервері бар құрылғыларда келесі порттарды ашыңыз: TCP 13000, UDP 13000 және TCP 17000.

3 Басқару сервері деректерді дерекқорға жібереді. MySQL сервері үшін 3306 порты немесе PostgreSQL не Postgres Pro үшін 5432 порты сияқты дерекқор орналасқан құрылғыда қажетті порттарды ашыңыз. Толығырақ ақпарат ДҚБЖ құжаттамасында көрсетілген.

4 Дерекқорды басқару жүйесі (ДҚБЖ) бар құрылғы. MariaDB Galera Cluster-ді ДҚБЖ ретінде пайдалансаңыз, бұл мақсат үшін арнайы құрылғы қажет емес. Әрбір түйінге MariaDB Galera кластерін орнатыңыз.

Kaspersky Security Center Linux ақауларға төзімді кластері.

Бұл орналастыру схемасы барлық компоненттердің жоғары қолжетімділігін қамтамасыз етуге мүмкіндік береді. Бұл схемада екі кластер түйініне де Басқару сервері, ДҚБЖ және Kaspersky Security Center Web Console орнатылған.



Географиялық таралған Kaspersky Security Center Linux ақауларға төзімді кластерін орналастыру схемасы

1 Географиялық таратылған Kaspersky Security Center Linux ақауларға төзімді кластерін орнатпас бұрын сіздің тарапыңызда орналастырылуы тиіс денсаулықты тексеру мүмкіндігі бар DNS теңгергіші.

> DNS теңгергіші кластер түйіндерінің күйін мезгіл-мезгіл тексеріп отырады. Кластерге домен атауы бойынша кірген кезде, DNS теңгергіші әрқашан белсенді түйіннің IP мекенжайын қайтарады.

2 Басқарылатын құрылғыларға қосылу үшін басқару сервері бар құрылғыларда келесі порттарды ашыңыз: TCP 13000, UDP 13000 және TCP 17000.

Ақауларға төзімді Kaspersky Security Center Linux кластері

Бұл бөлімде бір деректерді өңдеу орталығында орналастырылған Kaspersky Security Center Linux ақауларға төзімді кластері туралы жалпы ақпарат, сондай-ақ желіңізде Kaspersky Security Center Linux ақауларға төзімді кластерін дайындау және орналастыру нұсқаулары бар.

Сценарий: Ақауларға төзімді Kaspersky Security Center Linux кластерін орналастыру

Ақауларға төзімді Kaspersky Security Center Linux кластері Kaspersky Security Center Linux бағдарламасының жоғары қолжетімділігін қамтамасыз етеді және апат болған жағдайда басқару серверінің босқа тұрып қалуын азайтады. Ақауларға төзімді кластер екі компьютерде орнатылған екі бірдей Kaspersky Security Center Linux данасына негізделген. Даналардың бірі белсенді түйін ретінде, екіншісі пассивті түйін ретінде жұмыс істейді. Белсенді түйін клиент құрылғыларын қорғауды басқарады, ал пассивті белсенді түйін істен шыққан жағдайда – белсенді түйіннің барлық функцияларын қабылдауға дайын. Апат болған кезде пассивті түйін белсенді болады, ал белсенді түйін пассивті болады.

Kaspersky бағдарламалық жасақтамасын орналастыру келесі кезеңдерден тұрады:

Осы сценарийде сипатталған кезеңдердің ретін орындау ұсынылады.

1. **Аппараттық жасақтама талаптарын тексеру**

   Сізде ақауларға төзімді кластер талаптарына сәйкес келетін аппараттық жасақтама бар екеніне көз жеткізіңіз.

2. **Орналастыру схемасын таңдау**

   Орналастыру схемасын таңдаңыз. Бұл орналастырудың келесі кезеңдеріне әсер етеді.

3. **Kaspersky Security Center Linux қызметтері үшін есептік жазбаларды дайындау**

   Белсенді түйінде, енжар түйінде және файл серверінде келесі қадамдарды орындаңыз:

   1. `kladmins` тобын құрыңыз. Келесі пәрмендерді орындаңыз:

      ```
      sudo groupadd kladmins
      ```

      ```
      sudo groupmod -g <new_GID> kladmins
      ```

      Топтың барлық үш құрылғысында GID бірдей екеніне көз жеткізіңіз. Келесі пәрменді орындаңыз:

      ```
      getent group kladmins
      ```

      GID сәйкес келмесе, GID көрсету үшін келесі пәрменді пайдалануға болады:

      ```
      sudo groupmod -g <new_GID> kladmins
      ```

   2. `ksc` пайдаланушы есептік жазбасын жасаңыз. `kladmins` тобына пайдаланушы есептік жазбаларын тағайындаңыз. Келесі пәрмендерді орындаңыз:

      ```
      sudo adduser ksc
      ```

      ```
      sudo usermod -u <жаңа_UID> ksc
      ```

      ```
      sudo gpasswd -a ksc kladmins
      ```

      ```
      sudo usermod -g kladmins ksc
      ```

      Пайдаланушы есептік жазбасының барлық үш құрылғысында UID бірдей екеніне көз жеткізіңіз. Келесі пәрменді орындаңыз:

      ```
      getent passwd ksc
      ```

      UID сәйкес келмесе, UID көрсету үшін келесі пәрменді пайдалана аласыз:

      ```
      sudo usermod -u <new_UID> ksc
      ```

3. `rightless` пайдаланушы есептік жазбасын жасаңыз. `kladmins` тобына пайдаланушы есептік жазбаларын тағайындаңыз. Келесі пәрмендерді орындаңыз:

   ```
   sudo adduser rightless
   ```

   ```
   sudo usermod -u <жаңа_UID> rightless
   ```

   ```
   sudo gpasswd -a rightless kladmins
   ```

   ```
   sudo usermod -g kladmins rightless
   ```

   Пайдаланушы есептік жазбасының барлық үш құрылғысында UID бірдей екеніне көз жеткізіңіз. Келесі пәрменді орындаңыз:

   ```
   getent passwd rightless
   ```

   UID сәйкес келмесе, UID көрсету үшін келесі пәрменді пайдалана аласыз:

   ```
   sudo usermod -u <жаңа_UID> rightless
   ```

4. `ksciam` пайдаланушы есептік жазбасын жасаңыз. `kladmins` тобына пайдаланушы есептік жазбаларын тағайындаңыз. Келесі пәрмендерді орындаңыз:

   ```
   sudo adduser ksciam
   ```

   ```
   sudo usermod -u <жаңа_UID> ksciam
   ```

   ```
   sudo gpasswd -a ksciam kladmins
   ```

   ```
   sudo usermod -g kladmins ksciam
   ```

   Пайдаланушы есептік жазбасының барлық үш құрылғысында UID бірдей екеніне көз жеткізіңіз. Келесі пәрменді орындаңыз:

   ```
   getent passwd ksciam
   ```

   UID сәйкес келмесе, UID көрсету үшін келесі пәрменді пайдалана аласыз:

   ```
   sudo usermod -u <жаңа_UID> ksciam
   ```

5. Қажет болса, Kaspersky Security Center Linux қызметтерінің функциясы үшін қолданылатын есептік жазбаларға ашуға болатын (файл дескрипторлары) файлдардың әдепкі шегін арттырыңыз. Ол үшін /etc/security/limits.conf файлын ашып, жұмсақ және қатты файл дескрипторының шектеулерін төмендегідей көрсетіңіз:

   ```
   ksc soft nofile <max_number_of_opened_files>
   ```

   ```
   ksc hard nofile <max_number_of_opened_files>
   ```

   Әдепкісінше файл дескрипторларының шектері орнату кезінде көрсетіледі. Жұмсақ файл шегі — 32 768 файл, қатты файл шегі — 131 072 файл.

4 Файл серверін дайындау

Файл серверін ақауларға төзімді Kaspersky Security Center Linux кластерінің құрамында жұмыс істеуге дайындаңыз. Файл сервері аппараттық және бағдарламалық жасақтама талаптарына сәйкес келетініне көз жеткізіңіз, Kaspersky Security Center Linux деректері үшін екі ортақ қалта жасаңыз және ортақ қалталарға қатынасу құқықтарын конфигурациялаңыз.

Нұсқаулар: ақауларға төзімді Kaspersky Security Center Linux кластері үшін файлдық серверді дайындау

5 ДҚБЖ орнату

Kaspersky Security Center Linux үшін ДҚБЖ-ны орнатыңыз. Қолдау көрсетілетін ДҚБЖ-ның бірін таңдай аласыз. Таңдалған ДҚБЖ жүйесін қалай орнату керектігі туралы мәліметтер оның құжаттамасында келтірілген.

Егер Linux негізіндегі операциялық жүйеңіздің дистрибутивінде қолдау көрсетілетін ДҚБЖ болмаса, ДҚБЖ жүйесін үшінші тарап пакеттер қоймасынан орнатуға болады.

ДҚБЖ орнатқаннан кейін, сәйкес нұсқауды орындаңыз:

- Kaspersky Security Center Linux бағдарламасымен жұмыс істеу үшін PostgreSQL немесе Postgres Pro серверін конфигурациялау
- Kaspersky Security Center Linux нұсқасымен жұмыс істеу үшін MariaDB x64 серверінің конфигурациясы

IAM үшін дерекқор жасаңыз. Басқару сервері серверді жою немесе басқа құрылғыға жылжыту кезінде IAM дерекқорын автоматты түрде жоймайды, дерекқорды қолмен жою керек.

- PostgreSQL үшін келесі пәрменді іске қосыңыз:

  `sudo -i -u postgres psql -U postgres -c "CREATE DATABASE <iam_db_атауы>;"`

- MariaDB үшін келесі пәрменді іске қосыңыз:

  `sudo mysql -u root -p -e "CREATE DATABASE <iam_db_name>;"`

ДҚБЖ орнатылған құрылғыда белсенді және енжар түйіндер ретінде жұмыс істейтін құрылғылар қосылымын конфигурациялаңыз.

6 Белсенді және пассивті түйіндерді дайындау

Белсенді және белсенді емес түйіндер ретінде жұмыс істеу үшін аппараттық және бағдарламалық жасақтамасы бірдей екі құрылғыны дайындаңыз.

Нұсқаулар: ақауларға төзімді Kaspersky Security Center Linux кластері үшін түйіндерді дайындау

7 Kaspersky Security Center Linux орнату

Kaspersky Security Center Linux бағдарламасын істен шығуға төзімді кластер режимінде екі түйінге де орнатыңыз.

Алдымен Kaspersky Security Center Linux бағдарламасын белсенді түйін болатын құрылғыға, содан кейін енжар түйінге орнату керек.

Нұсқаулар: Kaspersky Security Center Linux бағдарламасын ақауларға төзімді Kaspersky Security Center Linux кластерінің түйіндеріне орнату.

8 Kaspersky Security Center Web Console орнату

Kaspersky Security Center Web Console веб-консолін кластер түйіні емес бөлек құрылғыға орнатыңыз.

Жауап файлындағы басқару сервері мекенжайы ретінде ақауларға төзімді кластерді көрсетіңіз.

Басқару серверінің сертификаты келесі жолда орналасқан:
/mnt/KlFocDataShare_klfoc/1093/cert/klserver.cer

Сертификат файлын Kaspersky Security Center Web Console орнатылып жатқан құрылғыға көшіріңіз. Жауап файлында сертификаттың жергілікті жолын көрсетіңіз.

9 Істен шығуға төзімді кластерді тестілеу

Істен шығуға төзімді кластерді дұрыс конфигурациялағаныңызға және оның дұрыс жұмыс істеп тұрғанына көз жеткізіңіз. Мысалы, енжар түйінге ауысуды бастау үшін келесі пәрменді іске қосуға болады:

`/opt/kaspersky/ksc64/sbin/klfoc -failover --stp klfoc`

Ақауларға төзімді кластерді басқару қызметінің екі түйінде де `Active: active (running)` екенін тексеру үшін келесі пәрменді пайдаланыңыз:

`systemctl status klfocsvc_klfoc`

Ақауларға төзімді басқа кластер қызметтерінің белсенді түйінде `Active: active (running)` екенін тексеру үшін келесі пәрмендерді пайдаланыңыз: Енжар түйінде келесі ақауларға төзімді кластер қызметтері `Active: inactive (dead)` немесе `Active: failed (Result: signal)` болуы керек.

- `systemctl status klnagent_klfoc`
- `systemctl status kladminserver_klfoc`
- `systemctl status klactprx_klfoc`
- `systemctl status klwebsrv_klfoc`

Ақауларға төзімді Kaspersky Security Center Linux кластері орналастырылды.

Ақауларға төзімді Kaspersky Security Center Linux кластері. Аппараттық және бағдарламалық талаптар

Kaspersky Endpoint Security for Linux бағдарламасын белсенді және пассивті түйіндерге, ДҚБЖ бар құрылғыға және файл серверіне орнатуды ұсынамыз. Kaspersky Security Center Linux ақауларға төзімді кластерін және Kaspersky Endpoint Security for Linux бағдарламасын бірлесіп орнату үшін түйіндер мен файл серверіне қойылатын талаптарға 1,5 ГБ жедел жадты және CPU-ға 15%-ды қосу керек, сондай-ақ кемінде 300 IOPS болуы қажет.

Ақауларға төзімді Kaspersky Security Center Linux кластерін орналастыру үшін сізде келесі жабдық болуы керек:

- Аппараттық және бағдарламалық жасақтамасы бірдей екі құрылғы. Бұл құрылғылар белсенді және белсенді емес түйіндер ретінде әрекет етеді.

  Белсенді және пассивті түйіндер үшін минималды конфигурация

Жабдық	Мән
Процессор	2 ядро, 2500 МГц
ЖЖҚ	6 ГБ
Диск кеңістігі	10 ГБ, 150 IOPS немесе одан жоғары
Желілік интерфейс контроллері	1 Гбит/с

- CIFS/SMB протоколының 2.0 немесе одан жоғары нұсқасын қолдайтын файл сервері. Файл сервері ретінде әрекет ететін арнайы құрылғы ұсынуыңыз керек.

  Файл серверінің конфигурациясы

Жабдық	Мән
Процессор	16 ядро, 2500 МГц
ЖЖҚ	32 ГБ
Диск кеңістігі	500 ГБ, 500 IOPS немесе одан жоғары
Желілік интерфейс контроллері	10 Гбит/с

  Файл сервері, белсенді және пассивті түйіндер арасында желінің жоғары өткізу қабілеттілігін қамтамасыз еткеніңізге көз жеткізіңіз.

- Дерекқорды басқару жүйесі (ДҚБЖ) бар құрылғы. MariaDB Galera Cluster-ді ДҚБЖ ретінде пайдалансаңыз, бұл мақсат үшін арнайы құрылғы қажет емес.

Ақауларға төзімді Kaspersky Security Center Linux кластері үшін файлдық серверді дайындау

Файлдық сервер ақауларға төзімді Kaspersky Security Center Linux кластерінің міндетті құрамдасы сияқты жұмыс істейді.

Файл серверін дайындау үшін:

1. Файл сервері аппараттық және бағдарламалық талаптарға сәйкес келетініне көз жеткізіңіз.

2. NFS серверін орнатыңыз және конфигурациялаңыз:

   - NFS серверінің параметрлеріндегі екі түйін үшін де файл серверіне кіру мүмкіндігін қосу керек.
   - NFS протоколының 4.0 немесе 4.1 нұсқасы болуы керек.
   - Linux ядросына қойылатын минималды талаптар:
     - NFS 4.0 пайдалансаңыз, 3.19.0-25
     - NFS 4.1 пайдалансаңыз, 4.4.0-176

   Linux дистрибутивіңізге байланысты тиісті пәрменді орындау арқылы nfs-utils бумасын немесе nfs-kernel-server бумасын орнатыңыз:

   ```
   sudo yum install nfs-utils
   sudo apt install nfs-kernel-server
   ```

3. Файл серверінде екі қалта жасаңыз және оларға NFS арқылы қатынас беріңіз. Олардың бірі істен шығуға төзімді кластердің күйі туралы ақпаратты сақтау үшін қолданылады. Екіншісі Kaspersky Security Center Linux деректері мен параметрлерін сақтау үшін қолданылады. Kaspersky Security Center Linux орнату кезінде ортақ қатынасы бар қалталарға жолдарды көрсету керек.

   Келесі қалталардың жоқ екеніне көз жеткізіңіз:

   - `/mnt/KlFocStateShare`
   - `/mnt/KlFocDataShare_klfoc`

   Осы қалталардың кез келгені бар болса, оны кері ретпен жойыңыз.

   Келесі пәрмендерді орындаңыз:

   ```
   sudo mkdir -p /mnt/KlFocStateShare
   sudo mkdir -p /mnt/KlFocDataShare_klfoc
   sudo chown ksc:kladmins /mnt/KlFocStateShare
   sudo chown ksc:kladmins /mnt/KlFocDataShare_klfoc
   sudo chmod -R 770 /mnt/KlFocStateShare /mnt/KlFocDataShare_klfoc
   sudo sh -c "echo /mnt/KlFocStateShare *\(rw,sync,no_subtree_check,no_root_squash\) >> /etc/exports"
   sudo sh -c "echo /mnt/KlFocDataShare_klfoc *\
   (rw,sync,no_subtree_check,no_root_squash\) >> /etc/exports"
   sudo exportfs -a
   ```

`sudo systemctl start rpcbind`

`sudo systemctl start nfs-server`

Келесі пәрменді орындау арқылы автоматты іске қосуды қосыңыз:

`sudo systemctl enable rpcbind`

Арнаулы қалталарды көрсетуге болады, бірақ онлайн анықтаманы пайдалану кезінде ыңғайлы болуы үшін, ұсынылған қалта атауларын пайдаланған жөн.

4. Файл серверін қайта іске қосыңыз.

Файл сервері дайындалды. Ақауларға төзімді Kaspersky Security Center Linux кластерін орналастыру үшін осы сценарий нұсқауларын орындаңыз.

Ақауларға төзімді Kaspersky Security Center Linux кластері үшін түйіндерді дайындау

Жалғастырмай тұрып, Сценарий: ақауларға төзімді Kaspersky кластерін орналастыру бөліміндегі алдыңғы қадамдарды аяқтағаныңызға көз жеткізіңіз.

Екі құрылғыны ақауларға төзімді Kaspersky Security Center Linux кластері үшін белсенді және белсенді емес түйін ретінде жұмыс істеуге дайындаңыз.

Жалпы қалталар конфигурациясы

Ортақ қалталарды конфигурациялау үшін:

1. Linux дистрибутивіңізге байланысты тиісті пәрменді орындау арқылы әр торапта nfs-utils бумасын немесе nfs-kernel-server бумасын орнатыңыз:

`yum install nfs-utils`

`apt install nfs-kernel-server`

2. Келесі пәрмендерді орындау арқылы қосылым нүктелерін жасаңыз:

`mkdir -p /mnt/KlFocStateShare`

`mkdir -p /mnt/KlFocDataShare_klfoc`

3. Қосылым нүктелері мен ортақ қалталарды салыстырыңыз:

`sudo sh -c "echo <файл сервері>:/mnt/KlFocStateShare /mnt/KlFocStateShare nfs vers=4,soft,timeo=50,retrans=2,auto,user,rw 0 0 >> /etc/fstab"`

`sudo sh -c "echo <файл сервері>:/mnt/KlFocDataShare_klfoc /mnt/KlFocDataShare_klfoc nfs vers=4,noauto,user,rw,exec 0 0 >> /etc/fstab"`

Мұндағы `{файл сервері}` — ортақ қалталары бар файл серверінің FQDN.

4. Келесі пәрмендерді орындау арқылы ортақ қалталарды іске қосыңыз:

`mount /mnt/KlFocStateShare`

`mount /mnt/KlFocDataShare_klfoc`

5. Ортақ қалта рұқсаттары ksc:kladmins иелігінде екеніне көз жеткізіңіз.

Келесі пәрменді орындаңыз:

`ls -la /mnt/`

Желілік адаптерлерді конфигурациялау

Қосымша желілік адаптер физикалық немесе виртуалды болуы мүмкін. Қосалқы желі адаптері бар орналастыру схемасын таңдасаңыз, екі түйінде де сәйкес процедураны орындаңыз:

- Физикалық желі адаптеріне (MACVLAN технологиясы) негізделген виртуалды қосалқы желі адаптерін пайдаланыңыз:

  1. iputils-arping пакетін орнатыңыз. Linux дистрибутивіне байланысты келесі пәрмендердің бірін іске қосыңыз:

     - `yum install iputils`

     Немесе

     - `apt install iputils-arping`

  2. NetworkManager физикалық желі адаптерін басқару үшін қолданылатынын тексеру мақсатында келесі пәрменді орындаңыз:

     `nmcli device status`

     Пәрмен шығысы физикалық желі адаптерінің басқарылмайтынын көрсетсе, физикалық желі адаптерін басқару үшін NetworkManager құралын конфигурациялаңыз. Нақты конфигурациялау қадамдары дистрибутивіне байланысты.

  3. Интерфейстерді анықтау үшін келесі пәрменді пайдаланыңыз:

     `ip a`

  4. Конфигурация профилін жасау үшін келесі пәрменді орындаңыз:

     `nmcli connection add type macvlan dev <физикалық интерфейс> mode bridge ifname <виртуалды интерфейс> ipv4.addresses <мекенжай маскасы> ipv4.method manual autoconnect no`

- Физикалық қосалқы желі адаптерін пайдаланыңыз немесе гипервизорды пайдаланып, виртуалды TAP құрылғысын жасаңыз. Бұл сценарийде NetworkManager бағдарламалық жасақтамасын өшіріңіз.

  1. Қосалқы желі адаптерін түйінге қосыңыз.

  2. iputils-arping пакетін орнатыңыз. Linux дистрибутивіне байланысты келесі пәрмендердің бірін іске қосыңыз:

     - `yum install iputils`

     Немесе

     - `apt install iputils-arping`

  3. Мақсатты интерфейске арналған NetworkManager қосылымын жою үшін келесі пәрменді орындаңыз:

     `nmcli con del <қосылым атауы>`

     Мақсатты интерфейс қосылымдарын тексеру үшін келесі пәрменді орындаңыз:

     `nmcli con show`

  4. NetworkManager.conf файлын өзгертіңіз. Кілт файлы бөлімін тауып, мақсатты интерфейсті `unmanaged-devices` параметріне тағайындаңыз.

`[keyfile]`

`unmanaged-devices=interface-name:<интерфейс атауы>`

5. NetworkManager құралын қайта іске қосу:

   `systemctl reload NetworkManager`

   Мақсатты интерфейс бұдан былай басқарылмайтынына көз жеткізу үшін келесі пәрменді орындаңыз:

   `nmcli dev status`

Жүктеме теңестіруші конфигурациясы

Жүктеме теңестіргішімен орналастыру схемасын таңдасаңыз, оны конфигурациялау үшін төмендегі нұсқауларды орындаңыз.

Жүктеме теңестіргішін конфигурациялау үшін:

1. nginx немесе басқа жүктеме теңестіруші орнатылған Linux негізіндегі арнайы құрылғыны дайындаңыз.
2. Жүктемені теңестіруді конфигурациялаңыз. Негізгі сервер ретінде белсенді түйінді және резервтік сервер ретінде пассивті түйінді орнатыңыз.
3. Nginx серверінде келесі мақалаға сәйкес басқару серверінің барлық портын ашыңыз: Kaspersky Security Center Linux пайдаланатын порттар.

Ақауларға төзімді Kaspersky Security Center Linux кластерін орналастыру үшін сценарий нұсқауларын орындаңыз.

Ақауларға төзімді кластер түйіндерінің қолжетімділігі басқару серверіне негізгі қосылым порттарының қолжетімділігімен анықталуы керек. Енжар түйін қосқыш пайда болғанша ешқандай сыртқы қосылымды қабылдамайды.

Kaspersky Security Center Linux бағдарламасын ақауларға төзімді Kaspersky Security Center Linux кластерінің түйіндеріне орнату

Жалғастырмай тұрып, Сценарий: ақауларға төзімді Kaspersky кластерін орналастыру бөліміндегі алдыңғы қадамдарды аяқтағаныңызға көз жеткізіңіз.

Бұл процедурада Kaspersky Security Center Linux-ті ақауларға төзімді Kaspersky Security Center Linux кластерінің түйіндеріне орнату жолы сипатталады. Kaspersky Security Center Linux бағдарламасы ақауларға төзімді Kaspersky Security Center Linux кластерінің екі түйініне жеке-жеке орнатылады. Алдымен бағдарламаны белсенді түйінге, содан кейін пассивті түйінге орнатасыз. Орнату кезінде сіз қай түйіннің белсенді және қайсысы пассивті болатынын таңдайсыз.

Құрылғыда орнатылған Linux дистрибутивіне байланысты келесі орнату файлдарының бірін пайдалануыңыз керек:

- ksc64_[version_number]_amd64.deb
- ksc64-[version_number].x86_64.rpm

Орнату файлын Kaspersky сайтынан жүктеу арқылы аласыз.

RED OS 7.3.4 не одан жаңа нұсқасын немесе MSVSPHERE 9.2 не одан жаңа нұсқасын пайдалансаңыз, екі түйінге де libxcrypt-compat пакетін орнатуыңыз керек.

Белсенді түйінге орнату

Kaspersky Security Center Linux жүйесін белсенді түйінге орнату үшін:

1. Kaspersky Security Center Linux орнатқыңыз келетін құрылғыда қолдау көрсетілетін Linux дистрибутивтерінің бірі жұмыс істейтініне көз жеткізіңіз.

2. Қосалқы желілік адаптерді пайдалансаңыз, сұралған кезде оның атауын енгізіңіз. Барлық желі интерфейсін көрсету үшін келесі пәрменді енгізуге болады:

   ```
   ip addr
   ```

3. Kaspersky Security Center Linux орнатуды іске қосыңыз. Linux дистрибутивіңізге байланысты келесі пәрмендердің бірін орындаңыз:

   - `sudo apt-get install /<path>/ksc64_<нұсқа_нөмірі>_amd64.deb`
   - `sudo yum install /<path>/ksc64-<нұсқа_нөмірі>.x86_64.rpm`

4. Kaspersky Security Center Linux конфигурациясын іске қосыңыз:

   ```
   /opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl
   ```

5. Лицензиялық келісімді және Құпиялылық саясатын оқыңыз. Мәтін пәрмен жолы терезесінде көрсетіледі. Мәтіннің келесі бөлігін көру үшін бос орын пернесін басыңыз. Сұрау көрсетілген кезде келесі мәндерді енгізіңіз:

   a. Лицензиялық келісімнің шарттарын түсініп, қабылдасаңыз, `y` енгізіңіз. Лицензиялық келісімнің шарттарын қабылдамасаңыз, `n` енгізіңіз. Kaspersky Security Center Linux бағдарламасын пайдалану үшін Лицензиялық келісімнің шарттарын қабылдау керек.

   b. Құпиялық саясатының шарттарын түсінсеңіз және қабылдасаңыз және деректеріңіз Құпиялылық саясатына сәйкес өңделетініне және жіберілетініне (соның ішінде үшінші елдерге) келіссеңіз `y` енгізіңіз. Құпиялық саясатының шарттарын қабылдамасаңыз, `n` енгізіңіз. Kaspersky Security Center Linux жүйесін пайдалану үшін Құпиялық саясатының шарттарын қабылдауыңыз керек.

6. Басқару серверінің орнату режимі ретінде **кластердің Негізгі түйінін** таңдаңыз.

7. Сұралған кезде, келесі параметрлерді көрсетіңіз:

   a. Күйдің ортақ қалтасының қосылым нүктесінің жергілікті жолын енгізіңіз: `/mnt/KlFocStateShare`

   b. Деректердің ортақ қалтасының қосылым нүктесінің жергілікті жолын енгізіңіз: `/mnt/KlFocDataShare_klfoc`

   c. Ақауларға төзімді кластердің қосылым режимін таңдаңыз: қосымша желілік адаптер немесе сыртқы жүктеме теңгергіші арқылы.

   d. Қосымша желілік адаптерді пайдалансаңыз, оның атауын енгізіңіз.

   e. Қосалқы желі адаптерінің FQDN/IP мекенжайын немесе сыртқы жүктеме теңестірушінің FQDN/IP мекенжайын енгізіңіз.

f. Басқару сервері SSL портының нөмірін енгізіңіз. Әдепкі бойынша порт нөмірі – 13000.

g. Басқаруды жоспарлап отырған құрылғылардың шамамен санын есептеңіз:

- 1-100 басқарылатын құрылғыңыз болса, 1 санын енгізіңіз.
- 101-1000 басқарылатын құрылғыңыз болса, 2 санын енгізіңіз.
- 1000-нан көп басқарылатын құрылғыңыз болса, 3 санын енгізіңіз.

Бұл параметр желі жүктемесін оңтайландыру үшін тапсырманың автоматты түрде рандомизацияланған кешігуі үшін пайдаланылады. Төмендегі тізімде кідіріс есептелетін аралық көрсетілген:

- 1-100 басқарылатын құрылғы, 1 мәні. Кідіріс қолданылмайды.
- 101-1000 басқарылатын құрылғы, 2 мәні. Кідіріс 5 минут.
- 1000-нан көп басқарылатын құрылғы, 3 мәні. Кідіріс 10 минут.

h. Қызметтер үшін қауіпсіздік тобының атын енгізіңіз. Әдепкісінше kladmins тобы пайдаланылады.

i. Басқару сервері қызметін іске қосу үшін есептік жазбаның атауын енгізіңіз. Есептік жазба көрсетілген қауіпсіздік тобының мүшесі болуы керек. Әдепкісінше ksc есептік жазбасы пайдаланылады.

j. Басқа қызметтерді іске қосу үшін есептік жазбаның атауын енгізіңіз. Есептік жазба көрсетілген қауіпсіздік тобының мүшесі болуы керек. Әдепкісінше ksc есептік жазбасы пайдаланылады.

k. Kaspersky Security Center Linux бағдарламасымен жұмыс істеу үшін орнатылған ДҚБЖ таңдаңыз:

- MySQL немесе MariaDB орнатқан болсаңыз, 1 енгізіңіз.
- PostgreSQL немесе Postgres Pro SQL орнатқан болсаңыз, 2 енгізіңіз.

l. Дерекқор орнатылған құрылғының DNS атауын немесе IP мекенжайын енгізіңіз.

m. Дерекқор портының нөмірін енгізіңіз. Бұл порт Басқару серверімен байланысу үшін пайдаланылады. Әдепкі бойынша келесі порттар пайдаланылады:

- MySQL немесе MariaDB үшін 3306 порты
- PostgreSQL немесе Postgres Pro үшін 5432 порты

n. Дерекқор атауын енгізіңіз.

o. Дерекқорға қатынасу үшін пайдаланылатын дерекқордың әкімші есептік жазбасының атауын енгізіңіз.

p. Дерекқорға қатынасу үшін пайдаланылатын дерекқордың әкімші есептік жазбасының құпия сөзін енгізіңіз.

q. IAM серверінің FQDN атауын енгізіңіз.

7е-қадамда енгізген Басқару серверінің DNS атауын көрсетуіңіз керек.

r. IAM қызметін іске қосу үшін есептік жазба атауын енгізіңіз. Есептік жазба көрсетілген қауіпсіздік тобының мүшесі болуы керек. Әдепкісінше ksciam есептік жазбасы пайдаланылады.

s. IAM қызметімен жұмыс істеу үшін орнатылған ДҚБЖ таңдаңыз:

- MySQL немесе MariaDB орнатқан болсаңыз, 1 енгізіңіз.
- PostgreSQL немесе Postgres Pro SQL орнатқан болсаңыз, 2 енгізіңіз.

t. IAM қызметі пайдаланатын IAM ДҚБЖ мекенжайын енгізіңіз.

u. IAM ДҚБЖ порт нөмірін енгізіңіз. Бұл порт IAM қызметімен байланысу үшін пайдаланылады. Әдепкі бойынша келесі порттар пайдаланылады:

- MySQL немесе MariaDB үшін 3306 порты
- PostgreSQL немесе Postgres Pro үшін 5432 порты

v. IAM қызметі пайдаланатын IAM дерекқор атауын енгізіңіз. IAM қызметі пайдаланатын дерекқордың атауы басқару сервері пайдаланатын дерекқордан өзгеше болуы керек.

w. IAM дерекқорына кіру үшін пайдаланылатын дерекқор есептік жазбасының атауын енгізіңіз.

x. IAM дерекқорына кіру үшін пайдаланылатын дерекқор есептік жазбасының құпиясөзін енгізіңіз.

8. Қызметтердің қосылуын және автоматты түрде іске қосылуын күтіңіз:

- klfocsvc_klfoc
- kladminserver_klfoc
- klwebsrv_klfoc
- klactprx_klfoc
- klnagent_klfoc
- kliam_klfoc

9. Басқару серверінің әкімшісінің рөлін орындайтын есептік жазбаны жасаңыз. Пайдаланушының аты мен құпиясөзін енгізіңіз. Пайдаланушының құпиясөзі 8 таңбадан кем немесе 256 таңбадан аспауы керек.

   Бұл қадамды өткізіп жіберсеңіз, есептік жазбаны келесі пәрменді іске қосу арқылы кейінірек жасауға болады:

   ```
   /opt/kaspersky/ksc64/sbin/kladduser -n kscadmin -p <құпиясөз>
   ```

Пайдаланушы қосылды және Kaspersky Security Center Linux бастапқы түйінге орнатылды.

Екіншілік (пассивті) түйінге орнату

Kaspersky Security Center Linux жүйесін екіншілік түйінге орнату үшін:

1. Kaspersky Security Center Linux орнатқыңыз келетін құрылғыда қолдау көрсетілетін Linux дистрибутивтерінің бірі жұмыс істейтініне көз жеткізіңіз.

2. Kaspersky Security Center Linux орнатуды іске қосыңыз. Linux дистрибутивіңізге байланысты келесі пәрмендердің бірін орындаңыз:

   - `sudo apt-get install /<path>/ksc64_<нұсқа_нөмірі>_amd64.deb`
   - `sudo yum install /<path>/ksc64-<нұсқа_нөмірі>.x86_64.rpm`

3. Kaspersky Security Center Linux конфигурациясын іске қосыңыз:

   `/opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl`

4. Лицензиялық келісімді және Құпиялылық саясатын оқыңыз. Мәтін пәрмен жолы терезесінде көрсетіледі. Мәтіннің келесі бөлігін көру үшін бос орын пернесін басыңыз. Сұрау көрсетілген кезде келесі мәндерді енгізіңіз:

   a. Лицензиялық келісімнің шарттарын түсініп, қабылдасаңыз, `y` енгізіңіз. Лицензиялық келісімнің шарттарын қабылдамасаңыз, `n` енгізіңіз. Kaspersky Security Center Linux бағдарламасын пайдалану үшін Лицензиялық келісімнің шарттарын қабылдау керек.

   b. Құпиялық саясатының шарттарын түсінсеңіз және қабылдасаңыз және деректеріңіз Құпиялылық саясатына сәйкес өңделетініне және жіберілетініне (соның ішінде үшінші елдерге) келіссеңіз `y` енгізіңіз. Құпиялық саясатының шарттарын қабылдамасаңыз, `n` енгізіңіз. Kaspersky Security Center Linux жүйесін пайдалану үшін Құпиялық саясатының шарттарын қабылдауыңыз керек.

5. Басқару серверінің орнату режимі ретінде **Екіншілік кластер түйінін** таңдаңыз.

6. Сұралғанда, күйдің ортақ қалтасын қосу нүктесінің жергілікті жолын енгізіңіз: `/mnt/KlFocStateShare`

Kaspersky Security Center Linux бағдарламасы екіншілік түйінге орнатылған.

Қызметтерді тексеру

Ақауларға төзімді басқару сервері `Active: active (running)` екенін тексеру үшін келесі пәрменді пайдаланыңыз:

```
systemctl status klfocsvc_klfoc
```

Ақауларға төзімді басқа кластер қызметтерінің `Active: inactive (dead)` екенін тексеру үшін келесі пәрмендерді пайдаланыңыз:

- `systemctl status klnagent_klfoc`
- `systemctl status kladminserver_klfoc`
- `systemctl status klactprx_klfoc`

- `systemctl status klwebsrv_klfoc`
- `systemctl status kliam_klfoc`

Енді сіз дұрыс конфигурациялағаныңызға және кластердің дұрыс жұмыс істеп тұрғанына көз жеткізу үшін ақауларға төзімді Kaspersky Security Center Linux кластерін тексере аласыз.

Кластер түйінін қолмен іске қосу және тоқтату

Сізге ақауларға төзімді барлық Kaspersky Security Center Linux кластерін тоқтату қажет болуы немесе қызмет көрсету үшін кластер түйіндерінің бірін уақытша өшіру қажет болуы мүмкін. Бұл жағдайда, осы бөлімдегі нұсқауларды орындаңыз. Басқа құралдардың көмегімен істен шығуға төзімді кластермен байланысты қызметтерді немесе процестерді істен шығуға немесе тоқтатуға тырыспаңыз. Бұл деректердің жоғалуына әкелуі мүмкін.

Қызмет көрсету үшін істен шығуға төзімді кластерді іске қосу және тоқтату

Барлық істен шығуға төзімді кластерді іске қосу немесе тоқтату үшін:

Белсенді түйінде келесі пәрмендердің бірін іске қосыңыз:

- Кластерді тоқтату үшін: `/opt/kaspersky/ksc64/sbin/klfoc -stopcluster --stp klfoc`
- Кластерді іске қосу үшін: `/opt/kaspersky/ksc64/sbin/klfoc -startcluster --stp klfoc`

Істен шығуға төзімді кластер пәрменге байланысты іске қосылады немесе тоқтайды.

Түйіндердің біріне қызмет көрсету

Түйіндердің біріне қызмет көрсету үшін:

1. Істен шығуға төзімді түйінде `klfoc -stopcluster --stp klfoc` пәрменінің көмегімен істен шығуға төзімді кластерді тоқтатыңыз.
2. Қызмет көрсеткіңіз келетін түйінде /opt/kaspersky/ksc64/sbin мекенжайына өтіңіз.
3. `detach_node.sh` пәрменін орындау арқылы пәрмен жолын ашып, түйінді кластерден ажыратыңыз.
4. Істен шығуға төзімді түйінде `klfoc -startcluster --stp klfoc` пәрменінің көмегімен істен шығуға төзімді кластерді іске қосыңыз.
5. Техникалық қызмет көрсету жұмыстарын орындаңыз.
6. Істен шығуға төзімді түйінде `klfoc -stopcluster --stp klfoc` пәрменінің көмегімен істен шығуға төзімді кластерді тоқтатыңыз.
7. Қызмет көрсетілген түйінде /opt/kaspersky/ksc64/sbin өтіңіз.
8. `attach_node.sh` пәрменін орындау арқылы пәрмен жолын ашып, түйінді кластерге қосыңыз.
9. Істен шығуға төзімді түйінде `klfoc -startcluster --stp klfoc` пәрменінің көмегімен істен шығуға төзімді кластерді іске қосыңыз.

10. Ағымдағы түйін белсенді екенін тексеру мақсатында қызметтердің іске қосылғанын тексеру үшін келесі пәрмендерді іске қосыңыз:

    `systemctl status klnagent_klfoc.service`

    `systemctl status kladminserver_klfoc.service`

    `systemctl status klactprx_klfoc.service`

    `systemctl status klwebsrv_klfoc.service`

    `systemctl status kliam_klfoc.service`

    Бұл қызметтер енжар түйінде емес, белсенді түйінде іске қосылады.

Түйінге қызмет көрсетіліп, ол істен шығуға төзімді кластерге қосылады.

Ақауларға төзімді кластер түйінін қайта орнату

Ақауларға төзімді кластер түйінін қайта орнату үшін:

1. Басқару серверінің сақтық көшірмесін жасаңыз.
2. Белсенді түйінді техникалық қызмет көрсету режиміне ауыстырыңыз.
3. Ағымдағы операциялық жүйені сақтау қажет болса, келесі қадамдарды орындаңыз.

   Құрылғыны немесе операциялық жүйені ауыстырғыңыз келсе, бұл қадамды өткізіп жіберіңіз.

   a. Ақауларға төзімді кластерді тоқтату үшін келесі пәрменді орындаңыз:
   `klfoc -stopcluster --stp klfoc`

   b. Ақауларға төзімді кластер қызметтерін мәжбүрлеп тоқтату үшін келесі пәрмендерді орындаңыз:
   `sudo systemctl stop klfocsvc_klfoc`
   `systemctl status kl*klfoc*`

   c. Ақауларға төзімді кластер каталогтерін ажырату үшін келесі пәрмендерді орындаңыз:
   `sudo umount /mnt/KlFocDataShare_klfoc`
   `sudo umount /mnt/KlFocStateShare`

   d. Kaspersky Security Center Linux бағдарламасын жою үшін Linux дистрибутивіне байланысты келесі пәрмендердің бірін орындаңыз:

   - `sudo dpkg --remove ksc64`

   Немесе

   - `sudo yum remove ksc64`

е. Енжар түйінге арналған келесі нұсқаулардағы барлық қадамды орындаңыз.

1. Ақауларға төзімді Kaspersky Security Center Linux кластері үшін түйіндерді дайындаңыз.

2. Kaspersky Security Center Linux бағдарламасын ақауларға төзімді Kaspersky Security Center Linux кластерінің түйіндеріне орнатыңыз.

4. Техникалық қызмет көрсету режимінен шығыңыз. Кластер түйіндерін қолмен іске қосу және тоқтату нұсқаулығының 6-қадамынан (ақауларға төзімді кластерді тоқтату) жалғастырыңыз.

Ақауларға төзімді Kaspersky Security Center Linux кластерінің түйіндерінде орнатылған басқару серверіне қосылған Kaspersky Security Center Web Console орнату

Бұл бөлімде ақауларға төзімді Kaspersky Security Center Linux немесе Microsoft кластерінің түйіндерінде орнатылған басқару серверіне қосылатын Kaspersky Security Center Web Console серверін (бұдан әрі — Kaspersky Security Center Web Console) орнату жолы сипатталған. Kaspersky Security Center Web Console серверін орнатпас бұрын, ДҚБЖ және Kaspersky Security Center Linux басқару серверін ақауларға төзімді Kaspersky Security Center Linux кластерінің түйіндеріне орнатыңыз.

> Kaspersky Security Center Web Console кластер түйіндерінде орнатуға қолдау көрсетпейді. Kaspersky Security Center Web Console-ді бөлек серверге орнатуды ұсынамыз.

Ақауларға төзімді Kaspersky Security Center Linux кластерінің түйіндерінде орнатылған басқару серверіне қосылатын Kaspersky Security Center Web Console орнату үшін:

1. Kaspersky Security Center Web Console орнату бөліміндегі 1-қадамды және 2-қадамды орындаңыз.

2. 3-қадамда жауап файлында Kaspersky Security Center Web Console консоліне Kaspersky Security Center Linux ақауларға төзімді кластеріне қосылуға мүмкіндік беретін `trusted` орнату параметрін көрсетіңіз.

   `trusted` орнату параметрінің құрамдастары

   SSO бар домен аутентификациясымен ақауларға төзімді Kaspersky Security Center Linux кластеріне қосылсаңыз, сенімді орнату параметрін келесідей көрсетіңіз: Kaspersky Security Center Web Console-ді басқару серверінің 16 немесе одан кейінгі нұсқасына қоссаңыз, Есептік деректер және қатынасу диспетчері (IAM) ұсынған бір рет кіру (SSO) мүмкіндігі бар домен аутентификациясы қолданылады. Бұл жағдайда `trusted` орнату параметрін келесідей көрсетіңіз:

```
"trusted":  {
  "<Басқару серверінің атауы>": {
    "iamHost": "ksc-iam.example.com",
    "iamOAuthPort": 4444,
    "iamProxyPort": 9050,
    "iamCertPath": "<ортақ деректер қалтасы>/iam/main_certificate.pem",
    "iamPATPath": "<ортақ деректер қалтасы>/iam/initial_token.txt",
    "kscPort": 13299,
    "kscCertPath": "<ортақ деректер қалтасы>/1093/cert/klserver.cer"
  }
}
```

мұндағы

- `< Басқару серверінің атауы >` — Kaspersky Security Center Web Console-іне кіру терезесінде көрсетілетін ақауларға төзімді Kaspersky Security Center Linux кластерінің атауы.

- `iamHost` — басқару сервері және IAM орнатылған құрылғының мекенжайы. Кластер түйіндерін дайындау кезінде қосалқы желі адаптерін жасасаңыз, адаптердің FQDN немесе хост атауын ақауларға төзімді Kaspersky Security Center Linux кластерінің мекенжайы ретінде пайдаланыңыз. Болмаса өзіңіз қолданатын үшінші тараптың жүктеме теңестіргішінің FQDN немесе хост атауын көрсетіңіз.

  Басқару серверін орнату бағдарламасы кезінде көрсетілген IAM мекенжайына `iamHost` мәні сәйкес келуі керек. Көрсетілген IAM мекенжайын алу үшін Басқару сервері хостында келесі пәрменді орындаңыз:

  ```
  grep "iam_address:" /var/opt/kaspersky/klnagent_srv/iam/iam_config.yaml
  ```

- `iamOAuthPort` – OpenID Connect аутентификация протоколы арқылы аутентификация токендерін алмастыру үшін пайдаланылатын порт (әдепкі мәні – 4444). Бұл порт Kaspersky Security Center Web Console Server мен басқару сервері арасындағы, сондай-ақ браузер (Kaspersky Security Center Web Console-мен пайдаланылады) мен басқару сервері арасындағы байланыс үшін де пайдаланылады.

- `iamProxyPort` – Kaspersky Security Center Web Console Server-ді басқару серверіне қосу үшін пайдаланылатын порт (әдепкі мән — 9050).

- `iamCertPath` — IAM сертификатының жолы. IAM сертификаты басқару серверін бірінші рет іске қосқанда автоматты түрде жасалады. Сертификат басқару сервері орнатылған құрылғыда орналасқан. Сертификаттың әдепкі жолы: `< ортақ деректер қалтасы >/iam/main_certificate.pem`. Сертификат ақауларға төзімді Kaspersky Security Center Linux кластерінің ортақ деректерді сақтау орнында орналасқан. Өздігінен қол қойылған IAM сертификаты автоматты түрде бұрылады.

- `iamPATPath` — IAM жүйесінде OAuth клиенті ретінде Kaspersky Security Center Web Console тіркеу үшін пайдаланылатын токен жолы. Бұл файл басқару серверін бірінші рет іске қосқан кезде жасалады. Токен басқару сервері орнатылған құрылғыда орналасқан. Токеннің әдепкі жолы: <ортақ деректер қалтасы>/iam/initial_token.txt. Сертификат ақауларға төзімді Kaspersky Security Center Linux кластерінің ортақ деректерді сақтау орнында орналасқан. Токен шексіз уақыт жарамды және бұруды қажет етпейді.

- `kscPort` — Security Center Web Console басқару серверіне қосылу үшін пайдаланатын OpenAPI порты (әдепкі мән — 13299).

- `kscCertPath` — ақауларға төзімді Kaspersky Security Center Linux кластерінің ортақ деректерді сақтау орнында орналасқан басқару серверінің сертификаты. Сертификат файлына әдепкі бойынша жол: `< ортақ деректер қалтасы >\1093\cert\klserver.cer`.

  > Басқару серверінің сертификат файлын (`kscCertPath` арқылы көрсетілген), IAM сертификат файлын (`iamCertPath` арқылы көрсетілген) және токен файлын (`iamPATPath` арқылы көрсетілген) ортақ деректерді сақтау орнынан Kaspersky Security Center Web Console орнататын құрылғыға көшіріңіз. Басқару серверінің сертификатына апаратын жергілікті жолды көрсетіңіз.

Kaspersky Security Center Web Console-ді басқару серверінің 15.4 немесе одан бұрынғы нұсқасына қоссаңыз, домен пайдаланушысының немесе ішкі пайдаланушының аты мен құпиясөзін көрсету арқылы аутентификациялау қолданылады. Бұл жағдайда сенімді орнату параметрін келесідей көрсетіңіз:

```
"trusted":  {
  "<Басқару серверінің атауы>": {
    "kscHost": "ksc.example.com",
    "kscPort": 13299,
    "kscCertPath": "<ортақ деректер қалтасы>/1093/cert/klserver.cer"
```

```
    }
}
```

мұндағы

- `< Басқару серверінің атауы >` — Kaspersky Security Center Web Console-іне кіру терезесінде көрсетілетін ақауларға төзімді Kaspersky Security Center Linux кластерінің атауы.
- `kscHost` — басқару серверінің мекенжайы (FQDN немесе хост атауы). Кластер түйіндерін дайындау кезінде қосалқы желі адаптерін жасасаңыз, адаптер мекенжайын ақауларға төзімді Kaspersky Security Center Linux кластерінің мекенжайы ретінде пайдаланыңыз. Болмаса өзіңіз пайдаланып жатқан үшінші тараптың жүктеме теңестіргішінің мекенжайын көрсетіңіз.
- `kscPort` — Kaspersky Security Center Web Console веб-консолі басқару серверіне қосылу үшін пайдаланатын OpenAPI порты (әдепкі мәні — 13299).
- `kscCertPath` — ақауларға төзімді Kaspersky Security Center Linux кластерінің ортақ деректерді сақтау орнында орналасқан басқару серверінің сертификаты. Сертификат файлына әдепкі бойынша жол: `< ортақ деректер қалтасы >\1093\cert\klserver.cer`. Сертификат файлын ортақ деректер қоймасынан Kaspersky Security Center Web Console орнатып жатқан құрылғыға көшіріңіз. Басқару серверінің сертификатына апаратын жергілікті жолды көрсетіңіз.

3. Kaspersky Security Center Web Console стандартты орнатуды жалғастырыңыз.

Орнату аяқталғаннан кейін, сіз Kaspersky Security Center Web Console веб-консолін ашып, жүйеге кіру үшін браузерді пайдалана аласыз.

Kaspersky Security Center Linux ақауларға төзімді кластері.

Бұл бөлімде географиялық таратылған Kaspersky Security Center Linux ақауларға төзімді кластері туралы жалпы ақпарат, сондай-ақ келесі конфигурациялар үшін желіңізде географиялық таратылған ақаулық кластерін дайындау және орналастыру нұсқаулары бар:

- PostgreSQL DBMS жүйесімен Ubuntu жұмыс істейтін кластер түйіндері
- Platform V Pangolin DBMS жүйесімен SberLinux жұмыс істейтін кластер түйіндері

PostgreSQL DBMS жүйесімен Ubuntu жұмыс істейтін географиялық таратылған кластер

Осы сценарий бойынша сіз инфрақұрылымыңызды дайындап, географиялық таралған Kaspersky Security Center Linux ақауларға төзімді кластерін орналастыра аласыз.

Алдын ала талаптар

- Денсаулықты тексеру арқылы жоғары қолжетімді DNS теңгергішін орналастырыңыз.
- Белсенді және пассивті кластер түйіндерінің бірдей аппараттық және бағдарламалық конфигурациялары бар екі құрылғы екеніне көз жеткізіңіз.
  - Аппараттық талаптар:
    - Орталық процессо – 16 ядро, 2500 МГц
    - Жедел жад — 32 ГБ
    - Дискілік кеңістік — 300 IOPS немесе одан жоғары жылдамдықпен 500 ГБ
    - Желілік интерфейс контроллері — 1 Гбит/с
  - Бағдарламалық талаптар:
    - Операциялық жүйе: Ubuntu Server 24.04 LTS (Noble Numbat), 64 разрядты
    - DBMS: PostgreSQL 17 64 разрядты

Кезеңдер

Kaspersky Security Center Linux ақауларға төзімді кластерін бір деректерді өңдеу орталығында орналастырылған географиялық таралған ақауларға төзімді кластеріне жаңарту мүмкін емес.

Географиялық таралған Kaspersky Security Center Linux ақауларға төзімді кластерін орналастыру кезең-кезеңімен жүреді:

1. **Ақауларға төзімді кластер түйіндерінің файлдық жүйесін дайындау**

   Екі кластер түйініндегі файлдық жүйені дайындаңыз. Дайындық LVM логикалық томдарын жасауды және каталогтарды орнату нүктелері ретінде конфигурациялауды қамтиды.

2. **Көшірмелі кластер файлдық жүйесін конфигурациялау**

   DRBD утилиталарын орнатыңыз және ақауларға төзімді кластер түйіндері арасында деректерді репликациялау үшін DRBD ресурстарын конфигурациялаңыз. Осыдан кейін, белсенді кластер түйінінде репликацияланған файлдық жүйені жасаңыз.

3. **Ақаулық кластер түйіндерінде Corosync және Pacemaker орнату және конфигурациялау**

   Кластерлік байланысты және ресурстарды басқаруды қамтамасыз ету үшін Corosync және Pacemaker орнатыңыз.

4. **PostgreSQL ДҚБЖ орнату және конфигурациялау**

   PostgreSQL бағдарламасын кластер түйіндеріне орнатыңыз және конфигурациялаңыз.

5. **Kaspersky Security Center Linux бағдарламасын Kaspersky Security Center Linux ақауларға төзімді кластерінің түйіндеріне орнатыңыз.**

   Kaspersky Security Center Linux бағдарламасын кластер түйіндеріне орнатыңыз, содан кейін кластер түйіндері арасында шифрлауды конфигурациялаңыз.

6 **Kaspersky Security Center Web Console веб-консолін ақауларға төзімді кластер түйіндеріне орнату**

Жоғары қолжетімділікті қамтамасыз ету үшін екі ақауларға төзімді кластер түйініне Kaspersky Security Center Web Console орнатыңыз.

Кластер түйіндерінің файлдық жүйесін дайындау

Географиялық таралған Kaspersky Security Center Linux ақауларға төзімді кластерін орналастыруға дайындықтың алғашқы қадамы ретінде екі кластер түйіндерінде де файл жүйесін орнатуыңыз керек. Дайындық LVM логикалық томдарын жасауды және каталогтарды орнату нүктелері ретінде конфигурациялауды қамтиды. Төмендегі процедураны екі кластер түйінде де орындаңыз.

Кластер түйіндерінің файлдық жүйесін дайындау үшін:

1. Басқару сервері деректері мен дерекқоры үшін LVM логикалық томын жасаңыз:

   ```
   lvcreate -L <volume size> -n klfocdata <volume group name>
   ```

   Жауап файлын сақтау үшін бөлек LVM логикалық томын жасаңыз:

   ```
   lvcreate -L <volume size> -n klfocstate <volume group name>
   ```

   мұндағы

   - `volume group name` LVM пайдаланатын том тобының атауы.
   - `klfocdata` және `klfocstate` – логикалық том атаулары. Бұл логикалық томдар осы том тобының ішінде жасалады.

     Біз бұл том атауларын үйлесімділік үшін пайдалануды ұсынамыз, дегенмен қажет болған жағдайда арнайы атауларды көрсете аласыз.
   - `volume size` томның өлшемі. Басқару серверінің деректері мен дерекқоры үшін кемінде 500 ГБ бөлуді ұсынамыз. Жауап файлын сақтауға арналған том аз орынды қажет етеді.

2. Логикалық томдар үшін бекіту нүктелері ретінде пайдаланылатын каталогтар жасаңыз.

   - Басқару серверінің деректері мен дерекқоры үшін:

     ```
     mkdir -p /mnt/KlFocDataShare_klfoc
     ```

   - Жауап файлы үшін:

     ```
     mkdir -p /mnt/KlFocStateShare_klfoc
     ```

Сәйкестік үшін `/mnt/KlFocDataShare_klfoc` және `/mnt/KlFocStateShare_klfoc` каталогтарын пайдалануды ұсынамыз, бірақ қажет болған жағдайда арнайы атауларды көрсете аласыз.

Кластер түйіндерінің файлдық жүйесі дайындалады. Осыдан кейін, сіз репликацияланған кластер файлдық жүйесін конфигурациялауыңыз керек.

Көшірмелі кластер файлдық жүйесін конфигурациялау

DRBD орнату және конфигурациялау

DRBD – деректерді репликациялау үшін қолданылатын үшінші тарап бағдарламалық жасақтамасы (әсіресе, алдыңғы қадамда дайындалған деректер көлемдері мен орнату нүктелері үшін).

Кластер түйіндерінің файлдық жүйесін дайындағаннан кейін, DRBD утилиталарын орнату және кластер түйіндері арасында деректерді репликациялау үшін DRBD ресурстарын конфигурациялау қажет. Төмендегі процедураны екі кластер түйінде де орындаңыз.

Кластер түйіндеріне DRBD орнату және конфигурациялау үшін:

1. DRBD утилиталарын орнатыңыз:

   ```
   apt update
   apt install -y drbd-utils
   ```

   Біз DRBD 9.2.6 немесе одан кейінгі нұсқасын пайдалануды ұсынамыз, себебі ол кіріктірілген трафикті шифрлауды қамтамасыз етеді.

   DRBD трафигін өзіңіздің VPN шешіміңізді пайдаланып шифрлауға болады.

2. Файл жүйесін дайындау кезінде жасалған әрбір логикалық том үшін DRBD ресурсының конфигурация файлдарын (`klfocdata` және `klfocstate`) жасаңыз.

   Барлық конфигурация файлдары `/etc/drbd.d/` ішіне орналастырылуы керек.

   - Ресурс `klfocdata` (Басқару сервері деректері және дерекқоры)

     klfocdata ресурсы үшін асинхронды репликацияны (A протоколы) пайдаланыңыз. Барлық басқа параметрлерді ортаңызға сәйкес конфигурациялаңыз.

     Манифест файлының мысалы

     ```
     resource klfocdata {
         protocol A;
         net {
             after-sb-0pri    discard-least-changes;
             after-sb-1pri    call-pri-lost-after-sb;
             after-sb-2pri    call-pri-lost-after-sb;
         }
         syncer {
             rate 110M;
         }
         # Hostname of the active node
         on db1 {
             device    /dev/drbd0;
             disk      /dev/<volume group name>/klfocdata;
             address   <disk IP address>;
             meta-disk internal;
         }
         # Hostname of the passive node
         on db2 {
             device    /dev/drbd0;
             disk      /dev/<volume group name>/klfocdata;
             address   <disk IP address>;
             meta-disk internal;
         }
     }
     ```

   - Ресурс `klfocstate` (жауап файлы)

     klfocstate ресурсын жасау үшін синхронды репликацияны (C протоколы) пайдаланыңыз. Барлық басқа параметрлерді ортаңызға сәйкес конфигурациялаңыз.

Манифест файлының мысалы

```
resource klfocstate {
    protocol C;
    net {
        after-sb-0pri    discard-least-changes;
        after-sb-1pri    call-pri-lost-after-sb;
        after-sb-2pri    call-pri-lost-after-sb;
    }
    syncer {
        rate 110M;
    }
    # Hostname of the active node
    on db1 {
        device    /dev/drbd2;
        disk      /dev/<volume group name>/klfocstate;
        address   <disk IP address>;
        meta-disk internal;
    }
    # Hostname of the passive node
    on db2 {
        device    /dev/drbd2;
        disk      /dev/<volume group name>/klfocstate;
        address   <disk IP address>;
        meta-disk internal;
    }
}
```

3. Екі ресурс үшін де DRBD метадеректерін инициализациялаңыз:

```
drbdadm create-md klfocdata
drbdadm create-md klfocstate
```

4. Барлық конфигурацияланған ресурстарды DRBD арқылы іске қосыңыз:

```
drbdadm up all
```

DRBD екі кластер түйініне де орнатылған және конфигурацияланған.

Белсенді кластер түйінінде репликацияланған файл жүйесін жасаңыз

Екі кластер түйініне де DRBD орнатып, конфигурациялағаннан кейін, белсенді кластер түйінінде репликацияланған файл жүйесін жасаңыз. Белсенді кластер түйінінде төмендегі процедураны орындаңыз.

Белсенді кластер түйінінде репликацияланған файл жүйесін жасау үшін:

1. Екі DRBD ресурсын да негізгі рөлге көтеріңіз:

```
drbdadm primary --force klfocdata
drbdadm primary --force klfocstate
```

2. Кластер түйіндерінде пайдалану үшін қайталанатын томдарды дайындау үшін DRBD құрылғыларын пішімдеңіз:

```
mkfs.ext4 /dev/drbd0
mkfs.ext4 /dev/drbd2
```

3. Файлдық жүйе параметрлерін конфигурациялау:

```
tune2fs -m 0 /dev/drbd0
tune2fs -m 0 /dev/drbd2
```

4. DRBD құрылғыларын бұрын жасалған каталогтарға орнатыңыз:

```
mount -o noatime /dev/drbd0 /mnt/KlFocDataShare_klfoc
mount -o noatime /dev/drbd2 /mnt/KlFocStateShare_klfoc
```

Егер multipathd қызметі орнатылған болса, ол екі кластер түйінінде де `/dev/drbd*` құрылғыларын елемеу үшін конфигурациялануы керек.

5. Репликация күйін тексеріңіз:

```
drbdadm status
```

Дұрыс файлдық жүйе конфигурациясының шығысы:

```
klfocdata role:Secondary
disk:UpToDate open:no
db2 role:Primary tls:yes
peer-disk:UpToDate

klfocstate role:Secondary
disk:UpToDate open:no
db2 role:Primary tls:yes
peer-disk:UpToDate
```

Белсенді кластер түйініндегі репликацияланған файлдық жүйе конфигурацияланған. Осыдан кейін, сіз кластер түйіндеріне Corosync және Pacemaker бағдарламаларын орнатып, конфигурациялауыңыз керек.

Түйіндерде Corosync және Pacemaker орнату және конфигурациялау

Corosync және Pacemaker бағдарламалары кластерлік байланысты және жоғары қолжетімділік үшін ресурстарды басқаруды қамтамасыз етеді. Олар істен шыққан жағдайда қызметтердің автоматты түрде сау түйінге ауыстырылуын қамтамасыз етеді, бұл жұмыстың тоқтап қалу уақытын азайтады.

Кластер түйіндеріне Corosync және Pacemaker бағдарламаларын орнату және конфигурациялау үшін:

1. Екі кластер түйініне де қажетті пакеттерді орнатыңыз:

```
sudo apt install pacemaker -y
sudo apt install crmsh -y
sudo apt install resource-agent-extra -y
```

2. Ресми құжаттамаға сәйкес екі кластер түйінінде де Corosync және Pacemaker параметрлерін конфигурациялаңыз. Бұған автоматты түрде іске қосуды қосу, аутентификация кілтін жасау және тарату, сондай-ақ аутентификация кілті файлына кіру рұқсаттарын конфигурациялау кіреді.

Параметрлердің дұрыс екеніне көз жеткізу үшін кластер түйіндерінің бірінде келесі пәрменді орындаңыз:

```
crm status
```

Күтілетін нәтиже кластер күйін көрсетіп, барлық белсенді түйіндердің тізімін көрсетуі керек, бұл Corosync дұрыс жұмыс істеп тұрғанын және түйіндер өзара әрекеттесіп жатқанын растайды.

3. Екі кластер түйінінде де Pacemaker кластерінің негізгі параметрлерін конфигурациялаңыз:

```
crm configure property stonith-enabled="false"
crm configure property symmetric-cluster="false"
crm configure rsc_defaults resource-stickiness="110"
crm configure rsc_defaults migration-threshold=3
crm configure property no-quorum-policy=ignore
```

4. Екі кластер түйінінде де Corosync басқаратын сценарийлердің іске қосылуын өшіріңіз:

```
systemctl disable drbd.service
```

5. Кластер түйіндерінің бірінде Pacemaker бағдарламасында DRBD негізіндегі ресурстарды жасаңыз.

- klfocdata үшін DRBD ресурсы

  a. `klfocdata` DRBD томы үшін кластер ресурсын жасаңыз, кластерге өз күйін басқаруға және оның денсаулығын автоматты түрде бақылауға мүмкіндік береді:

  ```
  crm configure primitive drbd_klfocdata ocf:linbit:drbd params drbd_resource="klfocdata" \
  op monitor interval="60s" op start interval="0" timeout="240s" op stop interval="0" \
  timeout="240s" op monitor role=Master interval="10s" op monitor role=Slave interval="30s"
  ```

  b. Жасалған `drbd_klfocdata` ресурсы негізінде `ms_drbd_klfocdata` кластер басқаратын ресурсын жасаңыз:

  ```
  crm configure ms ms_drbd_klfocdata drbd_klfocdata meta master-max="1" master-node-max="1" \
  clone-max="2" clone-node-max="1" notify="true"
  ```

  c. `fs_klfocdata` DRBD томы үшін бекіту нүктесін жасаңыз, ол құрылғыны, мақсатты каталогты, файлдық жүйе түрін және орнату параметрлерін көрсетеді:

  ```
  crm configure primitive fs_klfocdata ocf:heartbeat:Filesystem params device="/dev/drbd0" \
  directory="/mnt/KlFocDataShare_klfoc" fstype="ext4" options="data=journal"
  ```

- klfocstate үшін DRBD ресурсы

  a. `klfocstate` DRBD томы үшін кластер ресурсын жасаңыз, кластерге өз күйін басқаруға және оның денсаулығын автоматты түрде бақылауға мүмкіндік береді:

  ```
  crm configure primitive drbd_klfocstate ocf:linbit:drbd params drbd_resource="klfocstate" \
  op monitor interval="60s" op start interval="0" timeout="240s" op stop interval="0" \
  timeout="240s" op monitor role=Master interval="10s" op monitor role=Slave interval="30s"
  ```

  b. Жасалған `drbd_klfocstate` ресурсы негізінде ms_drbd_klfocstate кластер басқаратын ресурсын жасаңыз:

  ```
  crm configure ms ms_drbd_klfocstate drbd_klfocstate meta master-max="1" master-node-max="1" \
  clone-max="2" clone-node-max="1" notify="true"
  ```

c. Create a mount point for the DRBD volume `fs_klfocstate`, specifying the device, target directory, filesystem type, and mount options:

```
crm configure primitive fs_klfocstate ocf:heartbeat:Filesystem params device="/dev/drbd2" \
directory="/mnt/KlFocStateShare_klfoc" fstype="ext4" options="noatime"
```

6. Екі кластер түйінінде де DRBD қызметін автоматты түрде іске қосуды өшіріңіз:

```
systemctl disable drbd.service
```

Corosync және Pacemaker кластер түйіндеріне орнатылып, конфигурацияланады. Осыдан кейін сіз ДҚБЖ орнатып, Басқару сервері дерекқорын және IAM дерекқорын жасауыңыз керек.

PostgreSQL ДҚБЖ орнату және конфигурациялау

Кластер түйіндеріне Corosync және Pacemaker орнатып, конфигурациялағаннан кейін, екі кластер түйініне де ДҚБЖ орнатуыңыз керек.

ДҚБЖ орнату және конфигурациялау үшін:

1. Екі кластер түйініне де PostgreSQL 17 x64 немесе одан кейінгі нұсқасын орнатыңыз.

   Таңдалған PostgreSQL жүйесін қалай орнату керектігі туралы мәліметтер оның құжаттамасында берілген.

2. ДҚБЖ орнатылған кластер түйінінде келесідей аталатын ДҚБЖ пайдаланушы есептік жазбалары жоқ екеніне көз жеткізіңіз:

   - client
   - iam
   - ksc
   - locker
   - pat
   - scope
   - voltron

3. Екі кластер түйінінде де ДҚБЖ тоқтатыңыз, содан кейін ДҚБЖ қызметін автоматты түрде іске қосуды өшіріңіз:

```
sudo systemctl stop postgresql
sudo systemctl disable postgresql
```

4. Белсенді кластер түйінінде, `/mnt/KlFocDataShare_klfoc/dbms` каталогына ДҚБЖ каталогын көшіріңіз:

```
rsync -av /var/lib/postgresql/17/main/ /mnt/KlFocDataShare_klfoc/dbms
mv /var/lib/postgresql/17/main /var/lib/postgresql/17/main.bk
```

5. Белсенді кластер түйінінде, `/mnt/KlFocDataShare_klfoc/dbms` каталогына PostgreSQL конфигурация файлдарын көшіріңіз:

```
sudo cp /etc/postgresql/17/main/pg_hba.conf /mnt/KlFocDataShare_klfoc/dbms
sudo cp /etc/postgresql/17/main/pg_ident.conf /mnt/KlFocDataShare_klfoc/dbms
```

6. Екі кластер түйінінде де, `/etc/postgresql/17/main/postgresql.conf` конфигурация файлын ашыңыз, содан кейін дерекқор деректер каталогы ретінде `/mnt/KlFocDataShare_klfoc/dbms` каталогын орнатыңыз.

   Сондай-ақ, (`/mnt/KlFocDataShare_klfoc/dbms/pg_hba.conf` және `/mnt/KlFocDataShare_klfoc/dbms/pg_ident.conf`) конфигурация файлдарына апаратын жолдарды көрсетіңіз және `include_dir` параметрін алып тастаңыз:

```
data_directory = '/mnt/KlFocDataShare_klfoc/dbms'
hba_file = '/mnt/KlFocDataShare_klfoc/dbms/pg_hba.conf'
ident_file = '/mnt/KlFocDataShare_klfoc/dbms/pg_ident.conf'
listen_addresses = '*'
```

7. `/etc/postgresql/17/main/postgresql.conf` конфигурация файлында, Kaspersky Security Center Linux талаптарына сәйкес келетін ДҚБЖ конфигурациясын реттеңіз.

8. PostgreSQL-мен жұмыс істеуге арналған тіркелгілерді жасау және конфигурациялау.

9. PostgreSQL қызмет ресурсын жасаңыз:

```
crm configure primitive klfocsvc_dbms ocf:heartbeat:pgsql \
params pgctl="/usr/lib/postgresql/17/bin/pg_ctl" \
psql="/usr/bin/psql" \
pgdata="/mnt/KlFocDataShare_klfoc/dbms" \
config="/etc/postgresql/17/main/postgresql.conf" \
socketdir="/var/run/postgresql" \
op start timeout=60s \
op stop timeout=60s \
op monitor interval=30s timeout=60s
```

10. PostgreSQL ресурсын `group_klfoc` кластерлік тобына қосыңыз:

```
crm configure edit klfoc_group
```

11. Тізімнің соңында `klfocsvc_dbms` PostgreSQL ресурсының атауын қосыңыз, мысалы:

```
group klfoc_group {
...
klfocsvc_dbms
}
```

12. Белсенді кластер түйінінде, ДҚБЖ серверінде IAM үшін дерекқор жасаңыз. Дерекқор атауы Kaspersky Security Center Linux бағдарламасымен жұмыс істеу үшін орнатылған дерекқордан басқаша болуы керек. Басқару сервері серверді жою немесе басқа құрылғыға жылжыту кезінде IAM дерекқорын автоматты түрде өшірмейді, дерекқорды қолмен өшіру керек;

```
sudo -i -u postgres psql -U postgres -c "CREATE DATABASE <iam_db_name>;"
```

ДҚБЖ орнатылған және конфигурацияланған. Басқару сервері дерекқоры және IAM дерекқоры жасалады. Осыдан кейін, сіз кластер түйіндеріне Kaspersky Security Center Linux орнатуыңыз керек.

Kaspersky Security Center Linux бағдарламасын географиялық таралған ақауларға төзімді кластерінің түйіндеріне орнатыңыз

Kaspersky Security Center Linux жүйесі географиялық бөлінген ауысу кластерінің түйіндеріне жауап файлын үнсіз режимде, яғни пайдаланушының қатысуынсыз орнату арқылы орнатылады. Жауап файлында орнату параметрлерінің реттелетін жиынтықтығы бар: айнымалылар және олардың тиісті мәндері.

Алдын ала талаптар:

- Барлық дайындық қадамдарын орындаңыз:
  - Кластер түйіндерінің файлдық жүйесін дайындау
  - Көшірмелі кластер файлдық жүйесін конфигурациялау
  - Түйіндерде Corosync және Pacemaker орнату және конфигурациялау
  - PostgreSQL ДҚБЖ орнату және конфигурациялау
- Кластер түйіндерінің Ubuntu Server 24.04 LTS (Noble Numbat) x64 жүйесін іске қосатынына көз жеткізіңіз.
- Kaspersky веб-сайтынан `ksc64_[version_number]_amd64.deb` орнату файлын жүктеп алыңыз.

Белсенді түйінге орнату

Kaspersky Security Center Linux жүйесін белсенді түйінге тыныш режимге орнату үшін:

1. Лицензиялық келісімді оқып шығыңыз. Лицензиялық келісімнің шарттарын түсініп, қабылдаған жағдайда ғана төмендегі қадамдарды орындаңыз.
2. `kladmins` тобын және `kladmins` тобының мүшелері болуы керек артықшылықсыз `ksc` және `ksciam` есептік жазбаларын жасаңыз. Ол үшін root-құқықтары бар есептік жазба астында келесі пәрмендерді кезекпен орындаңыз:

   ```
   adduser ksc
   groupadd kladmins
   gpasswd -a ksc kladmins
   usermod -g kladmins ksc
   adduser ksciam
   gpasswd -a ksciam kladmins
   usermod -g kladmins ksciam
   ```

3. `/mnt/KlFocDataShare_klfoc/` каталогында, Kaspersky Security Center Linux файлдары үшін каталог жасаңыз:

   ```
   mkdir /mnt/KlFocDataShare_klfoc/ksc/
   ```

4. Жауап файлын (TXT пішімінде) жасаңыз және жауап файлына VARIABLE_NAME=variable_value пішіміндегі айнымалылар тізімінің әрбірін бөлек жолға қосыңыз.

   Kaspersky Security Center Linux жүйесін тыныш режимде орнату үшін пайдаланылатын параметрлер тізімінде географиялық таратылған кластерді орналастыру үшін қажетті келесі параметрлерді көрсетіңіз:

   - `KLFOC_UNATT_EXT_RESOURCE_MANAGEMENT=2`

     Географиялық таралған кластерді қосу үшін `2` мәнін орнатыңыз.

- `KLSRV_UNATT_SERVERADDRESS=<DNS balancer address>` және `KLSRV_UNATT_IAM_ADDRESS=<DNS balancer address>`

  Денсаулықты тексеру мүмкіндігі бар DNS теңгергіші бұрыннан орналастырылған болуы керек. Бұл параметрлердің мәндері бірдей болуы және DNS теңгергішінің FQDN-іне орнатылуы керек.

5. Түбірлік немесе пайдаланушы ортасындағы `KLAUTOANSWERS` ортасының жауап файлының толық атауын, соның ішінде жолды қамтитын айнымалы мәнін, мысалы, келесі пәрменді пайдалану арқылы орнатыңыз:

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

6. Kaspersky Security Center Linux жүйесін орнатуды келесі пәрмендерді орындау арқылы үнсіз режимде бастаңыз:

   - Түбірлік ортада:

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

   - Пайдаланушы ортасында:

     ```
     sudo -E apt-get install /<path>/ksc64_[version_number]_amd64.deb -y
     ```

7. klfocsvc_klfoc.service қызметін автоматты түрде іске қосуды өшіру:

   ```
   systemctl disable klfocsvc_klfoc.service
   ```

8. Kaspersky Security Center Linux орнатылғаннан кейін, белсенді кластер түйінін тоқтатыңыз.

9. Барлық кластер ресурстарын пассивті түйінге жылжытыңыз.

   Ол үшін `crm node standby` пәрменін пайдалануға болады (қайта қосу үшін `crm node online` пәрменін пайдаланыңыз).

Екіншілік (пассивті) түйінге орнату

Kaspersky Security Center Linux жүйесін пассивті түйінге орнату үшін:

1. Kaspersky Security Center Linux орнатуды іске қосыңыз:

   ```
   sudo apt-get install /<path>/ksc64_<version_number>_amd64.deb
   ```

2. Kaspersky Security Center Linux конфигурациясын іске қосыңыз:

   ```
   /opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl
   ```

3. Лицензиялық келісімді және Құпиялылық саясатын оқыңыз. Мәтін пәрмен жолы терезесінде көрсетіледі. Мәтіннің келесі бөлігін көру үшін бос орын пернесін басыңыз. Сұрау көрсетілген кезде келесі мәндерді енгізіңіз:

   - Лицензиялық келісімнің шарттарын түсініп, қабылдасаңыз, `y` енгізіңіз. Лицензиялық келісімнің шарттарын қабылдамасаңыз, `n` енгізіңіз. Kaspersky Security Center Linux бағдарламасын пайдалану үшін Лицензиялық келісімнің шарттарын қабылдау керек.

   - Құпиялық саясатының шарттарын түсінсеңіз және қабылдасаңыз және деректеріңіз Құпиялылық саясатына сәйкес өңделетініне және жіберілетініне (соның ішінде үшінші елдерге) келіссеңіз `y` енгізіңіз. Құпиялық саясатының шарттарын қабылдамасаңыз, n енгізіңіз. Kaspersky Security Center Linux жүйесін пайдалану үшін Құпиялық саясатының шарттарын қабылдауыңыз керек.

4. Басқару серверінің орнату режимі ретінде кластердің пассивті түйінін таңдаңыз.

5. Сұралғанда, күйдің ортақ қалтасын қосу нүктесінің жергілікті жолын енгізіңіз: `/mnt/KlFocStateShare_klfoc`.

6. klfocsvc_klfoc.service қызметін автоматты түрде іске қосуды өшіру:

```
systemctl disable klfocsvc_klfoc.service
```

7. `klfocsvc_klfoc` қызмет ресурсын жасаңыз:

```
crm configure primitive klfocsvc_klfoc systemd:klfocsvc_klfoc \
op start timeout="900s" interval="0" \
op stop timeout="900s" interval="0" \
op monitor interval="30s" timeout="90s"
```

8. `klfocsvc_klfoc` ресурсын `group_klfoc` тобына қосыңыз:

```
crm configure edit klfoc_group
```

9. Қосу `klfocsvc_klfoc` топтық жолдың соңында, мысалы:

```
group klfoc_group {
...
klfocsvc_klfoc
}
```

10. Белсенді түйінде барлық ресурстардың іске қосылған күйде екеніне көз жеткізіңіз.

```
crm status
```

Кластер түйіндері арасында шифрлауды конфигурациялау

Кластер түйіндері арасында шифрлауды конфигурациялау үшін:

Егер сіз репликацияланған кластер файлдық жүйесін конфигурациялау кезінде DRBD 9.2.6 немесе одан кейінгі нұсқасын орнатқан болсаңыз, кластер түйіндері арасындағы шифрлауды ресми DRBD құжаттамасына сәйкес конфигурациялаңыз.

Балама ретінде, сіз өзіңіздің VPN шешіміңізді пайдаланып кластер түйіндері арасындағы трафикті шифрлай аласыз.

Kaspersky Security Center Linux ақауларға төзімді кластері орнатылды. Осыдан кейін, сіз екі кластер түйініне де Kaspersky Security Center Web Console веб-консолін орнатуыңыз керек.

Platform V Pangolin DBMS жүйесімен SberLinux жұмыс істейтін географиялық таратылған кластер

Осы сценарий бойынша сіз инфрақұрылымыңызды дайындап, географиялық таралған Kaspersky Security Center Linux ақауларға төзімді кластерін орналастыра аласыз.

Алдын ала талаптар

- Денсаулықты тексеру арқылы жоғары қолжетімді DNS теңгергішін орналастырыңыз.
- Белсенді және пассивті кластер түйіндерінің бірдей аппараттық және бағдарламалық конфигурациялары бар екі құрылғы екеніне көз жеткізіңіз.
  - Аппараттық талаптар:
    - Орталық процессо – 16 ядро, 2500 МГц
    - Жедел жад — 32 ГБ
    - Дискілік кеңістік — 300 IOPS немесе одан жоғары жылдамдықпен 500 ГБ
    - Желілік интерфейс контроллері — 1 Гбит/с
  - Бағдарламалық талаптар:
    - Операциялық жүйе: Platform V SberLinux OS Server (SLO) 9.5.1 64 разрядты
    - ДҚБЖ: Platform V Pangolin 6.5.1 64 разрядты

Кезеңдер

> Kaspersky Security Center Linux ақауларға төзімді кластерін бір деректерді өңдеу орталығында орналастырылған географиялық таралған ақауларға төзімді кластеріне жаңарту мүмкін емес.

Географиялық таралған Kaspersky Security Center Linux ақауларға төзімді кластерін орналастыру кезең-кезеңімен жүреді:

1. **Ақауларға төзімді кластер түйіндерінің файлдық жүйесін дайындау**

   Екі кластер түйініндегі файлдық жүйені дайындаңыз. Дайындық LVM логикалық томдарын жасауды және каталогтарды орнату нүктелері ретінде конфигурациялауды қамтиды.

2. **Көшірмелі кластер файлдық жүйесін конфигурациялау**

   DRBD утиліталарын орнатыңыз және ақауларға төзімді кластер түйіндері арасында деректерді репликациялау үшін DRBD ресурстарын конфигурациялаңыз. Осыдан кейін, белсенді кластер түйінінде репликацияланған файлдық жүйені жасаңыз.

3. **Ақаулық кластер түйіндерінде Corosync және Pacemaker орнату және конфигурациялау**

   Кластерлік байланысты және ресурстарды басқаруды қамтамасыз ету үшін Corosync және Pacemaker орнатыңыз.

4. **Platform V Pangolin ДҚБЖ орнату және конфигурациялау**

   Кластер түйіндерінде Platform V Pangolin орнатыңыз және конфигурациялаңыз.

5. **Kaspersky Security Center Linux бағдарламасын Kaspersky Security Center Linux ақауларға төзімді кластерінің түйіндеріне орнатыңыз.**

   Kaspersky Security Center Linux бағдарламасын кластер түйіндеріне орнатыңыз, содан кейін кластер түйіндері арасында шифрлауды конфигурациялаңыз.

6. **Kaspersky Security Center Web Console веб-консолін ақауларға төзімді кластер түйіндеріне орнату**

   Жоғары қолжетімділікті қамтамасыз ету үшін екі ақауларға төзімді кластер түйініне Kaspersky Security Center Web Console орнатыңыз.

Кластер түйіндерінің файлдық жүйесін дайындау

Географиялық таралған Kaspersky Security Center Linux ақауларға төзімді кластерін орналастыруға дайындықтың алғашқы қадамы ретінде екі кластер түйіндерінде де файл жүйесін орнатуыңыз керек. Дайындық LVM логикалық томдарын жасауды және каталогтарды орнату нүктелері ретінде конфигурациялауды қамтиды. Төмендегі процедураны екі кластер түйінде де орындаңыз.

Кластер түйіндерінің файлдық жүйесін дайындау үшін:

1. Басқару сервері деректері мен дерекқоры үшін LVM логикалық томын жасаңыз:

   ```
   lvcreate -L <volume size> -n klfocdata <volume group name>
   ```

   Жауап файлын сақтау үшін бөлек LVM логикалық томын жасаңыз:

   ```
   lvcreate -L <volume size> -n klfocstate <volume group name>
   ```

   мұндағы

   - `volume group name` LVM пайдаланатын том тобының атауы.
   - `klfocdata` және `klfocstate` – логикалық том атаулары. Бұл логикалық томдар осы том тобының ішінде жасалады.

     Біз бұл том атауларын үйлесімділік үшін пайдалануды ұсынамыз, дегенмен қажет болған жағдайда арнайы атауларды көрсете аласыз.

   - `volume size` томның өлшемі. Басқару серверінің деректері мен дерекқоры үшін кемінде 500 ГБ бөлуді ұсынамыз. Жауап файлын сақтауға арналған том аз орынды қажет етеді.

2. Логикалық томдар үшін бекіту нүктелері ретінде пайдаланылатын каталогтар жасаңыз.

   - Басқару серверінің деректері мен дерекқоры үшін:

     ```
     mkdir -p /mnt/KlFocDataShare_klfoc
     ```

- Жауап файлы үшін:

```
mkdir -p /mnt/KlFocStateShare_klfoc
```

Сәйкестік үшін `/mnt/KlFocDataShare_klfoc` және `/mnt/KlFocStateShare_klfoc` каталогтарын пайдалануды ұсынамыз, бірақ қажет болған жағдайда арнайы атауларды көрсете аласыз.

Кластер түйіндерінің файлдық жүйесі дайындалады. Осыдан кейін, сіз репликацияланған кластер файлдық жүйесін конфигурациялауыңыз керек.

Көшірмелі кластер файлдық жүйесін конфигурациялау

DRBD орнату және конфигурациялау

DRBD – деректерді репликациялау үшін қолданылатын үшінші тарап бағдарламалық жасақтамасы (әсіресе, алдыңғы қадамда дайындалған деректер көлемдері мен орнату нүктелері үшін).

Кластер түйіндерінің файлдық жүйесін дайындағаннан кейін, DRBD утилиталарын орнату және кластер түйіндері арасында деректерді репликациялау үшін DRBD ресурстарын конфигурациялау қажет. Төмендегі процедураны екі кластер түйінде де орындаңыз.

Кластер түйіндеріне DRBD орнату және конфигурациялау үшін:

1. DRBD утилиталарын келесідей орнатыңыз:

   a. Екі түйінде де EPEL және ELRepo қоймаларын қосыңыз:

   ```
   dnf install https://dl.fedoraproject.org/pub/epel/epel-release-latest-9.noarch.rpm
   dnf install https://www.elrepo.org/elrepo-release-9.el9.elrepo.noarch.rpm
   ```

   b. kmod-drbd9x пакетінің барлық қолжетімді нұсқаларын шығарыңыз және el9_6 платформасы үшін жасалған пакеттер тізімін сүзіңіз (мысалы, Platform V SberLinux OS Server (SLO) 9.6 қолданылады):

   ```
   dnf search --showduplicates kmod-drbd9x | grep el9_6
   ```

   c. Тізімнен ең соңғы қолжетімді нұсқаны екі түйіндегі орнату бағдарламасы арқылы орнатыңыз. Platform V SberLinux OS Server (SLO) 9.6 үшін мысал:

   ```
   dnf install kmod-drbd9x-9.2.14-1.el9_6.elrepo.x86_64
   dnf install drbd drbd-utils drbd-udev drbd-pacemaker drbd-selinux
   modprobe drbd
   ```

   Егер болашақта жаңа нұсқа пайда болса, нұсқа жолын тиісінше ауыстырыңыз.

   Біз DRBD 9.2.6 немесе одан кейінгі нұсқасын пайдалануды ұсынамыз, себебі ол кіріктірілген трафикті шифрлауды қамтамасыз етеді.

   DRBD трафигін өзіңіздің VPN шешіміңізді пайдаланып шифрлауға болады.

2. Файл жүйесін дайындау кезінде жасалған әрбір логикалық том үшін DRBD ресурсының конфигурация файлдарын (`klfocdata` және `klfocstate`) жасаңыз.

   Барлық конфигурация файлдары `/etc/drbd.d/` ішіне орналастырылуы керек.

   - Ресурс `klfocdata` (Басқару сервері деректері және дерекқоры)

klfocdata ресурсы үшін асинхронды репликацияны (A протоколы) пайдаланыңыз. Барлық басқа параметрлерді ортаңызға сәйкес конфигурациялаңыз.

Манифест файлының мысалы

```
resource klfocdata {
    protocol A;
    net {
        after-sb-0pri    discard-least-changes;
        after-sb-1pri    call-pri-lost-after-sb;
        after-sb-2pri    call-pri-lost-after-sb;
    }
    syncer {
        rate 110M;
    }
    # Hostname of the active node
    on db1 {
        device    /dev/drbd0;
        disk      /dev/<volume group name>/klfocdata;
        address   <disk IP address>;
        meta-disk internal;
    }
    # Hostname of the passive node
    on db2 {
        device    /dev/drbd0;
        disk      /dev/<volume group name>/klfocdata;
        address   <disk IP address>;
        meta-disk internal;
    }
}
```

- Ресурс `klfocstate` (жауап файлы)

  klfocstate ресурсын жасау үшін синхронды репликацияны (C протоколы) пайдаланыңыз. Барлық басқа параметрлерді ортаңызға сәйкес конфигурациялаңыз.

  Манифест файлының мысалы

```
resource klfocstate {
    protocol C;
    net {
        after-sb-0pri    discard-least-changes;
        after-sb-1pri    call-pri-lost-after-sb;
        after-sb-2pri    call-pri-lost-after-sb;
    }
    syncer {
        rate 110M;
    }
    # Hostname of the active node
    on db1 {
        device    /dev/drbd2;
        disk      /dev/<volume group name>/klfocstate;
        address   <disk IP address>;
        meta-disk internal;
    }
    # Hostname of the passive node
    on db2 {
        device    /dev/drbd2;
        disk      /dev/<volume group name>/klfocstate;
        address   <disk IP address>;
        meta-disk internal;
    }
}
```

3. Екі ресурс үшін де DRBD метадеректерін инициализациялаңыз:

```
drbdadm create-md klfocdata
drbdadm create-md klfocstate
```

4. Барлық конфигурацияланған ресурстарды DRBD арқылы іске қосыңыз:

```
drbdadm up all
```

DRBD екі кластер түйініне де орнатылған және конфигурацияланған.

Белсенді кластер түйінінде репликацияланған файл жүйесін жасаңыз

Екі кластер түйініне де DRBD орнатып, конфигурациялағаннан кейін, белсенді кластер түйінінде репликацияланған файл жүйесін жасаңыз. Белсенді кластер түйінінде төмендегі процедураны орындаңыз.

Белсенді кластер түйінінде репликацияланған файл жүйесін жасау үшін:

1. Екі DRBD ресурсын да негізгі рөлге көтеріңіз:

```
drbdadm primary --force klfocdata
drbdadm primary --force klfocstate
```

2. Кластер түйіндерінде пайдалану үшін қайталанатын томдарды дайындау үшін DRBD құрылғыларын пішімдеңіз:

```
mkfs.ext4 /dev/drbd0
mkfs.ext4 /dev/drbd2
```

3. Файлдық жүйе параметрлерін конфигурациялау:

```
tune2fs -m 0 /dev/drbd0
tune2fs -m 0 /dev/drbd2
```

4. DRBD құрылғыларын бұрын жасалған каталогтарға орнатыңыз:

```
mount -o noatime /dev/drbd0 /mnt/KlFocDataShare_klfoc
mount -o noatime /dev/drbd2 /mnt/KlFocStateShare_klfoc
```

Егер multipathd қызметі орнатылған болса, ол екі кластер түйінінде де `/dev/drbd*` құрылғыларын елемеу үшін конфигурациялануы керек.

5. Репликация күйін тексеріңіз:

```
drbdadm status
```

Дұрыс файлдық жүйе конфигурациясының шығысы:

```
klfocdata role:Secondary
disk:UpToDate open:no
db2 role:Primary tls:yes
peer-disk:UpToDate

klfocstate role:Secondary
disk:UpToDate open:no
db2 role:Primary tls:yes
peer-disk:UpToDate
```

Белсенді кластер түйініндегі репликацияланған файлдық жүйе конфигурацияланған. Осыдан кейін, сіз кластер түйіндеріне Corosync және Pacemaker бағдарламаларын орнатып, конфигурациялауыңыз керек.

Түйіндерде Corosync және Pacemaker орнату және конфигурациялау

Corosync және Pacemaker бағдарламалары кластерлік байланысты және жоғары қолжетімділік үшін ресурстарды басқаруды қамтамасыз етеді. Олар істен шыққан жағдайда қызметтердің автоматты түрде сау түйінге ауыстырылуын қамтамасыз етеді, бұл жұмыстың тоқтап қалу уақытын азайтады.

Кластер түйіндеріне Corosync және Pacemaker бағдарламаларын орнату және конфигурациялау үшін:

1. Екі кластер түйініне де қажетті пакеттерді орнатыңыз:

```
dnf install pcs
dnf install drbd-pacemaker
```

2. Ресми құжаттамаға сәйкес екі кластер түйінінде де Corosync және Pacemaker параметрлерін конфигурациялаңыз. Бұған автоматты түрде іске қосуды қосу, аутентификация кілтін жасау және тарату, сондай-ақ аутентификация кілті файлына кіру рұқсаттарын конфигурациялау кіреді.

   Параметрлердің дұрыс екеніне көз жеткізу үшін кластер түйіндерінің бірінде келесі пәрменді орындаңыз:

```
crm status
```

   Күтілетін нәтиже кластер күйін көрсетіп, барлық белсенді түйіндердің тізімін көрсетуі керек, бұл Corosync дұрыс жұмыс істеп тұрғанын және түйіндер өзара әрекеттесіп жатқанын растайды.

3. Екі кластер түйінінде де Pacemaker кластерінің негізгі параметрлерін конфигурациялаңыз:

```
pcs property set stonith-enabled=false
pcs property set symmetric-cluster=false
pcs resource defaults resource-stickiness=110
pcs resource defaults migration-threshold=3
pcs property set no-quorum-policy=ignore
```

4. Екі кластер түйінінде де Corosync басқаратын сценарийлердің іске қосылуын өшіріңіз:

```
systemctl disable drbd.service
```

5. Кластер түйіндерінің бірінде Pacemaker бағдарламасында DRBD негізіндегі ресурстарды жасаңыз.

- klfocdata үшін DRBD ресурсы

  a. `klfocdata` DRBD томы үшін кластер ресурсын жасаңыз, кластерге өз күйін басқаруға және оның денсаулығын автоматты түрде бақылауға мүмкіндік береді:

  ```
  pcs resource create drbd_klfocdata ocf:linbit:drbd \
  drbd_resource="klfocdata" \
  op monitor interval=60s \
  op start interval=0 timeout=240s \
  op stop interval=0 timeout=240s \
  op monitor role=Master interval=10s \
  op monitor role=Slave interval=30s \
  ```

  b. Жасалған `drbd_klfocdata` ресурсы негізінде `ms_drbd_klfocdata` кластер басқаратын ресурсын жасаңыз:

  ```
  pcs resource clone drbd_klfocdata promotable=true
  master-max=1
  clone-max=2
  clone-node-max=1 notify=true
  ```

  c. `fs_klfocdata` DRBD томы үшін бекіту нүктесін жасаңыз, ол құрылғыны, мақсатты каталогты, файлдық жүйе түрін және орнату параметрлерін көрсетеді:

  ```
  pcs resource create fs_klfocdata ocf:heartbeat:Filesystem \
  device="/dev/drbd0" \
  directory="/mnt/KlFocDataShare_klfoc" \
  fstype="ext4" \
  options="data=journal"
  ```

- klfocstate үшін DRBD ресурсы

  a. `klfocstate` DRBD томы үшін кластер ресурсын жасаңыз, кластерге өз күйін басқаруға және оның денсаулығын автоматты түрде бақылауға мүмкіндік береді:

  ```
  pcs resource create drbd_klfocstate ocf:linbit:drbd \
  drbd_resource=klfocstate \
  op monitor interval=60s \
  op start interval=0 timeout=240s \
  op stop interval=0 timeout=240s \
  op monitor role=Promoted interval=10s \
  op monitor role=Unpromoted interval=30s \
  ```

  b. Жасалған `drbd_klfocstate` ресурсы негізінде ms_drbd_klfocstate кластер басқаратын ресурсын жасаңыз:

  ```
  pcs resource clone drbd_klfocstate promotable=true \
  master-max=1 \
  clone-max=2 \
  clone-node-max=1 \
  notify=true
  ```

c. Create a mount point for the DRBD volume `fs_klfocstate`, specifying the device, target directory, filesystem type, and mount options:

```
pcs resource create fs_klfocstate ocf:heartbeat:Filesystem \
device="/dev/drbd2" \
directory="/mnt/KlFocStateShare_klfoc" \
fstype="ext4" \
options="noatime"
```

6. Екі кластер түйінінде де DRBD қызметін автоматты түрде іске қосуды өшіріңіз:

```
systemctl disable drbd.service
```

Corosync және Pacemaker кластер түйіндеріне орнатылып, конфигурацияланады. Осыдан кейін сіз ДҚБЖ орнатып, Басқару сервері дерекқорын және IAM дерекқорын жасауыңыз керек.

Platform V Pangolin ДҚБЖ орнату және конфигурациялау

Кластер түйіндеріне Corosync және Pacemaker орнатып, конфигурациялағаннан кейін, екі кластер түйініне де ДҚБЖ орнатуыңыз керек.

ДҚБЖ орнату және конфигурациялау үшін:

1. Екі кластер түйініне де Platform V Pangolin 6.5.1 x64 немесе одан кейінгі нұсқасын орнатыңыз.

   Platform V Pangolin жүйесін қалай орнату керектігі туралы мәліметтер оның құжаттамасында берілген.

2. ДҚБЖ орнатылған кластер түйінінде келесідей аталатын ДҚБЖ пайдаланушы есептік жазбалары жоқ екеніне көз жеткізіңіз:

   - client
   - iam
   - ksc
   - locker
   - pat
   - scope
   - voltron

3. Белсенді кластер түйінінде, `/mnt/KlFocDataShare_klfoc/dbms` каталогына ДҚБЖ каталогын көшіріңіз:

```
sudo rsync -av  /pgdata/06/data/ /mnt/KlFocDataShare_klfoc/dbms
sudo mv /pgdata/06/data/ /pgdata/06/data.bk/
```

4. Екі кластер түйінінде де `/mnt/KlFocDataShare_klfoc/dbms/postgresql.conf` конфигурация файлын ашыңыз, содан кейін дерекқор деректер каталогы ретінде `/mnt/KlFocDataShare_klfoc/dbms` каталогын орнатыңыз.

   Сондай-ақ, (`/mnt/KlFocDataShare_klfoc/dbms/pg_hba.conf` және `/mnt/KlFocDataShare_klfoc/dbms/pg_ident.conf`) конфигурация файлдарына апаратын жолдарды көрсетіңіз және `include_dir` параметрін алып тастаңыз:

   ```
   data_directory = '/mnt/KlFocDataShare_klfoc/dbms'
   hba_file = '/mnt/KlFocDataShare_klfoc/dbms/pg_hba.conf'
   ident_file = '/mnt/KlFocDataShare_klfoc/dbms/pg_ident.conf'
   listen_addresses = '*'
   ```

5. `/mnt/KlFocDataShare_klfoc/dbms/postgresql.conf` конфигурация файлында, Kaspersky Security Center Linux талаптарына сәйкес келетін ДҚБЖ конфигурациясын реттеңіз.

6. PostgreSQL-мен жұмыс істеуге арналған тіркелгілерді жасау және конфигурациялау.

7. ДҚБЖ қызмет ресурсын жасаңыз:

   ```
   pcs resource create klfocsvc_dbms pgsql \
   pgctl="/usr/pangolin-6.5/bin/pg_ctl"  psql="/usr/bin/psql" pgdata="/mnt/KlFocDataShare_klfoc/dbms"
   config="/mnt/KlFocDataShare_klfoc/dbms/postgresql.conf" socketdir="/tmp" \
   op start timeout=60s interval=0s \
   op stop timeout=60s interval=0s \
   op monitor interval=30s timeout=60s \
   op promote timeout=120s interval=0s \
   op demote timeout=120s interval=0s \
   meta target-role=Started
   ```

8. Екі кластер түйінінде де ДҚБЖ қызметін автоматты түрде іске қосуды өшіріңіз:

   ```
   sudo systemctl disable pangolin.service
   ```

9. `klfocsvc_dbms` ДҚБЖ ресурсын `group_klfoc` кластерлік тобына қосыңыз:

   ```
   pcs resource group add group_klfoc klfocsvc_dbms
   ```

10. Тізімнің соңында `klfocsvc_dbms` PostgreSQL ресурсының атауын қосыңыз, мысалы:

    ```
    group klfoc_group {
    ...
    klfocsvc_dbms
    }
    ```

11. Белсенді кластер түйінінде, ДҚБЖ серверінде IAM үшін дерекқор жасаңыз. Дерекқор атауы Kaspersky Security Center Linux бағдарламасымен жұмыс істеу үшін орнатылған дерекқордан басқаша болуы керек. Басқару сервері серверді жою немесе басқа құрылғыға жылжыту кезінде IAM дерекқорын автоматты түрде өшірмейді, дерекқорды қолмен өшіру керек;

    ```
    sudo -i -u postgres psql -U postgres -c "CREATE DATABASE <iam_db_name>;"
    ```

ДҚБЖ орнатылған және конфигурацияланған. Басқару сервері дерекқоры және IAM дерекқоры жасалады. Осыдан кейін, сіз кластер түйіндеріне Kaspersky Security Center Linux орнатуыңыз керек.

Kaspersky Security Center Linux бағдарламасын географиялық таралған ақауларға төзімді кластерінің түйіндеріне орнатыңыз

Kaspersky Security Center Linux жүйесі географиялық бөлінген ауысу кластерінің түйіндеріне жауап файлын үнсіз режимде, яғни пайдаланушының қатысуынсыз орнату арқылы орнатылады. Жауап файлында орнату параметрлерінің реттелетін жиынтықтығы бар: айнымалылар және олардың тиісті мәндері.

Алдын ала талаптар:

- Барлық дайындық қадамдарын орындаңыз:
  - Кластер түйіндерінің файлдық жүйесін дайындау
  - Көшірмелі кластер файлдық жүйесін конфигурациялау
  - Түйіндерде Corosync және Pacemaker орнату және конфигурациялау
  - Platform V Pangolin ДҚБЖ орнату және конфигурациялау
- Кластер түйіндерінің Platform V SberLinux OS Server (SLO) 9.5.1 x64 жүйесінде жұмыс істейтініне көз жеткізіңіз.
- Kaspersky веб-сайтынан `ksc64_[version_number]_amd64.deb` орнату файлын жүктеп алыңыз.

Белсенді түйінге орнату

Kaspersky Security Center Linux жүйесін белсенді түйінге тыныш режимге орнату үшін:

1. Лицензиялық келісімді оқып шығыңыз. Лицензиялық келісімнің шарттарын түсініп, қабылдаған жағдайда ғана төмендегі қадамдарды орындаңыз.
2. `kladmins` тобын және `kladmins` тобының мүшелері болуы керек артықшылықсыз `ksc` және `ksciam` есептік жазбаларын жасаңыз. Ол үшін root-құқықтары бар есептік жазба астында келесі пәрмендерді кезекпен орындаңыз:

   ```
   adduser ksc
   groupadd kladmins
   gpasswd -a ksc kladmins
   usermod -g kladmins ksc
   adduser ksciam
   gpasswd -a ksciam kladmins
   usermod -g kladmins ksciam
   ```

3. `/mnt/KlFocDataShare_klfoc/` каталогында, Kaspersky Security Center Linux файлдары үшін каталог жасаңыз:

   ```
   mkdir /mnt/KlFocDataShare_klfoc/ksc/
   ```

4. Жауап файлын (TXT пішімінде) жасаңыз және жауап файлына VARIABLE_NAME=variable_value пішіміндегі айнымалылар тізімінің әрбірін бөлек жолға қосыңыз.

Kaspersky Security Center Linux жүйесін тыныш режимде орнату үшін пайдаланылатын параметрлер тізімінде географиялық таратылған кластерді орналастыру үшін қажетті келесі параметрлерді көрсетіңіз:

- `KLFOC_UNATT_EXT_RESOURCE_MANAGEMENT=2`

  Географиялық таралған кластерді қосу үшін `2` мәнін орнатыңыз.

- `KLSRV_UNATT_SERVERADDRESS=<DNS balancer address>` және `KLSRV_UNATT_IAM_ADDRESS=<DNS balancer address>`

  Денсаулықты тексеру мүмкіндігі бар DNS теңгергіші бұрыннан орналастырылған болуы керек. Бұл параметрлердің мәндері бірдей болуы және DNS теңгергішінің FQDN-іне орнатылуы керек.

5. Түбірлік немесе пайдаланушы ортасындағы `KLAUTOANSWERS` ортасының жауап файлының толық атауын, соның ішінде жолды қамтитын айнымалы мәнін, мысалы, келесі пәрменді пайдалану арқылы орнатыңыз:

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

6. Kaspersky Security Center Linux жүйесін орнатуды келесі пәрмендерді орындау арқылы үнсіз режимде бастаңыз:

   - Түбірлік ортада:

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

   - Пайдаланушы ортасында:

     ```
     sudo -E apt-get install /<path>/ksc64_[version_number]_amd64.deb -y
     ```

7. klfocsvc_klfoc.service қызметін автоматты түрде іске қосуды өшіру:

   ```
   systemctl disable klfocsvc_klfoc.service
   ```

8. Kaspersky Security Center Linux орнатылғаннан кейін, белсенді кластер түйінін тоқтатыңыз.

9. Барлық кластер ресурстарын пассивті түйінге жылжытыңыз.

   Ол үшін `pcs node standby` пәрменін пайдалануға болады (қайта қосу үшін `pcs node online` пәрменін пайдаланыңыз).

Екіншілік (пассивті) түйінге орнату

Kaspersky Security Center Linux жүйесін пассивті түйінге орнату үшін:

1. Kaspersky Security Center Linux орнатуды іске қосыңыз:

   ```
   sudo apt-get install /<path>/ksc64_<version_number>_amd64.deb
   ```

2. Kaspersky Security Center Linux конфигурациясын іске қосыңыз:

   ```
   /opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl
   ```

3. Лицензиялық келісімді және Құпиялылық саясатын оқыңыз. Мәтін пәрмен жолы терезесінде көрсетіледі. Мәтіннің келесі бөлігін көру үшін бос орын пернесін басыңыз. Сұрау көрсетілген кезде келесі мәндерді енгізіңіз:

   - Лицензиялық келісімнің шарттарын түсініп, қабылдасаңыз, `y` енгізіңіз. Лицензиялық келісімнің шарттарын қабылдамасаңыз, `n` енгізіңіз. Kaspersky Security Center Linux бағдарламасын пайдалану үшін Лицензиялық келісімнің шарттарын қабылдау керек.

   - Құпиялық саясатының шарттарын түсінсеңіз және қабылдасаңыз және деректеріңіз Құпиялылық саясатына сәйкес өңделетініне және жіберілетініне (соның ішінде үшінші елдерге) келіссеңіз `y` енгізіңіз. Құпиялық саясатының шарттарын қабылдамасаңыз, n енгізіңіз. Kaspersky Security Center Linux жүйесін пайдалану үшін Құпиялық саясатының шарттарын қабылдауыңыз керек.

4. Басқару серверінің орнату режимі ретінде кластердің пассивті түйінін таңдаңыз.

5. Сұралғанда, күйдің ортақ қалтасын қосу нүктесінің жергілікті жолын енгізіңіз: `/mnt/KlFocStateShare_klfoc`.

6. klfocsvc_klfoc.service қызметін автоматты түрде іске қосуды өшіру:

```
systemctl disable klfocsvc_klfoc.service
```

7. `klfocsvc_klfoc` қызмет ресурсын жасаңыз:

```
crm configure primitive klfocsvc_klfoc systemd:klfocsvc_klfoc \
op start timeout="900s" interval="0" \
op stop timeout="900s" interval="0" \
op monitor interval="30s" timeout="90s"
```

8. `klfocsvc_klfoc` ресурсын `group_klfoc` тобына қосыңыз:

```
pcs resource group add group_klfoc klfocsvc_klfoc
```

9. Қосу `klfocsvc_klfoc` топтық жолдың соңында, мысалы:

```
group klfoc_group {
...
klfocsvc_klfoc
}
```

10. Белсенді түйінде барлық ресурстардың іске қосылған күйде екеніне көз жеткізіңіз.

```
pcs status
```

Кластер түйіндері арасында шифрлауды конфигурациялау

Кластер түйіндері арасында шифрлауды конфигурациялау үшін:

Егер сіз репликацияланған кластер файлдық жүйесін конфигурациялау кезінде DRBD 9.2.6 немесе одан кейінгі нұсқасын орнатқан болсаңыз, кластер түйіндері арасындағы шифрлауды ресми DRBD құжаттамасына сәйкес конфигурациялаңыз.

Балама ретінде, сіз өзіңіздің VPN шешіміңізді пайдаланып кластер түйіндері арасындағы трафикті шифрлай аласыз.

Kaspersky Security Center Linux ақауларға төзімді кластері орнатылды. Осыдан кейін, сіз екі кластер түйініне де Kaspersky Security Center Web Console веб-консолін орнатуыңыз керек.

Kaspersky Security Center веб-консолін географиялық таратылған ақауларға төзімді кластер түйіндеріне орнату

Географиялық таралған Kaspersky Security Center Linux ақауларға төзімді кластерін орналастыру үшін Kaspersky Security Center Web Console веб-консолінің жоғары қолжетімділігін қолдау қажет. Мұны істеу үшін Kaspersky Security Center Web Console веб-консолі екі кластер түйініне де орнатылуы керек.

Kaspersky Security Center Web Console орнату үшін:

1. Екі түйінде де, Kaspersky Security Center Web Console веб-консолімен жұмыс істеу үшін есептік жазбаны жасаңыз. Ол үшін келесі пәрменді root құқықтары бар есептік жазбамен келесі пәрменді орындаңыз:

   ```
   /opt/kaspersky/ksc64/sbin/kladduser -n kscadmin -p <password>
   ```

   мұнда құпия сөз кемінде 8 таңбадан тұруы керек.

2. Екі түйінде де, Лицензиялық келісімді (EULA) оқып шығыңыз. Kaspersky Security Center Linux дистрибутиві құрамына Лицензиялық келісім мәтіні бар TXT файлы кірмесе, бұл файлды Kaspersky сайтынан жүктеп алуға болады. Егер сіз Лицензиялық келісімнің шарттарымен келіспесеңіз, бағдарламаны орнатпаңыз.

3. Түйіндердің екеуінде де, Kaspersky Security Center Web Console веб-консолін Басқару сервері қосу параметрлері бар жауаптар файлын жасаңыз: `/etc/ksc-web-console-setup.json`.

   Параметрлердің ең аз жинағын қамтитын жауап файлының мысалы

   Жауап файлының параметрлер жинағы Kaspersky Security Center Web Console қосылатын басқару серверінің нұсқасына байланысты:

   - Басқару серверінің 16 және одан жоғары нұсқасы

     Басқару серверінің 16 немесе одан кейінгі нұсқасына кіруге арналған параметрлердің минималды жинағы бар жауап файлының мысалы:

     ```
     {
         "address": "ksc-web-console.example.com",
         "port": 8080,
         "trusted":  {
             "Administration Server v16": {
                 "iamHost": "ksc16.example.com",
                 "iamOAuthPort": 4444,
                 "iamProxyPort": 9050,
                 "iamCertPath": "/var/opt/kaspersky/klnagent_srv/iam/main_certificate.pem",
                 "iamPATPath": "/var/opt/kaspersky/klnagent_srv/iam/initial_token.txt",
                 "kscPort": 13299,
                 "kscCertPath": "/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer"
             }
         },
         "certDomain":"ksc-web-console.example.com",
         "acceptEula": true
     }
     ```

- Басқару серверінің 15.4 немесе одан кейінгі нұсқасы

  Басқару серверінің 1.4 немесе одан кейінгі нұсқасына кіруге арналған параметрлердің минималды жинағы бар жауап файлының мысалы:

```
{
    "address": "ksc-web-console.example.com",
    "port": 8080,
    "trusted":  {
         "Administration Server v15.4": {
             "kscHost": "ksc.example.com",
             "kscPort": 13299,
             "kscCertPath": "/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer"
         }
    },
    "certDomain":"ksc-web-console.example.com",
    "acceptEula": true
}
```

Kaspersky Security Center Web Console-ді басқару серверімен бір құрылғыға немесе басқа құрылғыға орнатуға болады. Егер Kaspersky Security Center Web Console басқа құрылғыға орнатылған болса, Kaspersky Security Center Web Console-ның веб-мекенжайы (көрсетілген `address`) және Басқару серверінің веб-мекенжайы (көрсетілген `iamHost` немесе `kscHost`) ерекшеленеді. Егер Kaspersky Security Center Web Console Басқару серверімен бір құрылғыда орнатылған болса, бұл параметрлердің мәндері бірдей болады.

Басқару серверін орнату бағдарламасы кезінде көрсетілген IAM мекенжайына `iamHost` мәні сәйкес келуі керек. Көрсетілген IAM мекенжайын алу үшін Басқару сервері орнатылған құрылғыда келесі пәрменді орындаңыз:

```
grep "iam_address:" /var/opt/kaspersky/klnagent_srv/iam/iam_config.yaml
```

Толық ақпарат алу үшін Kaspersky Security Center Web Console орнату параметрлері мақаласын қараңыз.

Сенімді серверлер тізіміне әртүрлі нұсқалардың бірнеше басқару серверін қосуға болады. Бұл жағдайда серверлер әртүрлі аутентификация әдістерін қолдануы мүмкін.

1024-тен жоғары порт нөмірлерін көрсету ұсынылады. Kaspersky Security Center Web Console 1024-тен төмен порттарда жұмыс істегенін қаласаңыз, орнатудан кейін сізде setcup утилитасы бар екеніне көз жеткізіп, келесі пәрменді орындауыңыз керек:

```
sudo setcap 'cap_net_bind_service=+ep' /var/opt/kaspersky/ksc-web-console/node
```

setcap утилитасы болмаса, оны орнатуға болады. **Пәрмендерді көру үшін осы сілтемені басыңыз**.

Debian және Ubuntu операциялық жүйелері үшін келесі пәрмендердің бірін іске қосыңыз:

- `sudo apt-get install libcap2-bin`
- `sudo apt install libcap2-bin`

SUSE Linux Enterprise Server және Red Hat Enterprise Linux үшін пәрменді іске қосыңыз:

- `sudo zypper install libcap-progs`

4. Екі түйінде де орнату файлын root құқықтары бар есептік жазба арқылы іске қосыңыз.

```
sudo apt-get install ksc-web-console-<build number>.x86_64.deb
```

Орнату файлын ашу басталады. Орнату аяқталғанша күте тұрыңыз. Kaspersky Security Center Web Console келесі директорияға орнатылады: `/var/opt/kaspersky/ksc-web-console`.

5. Кластер түйіндерінің бірінде KSCWebConsole қызметіне арналған Pacemaker ресурсын жасаңыз, осылайша KSCWebConsole қызметін Pacemaker басқаратын қызметке айналдырыңыз:

```
crm configure primitive ksc_webconsole systemd:KSCWebConsole \
op monitor interval=30s timeout=60s \
op start timeout=120s \
op stop timeout=120s \
meta target-role=Stopped
```

6. Екі түйінде де KSCWebConsole қызметін тоқтатып, оның автоматты түрде іске қосылуын өшіріңіз:

```
sudo systemctl stop KSCWebConsole
sudo systemctl disable KSCWebConsole
```

7. Кластер түйіндерінің бірінде `ksc_webconsole` ресурсын `group_klfoc` тобына қосыңыз:

```
crm configure edit klfoc_group
```

8. Топтық сызықтың соңында `ksc_webconsole`, кейін `klfocsvc_dbms` қосыңыз, мысалы:

```
group klfoc_group {
...
klfocsvc_dbms
ksc_webconsole
}
```

Орнату аяқталғаннан кейін, сіз Kaspersky Security Center Web Console веб-консолін ашып, жүйеге кіру үшін браузерді пайдалана аласыз.

ДҚБЖ-мен жұмыс істеуге арналған есептік жазбалар

Басқару серверін орнату және онымен жұмыс істеу үшін ішкі ДҚБЖ ішкі есептік жазбасы қажет. Бұл есептік жазба ДҚБЖ-ға қол жеткізуге мүмкіндік береді және арнайы құқықтарды талап етеді. Қажетті құқықтардың жиынтығы келесі критерийлерге байланысты болады:

- ДҚБЖ түрі:
  - MySQL немесе MariaDB
  - PostgreSQL немесе Postgres Pro
- Басқару сервері дерекқорын құру тәсілі:
  - **Автоматты түрде**. Басқару серверін орнатқан кезде Басқару серверін (инсталляторды) орнату бағдарламасы көмегімен Басқару серверінің дерекқорын (бұдан әрі Сервер дерекқоры деп те аталады) автоматты түрде жасауға болады.
  - **Қолмен**. Бос дерекқорды жасау үшін үшінші тарап қолданбасын немесе скриптті пайдалануға болады. Содан соң, Басқару серверін орнату кезінде осы дерекқорды Сервердің дерекқоры ретінде көрсете аласыз.

Есептік жазбаларға құқықтар мен рұқсаттар беру кезінде ең аз артықшылықтар қағидатын ұстаныңыз. Бұл, берілген құқықтар тек қажетті әрекеттерді орындау үшін жеткілікті екенін білдіреді.

Басқару сервері дерекқорына және IAM дерекқорына мәндерді өзгерту, схемаларды, кестелерді, индекстерді жою немесе қосуды қоса алғанда, қолмен өзгертулер енгізбеңіз. Басқару серверінің өзі орындамаған дерекқорларға енгізілген кез келген өзгерістер Басқару серверінің дұрыс жұмыс істеуін бірден немесе кейінірек, мысалы, жаңа нұсқаға жаңартқаннан кейін немесе сақтық көшірмеден қалпына келтіру кезінде және т.б. бұзады. Дерекқорларды өңдеуге тек Kaspersky техникалық қолдау қызметінен нақты нұсқаулар алған кезде ғана рұқсат етіледі.

Төмендегі кестелерде, Басқару серверін орнатпас бұрын және іске қоспас бұрын есептік жазбаларға ұсынылуы тиісті ДҚБЖ-не арналған құқықтар туралы ақпарат бар.

MySQL және MariaDB

ДҚБЖ ретінде MySQL немесе MariaDB таңдасаңыз, ДҚБЖ кіру үшін ДҚБЖ ішкі есептік жазбасын жасаңыз, содан кейін осы есептік жазбаға қажетті құқықтарды беріңіз. Дерекқорды құру тәсілі құқықтар жиынтығына әсер етпейтінін ескеріңіз. Қажетті құқықтар төменде көрсетілген:

- Артықшылықтар схемасы:
  - Басқару сервері дерекқоры: ALL (GRANT OPTION қоспағанда).
  - Жүйе схемалары (mysql және sys): SELECT, SHOW VIEW.
  - Сақталатын sys.table_exists процедурасы: EXECUTE (MariaDB 10.5 немесе одан бұрынғы нұсқасын ДҚБЖ ретінде пайдалансаңыз, сізге EXECUTE құқығын берудің қажеті жоқ).
- Барлық схемаларға арналған жаһандық артықшылықтар: PROCESS, SUPER.

Есептік жазба құқықтарын конфигурациялау туралы қосымша ақпаратты MySQL және MariaDB-мен жұмыс істеу үшін DBMS есептік жазбасын конфигурациялау бөлімінен қараңыз.

Деректерді ортақ кесте кеңістігінен әр кестедегі файл кеңістігіне жіберу жолы туралы мәліметтерді Деректерді MySQL және MariaDB ДҚБЖ-лардағы ортақ кесте кеңістігінен әр кестедегі файл кеңістігіне жіберу бөлімін қараңыз.

Басқару сервері деректерін қалпына келтіру құқықтарын конфигурациялау

ДҚБЖ ішкі есептік жазбасы үшін берген құқықтарыңыз сақтық көшірмеден Басқару сервері деректерін қалпына келтіруге жеткілікті.

PostgreSQL немесе Postgres Pro

PostgreSQL немесе Postgres Pro жүйесін ДҚБЖ ретінде таңдасаңыз, *Postgres* пайдаланушысын (әдепкі бойынша Postgres рөлін) қолдана аласыз немесе ДҚБЖ-не қатынасу үшін Postgres рөлін (бұдан әрі рөл деп те аталады) жасай аласыз. Сервер дерекқорын жасау тәсіліне байланысты, төмендегі кестеде сипатталғандай рөлге қажетті құқықтарды беріңіз. Рөл құқықтарын конфигурациялау туралы қосымша ақпаратты PostgreSQL немесе Postgres Pro жүйесімен жұмыс істеу үшін ДҚБЖ есептік жазбасын конфигурациялау бөлімін қараңыз.

Postgres рөлі құқықтары

Дерекқорды автоматты түрде жасау		Дерекқорды қолмен жасау
Postgres пайдаланушысына қосымша құқықтар қажет емес.	Жаңа рөлге арналған құқықтар: CREATEDB.	Жаңа рөл үшін: • Басқару сервері дерекқорына қатынасу құқықтары: ALL. • Жалпыға ортақ схемадағы барлық кестелерге қатынасу құқықтары: ALL. • Жалпыға ортақ схемадағы барлық бірізділіктерге қатынасу құқықтары: ALL.

Сенімділігі жоғары Postgres кластерін (14 немесе одан кейінгі нұсқа) дерекқор ретінде пайдаланған кезде, пайдаланушының `pg_read_all_stats` артықшылығы болуы керек. Бұл артықшылықты келесі пәрменді іске қосу арқылы беруге болады:

```
GRANT pg_read_all_stats TO "%1";
```

Бұл жерде `%1` — дерекқор пайдаланушысының аты.

Пайдаланушы аты `KLSRV_UNATT_DBMS_LOGIN` параметрінде басқару серверін орнатқан кезде көрсетіледі.

Басқару сервері деректерін қалпына келтіру құқықтарын конфигурациялау

Басқару серверінің деректерін сақтық көшірмеден қалпына келтіру үшін, ДҚБЖ қол жеткізу үшін пайдаланылатын Postgres рөлі Басқару серверінің дерекқорына иелік құқықтарына ие болуы керек.

MySQL және MariaDB-мен жұмыс істеу үшін ДҚБЖ есептік жазбасын конфигурациялау

Алдын ала талаптар

ДҚБЖ есептік жазбаларға құқықтарды тағайындамас бұрын келесі әрекеттерді орындаңыз:

1. Жергілікті әкімші есептік жазбасымен кіргеніңізге көз жеткізіңіз.
2. MySQL немесе MariaDB жүйесімен жұмыс істеу үшін ортаны орнатыңыз.

Басқару сервері дерекқорына және IAM дерекқорына мәндерді өзгерту, схемаларды, кестелерді, индекстерді жою немесе қосуды қоса алғанда, қолмен өзгертулер енгізбеңіз. Басқару серверінің өзі орындамаған дерекқорларға енгізілген кез келген өзгерістер Басқару серверінің дұрыс жұмыс істеуін бірден немесе кейінірек, мысалы, жаңа нұсқаға жаңартқаннан кейін немесе сақтық көшірмеден қалпына келтіру кезінде және т.б. бұзады. Дерекқорларды өңдеуге тек Kaspersky техникалық қолдау қызметінен нақты нұсқаулар алған кезде ғана рұқсат етіледі.

Басқару серверін орнату үшін ДҚБЖ есептік жазбасын конфигурациялау

Басқару серверін орнату үшін ДҚБЖ есептік жазбасын конфигурациялау үшін:

1. ДҚБЖ орнату кезінде жасаған root есептік жазбасының астында MySQL немесе MariaDB жұмыс ортасын іске қосыңыз.
2. Құпиясөзі бар ішкі ДҚБЖ есептік жазбасын жасаңыз. Басқару сервері қызметі және Басқару серверін орнату бағдарламасы (бұдан әрі - орнату бағдарламасы) ДҚБЖ-не қатынасу үшін осы ДҚБЖ ішкі есептік жазбасын пайдаланады.

   Құпиясөзбен ДҚБЖ есептік жазбасын жасау үшін келесі пәрменді орындаңыз:

   ```
   /* kscdbadmin атты пайдаланушыны жасаңыз және kscdbadmin үшін құпиясөз беріңіз */
   CREATE USER 'kscdbadmin' IDENTIFIED BY '<құпиясөз>';
   ```

3. Жасалған ДҚБЖ есептік жазбасына келесі құқықтарды беріңіз:

   - Артықшылықтар схемасы:
     - Басқару сервері дерекқоры: ALL (GRANT OPTION қоспағанда).
     - Жүйе схемалары (mysql және sys): SELECT, SHOW VIEW.
     - sys.table_exists сақталатын рәсімі: EXECUTE.
   - Барлық схемаларға арналған жаһандық артықшылықтар: PROCESS, SUPER.

   Жасалған ДҚБЖ есептік жазбасының қажетті құқықтарын беру үшін келесі скрипті іске қосыңыз:

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

MariaDB 10.5 немесе одан бұрынғы нұсқасын ДҚБЖ ретінде пайдалансаңыз, сізге EXECUTE құқығын берудің қажеті жоқ. Бұл жағдайда скриптіден келесі пәрменді алып тастаңыз: `GRANT EXECUTE ON PROCEDURE sys.table_exists TO 'kscdbadmin'`.

4. ДҚБЖ есептік жазбасына берілген артықшылықтар тізімін көру үшін келесі пәрменді орындаңыз:

   ```
   SHOW grants for 'kscdbadmin';
   ```

5. IAM үшін ДҚБЖ есептік жазбасын жасаңыз. Келесі пәрменді орындаңыз:

   ```
   /* iamdbadmin атты пайдаланушыны жасаңыз және iamdbadmin үшін құпиясөз беріңіз */
   CREATE USER 'iamdbadmin' IDENTIFIED BY '<password>';
   ```

   ДҚБЖ ретінде MySQL 8.0 немесе одан бұрынғы нұсқасын пайдалансаңыз, бұл нұсқалар үшін "SHA2 құпиясөзін кэштеу" аутентификациясына қолдау көрсетілмейтінін ескеріңіз. Әдепкі аутентификацияны "SHA2 құпиясөзін кэштеу" күйінен "MySQL жеке құпиясөзі" параметріне өзгертіңіз:

   - "MySQL жеке құпиясөзі" пайдаланып ДҚБЖ есептік жазбасын жасау үшін келесі пәрменді орындаңыз:

     ```
     CREATE USER 'iamdbadmin'@'%' IDENTIFIED WITH mysql_native_password BY '< құпиясөз >';
     ```

   - Қолданыстағы ДҚБЖ есептік жазбасының аутентификациясын өзгерту үшін келесі пәрменді орындаңыз:

     ```
     ALTER USER 'iamdbadmin'@'%' IDENTIFIED WITH mysql_native_password BY '< құпиясөз >';
     ```

6. Жасалған ДҚБЖ есептік жазбасына келесі құқықтарды беріңіз:

   - Артықшылықтар схемасы:
     - Басқару сервері дерекқоры: ALL (GRANT OPTION қоспағанда).
     - Жүйе схемалары (mysql және sys): SELECT, SHOW VIEW.
     - sys.table_exists сақталатын рәсімі: EXECUTE.
   - Барлық схемаларға арналған жаһандық артықшылықтар: PROCESS, SUPER.

   Жасалған ДҚБЖ есептік жазбасының қажетті құқықтарын беру үшін келесі скрипті іске қосыңыз:

   ```
   /* iamdbadmin артықшылықтарын ұсыну */
   GRANT USAGE ON *.* TO 'iamdbadmin';
   GRANT ALL ON iamdb.* TO 'iamdbadmin';
   GRANT SELECT, SHOW VIEW ON mysql.* TO 'iamdbadmin';
   GRANT SELECT, SHOW VIEW ON sys.* TO 'iamdbadmin';
   GRANT EXECUTE ON PROCEDURE sys.table_exists TO 'iamdbadmin';
   GRANT PROCESS ON *.* TO 'iamdbadmin';
   ```

```
GRANT SUPER ON *.* TO 'iamdbadmin';
```

MariaDB 10.5 немесе одан бұрынғы нұсқасын ДҚБЖ ретінде пайдалансаңыз, сізге EXECUTE құқығын берудің қажеті жоқ. Бұл жағдайда скриптіден келесі пәрменді алып тастаңыз: `GRANT EXECUTE ON PROCEDURE sys.table_exists TO 'iamdbadmin'`.

7. ДҚБЖ есептік жазбасына берілген артықшылықтар тізімін көру үшін келесі пәрменді орындаңыз:

   ```
   SHOW grants for 'iamdbadmin';
   ```

8. Басқару сервері дерекқорын қолмен жасау үшін, келесі скриптті іске қосыңыз (бұл скриптте Басқару сервері дерекқорының атауы – *kav*):

   ```
   CREATE DATABASE kav
   ```

   Сондай-ақ, ДҚБЖ есептік жазбасын жасайтын сценарийде көрсеткен дерекқордың атауын пайдаланыңыз.

9. IAM дерекқорын қолмен жасау үшін келесі скриптті іске қосыңыз (бұл пәрменде IAM дерекқорының атауы *iam*):

   ```
   CREATE DATABASE iam
   ```

   Басқару сервері серверді жою немесе басқа құрылғыға жылжыту кезінде IAM дерекқорын автоматты түрде өшірмейді, дерекқорды қолмен өшіру керек.

10. Басқару серверін орнатыңыз.

Орнату аяқталғаннан кейін, Басқару серверінің дерекқоры құрылады және Басқару сервері жұмыс істеуге дайын.

PostgreSQL және Postgres Pro жүйесімен жұмыс істеу үшін ДҚБЖ есептік жазбасын конфигурациялау

Алдын ала талаптар

ДҚБЖ есептік жазбаларға құқықтарды тағайындамас бұрын келесі әрекеттерді орындаңыз:

1. Жергілікті әкімші есептік жазбасымен кіргеніңізге көз жеткізіңіз.
2. PostgreSQL және Postgres Pro-мен жұмыс істеу үшін ортаны орнатыңыз.
3. Kaspersky Security Center Linux-пен жұмыс істеу үшін PostgreSQL немесе Postgres Pro серверін конфигурациялау.

Басқару сервері дерекқорына және IAM дерекқорына мәндерді өзгерту, схемаларды, кестелерді, индекстерді жою немесе қосуды қоса алғанда, қолмен өзгертулер енгізбеңіз. Басқару серверінің өзі орындамаған дерекқорларға енгізілген кез келген өзгерістер Басқару серверінің дұрыс жұмыс істеуін бірден немесе кейінірек, мысалы, жаңа нұсқаға жаңартқаннан кейін немесе сақтық көшірмеден қалпына келтіру кезінде және т.б. бұзады. Дерекқорларды өңдеуге тек Kaspersky техникалық қолдау қызметінен нақты нұсқаулар алған кезде ғана рұқсат етіледі.

Басқару серверін орнату үшін ДҚБЖ есептік жазбаларын конфигурациялау

Басқару серверін орнату үшін ДҚБЖ есептік жазбаларын конфигурациялау үшін:

1. Postgres-пен жұмыс істеу үшін ортаны іске қосыңыз.
2. *Postgres* дерекқорындағы *Postgres* пайдаланушысымен кіріңіз.
3. Жаңа Postgres рөлін жасаңыз (бұл мысалда рөл — *kscdbadmin*):

```
CREATE USER "kscdbadmin" WITH PASSWORD '<password>';
```

4. Басқару серверінің дерекқорын жасаңыз (бұл мысалда Басқару сервері дерекқорының атауы – `kav`):

```
CREATE DATABASE "kav" ENCODING 'UTF8' OWNER "kscdbadmin";
```

Бұл нұсқаулықтың 3-қадамында жасалған Postgres рөлін дерекқор иесі ретінде көрсетуді ұсынамыз (бұл мысалдағы рөл – *kscdbadmin*).

Басқа пайдаланушыны дерекқор иесі ретінде көрсету

Егер басқа Postgres рөлін көрсету қажет болса, осы иесі (немесе суперпайдаланушы) рөлімен Басқару серверінің дерекқорына қосылып, келесі пәрмендерді орындаңыз:

```
GRANT ALL PRIVILEGES ON DATABASE "kav" TO "kscdbadmin";
GRANT USAGE ON SCHEMA public TO "kscdbadmin";
GRANT CREATE ON SCHEMA public TO "kscdbadmin";
GRANT ALL PRIVILEGES ON ALL TABLES IN SCHEMA "public" TO "kscdbadmin";
GRANT ALL PRIVILEGES ON ALL SEQUENCES IN SCHEMA "public" TO "kscdbadmin";
```

Дерекқор иесі рөлінің ҚОСУ және УАҚЫТША артықшылықтары бар екеніне көз жеткізіңіз.

Егер сіз "New encoding (UTF8) is incompatible with the encoding of the template database" қатесін алсаңыз, пәрменді пайдаланып дерекқорды жасаңыз:
`CREATE DATABASE "kav" ENCODING 'UTF8' OWNER "kscdbadmin" TEMPLATE template0;`
осының орнына:
`CREATE DATABASE "kav" ENCODING 'UTF8' OWNER "kscdbadmin";`

5. IAM үшін жаңа Postgres рөлін жасаңыз (бұл мысалдағы рөл – `iamdbadmin`):

```
CREATE USER "iamdbadmin" WITH PASSWORD '<password>';
```

6. IAM дерекқорын жасаңыз (бұл мысалда, IAM дерекқорының атауы – `iam`):

```
CREATE DATABASE "iam" ENCODING 'UTF8' OWNER "iamdbadmin";
```

Бұл нұсқаулықтың 5-қадамында жасалған Postgres рөлін дерекқор иесі ретінде көрсетуді ұсынамыз (бұл мысалдағы рөл – *iamdbadmin*).

IAM дерекқорының иесі ретінде басқа пайдаланушыны көрсету

Егер сізге басқа Postgres рөлін көрсету қажет болса, осы иесі (немесе суперпайдаланушы) рөлі астындағы IAM дерекқорға қосылып, келесі командаларды орындаңыз:

```
GRANT ALL PRIVILEGES ON DATABASE "iam" TO "iamdbadmin";
GRANT USAGE ON SCHEMA public TO "iamdbadmin";
GRANT CREATE ON SCHEMA public TO "iamdbadmin";
GRANT ALL PRIVILEGES ON ALL TABLES IN SCHEMA "public" TO "iamdbadmin";
GRANT ALL PRIVILEGES ON ALL SEQUENCES IN SCHEMA "public" TO "iamdbadmin";
```

Дерекқор иесі рөлінің ҚОСУ және УАҚЫТША артықшылықтары бар екеніне көз жеткізіңіз.

Егер сіз "New encoding (UTF8) is incompatible with the encoding of the template database" қатесін алсаңыз, пәрменді пайдаланып дерекқорды жасаңыз:
`CREATE DATABASE "iam" ENCODING 'UTF8' OWNER "iamdbadmin" TEMPLATE template0;`
осының орнына:
`CREATE DATABASE "iam" ENCODING 'UTF8' OWNER "iamdbadmin";`

Басқару сервері серверді жою немесе басқа құрылғыға жылжыту кезінде IAM дерекқорын автоматты түрде өшірмейді, дерекқорды қолмен өшіру керек.

7. Басқару серверін орнатыңыз.

Орнату аяқталғаннан кейін, Басқару сервері Басқару серверінің деректерін сақтау үшін құрылған дерекқорды пайдаланады. Басқару сервері жұмыс істеуге дайын.

Деректерді MySQL және MariaDB ДҚБЖ-лардағы ортақ кесте кеңістігінен әр кестедегі файл кеңістігіне жіберу

MySQL және MariaDB ДҚБЖ үшін деректерді келесі жолдармен сақтауға болады:

- Барлық пайдаланушы дерекқорының деректері бір файлда (әдетте `ibdata1` файлында) сақталған кезде, ортақ кесте кеңістігі ретінде.
- Әр кесте үшін бөлек деректер кеңістігі жеке файл ретінде жасалғанда, әр кестедегі файл кеңістігі ретінде.

Ортақ кесте кеңістігін пайдалану кесте кеңістігінің фрагментациялану қаупін арттырады. `SHRINK` мүмкін болмағандықтан, ортақ кесте кеңістігіндегі файл диск кеңістігінің шамамен 90%-ын алуы мүмкін. Бұл дискінің ішкі жүйесінің жұмысына теріс әсер етеді. Осылайша әр кестедегі файл кеңістігін таңдау пайдалы.

Бұл мақалада деректерді ортақ кесте кеңістігінен әр кестедегі файл кеңістігіне жіберу жолы сипатталған. MySQL немесе MariaDB ДҚБЖ басқа қолданбалармен де пайдаланылса, осы қолданбалардың дерекқорларын әр кестедегі файл кеңістігіне жіберу керек.

Бұл процедураны тек Басқару сервері үшін MySQL немесе MariaDB ДҚБЖ пайдалансаңыз ғана орындауды ұсынамыз.
Деректерді ортақ кестелік кеңістіктен жеке файлдық кестелік кеңістікке жылжыту диск ішкі жүйесіне жүктемені арттыруы мүмкін.

Алдын ала талаптар

Бастамай тұрып, келесілерді тексеріңіз:

- Деректердің сақтық көшірмесін жасау тапсырмасын немесе klbackup утилитасын іске қосу арқылы басқару сервері деректерінің сақтық көшірмесін жасадыңыз.
- Дерекқорлары MySQL немесе MariaDB ДҚБЖ (бар болса) арқылы басқарылатын басқа қолданбалардың сақтық көшірмесін жасадыңыз.
- ДҚБЖ орнатылған құрылғыда дерекқор бар бөлімде бос диск кеңістігі бар.

Қажетті диск кеңістігі ағымдағы жалпы дерекқорлар өлшемінің 150%-ын құрайды (`ibdata1` файлының ағымдағы өлшемі).

Процесс

Деректерді ортақ кесте кеңістігінен әр кестедегі файл кеңістігіне жіберу үшін:

1. Осы процедураны орындағыңыз келетін ДҚБЖ данасын пайдаланып, Kaspersky Security Center басқару сервері қызметін және басқа қолданбаларды тоқтатыңыз.
2. ДҚБЖ нұсқасына байланысты ДҚБЖ-ға суперпайдаланушы ретінде кіріңіз, содан кейін кез келген ыңғайлы қолданбада `fix_tablespace.sql` скриптісін іске қосыңыз.

   Осы сілтемелерді басып, `fix_tablespace.sql` скриптілерін көруге болады:

   MySQL 5.7 және MariaDB 10.1+ скриптісін көру

```
DROP PROCEDURE IF EXISTS upgd_alter_all_tables_for_all_databases_to_innodb;
DELIMITER //
CREATE PROCEDURE `upgd_alter_all_tables_for_all_databases_to_innodb` ()
BEGIN
    DECLARE __st_FETCH_STATUS INT;
    DECLARE `schemaName` VARCHAR(192);
    DECLARE `tableName` VARCHAR(192);
    DECLARE `curIX` CURSOR FOR
    SELECT `TABLE_SCHEMA` , `TABLE_NAME`
    FROM information_schema.TABLES
    WHERE `TABLE_SCHEMA` NOT IN ('mysql', 'performance_schema', 'sys') AND TABLE_TYPE = 'BASE TABLE';
    DECLARE CONTINUE HANDLER FOR SQLSTATE '02000' SET __st_FETCH_STATUS = 1;
    OPEN `curIX`;
    SET `__st_FETCH_STATUS` = 0; FETCH `curIX` INTO `schemaName`, `tableName`;
    while1 : WHILE (0 = 0 AND __st_FETCH_STATUS = 0 ) DO
        SET @`strSQL` = CONCAT( 'ALTER TABLE `' , `schemaName`, '`.`',`tableName`, '` ENGINE=''InnoDB'';' );
        PREPARE stmt1 FROM @`strSQL`;
        EXECUTE stmt1;
        DEALLOCATE PREPARE stmt1;
        SET `__st_FETCH_STATUS` = 0; FETCH `curIX` INTO `schemaName`, `tableName`;
    END WHILE;
    CLOSE `curIX`;
END
//
DELIMITER ;
SET GLOBAL innodb_file_per_table = 1;
CALL upgd_alter_all_tables_for_all_databases_to_innodb();
DROP PROCEDURE IF EXISTS upgd_alter_all_tables_for_all_databases_to_innodb;
```

MySQL 8.0+ үшін скриптіні көру

```
DROP PROCEDURE IF EXISTS upgd_alter_all_tables_for_all_databases_to_innodb;
DELIMITER //
CREATE PROCEDURE `upgd_alter_all_tables_for_all_databases_to_innodb` ()
BEGIN
    DECLARE __st_FETCH_STATUS INT;
    DECLARE `schemaName` VARCHAR(192);
    DECLARE `tableName` VARCHAR(192);
    DECLARE `curIX` CURSOR FOR
    SELECT `TABLE_SCHEMA` , `TABLE_NAME`
    FROM information_schema.TABLES
    WHERE `TABLE_SCHEMA` NOT IN ('mysql', 'performance_schema', 'sys') AND TABLE_TYPE = 'BASE TABLE';
    DECLARE CONTINUE HANDLER FOR SQLSTATE '02000' SET __st_FETCH_STATUS = 1;
    OPEN `curIX`;
    SET `__st_FETCH_STATUS` = 0; FETCH `curIX` INTO `schemaName`, `tableName`;
    while1 : WHILE (0 = 0 AND __st_FETCH_STATUS = 0 ) DO
        SET @`strSQL` = CONCAT( 'ALTER TABLE `' , `schemaName`, '`.`',`tableName`, '` ENGINE=''InnoDB'';' );
        PREPARE stmt1 FROM @`strSQL`;
        EXECUTE stmt1;
        DEALLOCATE PREPARE stmt1;
        SET @`strSQL` = CONCAT( 'ALTER TABLE `' , `schemaName`, '`.`',`tableName`, '` TABLESPACE =
innodb_file_per_table;' );
        PREPARE stmt2 FROM @`strSQL`;
        EXECUTE stmt2;
        DEALLOCATE PREPARE stmt2;
        SET `__st_FETCH_STATUS` = 0; FETCH `curIX` INTO `schemaName`, `tableName`;
    END WHILE;
    CLOSE `curIX`;
END
//
DELIMITER ;
SET GLOBAL innodb_file_per_table = 1;
CALL upgd_alter_all_tables_for_all_databases_to_innodb();
DROP PROCEDURE IF EXISTS upgd_alter_all_tables_for_all_databases_to_innodb;
```

Скриптінің орындалуын тоқтатпау керек.
Ешбір ДҚБЖ қатесі орын алмаса, бірақ скриптінің орындалуын тоқтатсаңыз, скриптіні қайта іске қосыңыз немесе осы процедураның қадамдарын орындауды тоқтатыңыз, ДҚБЖ қызметін қайта іске қосыңыз және сақтық көшірмеден басқару серверінің деректерін қалпына келтіріңіз.

3. my.cnf файлының `[mysqld]` бөлімінде `innodb_file_per_table` параметрін `1` мәніне орнатыңыз.

4. MySQL немесе MariaDB қызметін қайта іске қосыңыз.

5. Kaspersky Security Center басқару сервері қызметін қайта іске қосыңыз.

Деректер ортақ кесте кеңістігінен әр кестедегі файл кеңістігіне жіберіледі.

Kaspersky Security Center Linux-пен жұмыс істеуге арналған сертификаттар

Бұл бөлімде Kaspersky Security Center Linux сертификаттары туралы ақпарат және Kaspersky Security Center Web Console сертификаттарын қалай шығару және ауыстыру керектігі, сондай-ақ Сервер Kaspersky Security Center Web Console-імен өзара әрекеттесетін болса, Басқару сервері сертификатын қалай жаңарту керектігі сипатталған.

Kaspersky Security Center сертификаттары туралы

Kaspersky Security Center, бағдарламаның құрамдастары арасында қауіпсіз өзара әрекеттесуді қамтамасыз ету үшін келесі сертификат түрлерін пайдаланады:

- Басқару сервері сертификаты
- Ұялы құрылғы сертификаты
- Веб-сервер сертификаты
- Kaspersky Security Center Web Console сертификаты
- Есептік деректер және қатынасу диспетчерінің сертификаты

Әдепкісінше Kaspersky Security Center өздігінен қол қойылған сертификаттарды (яғни Kaspersky Security Center өзі шығарған) пайдаланады, бірақ ұйымыңыздың желісінің талаптарына жақсырақ жауап беру және қауіпсіздік стандарттарына сәйкес болу үшін оларды арнаулы сертификаттармен ауыстыруға болады. Арнайы сертификатты пайдаланған кезде, сертификат файлында негізгі сертификаттау органына (CA) дейінгі барлық аралық сертификаттарды қоса алғанда, ашық кілттердің толық тізбегі болуы керек. Басқару сервері пайдаланушы сертификатының барлық қолданыстағы талаптарға сәйкестігін тексергеннен кейін, бұл сертификат өздігінен қол қойылған сертификатпен бірдей әрекет ету ауқымына ие болады. Жалғыз айырмашылығы, пайдаланушы сертификаты жарамдылық мерзімі аяқталғаннан кейін автоматты түрде қайта шығарылмайды. Сіз сертификаттарды klsetsrvcert утилитасы арқылы немесе сертификат түріне байланысты Басқару сервері сипаттарындағы Kaspersky Security Center Web Console-інде ауыстырасыз. klsetsrvcert утилитасын пайдалану кезінде келесі мәндердің бірін пайдаланып, сертификат түрін көрсету қажет:

- C – 13000 және 13291 порттары үшін жалпы сертификат.
- CR – 13000 және 13291 порттары үшін жалпы резервтік сертификат.
- M – 13292-порт үшін ұялы құрылғы сертификаты.
- MR – 13292-порт үшін резервтік ұялы құрылғы сертификаты.
- MCA – пайдаланушы сертификаттарын автоматты түрде жасау үшін сенімді сертификаттау орталығынан алынған мобильдік құрылғы сертификаты.

Кез келген Басқару сервері сертификатының ең көп жарамдылық мерзімі 397 күннен аспауы керек.

Басқару серверінің сертификаттары

Басқару сервері сертификаты келесі мақсаттар үшін қажет:

- Kaspersky Security Center Web Console қосылған кездегі басқару серверінің аутентификациясы.
- Басқарылатын құрылғылардағы басқару серверінің және желілік агенттің қауіпсіз өзара әрекеті.
- Негізгі басқару серверлерін қосалқы басқару серверлеріне қосқан кездегі аутентификация.

Басқару серверінің сертификаты, Басқару сервері құрамдасын орнату кезінде автоматты түрде жасалады және /var/opt/kaspersky/klnagent_srv/1093/cert/қалтасында сақталады. Kaspersky Security Center Web Console-ін орнату үшін жауап файлын жасау кезінде Басқару сервері сертификатын көрсетесіз. Мұндай сертификат жалпы ("C") деп аталады.

Басқару сервері сертификаты 397 күн бойы жарамды. Kaspersky Security Center бағдарламасы жалпы резервтік сертификатты ("CR") жалпы сертификаттың мерзімі аяқталғанға дейін 90 күн бұрын автоматты түрде жасайды. Жалпы резервтік сертификат кейіннен Басқару сервері сертификатын ауыстыру үшін қолданылады. Жалпы сертификаттың мерзімі аяқталған кезде, басқарылатын құрылғыларда орнатылған Желілік агент үлгілерімен байланысты сақтау үшін жалпы резервтік сертификат қолданылады. Осы мақсатта жалпы резервтік сертификат ескі жалпы сертификаттың мерзімі аяқталғанға дейін 24 сағат бұрын автоматты түрде жаңа жалпы сертификатқа айналады.

Кез келген Басқару сервері сертификатының ең көп жарамдылық мерзімі 397 күннен аспауы керек.

Қажет болса, Басқару сервері сертификатына пайдаланушы сертификатын тағайындауға болады. Мысалы, бұл сіздің ұйымыңыздың бұрыннан бар PKI жүйесімен жақсырақ интеграциялау үшін немесе сертификат өрістерінің қажетті конфигурациясы үшін қажет болып қалуы мүмкін. Сертификатты ауыстырған кезде, бұрын SSL арқылы Басқару серверіне қосылған барлық Желілік агенттер Серверге "Басқару серверінің түпнұсқалық растамасы қатесі" қатесімен қосылуды тоқтатады. Бұл қатені жою үшін, сізге сертификатты ауыстырғаннан кейін қосылымды қалпына келтіру керек.

Басқару серверінің сертификаты резервтік немесе арнаулы сертификатпен ауыстырылғаннан кейін, жауап файлында жаңа сертификатты көрсетіңіз, содан кейін осы файлмен Kaspersky Security Center Web Console-ді қайта орнатыңыз. Әйтпесе, Kaspersky Security Center Web Console Басқару серверіне қосыла алмайды.

Басқару серверінің сертификаты жоғалған болса, оны қалпына келтіру үшін Басқару сервері құрамдасын қайта орнату және деректерді қалпына келтіру керек болады.

Сондай-ақ, Басқару серверін деректерді жоғалтпай бір құрылғыдан екіншісіне тасымалдау үшін Басқару сервері сертификатының сақтық көшірмесін Басқару серверінің басқа параметрлерінен бөлек жасауға болады.

Егер сіз әртүрлі браузерлерде Kaspersky Security Center Web Console бағдарламасын ашып, Басқару сервері сипаттары терезесінде Басқару сервері сертификатының файлын жүктесеңіз, жүктелген файлдардың атаулары әртүрлі болады.

Ұялы құрылғы сертификаттары

Мобильді сертификаты ("M") ұялы құрылғылардағы Басқару серверінің түпнұсқалық растамасы үшін керек. Басқару сервер сипаттарында мобильді сертификатты көрсетесіз.

Сондай-ақ, резервтік ұялы құрылғы сертификаты ("MR") бар: ол ұялы құрылғы сертификатын ауыстыру үшін қолданылады. Kaspersky Security Center бағдарламасы бұл сертификатты жалпы сертификаттың мерзімі аяқталғанға дейін 60 күн бұрын автоматты түрде жасайды. Ұялы құрылғы сертификатының мерзімі аяқталған кезде, басқарылатын ұялы құрылғыларда орнатылған Желілік агентпен байланысты сақтау үшін резервтік ұялы құрылғы сертификаты қолданылады. Осы мақсатта резервтік ұялы құрылғы сертификаты ескі ұялы құрылғы сертификатының мерзімі аяқталғанға дейін 24 сағат бұрын автоматты түрде жаңа ұялы құрылғы сертификатына айналады.

Қосылу сценарийі мобильдік құрылғыларда клиент сертификатын пайдалануды талап етсе (екі жақты SSL түпнұсқалық растамасы арқылы қосылу), бұл сертификаттарды автоматты түрде жасалған пайдаланушы сертификаттары ("MCA") үшін сенімді сертификаттау орталығы арқылы жасайсыз. Сонымен қатар ұйымыңыздағы ашық кілттер инфрақұрылымымен интеграция (PKI) доменнің орталық сертификаттауы көмегімен клиенттер сертификаттарын шығаруға мүмкіндік берсе, басқару сервері сипаттарында басқа сенімді сертификаттау орталығы шығарған пайдаланушы сертификаттарын көрсетуге болады.

Сондай-ақ iOS операциялық жүйесімен жұмыс істейтін мобильдік құрылғылардағы басқару серверінің аутентификациясы үшін iOS MDM серверінің сертификаты қажет. Қосымша мәліметтер алу үшін iOS MDM серверінің сертификатын реттеу бөлімін қараңыз.

Веб-сервер сертификаты

Веб-сервер Kaspersky Security Center Басқару серверінің құрамдас бөлігі болып табылады және арнайы сертификат түрін пайдаланады. Бұл сертификат кейіннен басқарылатын құрылғыларға жүктеп алынатын желілік агенттің орнату пакеттерін, сондай-ақ Kaspersky Security for Mobile орнату пакеттерін жариялау үшін қажет. Ол үшін Веб-сервер әртүрлі сертификаттарды қолдана алады.

Егер ұялы құрылғыларды қолдау өшірулі болса, онда Веб-сервер келесі сертикаттардың бірін басымдық тәртібінде қолданады:

1. Басқару консолі арқылы қолмен көрсетілген Веб-сервердің пайдаланушы сертификаты.
2. Басқару серверінің жалпы сертификаты ("C").

Егер ұялы құрылғыларды қолдау қосулы болса, онда Веб-сервер келесі сертикаттардың бірін басымдық тәртібінде қолданады:

1. Басқару консолі арқылы қолмен көрсетілген Веб-сервердің пайдаланушы сертификаты.
2. Пайдаланушы ұялы құрылғы сертификаты.
3. Өздігінен қол қойылған ұялы құрылғы сертификаты ("M").
4. Басқару серверінің жалпы сертификаты ("C").

Kaspersky Security Center Web Console сертификаты

Kaspersky Security Center Web Console Server серверінің (бұдан әрі Web Console деп те аталады) өз сертификаты бар. Сіз сайтты ашқан кезде, браузер сіздің қосылымыңыздың сенімді ме екенін тексереді. Web Console сертификаты Web Console түпнұсқалық растамасын жасауға мүмкіндік береді және браузер мен Web Console арасындағы трафикті шифрлау үшін қолданылады.

Web Console ашқан кезде, браузер сізге Web Console қосылымы жеке емес екенін және Web Console сертификаты жарамсыз екенін хабарлауы мүмкін. Бұл ескерту, Kaspersky Security Center Web Console сертификаты өздігінен қол қоятындықтан және оны Kaspersky Security Center автоматты түрде жасайтындықтан пайда болады. Бұл ескертуді жою үшін келесі әрекеттердің бірін орындауға болады:

- Kaspersky Security Center Web Console сертификатын пайдаланушы сертификатына ауыстырыңыз (ұсынылатын параметр). Сіздің инфрақұрылымыңызда сенімді болып табылатын және пайдаланушы сертификаттарының талаптарына сәйкес келетін сертификат жасау.

- Web Console сертификатын браузердің сенімді сертификаттары тізіміне қосу. Бұл параметрді пайдаланушы сертификатын жасай алмаған жағдайда ғана пайдалану ұсынылады.

Есептік деректер және қатынасу диспетчерінің сертификаты

Есептік деректер және қатынасу диспетчерінің сертификаты (IAM сертификаты) келесі мақсаттар үшін қажет:

- Пайдаланушы браузері оған OAuth протоколы арқылы қосылған кезде басқару серверін аутентификациялау.

- Kaspersky Security Center Web Console қосылған кездегі басқару серверінің аутентификациясы.

IAM сертификаты басқару серверін бірінші рет іске қосқанда автоматты түрде жасалады. Сертификат басқару серверіндегі келесі каталогке сақталады: /var/opt/kaspersky/klnagent_srv/iam/main_certificate.pem (Ақауларға төзімді Kaspersky Security Center кластері үшін: <ортақ деректер қалтасы>/iam/main_certificate.pem). Kaspersky Security Center Web Console орнатуға арналған жауап файлын жасаған кезде, `iamCertPath` параметрі көмегімен IAM сертификатының жолын көрсетуіңіз керек.

IAM сертификаты 395 күн бойы жарамды. Kaspersky Security Center қазіргі сертификаттың мерзімі аяқталғанға дейін 48 күн бұрын резервтік IAM сертификатын автоматты түрде жасайды. Резервтік сертификат кейін мерзімі өткен IAM сертификатының орнын бірден ауыстыру үшін қолданылады.

Кез келген IAM сертификатының ең көп жарамдылық мерзімі 397 күн немесе одан аз болуы керек.

Қажет болса, арнаулы IAM сертификатын тағайындай аласыз. Мысалы, бұл сіздің ұйымыңыздың бұрыннан бар PKI жүйесімен жақсырақ интеграциялау үшін немесе сертификат өрістерінің қажетті конфигурациясы үшін қажет болып қалуы мүмкін.

> IAM сертификаты резервтік немесе арнаулы сертификатпен ауыстырылғаннан кейін, жауап файлында жаңа сертификатты көрсетіңіз, содан кейін осы файлмен Kaspersky Security Center Web Console-ді қайта орнатыңыз. Әйтпесе Kaspersky Security Center Web Console басқару серверіне қосыла алмайды.

Kaspersky Security Center Web Console-ге кірген кезде, аутентификация үшін браузер басқару серверінің кіру бетіне (https://<`басқару серверінің мекенжайы`>:4444) бағытталады. Браузер мен басқару сервері арасындағы трафик TLS протоколы мен IAM сертификаты арқылы шифрланады.

Браузер сізге басқару серверіне қосылу құпия емес және IAM сертификаты жарамсыз екенін хабарлауы мүмкін. Бұл ескерту IAM сертификаты өздігінен қол қоятындықтан және оны Kaspersky Security Center автоматты түрде жасайтындықтан пайда болады. Бұл ескертуді жою үшін келесі әрекеттердің бірін орындауға болады:

- IAM сертификатын арнаулысымен ауыстырыңыз (ұсынылатын опция). Сіздің инфрақұрылымыңызда сенімді болып табылатын және пайдаланушы сертификаттарының талаптарына сәйкес келетін сертификат жасау.
- IAM сертификатын браузердің сенімді сертификаттары тізіміне қосыңыз. Бұл параметрді пайдаланушы сертификатын жасай алмаған жағдайда ғана пайдалану ұсынылады.

Kaspersky Security Center Linux-те қолданылатын пайдаланушы сертификаттарына қойылатын талаптар

Төмендегі кестеде, Kaspersky Security Center Linux түрлі құрамдастарына қатысты пайдаланушы сертификаттарына қойылатын талаптар көрсетілген.

Kaspersky Security Center Linux сертификаттарына қойылатын талаптар

Сертификат түрі	Талаптар	Түсіндірмелер
Жалпы сертификат, жалпы резервтік сертификат ("C", "CR")	Кілттің минималды ұзындығы: 2048. Негізгі шектеулер: • Жол ұзындығын шектеу: Жоқ. Кілтті пайдалану: • Сандық қолтаңба. • Сертификат қолтаңбасы. • Кілттерді шифрлау. • Кері қайтару тізіміне (CRL) қол қою. Кілтті кеңейтілген пайдалану (Extended Key Usage, EKU) (міндетті емес): Сервердің түпнұсқалық растамасы, клиенттің түпнұсқалық растамасы. Сертификатта Басқару серверінің кері байланыс мекенжайын қамтитын жарамды Субъектінің баламалы атауы (SAN) болуы керек: • IPv4 үшін: 127.0.0.1 • IPv6 үшін: 0:0:0:0:0:0:0:1	Extended Key Usage параметрі міндетті емес. Жол ұзындығын шектеу мәні "None" мәнінен басқа, бірақ 1-ден кем емес бүтін сан болуы мүмкін.
Веб-сервер сертификаты	Кеңейтілген кілт қолданысы (EKU): Сервердің түпнұсқалық растамасы. Сертификаты көрсетілетін PKCS #12 / PEM контейнері жалпыға ортақ кілттердің толық тізбегін қамтиды. Субъектінің баламалы атауы (SAN) бар; яғни `subjectAltName` өрісі толтырылған. Сертификат серверлер сертификаттарына қойылатын браузерлердің қолданыстағы талаптарына, сондай-ақ CA/Browser Forum ағымдағы базалық талаптарына сай келеді.	—
Kaspersky Security Center Web Console сертификаты	Кілтті кеңейтілген пайдалану (Extended Key Usage, EKU): Сервердің түпнұсқалық растамасы, клиенттің түпнұсқалық растамасы. Сертификаты көрсетілетін PEM контейнері жалпыға ортақ кілттердің толық тізбегін қамтиды. Субъектінің баламалы атауы (SAN) бар; яғни `subjectAltName` өрісі толтырылған. Басқару серверін орнату бағдарламасы кезінде көрсетілген IAM мекенжайына мән сәйкес келуі керек. Көрсетілген IAM мекенжайын алу үшін Басқару сервері хостында келесі пәрменді орындаңыз: `grep "iam_address:" /var/opt/kaspersky/klnagent_srv/iam/iam_config.yaml` Сертификат серверлер сертификаттарына қойылатын браузерлердің қолданыстағы талаптарына, сондай-ақ CA/Browser Forum ағымдағы базалық талаптарына сай келеді.	Шифрланған сертификаттарға Kaspersky Security Center Web Console қолдау көрсетпейді.

Сертификат түрі	Талаптар	Түсіндірмелер
Есептік деректер және қатынасу диспетчерінің сертификаты (IAM сертификаты)	Кеңейтілген кілт қолданысы (EKU): Сервердің түпнұсқалық растамасы. Сертификаты көрсетілетін PEM контейнері жалпыға ортақ кілттердің толық тізбегін қамтиды. Сертификат жарамды болуы және клиенттің аутентификациясына қолдау көрсетуі керек. Сертификат серверлер сертификаттарына қойылатын браузерлердің қолданыстағы талаптарына, сондай-ақ CA/Browser Forum ағымдағы базалық талаптарына сай келеді.	Шифрланған сертификаттарға Kaspersky Security Center Web Console қолдау көрсетпейді.

Kaspersky Security Center Web Console үшін сертификатты қайта шығару

Көптеген браузерлер сертификаттың жарамдылық мерзімін шектейді. Бұл шектеуге кіру үшін Kaspersky Security Center Web Console сертификатының жарамдылық мерзімі 397 күнге тең. Жаңа өздігінен қол қойылған сертификатты қолмен шығарған кезде, сенімді сертификаттау орталығынан (CA) алынған қолданыстағы сертификатты ауыстыруға болады. Сондай-ақ, Kaspersky Security Center Web Console ескірген сертификатын қайта шығаруға болады.

Kaspersky Security Center Web Console үшін сертификатты автоматты түрде қайта шығаруға қолдау көрсетілмейді. Сертификатты қолмен қайта шығаруыңыз керек.

Егер сіз сертификат жасауды таңдасаңыз, Kaspersky Security Center Web Console бағдарламасын ашқан кезде, браузер сізге Kaspersky Security Center Web Console бағдарламасына қосылудың жекеше емес екенін және Kaspersky Security Center Web Console сертификаты жарамсыз екенін хабарлауы мүмкін. Бұл ескерту, Kaspersky Security Center Web Console сертификаты өздігінен қол қоятындықтан және оны Kaspersky Security Center Linux автоматты түрде жасайтындықтан пайда болады. Бұл ескертуді жою немесе болдырмау үшін келесі әрекеттердің бірін орындауға болады:

- Пайдаланушы сертификатын қайта шығарылған кезде көрсетіңіз (ұсынылған нұсқа). Сіздің инфрақұрылымыңызда сенімді болып табылатын және пайдаланушы сертификаттарының талаптарына сәйкес келетін сертификат жасау.
- Сертификатты қайта шығарғаннан кейін, сенімді браузер сертификаттарының тізіміне Kaspersky Security Center Web Console сертификатын қосыңыз. Бұл параметрді пайдаланушы сертификатын жасай алмаған жағдайда ғана пайдалану ұсынылады.

Мерзімі өткен Kaspersky Security Center Web Console сертификатын қайта шығару үшін:

Kaspersky Security Center Web Console-ін, келесі әрекеттердің бірін орындау арқылы қайта орнатыңыз:

- Kaspersky Security Center Web Console-інің бірдей орнату файлын пайдаланғыңыз келсе, Kaspersky Security Center Web Console бағдарламасын жойып, Kaspersky Security Center Web Console-інің бірдей нұсқасын орнатыңыз.
- Жаңартылған нұсқаның орнату файлын пайдаланғыңыз келсе, жаңарту пәрменін орындаңыз.

Kaspersky Security Center Web Console сертификаты 397 күндік жарамдылық мерзімімен қайта шығарылған.

Kaspersky Security Center Web Console үшін сертификатты ауыстыру

Әдепкі бойынша, Kaspersky Security Center Web Console серверін (бұдан әрі Kaspersky Security Center Web Console Server) орнату кезінде бағдарламаға арналған браузер сертификаты автоматты түрде жасалады. Сіз автоматты түрде жасалған сертификатты пайдаланушы сертификатымен ауыстыра аласыз.

Kaspersky Security Center Web Console үшін сертификатты пайдаланушы сертификатына ауыстыру үшін:

1. Kaspersky Security Center Web Console орнату кезінде жасалған жауап файлын ашыңыз.

   Қажет болса, жаңа жауап файлын жасауға болады.

2. Файлда келесі жолдарды көрсетіңіз:

   - `certPath` параметрін пайдалану арқылы Kaspersky Security Center Web Console арнаулы сертификат файлына
   - `keyPath` параметрін пайдалану арқылы Kaspersky Security Center Web Console арнаулы сертификатымен байланыстырылған жеке кілтке.

   > Екі жолды да көрсету керек. Әйтпесе веб-браузер қосылымыңыз құпия емес екенін хабарлай береді.

3. Жаңа жауап файлын көрсету арқылы Kaspersky Security Center Web Console қайта орнатыңыз. Келесі әрекеттердің бірін орындаңыз:

   - Kaspersky Security Center Web Console-інің бірдей орнату файлын пайдаланғыңыз келсе, Kaspersky Security Center Web Console бағдарламасын жойып, Kaspersky Security Center Web Console-інің бірдей нұсқасын орнатыңыз.
   - Жаңартылған нұсқаның орнату файлын пайдаланғыңыз келсе, жаңарту пәрменін орындаңыз.

Kaspersky Security Center Web Console сервері көрсетілген сертификатпен жұмыс істейді.

Сертификатты PFX пішімінен PEM пішіміне түрлендіру

Kaspersky Security Center Web Console бағдарламасында PFX пішіміндегі сертификатты пайдалану үшін, оны кез келген OpenSSL негізіндегі кроссплатформалық утилита арқылы PEM пішіміне алдын ала түрлендіру қажет.

Linux операциялық жүйесінде сертификатты PFX пішімінен PEM пішіміне түрлендіру үшін:

1. OpenSSL негізіндегі кроссплатформалық утилитада келесі пәрмендерді орындаңыз:

   ```
   openssl pkcs12 -in <файл атауы.pfx> -clcerts -nokeys | sed -ne '/-BEGIN CERTIFICATE-/,/-END CERTIFICATE-/p' > server.crt
   ```

   ```
   openssl pkcs12 -in <файл атауы.pfx> -nocerts -nodes | sed -ne '/-BEGIN PRIVATE KEY-/,/-END PRIVATE KEY-/p' > key.pem
   ```

2. Сертификат файлы мен жеке кілт PFX файлы сақталатын қалтада жасалғанына көз жеткізіңіз.

3. Kaspersky Security Center Web Console сервері құпиясөз тіркесімен қорғалған сертификаттарды қолдамайды. Сондықтан, .pem файлынан құпиясөз тіркесін жою үшін OpenSSL негізіндегі кроссплатформалық утилитада келесі пәрменді орындаңыз:

   ```
   openssl rsa -in key.pem -out key-without-passphrase.pem
   ```

   > .PEM кіріс және шығыс файлдары үшін бірдей атты қолданбаңыз.

   Нәтижесінде, жаңа .pem файлы шифрланбаған. Оны пайдалану үшін құпиясөз тіркесін енгізудің қажеті жоқ.

.crt және .pem файлдары пайдалануға дайын, сондықтан оларды Kaspersky Security Center Web Console орнату шеберінде көрсетуге болады.

Сценарий: Басқару серверінің пайдаланушы сертификатын белгілеу

Сіз өзіңіздің ұйымыңыздың қолданыстағы жалпыға ортақ кілттер инфрақұрылымымен (PKI) жақсырақ біріктіру үшін немесе сертификат параметрлерінің пайдаланушы конфигурациясы үшін Басқару серверінің пайдаланушы сертификатын тағайындай аласыз. Сертификатты, Басқару серверін орнатқаннан кейін, бағдарламаны жылдам іске қосу шеберінің жұмысы аяқталғанға дейін ауыстырған жөн.

> Кез келген Басқару сервері сертификатының ең көп жарамдылық мерзімі 397 күннен аспауы керек.

Алдын ала талаптар

Келесі шарттар орындалуы керек:

- Сертификат PKCS#12 пішімінде жасалуы керек (мысалы, ұйымның PKI арқылы).
- Жаңа сертификат үшін төмендегі кестеде көрсетілген талаптар орындалуы керек.

  Төмендегі кестеде "CA: true" талабына назар аударыңыз, бұл жаңа сертификатты сенімді сертификаттау орталығы (CA) беруі керек дегенді білдіреді. "CA: true" талабы бар жаңа сертификат бүкіл сенім тізбегін және pfx немесе p12 кеңейтімі бар файлда сақталуы тиісті жеке кілтті қамтуы керек.

Сертификат түрі	Талаптар
Жалпы сертификат, жалпы резервтік сертификат ("C", "CR")	Кілттің минималды ұзындығы: 2048. Негізгі шектеулер: • Жол ұзындығын шектеу: Жоқ. Жол ұзындығын шектеу мәні "None" мәнінен басқа, бірақ 1-ден кем емес бүтін сан болуы мүмкін. Кілтті пайдалану: • Сандық қолтаңба. • Сертификат қолтаңбасы. • Кілттерді шифрлау. • Кері қайтару тізіміне (CRL) қол қою. Кеңейтілген кілт қолданысы (Extended Key Usage, EKU) (міндетті емес): Сервердің түпнұсқалық растамасы және клиенттің түпнұсқалық растамасы. EKU міндетті емес, бірақ ол сіздің сертификатыңызда болса, Сервер мен клиенттің түпнұсқалық растамасы деректері EKU-да көрсетілуі керек. Сертификатта Басқару серверінің кері байланыс мекенжайын қамтитын жарамды Субъектінің баламалы атауы (SAN) болуы керек: • IPv4 үшін: 127.0.0.1 • IPv6 үшін: 0:0:0:0:0:0:0:1
Ұялы құрылғы сертификаты, резервтік ұялы құрылғы сертификаты ("M", "MR")	Кілттің минималды ұзындығы: 2048. Негізгі шектеулер: • CA: Иә. • Жол ұзындығын шектеу: Жоқ. Егер жалпы сертификатта жол ұзындығын шектеу мәні кемінде 1 болса, жол ұзындығын шектеу мәні "None" мәнінен басқа бүтін сан болуы мүмкін. Кілтті пайдалану: • Сандық қолтаңба. • Сертификат қолтаңбасы. • Кілттерді шифрлау. • Кері қайтару тізіміне (CRL) қол қою. Кеңейтілген кілт қолданысы (EKU): Сервердің түпнұсқалық растамасы. EKU міндетті емес, бірақ ол сіздің сертификатыңызда болса, Сервердің түпнұсқалық растамасы деректері EKU-да көрсетілуі керек.
Автоматты түрде жасалатын пайдаланушы сертификаттары (MCA) үшін сенімді сертификаттау орталығы (CA) шығарған сертификат	Кілттің минималды ұзындығы: 2048. Негізгі шектеулер: • CA: Иә. • Жол ұзындығын шектеу: Жоқ. Егер жалпы сертификатта жол ұзындығын шектеу мәні кемінде 1 болса, жол ұзындығын шектеу мәні "None" мәнінен басқа бүтін сан болуы мүмкін. Кілтті пайдалану: • Сандық қолтаңба. • Сертификат қолтаңбасы. • Кілттерді шифрлау. • Кері қайтару тізіміне (CRL) қол қою. Кеңейтілген кілт қолданысы (EKU): клиент аутентификациясы. EKU міндетті емес, бірақ ол сіздің сертификатыңызда болса, клиенттің түпнұсқалық растамасы деректері EKU-да көрсетілуі керек.

Сенімді сертификаттау орталығы (ағылшынша certificate authority, CA) шығарған сертификаттардың сертификаттарға қол қоюға рұқсаты жоқ. Мұндай сертификаттарды пайдалану үшін, желіңіздегі тарату нүктелерінде немесе қосылым шлюздерінде 13 немесе одан жоғары нұсқадағы Желілік агент орнатылғанына көз жеткізіңіз. Әйтпесе, сіз қол қою рұқсатынсыз сертификаттарды пайдалана алмайсыз.

Кезеңдер

Басқару сервері сертификатын көрсету келесі кезеңдерден тұрады:

1. **Басқару серверінің сертификатын ауыстыру**

   Осы мақсат үшін klsetsrvcert пәрмен жолы утилитасын пайдаланыңыз.

2. **Жаңа сертификатты көрсету және Желілік агенттердің Басқару серверімен байланысын қалпына келтіру**

   Сертификатты ауыстырған кезде, бұрын SSL арқылы Басқару серверіне қосылған барлық Желілік агенттер Серверге "Басқару серверінің түпнұсқалық растамасы қатесі" қатесімен қосылуды тоқтатады. Жаңа сертификатты көрсету және қосылымды қалпына келтіру үшін klmover утилитасының пәрмен жолын пайдаланыңыз.

3. **Kaspersky Security Center Web Console параметрлерінде жаңа сертификатты көрсету**

   Сертификатты ауыстырғаннан кейін, оны жауап файлында көрсетіңіз, содан кейін осы файлды пайдаланып, Kaspersky Security Center Web Console-ді жаңартыңыз. Әйтпесе, Kaspersky Security Center Web Console Басқару серверіне қосыла алмайды.

Нәтижелер

Сценарий аяқталғаннан кейін, Басқару сервері сертификаты ауыстырылады, басқарылатын құрылғылардағы Желілік агент сервері жаңа сертификатты пайдалану арқылы Серверді аутентификациялайды.

klsetsrvcert утилитасын пайдаланып, Басқару сервері сертификатын ауыстыру

Құрылғыларды басқаруды жоғалтып алмау үшін, жалғастырмас бұрын сценарийді қараңыз: Басқару серверінің арнайы сертификатын көрсету.

Басқару сервері сертификатын ауыстыру үшін:

Пәрмен жолында келесі пәрменді орындаңыз:

```
/opt/kaspersky/ksc64/sbin/klsetsrvcert [-t <certificate type> {-i <path to new certificate> [-p <password>] [-o
<validation parameters>] | -g <dns name>}][-f <replacement time>][-r <root certificates>][-l <log file path>]
```

klsetsrvcert утилитасының параметрлерінің сипаттамасы төмендегі кестеде келтірілген.

klsetsrvcert утилитасының параметрлерінің мәндері

Параметр	Мән
`-t < сертификат түрі >`	Ауыстырылатын сертификат түрі. `< сертификат түрі >` параметрінің ықтимал мәндері: • `C` – 13000 және 13291 порттары үшін жалпы сертификатты ауыстыру. • `CR` – 13000 және 13291 порттары үшін жалпы резервтік сертификатты ауыстыру.

Параметр	Мән
`-f < ауыстыру уақыты >`	Сертификатты ауыстыру кестесі "КК-АА-ЖЖЖЖ СС:ММ" пішімін қолданады (13000 және 13291 порттары үшін). Жалпы сертификат мерзімі аяқталмай тұрып, оны жалпы резервтік сертификатпен ауыстырғыңыз келсе, осы параметрді қолданыңыз. Басқарылатын құрылғылардың жаңа сертификатты пайдаланып Басқару серверімен синхрондау уақытын көрсетіңіз.
`-i < жаңа сертификатқа жол >`	Сертификаты бар контейнер және PKCS#12 пішіміндегі жеке кілт (p12 немесе pfx кеңейтімі бар файл).
`-p < құпиясөз >`	p12 контейнерін қорғайтын құпиясөз. Сертификат пен жеке кілт контейнерде сақталады, сондықтан контейнер файлын шифрсыздау үшін құпиясөз қажет.
`-o < тексеру параметрлері >`	Сертификатты тексеру параметрлері (нүктелі үтірмен бөлінген). Қол қоюға рұқсатсыз пайдаланушы сертификатын пайдалану үшін klsetsrvcert утилитасында `-o NoCA` көрсетіңіз. Бұл сенімді сертификаттау орталығы шығарған сертификаттар үшін пайдалы (ағылшынша certificate authority, CA). C немесе CR түріндегі сертификаттар үшін шифрлау кілтінің ұзындығын өзгерту үшін klsetsrvcert утилитасында `-o RsaKeyLen:< кілт ұзындығы >` деп көрсетіңіз, мұндағы `< кілт ұзындығы >` параметрі – қажетті кілт ұзындығы. Әйтпесе, ағымдағы сертификат кілтінің ұзындығы пайдаланылады.
`-g < dns атауы >`	Көрсетілген DNS атауы үшін жаңа сертификат жасалады (Жалпы атау және Субъектінің баламалы атауы).
`-r < түбірлік сертификаттар >`	Сенімді сертификаттау орталығы қол қойған PEM пішіміндегі сенімді түбірлік сертификаттардың тізімі.
`-l < журнал файлының жолы >`	Нәтижелерді шығару файлы. Әдепкі бойынша, шығару стандартты шығару ағынында жүзеге асырылады.

Мысалы, Басқару серверінің пайдаланушы сертификатын көрсету үшін келесі пәрменді пайдаланыңыз:

```
klsetsrvcert -t C -i <жаңа сертификатқа жол> -p <құпиясөз> -o NoCA
```

Сертификатты ауыстырғаннан кейін, SSL протоколы арқылы Басқару серверіне қосылған барлық Желілік агенттер байланысын жоғалтады. Байланысты қалпына келтіру үшін, klmover утилитасы пәрмен жолағын қолданыңыз.

Желілік агенттердің қосылымдарын жоғалтпау үшін келесі пәрмендерді пайдаланыңыз:

1. Жаңа сертификатты орнату үшін,

   ```
   klsetsrvcert -t CR -i <жаңа сертификатқа жол> -p <құпиясөз> -o NoCA
   ```

2. Жаңа сертификатқа өтінім беру күнін көрсету үшін,

   ```
   klsetsrvcert -f "DD-MM-YYYY hh:mm"
   ```

мұндағы "`DD-MM-YYYY hh:mm`" күні ағымдағы күннен 3-4 аптаға көбірек. Сертификатты жаңа сертификатқа ауыстыру уақытын ауыстыру жаңа сертификатты барлық Желілік агенттерге таратуға мүмкіндік береді.

Сұрақтар мен жауаптар

Басқару серверінің жалпы сертификатын ауыстырғаннан кейін қандай қосымша қадамдар қажет?

1. **Тапсырыс бойынша жасалған сертификаттарға қойылатын талаптардың орындалғанына** көз жеткізіңіз.

   Егер сіз өздігінен қол қойылған сертификаттың орнына арнайы сертификатты пайдалансаңыз, Kaspersky Security Center Linux жүйесін кейінгі нұсқасына жаңартпас бұрын, сертификатта Субъектінің балама атауы (SAN) бар екеніне көз жеткізуіңіз керек. Олай болмаса, Kaspersky Security Center Linux жүйесін жаңартпас бұрын сертификатты ауыстыру маңызды. Әйтпесе, жаңартудан кейін Web Console веб-консоліне кіре алмайсыз.

   Сертификатта SAN бар екеніне көз жеткізу үшін:

   1. Басқару сервер орнатылған құрылғыда келесі пәрменді орындаңыз:

      - Linux құрылғысы үшін:

        ```
        sudo openssl x509 -in /var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer -noout -ext subjectAltName
        ```

      - Windows құрылғысы үшін:

        ```
        certutil -dump %ProgramData%\KasperskyLab\adminkit\1093\cert\klserver.cer
        ```

   2. Пәрмен шығысында Субъектінің балама атауының бар екеніне және Басқару сервері құрылғысының мекенжайын қамтитынына көз жеткізіңіз.

   3. Егер Тақырыптың балама атауы болмаса, klsetsrvcert утилитасын пайдаланып, реттелетін сертификатыңызды талаптарға сай келетін сертификатпен ауыстырыңыз.

2. IAM серверінің конфигурация файлында ағымдағы Басқару серверінің мекенжайы бар екеніне көз жеткізіңіз. Егер жоқ болса, мекенжайды конфигурация файлына қосыңыз.

3. Келесі қатені болдырмау үшін Web Console веб-консолін қайта орнатыңыз:

   Басқару сервері сенімсіз сертификатты пайдаланады. Қолданбаны жарамды сертификатты көрсету арқылы қайта конфигурациялаңыз немесе негізгі әкімшіге хабарласыңыз.

Желілік агенттерді klmover утилитасын пайдаланып Басқару серверіне қосу

Басқарылмайтын құрылғылардан басқару серверіне қосылымды қалпына келтіру үшін klmover утилитасын пайдаланыңыз (мысалы, басқару серверінің сәтсіздігінен кейін сақтық көшірмеден қалпына келтіру мүмкін болмаса).

Қосылымды қалпына келтіру үшін пәрмен жолында klmover утилитасын іске қосыңыз:

- Linux үшін:
  - 32 биттік жүйелер үшін: `/opt/kaspersky/klnagent/bin/klmover [-address <сервер мекенжайы>] [-pn <порт нөмірі>] [-ps <SSL порт нөмірі>] [-nossl] [-cert <сертификат файлының жолы>]`
  - 64 биттік жүйелер үшін: `/opt/kaspersky/klnagent64/bin/klmover [-address <сервер мекенжайы>] [-pn <порт нөмірі>] [-ps <SSL порт нөмірі>] [-nossl] [-cert <сертификат файлының жолы>]`
- Windows үшін:
  - 64 биттік жүйелер үшін: `<path>\klmover.exe [-address <сервер мекенжайы>] [-pn <порт нөмірі>] [-ps <SSL порт нөмірі>] [-nossl] [-cert <сертификат файлының жолы>]`
  - 64 биттік жүйелер үшін: `<path>\klmover.exe [-address <сервер мекенжайы>] [-pn <порт нөмірі>] [-ps <SSL порт нөмірі>] [-nossl] [-cert <сертификат файлының жолы>]`
- macOS үшін:

  `/Library/Application Support/Kaspersky Lab/klnagent/Binaries/klmover [-address <сервер мекенжайы>] [-pn <порт нөмірі>] [-ps <SSL порт нөмірі>] [-nossl] [-cert <сертификат файлының жолы>]`

мұндағы `<path>` — желілік агентке арналған әдепкі орнату жолы немесе желілік агенттің орнату пакетінің параметрлерінде сіз көрсеткен орнату жолы.

Зиянкестер құрылғыларды Басқару серверіңіздің басқаруынан шығаруына жол бермеу үшін klmover утилитасын іске қосқан кезде құпия сөзбен қорғауды міндетті түрде қосу ұсынылады. Құпиясөз қорғанысын қосу үшін Желілік агент саясаты параметрлерінде **Жою құпиясөзін пайдалану** опциясын таңдаңыз.

Енді Kaspersky Security Center Linux басқармайтын құпиясөзбен қорғалған құрылғыда орнатылған желілік агенттің құпиясөзін жоғалтып алсаңыз немесе ұмытып қалсаңыз, klmover утилитасын немесе пәрмен жолын пайдаланып, желілік агентті жоя алмайсыз. Бұл жағдайда құпиясөзбен қорғалған желілік агент орнатылған құрылғыда операциялық жүйені қайта орнату қажет.

klmover утилитасына жергілікті әкімші құқықтары қажет.

Windows құрылғыларында **Жою құпиясөзін пайдалану** опциясы қосылса, Cleaner құралы (cleaner.exe) үшін құпиясөз қорғанысы да қосылады.

Қосылым шлюздері арқылы басқару серверіне қосылған клиент құрылғылары үшін klmover утилитасын пайдалана алмайсыз. Мұндай құрылғылар үшін Желілік агентті қайта конфигурациялау немесе желілік агентті қайта орнату және қосылым шлюзін көрсету керек.

klmover утилитасының параметрлерінің сипаттамасы төмендегі кестеде келтірілген.

Параметр	Мән
`-address < сервер мекенжайы >`	Қосылу үшін Басқару сервері мекенжайы. Мекенжай ретінде IP мекенжайын немесе DNS атауын көрсетуге болады.
`-pn < порт нөмірі >`	Басқару серверіне шифрланбаған қосылу орындалатын порт нөмірі. Әдепкі бойынша 14000-порт орнатылған.
`-ps < SSL порты нөмірі >`	SSL протоколын қолдана отырып, Басқару серверіне шифрланған қосылу жүзеге асырылатын SSL порты нөмірі. Әдепкі бойынша 13000-порт орнатылған.
`-nossl`	Басқару серверіне шифрланбаған қосылымды пайдалану. Егер кілт пайдаланылмаса, Желілік агент Серверге қорғалған SSL протоколы арқылы қосылады.
`-cert < сертификат файлының жолы >`	Басқару серверіне қатынасудың түпнұсқалық растамасын жасау үшін көрсетілген сертификат файлын пайдалану.
`-nauninstpwd < құпиясөз >`	Бұл параметрді желілік агенттің жою құпиясөзін көрсету үшін пайдаланыңыз. Параметр міндетті емес.

Веб-сервер сертификатын қайта шығару

Kaspersky Security Center Linux бағдарламасында қолданылатын Веб-сервер сертификаты, сіз кейіннен басқарылатын құрылғыларға жүктейтін Желілік агенттің орнату пакеттерін жариялау үшін, сондай-ақ iOS MDM профильдерін, iOS қолданбаларын және Kaspersky Endpoint Security for Mobile орнату пакеттерін жариялау үшін қажет. Ағымдағы қолданба конфигурациясына байланысты әртүрлі сертификаттар веб-сервер сертификаты ретінде жұмыс істейді (қосымша ақпаратты Kaspersky Security Center Linux сертификаттары туралы ақпарат бөлімінен қараңыз).

Қолданбаны жаңартуды бастамай тұрып, ұйымыңыздың қауіпсіздік талаптарына сай болуын қамтамасыз ету немесе басқарылатын құрылғыларыңыздың тұрақты қосылымын қолдау үшін веб-сервер сертификатын қайта шығару қажет болуы мүмкін. Kaspersky Security Center Linux веб-сервер сертификатын қайта шығарудың екі жолын ұсынады; екі әдіс арасындағы таңдау мобильдік құрылғылардың қосылғанына және мобильдік протокол арқылы басқарылатынына байланысты (яғни мобильдік сертификатты пайдалану арқылы).

Егер сіз ешқашан Басқару сервері сипаттарының **Веб-сервер** терезесінде Веб-сервер сертификаты ретінде пайдаланушы сертификатын көрсетпеген болсаңыз, ұялы құрылғы сертификаты Веб-сервер сертификаты ретінде қолданылады. Бұл жағдайда, Веб-сервер сертификатын қайта шығару мобильді протоколдың өзін қайта шығару арқылы жүзеге асырылады.

Мобильді протокол арқылы басқарылатын ұялы құрылғылар болған кезде Веб-сервер сертификатын қайта шығару үшін:

1. Пайдаланушы сертификатын жасаңыз және оны Kaspersky Security Center Linux-те пайдалануға дайындаңыз. Сіздің арнайы сертификатыңыз Kaspersky Security Center Linux талаптарына сәйкес келетінін тексеріңіз. Қажет болса, сертификатты өзгертіңіз.

2. Негізгі мәзірдегі басқару серверінің атауын басыңыз.

   Басқару серверінің сипаттары терезесі ашылады.

3. **Жалпы** қойыншасында **Веб-сервер** бөлімін таңдаңыз.

4. **HTTP протоколы бойынша** ішкі бөлімінде **Сертификатты файлдан жүктеп салу** нұсқасын таңдап, **Сертификатты өзгерту** түймесін басыңыз.

5. Ашылған терезеде, **Сертификат форматы** өрісінде, сертификатыңыздың түрін таңдаңыз:

   - **PKCS #12 контейнері** тармағын таңдасаңыз, **Сертификат** өрісінің жанындағы **Шолу** түймесін басыңыз және қатты дискідегі сертификат файлын көрсетіңіз. Сертификат файлы құпиясөзбен қорғалған болса, **Құпиясөз** өрісінде құпиясөзді енгізіңіз.

   - **X.509 сертификаты** таңдасаңыз, **Жеке кілт** өрісінің жанындағы **Шолу** түймесін басыңыз және қатты дискідегі жеке кілтті көрсетіңіз. Жеке кілт құпиясөзбен қорғалған болса, **Құпиясөз** өрісінде құпиясөзді енгізіңіз.

6. **Сақтау** түймесін, содан кейін **OK** түймесін басыңыз.

   Терезе жабық.

7. Қажет болса, **Веб-сервердің HTTPS порты** өрісінде Веб-серверге арналған HTTPS портының нөмірін өзгертіп, **Сақтау** түймесін басыңыз.

Веб-сервер сертификаты қайта шығарылды.

Мобильді протокол арқылы басқарылатын ұялы құрылғылар болмаған кезде Веб-сервер сертификатын қайта шығару үшін:

1. Негізгі мәзірдегі басқару серверінің атауын басыңыз.

   Басқару серверінің сипаттары терезесі ашылады.

2. **Жалпы** қойыншасында **Сертификаттар** бөлімін таңдаңыз.

3. Егер сіз Kaspersky Security Center берген сертификатты одан әрі пайдалануды жоспарласаңыз:

   a. **Сертификат Басқару серверінің құралдары арқылы шығарылған** нұсқасын таңдап, **Шолу** түймесін басыңыз.

   b. **Байланыстың мекенжайы** және **Белсендіру мерзімі** параметрлер блоктарының ашылған терезесінде тиісті параметрлерді таңдап, **OK** түймесін басыңыз.

Егер сіз өзіңіздің сертификатыңызды пайдалануды жоспарласаңыз, келесі әрекеттерді орындаңыз:

a. Сіздің арнайы сертификатыңыз Kaspersky Security Center Linux талаптарына сәйкес келетінін тексеріңіз. Қажет болса, сертификатты өзгертіңіз.

b. **Басқа сертификат** нұсқасын таңдап, **Сертификатты басқару** түймесін басыңыз және ашылған терезеде **Шолу** түймесін басыңыз.

c. Ашылған терезеде, **Сертификат форматы** өрісінде, сертификатыңыздың түрін таңдаңыз:

   - **PKCS #12 контейнері** тармағын таңдасаңыз, **Сертификат** өрісінің жанындағы **Шолу** түймесін басыңыз және қатты дискідегі сертификат файлын көрсетіңіз. Сертификат файлы құпиясөзбен қорғалған болса, **Құпиясөз** өрісінде құпиясөзді енгізіңіз.

   - **X.509 сертификаты** таңдасаңыз, **Жеке кілт** өрісінің жанындағы **Шолу** түймесін басыңыз және қатты дискідегі жеке кілтті көрсетіңіз. Жеке кілт құпиясөзбен қорғалған болса, **Құпиясөз** өрісінде құпиясөзді енгізіңіз.

d. **Сақтау** түймесін, содан кейін **OK** түймесін басыңыз.

Ұялы құрылғы сертификаты Веб-сервер сертификаты ретінде пайдалану үшін қайта шығарылды.

Әдепкі IAM сертификатын арнаулы сертификатқа өзгерту

Әдепкі IAM сертификатын өзгерту үшін:

1. Пайдаланушы сертификатын жасаңыз және оны Kaspersky Security Center Linux-те пайдалануға дайындаңыз. Сіздің арнайы сертификатыңыз Kaspersky Security Center Linux талаптарына сәйкес келетінін тексеріңіз.

2. kladmins тобының IAM сертификат файлдарына кіру рұқсаты бар екеніне көз жеткізіңіз.

3. IAM конфигурация файлын табыңыз: `/var/opt/kaspersky/klnagent_srv/iam/iam_config.yaml`

   Бұл файлда `server_iam` бөліміне IAM сертификат файлдарына жолдарды қосыңыз:

   - `certificates.main.cert`: Негізгі сертификат файлының жолы.
   - `certificates.main.key`: Негізгі сертификаттың жеке кілтінің жолы. Жеке кілт құпиясөзбен қорғалмаған болуы керек.

4. Web Console конфигурация файлын табыңыз: `/etc/ksc-web-console-setup.json`

   Бұл файлда `iamCertPath` өріс мәнін негізгі сертификаттың ашық кілтінің жолына орнатыңыз.

5. Келесі пәрменді орындау арқылы kliam қызметін қайта іске қосыңыз:

   ```
   sudo service kliam_srv restart
   ```

6. Web Console-ді қайта орнатыңыз.

   Қайта орнатылғаннан кейін, Web Console арнаулы IAM сертификатын пайдаланады.

Сақтық IAM сертификатын өзгерту үшін:

1. IAM конфигурация файлын табыңыз: `/var/opt/kaspersky/klnagent_srv/iam/iam_config.yaml`

   Бұл файлда IAM сертификаты файлдарының жолдарын көрсетіңіз:

   - `server_iam.certificates.reserve.cert`: Негізгі сертификат файлының жолы.
   - `server_iam.certificates.reserve.key`: Негізгі сертификаттың жеке кілтінің жолы. Жеке кілт құпиясөзбен қорғалмаған болуы керек.

2. Келесі пәрменді орындау арқылы kliam қызметін қайта іске қосыңыз:

   ```
   sudo systemctl restart kliam_srv.service
   ```

   Негізгі сертификат файлының мерзімі аяқталғаннан кейін оның орнына резервтік IAM сертификаты пайдаланылады.

IAM серверінің конфигурациясына Басқару серверінің мекенжайын қосу

Жаңарту, жылжыту немесе көшіру кезінде Жалпы Басқару сервері сертификатын ("C") өзгерткеннен кейін, IAM сервері мен Басқару сервері арасында сертификаттың дұрыс расталуын қамтамасыз ету үшін IAM сервер конфигурация файлында Басқару сервері мекенжайын көрсету қажет.

IAM сервер конфигурациясына Басқару серверін мекенжайын қосу үшін:

1. Келесі пәрменді орындау арқылы Жалпы Басқару сервері сертификатынан («C») Субъектінің балама атауы (SAN) мәнін алыңыз:

   ```
   sudo openssl x509 -in /var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer -noout -ext subjectAltName
   ```

2. Пәрмен шығысына байланысты келесі әрекеттердің бірін орындаңыз:

   - Егер шығыс мәннің жоқ екенін көрсетсе, **арнайы сертификатқа қойылатын талаптарды** тексеріңіз.

     Егер сіз өздігінен қол қойылған сертификаттың орнына арнайы сертификатты пайдалансаңыз, Kaspersky Security Center Linux жүйесін кейінгі нұсқасына жаңартпас бұрын, сертификатта Субъектінің балама атауы (SAN) бар екеніне көз жеткізуіңіз керек. Олай болмаса, Kaspersky Security Center Linux жүйесін жаңартпас бұрын сертификатты ауыстыру маңызды. Әйтпесе, жаңартудан кейін Web Console веб-консолін кіре алмайсыз.

     Сертификатта SAN бар екеніне көз жеткізу үшін:

     1. Басқару сервер орнатылған құрылғыда келесі пәрменді орындаңыз:

        - Linux құрылғысы үшін:

          ```
          sudo openssl x509 -in /var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer -noout -ext subjectAltName
          ```

        - Windows құрылғысы үшін:

          ```
          certutil -dump %ProgramData%\KasperskyLab\adminkit\1093\cert\klserver.cer
          ```

     2. Пәрмен шығысында Субъектінің балама атауының бар екеніне және Басқару сервері құрылғысының мекенжайын қамтитынына көз жеткізіңіз.

     3. Егер Тақырыптың балама атауы болмаса, klsetsrvcert утилитасын пайдаланып, реттелетін сертификатыңызды талаптарға сай келетін сертификатпен ауыстырыңыз.

     Егер ол талаптарға сай келмесе, klsetsrvcert утилитасын пайдаланып, алдыңғы Басқару серверіндегі Басқару серверінің жалпы сертификатын ауыстырыңыз. Осыдан кейін жаңарту, жылжыту немесе көшіру рәсімін қайталаңыз.

   - Егер мән Kaspersky Security Center Linux орнату кезінде көрсетілген мәнге сәйкес келсе (орнату шеберінің **IAM серверінің DNS атауын енгізу** қадамында немесе үнсіз орнату үшін, `KLSRV_UNATT_IAM_ADDRESS` параметрінде), қосымша әрекет қажет емес. IAM сервері мен Басқару сервері дұрыс өзара әрекеттеседі.

   - Егер мәнде циклдік кері байланыс мекенжайлары (127.0.0.1 және/немесе 0:0:0:0:0:0:0:1) болса, конфигурация файлында олардың бірін пайдаланыңыз. 127.0.0.1 пайдалану ұсынылады.

3. Басқару серверінің жалпы сертификатынан SAN мекенжайы мәндерінің бірін IAM серверінің конфигурациялық файлындағы `server_iam` блогына келесі форматта қосыңыз: `ksc_address: "<SAN_address>"`.

   IAM Server конфигурация файлын өзгерту үшін мәтіндік редакторды пайдалануға болады, мысалы, vi. Келесі команда файлды vi мәтіндік редакторында ашады:

   ```
   vi /var/opt/kaspersky/klnagent_srv/iam/iam_config.yaml
   ```

IAM Server конфигурация файлындағы server_iam блогының мысалы:

```
server_iam:
    iam_address: "ksc.example.com"
    server_display_name: "ksc.example.com"
    ksc_address: "oldksc.example.internal"
    ksc_ca: "/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer"
```

Мысалдағыдай бос орынды пайдалануды ұмытпаңыз.

4. `ksc_address` параметріндегі желі атауының Басқару серверінің IP мекенжайына анықталады. Ол үшін Басқару серверіндегі Ping утилитасын пайдалануға болады.

   Егер шешілген мекенжай басқаша болса, ескі Басқару серверінің желіден ажыратылғанына және ескі IP мекенжайы бар DNS жазбаларының қалмағанына көз жеткізіңіз. Егер мекенжайды шешу мүмкін болмаса, оны корпоративтік DNS-тегі DNS жазбасын пайдаланып салыстырыңыз немесе Басқару серверіндегі хосттар файлына жазба қосыңыз.

5. Конфигурация өзгерістерін қолдану үшін келесі пәрменді орындау арқылы IAM сервер қызметін қайта іске қосыңыз:

   ```
   sudo systemctl restart kliam_srv.service
   ```

Басқару серверінің мекенжайы Басқару серверінің жалпы сертификатынан IAM серверінің конфигурация файлына қосылады.

Ақаулықтарды жою

IAM серверіндегі конфигурация мәселелері веб-консольге кіру кезінде қателер тудыруы мүмкін. Төмендегі кестеде мүмкін қателер мен шешімдер сипатталған.

Сәтсіз аяқталды	Сипаттамасы	Шешім
Сіздің сұрауыңызды қазір өңдеу мүмкін емес. Күте тұрып, қайталап көріңіз.	Kaspersky Security Center Linux жүйесін жаңартқаннан немесе қалпына келтіргеннен кейін деректерді инициализациялау процесінен басқа, көрсетілген желі мекенжайын пайдаланып Басқару серверіне қосылу сәтсіз болған жағдайда бұл қате орын алуы мүмкін.	Ping утилитасын пайдаланып желі атауы қай IP мекенжайына сәйкес келетінін тексеріңіз.
Басқару сервері сенімсіз сертификатты пайдаланады. Қолданбаны жарамды сертификатты көрсету арқылы қайта конфигурациялаңыз немесе негізгі әкімшіге хабарласыңыз.	Қате IAM серверінің конфигурация файлындағы мекенжай мәні Басқару серверінің жалпы сертификатының Тақырыптың балама атауы (SAN) атрибутындағы мәнге сәйкес келмеген жағдайда орын алуы мүмкін.	Жоғарыдағы нұсқауларды орындаңыз.
Пайдаланушы аты немесе құпия сөз дұрыс емес.	Дұрыс емес есептік деректерінен басқа, бұл қате желіде дәл осындай атаумен басқа Басқару сервері болған жағдайда орын алуы мүмкін.	Көрсетілген мекенжайдың ағымдағы Басқару серверінің IP мекенжайына сәйкес келетінін тексеріңіз.

Ортақ қатынасы бар қалтаны белгілеу

Басқару сервері орнатылғаннан кейін Басқару серверінің сипаттарында ортақ қалтаның орнын көрсетуге болады. Әдепкі бойынша ортақ қалта Басқару сервері бар құрылғыда жасалады. Алайда кейбір жағдайларда (жоғары жүктеме немесе оқшауланған желіден қатынасу қажеттілігі сияқты) ортақ қатынасы бар қалтаны мамандандырылған файлдық ресурсқа орналастырған жөн.

Ортақ қатынасы бар қалта Желілік агентті орналастырудың бірнеше сценарийінде пайдаланылады.

Ортақ қатынасы бар қалта үшін тіркелімді есепке алу сөндірілуі тиіс.

Kaspersky Security Center Web Console бағдарламасына кіру және одан шығу

Kaspersky Security Center Web Console веб-консоліне Басқару серверін және Kaspersky Security Center Web Console веб-консолін орнатқаннан кейін кіре аласыз. Сіз орнату барысында көрсетілген Басқару серверінің веб-мекенжайын білуіңіз керек (әдепкі бойынша 8080-порт қолданылады). Сіздің браузеріңізде JavaScript қосулы болуы тиіс.

Kaspersky Security Center Web Console веб-консоліне келесі тәсілдердің бірімен кіруге болады:

- Домен аутентификациясын пайдалану (бір рет кіру) арқылы

  Бұл әдіс басқару серверінің 16 және одан кейінгі нұсқасына қосылған Kaspersky Security Center Web Console-де қауіпсіз аутентификация үшін пайдаланылады. Домен аутентификациясын пайдаланғыңыз келсе, Kaspersky Security Center Web Console орнату кезінде Есептік деректер және қатынасу диспетчерімен (IAM) өзара әрекеттесу үшін қосымша параметрлерді көрсетуіңіз керек.

- Домен пайдаланушысының аты мен құпиясөзін көрсету арқылы

  Домен пайдаланушы тіркелгісі көмегімен жүйеге кірмес бұрын, домен пайдаланушыларының тізімін алу үшін домен контроллерлерінен сұраңыз. Содан кейін басқару серверіне кіру үшін домен пайдаланушысының аты мен құпиясөзін көрсетуіңіз керек. Бұл әдіс тек Microsoft Active Directory арқылы аутентификация үшін қолдау көрсетіледі.

- Ішкі пайдаланушының аты мен құпиясөзін көрсету арқылы

Kaspersky Security Center Web Console-ге кіргіңіз келетін Пайдаланушы есептік жазбасына рөл тағайындалған болуы керек. Кірмес бұрын, доменге немесе ішкі пайдаланушы есептік жазбасына рөл тағайындалғанына көз жеткізіңіз. Әйтпесе, кіру қатесі орын алады.

Домен аутентификациясы арқылы жүйеге кіру (бірыңғай кіру)

Домендік түпнұсқалық растаманы қолдану арқылы Kaspersky Security Center Web Console веб-консоліне кіру үшін:

1. Браузерден https://<Kaspersky Security Center Web Console address>:<Порт нөмірі> бетіне өтіңіз.

   Басқару серверін таңдау беті көрсетіледі.

2. Бірнеше сенімді Басқару серверін қосқан болсаңыз, тізімнен қосылғыңыз келетін Басқару серверін таңдаңыз.

   Тек бір басқару серверін қосқан болсаңыз, басқару серверлерінің тізімі көрсетілмейді.

   Браузер https://<Administration Server address>:4444 мекенжайына бағытталады.

3. Kerberos домен аутентификациясын конфигурациялау.

4. Келесі әрекеттердің бірін орындаңыз:

   - **Домен аутентификациясын пайдалану** түймесін басыңыз.
   - Егер Серверде бір немесе бірнеше виртуалды Басқару сервері жасалған болса және сіз домендік түпнұсқалық растама арқылы виртуалды Серверге кіргіңіз келсе:

     a. **Виртуалды сервер опцияларын көрсету** түймесін басыңыз.

     b. Виртуалды Серверді жасау кезінде көрсетілген виртуалды Басқару сервері атауын енгізіңіз.

     c. **Домен аутентификациясын пайдалану** түймесін басыңыз.

5. Ұялы құрылғыдағы аутентификация қолданбасы арқылы жасалған бір реттік қауіпсіздік кодын көрсетіңіз.

   Бірінші кіру кезінде аккаунтыңыз үшін екі сатылы аутентификацияны конфигурациялаңыз. Егер екі факторлы аутентификация конфигурациясы сізге қолжетімді болмаса, **Жалпы мүмкіндіктер**: **Жалпы функционал** функционалдық аймағында Пайдаланушы рұқсаттары бар және аккаунтыңызды екі факторлы аутентификацияға рұқсат тізіміне қосу үшін екі факторлы аутентификацияны конфигурациялаған пайдаланушыға хабарласыңыз.

Жүйеге кіргеннен кейін, соңғы рет пайдаланған тіл мен тақырыпты қамтитын Kaspersky Security Center Web Console басты беті көрсетіледі. Сіз Kaspersky Security Center Web Console шарлай аласыз және оны Kaspersky Security Center Linux бағдарламасымен жұмыс істеу үшін қолдана аласыз.

Доменнің немесе ішкі пайдаланушының атын және құпиясөзін көрсету арқылы жүйеге кіру

Пайдаланушы аты мен құпиясөзін көрсету арқылы Kaspersky Security Center Web Console жүйесіне кіру үшін:

1. Браузерден https://<Kaspersky Security Center Web Console address>:<Порт нөмірі> бетіне өтіңіз.

   Басқару серверін таңдау беті көрсетіледі.

2. Бірнеше сенімді Басқару серверін қосқан болсаңыз, тізімнен қосылғыңыз келетін Басқару серверін таңдаңыз.

   Тек бір басқару серверін қосқан болсаңыз, басқару серверлерінің тізімі көрсетілмейді.

   Браузер https://<Administration Server address>:4444 мекенжайына бағытталады.

3. Келесі әрекеттердің бірін орындаңыз:

   - Басқару серверіне домен пайдаланушы тіркелгісімен кіру үшін домен пайдаланушының аты мен құпиясөзін енгізіңіз.

     Домен пайдаланушы атын келесі пішімдердің бірімен енгізуге болады:

     - `Пайдаланушы аты@dns.domain`
     - `NTDOMAIN\Username`

     Домен пайдаланушы тіркелгісімен жүйеге кірмес бұрын, домен пайдаланушыларының тізімін алу үшін домен контроллерлерінен сұраңыз.

- Басқару серверіне әкімшінің пайдаланушы аты мен құпиясөзін көрсетіп кіру үшін ішкі пайдаланушының аты мен құпиясөзін енгізіңіз.

- Егер Серверде бір немесе бірнеше виртуалды Басқару сервері жасалған болса және сіз виртуалды Серверге кіргіңіз келсе:

  a. **Виртуалды сервер опцияларын көрсету** түймесін басыңыз.

  b. Виртуалды Серверді жасау кезінде көрсетілген виртуалды Басқару сервері атауын енгізіңіз.

  c. Виртуалды Басқару серверінде құқықтары бар әкімшінің пайдаланушы аты мен құпиясөзін енгізіңіз.

4. **Кіру** түймесін басыңыз.

5. Ұялы құрылғыдағы аутентификация қолданбасы арқылы жасалған бір реттік қауіпсіздік кодын көрсетіңіз.

   Бірінші кіру кезінде аккаунтыңыз үшін екі сатылы аутентификацияны конфигурациялаңыз. Егер екі факторлы аутентификация конфигурациясы сізге қолжетімді болмаса, **Жалпы мүмкіндіктер**: **Жалпы функционал** функционалдық аймағында Пайдаланушы рұқсаттары бар және аккаунтыңызды екі факторлы аутентификацияға рұқсат тізіміне қосу үшін екі факторлы аутентификацияны конфигурациялаған пайдаланушыға хабарласыңыз.

6. Есептік жазбаңыз үшін құпиясөзді өзгертуге мәжбүрлеу қосылса немесе құпиясөз мерзімі өтіп кетсе, құпиясөзді өзгерту терезесі пайда болады. Kaspersky Security Center Web Console веб-консоліне кіруге арналған жаңа құпиясөзді орнатыңыз.

Жүйеге кіргеннен кейін, соңғы рет пайдаланған тіл мен тақырыпты қамтитын Kaspersky Security Center Web Console басты беті көрсетіледі. Сіз Kaspersky Security Center Web Console шарлай аласыз және оны Kaspersky Security Center Linux бағдарламасымен жұмыс істеу үшін қолдана аласыз.

Шығу

Kaspersky Security Center Web Console веб-консолінен шығу үшін,

Жоғарғы панельде есептік жазба атауын басу арқылы есептік жазба мәзіріне өтіңіз де, **Шығу** опциясын таңдаңыз.

Kaspersky Security Center Web Console бағдарламасы жабық, бағдарламаға кіру беті көрсетіледі.

Kaspersky Security Center Web Console интерфейсі

Kaspersky Security Center Linux жүйесі Kaspersky Security Center Web Console интерфейсі арқылы басқарылады.

Kaspersky Security Center Web Console қолданбасының терезесі келесі элементтерді қамтиды:

- Терезенің сол жағындағы негізгі мәзір
- Терезенің жоғарғы бөлігіндегі жоғарғы панель
- Терезенің оң жағындағы жұмыс аймағы

Негізгі мәзір

Негізгі мәзір келесі бөлімдерден тұрады:

- **Басқару сервері**. Қазіргі уақытта қосылған Басқару серверінің атауын көрсетеді. Басқару серверінің атауын басып, Басқару серверінің сипаттарын ашуға болады.
- **Консольді шарлау**. Негізгі мәзір картасын көрсетеді. Көрсетілген бөлімдердің көпшілігін бетбелгілерге қосуға немесе басты бет ретінде орнатуға болады. Әдепкісінше **Консольді шарлау** басты бет ретінде орнатылады. Бұл параметрлерді өзгертуге болады.
- **Мониторинг**. Желіңіздің инфрақұрылымы, қорғаныс күйі, сондай-ақ статистика туралы мәлімет береді.
- **Активтерді басқару**. Құрылғы мен аппараттық құралдарды басқару құралдарын және Kaspersky қолданба саясаттарын қамтиды.
- **Тапсырмалар**. Тапсырмаларды жасау және іске қосу құралдарын қамтиды.
- **Пайдаланушылар және рөлдер**. Пайдаланушылар мен рөлдерді басқаруға, пайдаланушы құқықтарын конфигурациялауға, пайдаланушыларға рөлдерді тағайындауға және саясат профильдерін рөлдермен байланыстыруға мүмкіндік береді.
- **Қоймалар**. Сонымен қатар, қолданбалар қоймаларына қол жеткізуге мүмкіндік беріледі.
- **Бағдарламалық жасақтаманы басқару**. Kaspersky және үшінші тарап қолданбаларын, сондай-ақ орнату пакеттері мен патчтарын басқаруға мүмкіндік береді.
- **Операциялар**. Қолданбаны лицензиялау, шифрланған дискілерді және шифрлау оқиғаларын көру және басқару сияқты әртүрлі параметрлерді қамтиды.
- **Құрылғыларды табу және орналастыру**. Клиент құрылғыларын анықтау және құрылғыларды басқару топтарына қолмен немесе автоматты түрде тарату үшін желіде сауалнама жүргізуге мүмкіндік береді. Бұл бөлімде бастапқы орнату шебері және қорғанысты орналастыру шебері бар.
- **Marketplace**. Kaspersky бизнес-шешімдері туралы ақпаратты қамтиды, сізге қажет шешімдерді таңдауға және Kaspersky сайтында осы шешімдерді сатып алуды жалғастыруға мүмкіндік береді.
- **Параметрлер**. Сізге сақталған күйді кейін қалпына келтіру үшін веб-плагиннің ағымдағы күйін сақтық көшірмелеуге мүмкіндік береді. Интерфейс тілі немесе тақырыбы сияқты интерфейстің сыртқы түріне қатысты жеке параметрлерді қамтиды.

Қажет болса, экранның төменгі жағындағы шеврон (<<) белгісін басып, негізгі мәзірді белгішелерге дейін кішірейтуге болады.

Жоғарғы панель

Жоғарғы панель әрқашан барлық консоль бөлімінде көрсетіледі және оны жасыру мүмкін емес.

Панельдің сол жағында қолданба атауы мен логотипі бар. Қолданба атауын немесе логотипті бассаңыз, Kaspersky Security Center Web Console басты беті ашылады.

Панельдің оң жағында келесі опция көрсетіледі:

- Хабарландыру белгішесі (🔔). Белгішені бассаңыз, хабарландырулары бар панель ашылады.
- Есептік жазба мәзірі. Kaspersky Security Center Linux анықтамасына сілтемені қамтиды. Сондай-ақ Kaspersky Security Center Linux жүйесінен шығып, есептік жазба құпиясөзін өзгертіп, Kaspersky Security Center Web Console нұсқасын және орнатылған веб-басқару плагиндерінің тізімін көруге болады.

Жұмыс аймағы

Жұмыс аймағы Kaspersky Security Center Web Console интерфейсі терезесінің бөлімдерінде көру үшін таңдалған ақпаратты көрсетеді. Сондай-ақ, ол ақпаратты көрсетуді конфигурациялау үшін пайдалануға болатын басқару элементтерін қамтиды.

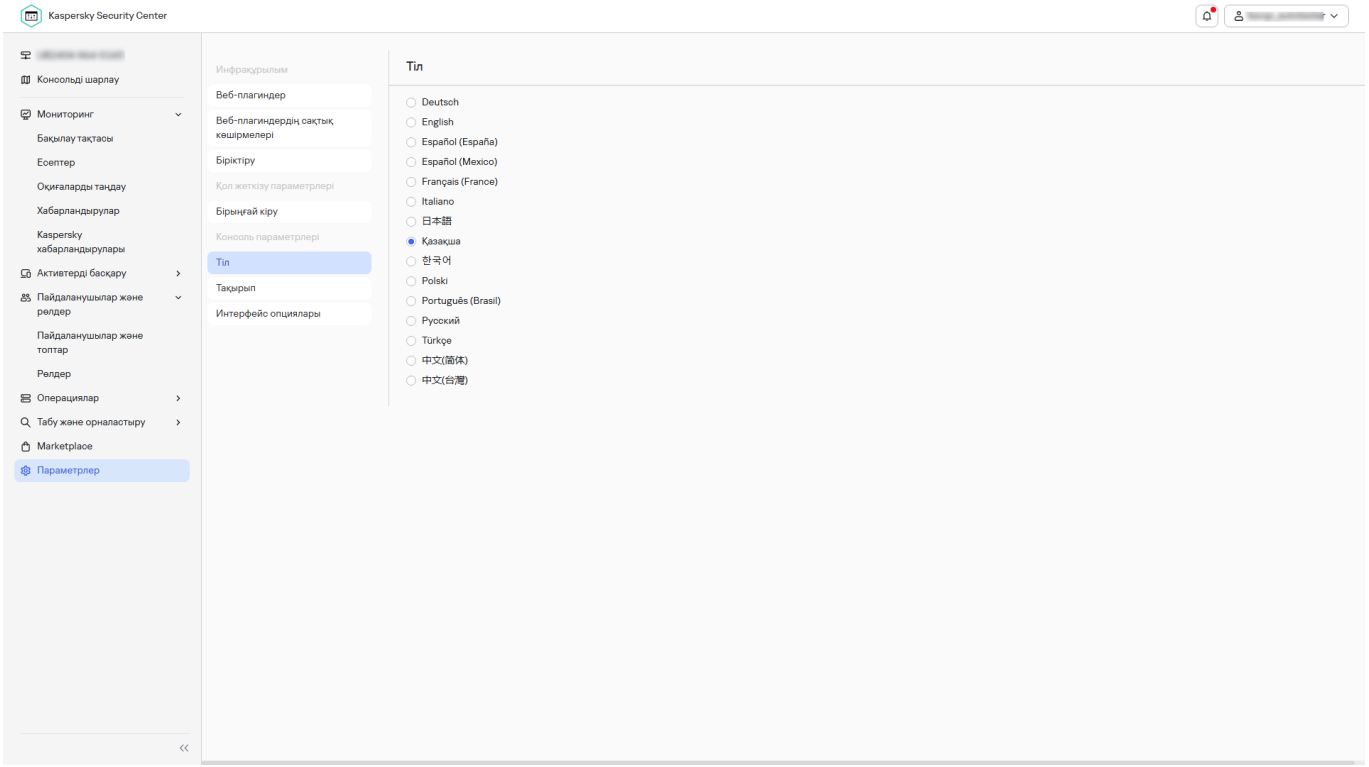
Kaspersky Security Center Web Console-мен жұмыс істеу үшін бір браузер қойындысын пайдалануға кеңес береміз.

Kaspersky Security Center Web Console интерфейсінің тілін өзгерту

Kaspersky Security Center Web Console интерфейсінің тілін таңдауға болады.

Интерфейс тілін өзгерту үшін:

1. Қолданбаның негізгі терезесінде **Параметрлер** → **Тіл** бөліміне өтіңіз.
2. Қолдау көрсетілетін локализация тілдерінің бірін таңдаңыз.



Kaspersky Security Center Web Console интерфейсінің тілін өзгерту

Kaspersky Security Center Web Console басты бетін өзгерту

Басты бет Kaspersky Security Center Web Console жүйесіне кіргеннен кейін көрсетіледі.

Әдепкісінше **Консольді шарлау** бөлімі басты бет ретінде орнатылады. Қажет болса, басты бетті өзгертуге болады.

Басты бетті өзгерту үшін:

1. **Консольді шарлау** бөлімінде басты бет ретінде орнатқыңыз келген элементке тінтуір курсорын апарыңыз.
2. Басты бет (⌂) белгішесі көрсетіледі, оны басыңыз.

   Басты бет өзгертіледі, экранда тиісті хабар көрсетіледі және басты бет ретінде таңдалған элемент басты бет (⌂) белгішесімен белгіленеді.

Marketplace және **Параметрлер** бөлімдерін басты бет ретінде орнату мүмкін емес.

Бетбелгілерді қосу және өшіру

Басты мәзірдегі **Бетбелгілер** бөлімінен жылдам қол жеткізу үшін бетбелгілерге Kaspersky Security Center Web Console жиі қолданылатын бөлімдерін қосуға болады.

Бетбелгілерге ешқандай бөлім қоспасаңыз, басты мәзірде **Бетбелгілер** бөлімі көрсетілмейді.

Бетбелгілерге беттерді көрсететін бөлімдерді ғана қосуға болады. Мысалы, **Активтерді басқару → Активтер (құрылғылар)** тармағына өтсеңіз, құрылғылар кестесі бар бет ашылады, яғни бұл бөлімді бетбелгілерге қосуға болады. Негізгі мәзірден бөлім таңдағаннан кейін, терезе көрсетілсе не ешқандай элемент көрсетілмесе, мұндай бөлімді бетбелгілерге қосу мүмкін емес.

Бетбелгілерге бөлім қосу үшін:

1. Негізгі мәзірден тінтуірді бекіткіңіз келетін бөлімнің үстіне апарыңыз.
2. Бетбелгілер (⌑) белгішесі көрсетілгеннен кейін, белгішені басыңыз.

   Бөлім **Бетбелгілер** бөлімінде көрсетіледі.

Бетбелгілерден бөлімді өшіру үшін:

1. Негізгі мәзірдегі **Бетбелгілер** бөліміне өтіңіз.
2. Тінтуірді өшіргіңіз келетін бөлімге апарып, бетбелгі (⌑) белгішесін басыңыз.

   Бөлім бетбелгілерден өшіріледі.

Консольді шарлау бөліміндегі бөлімдерге тінтуір курсорын апарып, бетбелгі (🔖) белгішесін басу арқылы да бөлімдерді бетбелгілерге қосуға және өшіруге болады. Таңдалған элемент бетбелгі (🔖) белгішесімен белгіленеді және басты мәзірдің **Бетбелгілер** бөлімінде көрсетіледі. Элементті бетбелгілерден өшіргіңіз келсе, бетбелгі (🔖) белгішесін басыңыз.

Бетбелгілер бөлімі тек негізгі мәзірде көрсетіледі. Ол **Консольді шарлау** бетінде көрсетілмейді.

Kaspersky Security Center Web Console веб-консолін жою

Келесі жағдайларда Kaspersky Security Center Web Console Server серверін (сонымен қатар Kaspersky Security Center Web Console веб-консолі деп те аталады) жою қажет болуы мүмкін:

- Басқа ортақ сертификатпен сақтық көшірмеден деректерді қалпына келтіру.
- Басқару серверінің ортақ сертификатын қайта шығару.
- Веб-консоль сертификатын арнайы сертификатпен ауыстыру.
- Kaspersky Security Center Web Console веб-консолі енді құрылғыда пайдаланылмайды.

Kaspersky Security Center Web Console жаңарту үшін:

1. Linux дистрибутивіңізге байланысты келесі пәрмендердің бірін іске қосыңыз:
   - `sudo dnf remove ksc-web-console`
   - `sudo apt remove ksc-web-console`
2. Нәтижені келесі пәрменді орындау арқылы тексеріңіз:
   `sudo systemctl status KSC*`
   Kaspersky Security Center Web Console веб-консолі пәрмен шығысында болмауы керек.

Егер сіз Kaspersky Security Center Web Console веб-консолін қалпына келтіргіңіз келсе, оны құрылғыға мақалада сипатталғандай орнатыңыз: Kaspersky Security Center Web Console веб-консолін орнату.

Бағдарламаны жылдам іске қосу шебері

Kaspersky Security Center Linux бағдарламасы, желіні қауіпсіздік қауіптерінен қорғауды қамтамасыз ететін орталықтандырылған басқару жүйесін құру үшін қажетті параметрлердің ең аз жиынтығын конфигурациялауға мүмкіндік береді. Бұл конфигурация бағдарламаны жылдам іске қосу шеберінде орындалады. Шебердің жұмысы барысында, сіз бағдарламаға келесі өзгерістерді енгізе аласыз:

- Басқару топтарындағы құрылғыларға автоматты түрде таратуға болатын кілт файлдарын қосу немесе белсендіру кодтарын енгізу.
- Басқару серверінің және басқарылатын қолданбалардың жұмысы барысында орын алатын оқиғалар туралы хабарландыруларды электрондық пошта арқылы конфигурациялау.

- Жұмыс станциялары мен серверлерді қорғау саясатын, сондай-ақ зиянды БҚ іздеу, жаңартуларды алу және басқарылатын құрылғылар иерархиясының жоғарғы деңгейі үшін деректерді сақтық көшірмелеу тапсырмаларын қалыптастыру.

  Бағдарламаны жылдам іске қосу шебері **Активтер (құрылғылар)** қалтасында саясаттары әлі жасалмаған бағдарламалар үшін ғана саясаттар жасайды. Осындай аттары бар тапсырмалар басқарылатын құрылғылар иерархиясының жоғары деңгейі үшін әлдеқашан жасалған болса, бағдарламаны жылдам іске қосу шебері мұндай тапсырмаларды жасамайды.

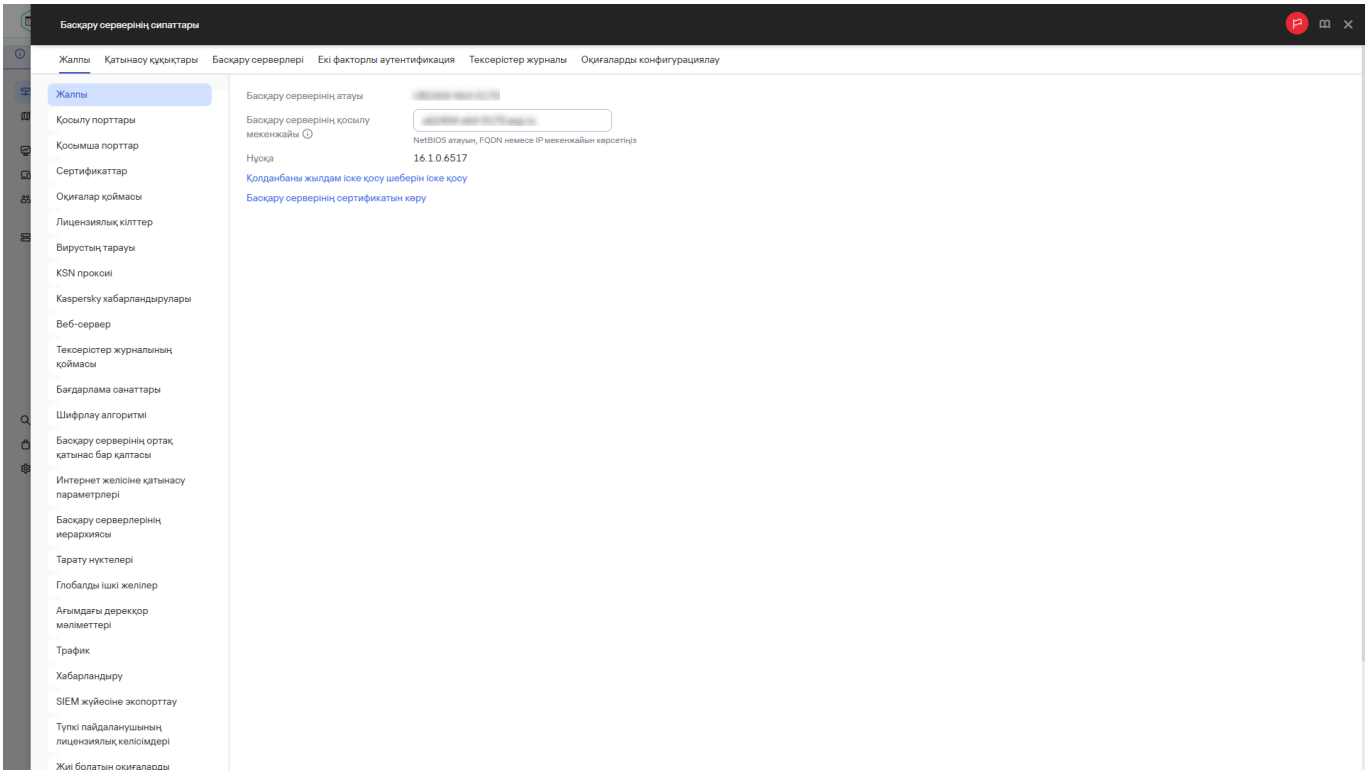
Серверге бірінші рет қосылу кезінде Басқару серверін орнатқаннан кейін, бағдарлама автоматты түрде бағдарламаны жылдам іске қосу шеберін іске қосуды ұсынады. Сондай-ақ, бағдарламаны жылдам іске қосу шеберін кез келген уақытта қолмен іске қоса аласыз.

Бағдарламаны жылдам іске қосу шеберін қолмен іске қосу үшін:

1. Негізгі мәзірдегі басқару серверінің атауын басыңыз.

   Басқару серверінің сипаттары терезесі ашылады.

2. **Жалпы** қойыншасында **Жалпы** бөлімін таңдаңыз.



Басқару серверінің сипаттары терезесі

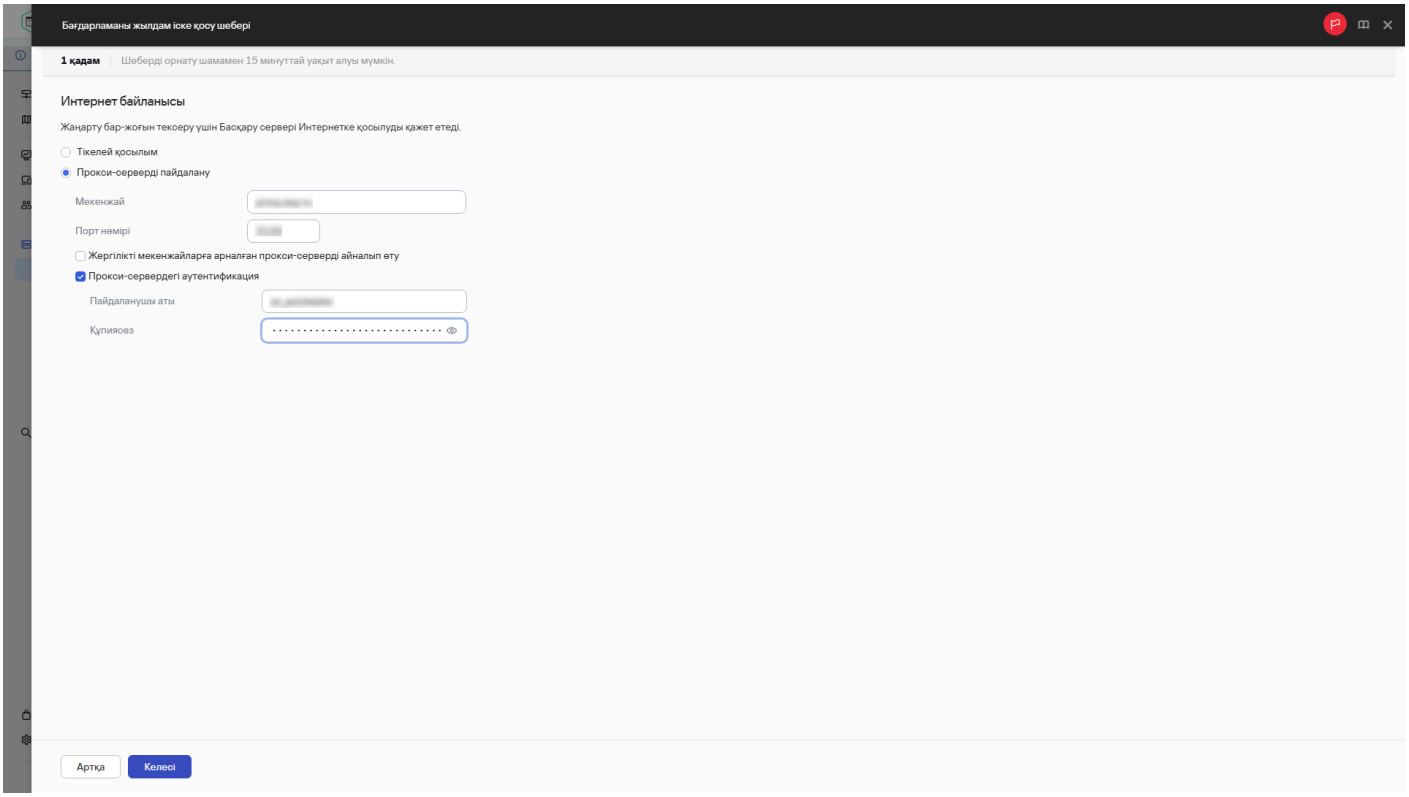
3. **Қолданбаны жылдам іске қосу шеберін іске қосу** түймесін басыңыз.

   Шебер Басқару серверін бастапқы конфигурациялауды ұсынады. Содан кейін, шебердің нұсқауларын орындаңыз. Шебердің жұмысын жалғастыру үшін **Келесі** түймесін басыңыз.

1-қадам. Интернетке қосылу параметрлерін көрсету

Басқару серверінің интернетке қатынасу параметрлерін көрсетіңіз. Kaspersky Security Network пайдалану, сондай-ақ Kaspersky Security Center Linux және Kaspersky басқарылатын бағдарламалары үшін антивирустық дерекқорлар жаңартуларын жүктеу үшін интернетке қатынасуды конфигурациялау қажет.

Интернетке қосу үшін прокси-серверді қолдану керек болса, **Прокси-серверді пайдалану** параметрін қосыңыз. Параметр қосулы болса, параметрлерді енгізу өрістері қолжетімді болады. Прокси-серверге қосылудың келесі параметрлерін конфигурациялаңыз:



Internet connection settings

- **Мекенжай**

  Kaspersky Security Center Linux-ті интернетке қосу үшін прокси-сервер мекенжайы.

- **Порт нөмірі**

  Kaspersky Security Center Linux прокси-қосылымы орнатылатын порт нөмірі.

- **Жергілікті мекенжайларға арналған прокси-серверді айналып өту**

  Жергілікті желідегі құрылғыларға қосылған кезде прокси-сервер қолданылмайды.

- **Прокси-сервердегі аутентификация**

  Жалауша қойылған болса, енгізу өрістерінде прокси-сервердегі түпнұсқалық растама үшін есептік деректерді көрсетуге болады.

  Прокси-серверді пайдалану жалаушасы қойылған болса, енгізу өрісі қолжетімді.

- **Пайдаланушы аты**

  Прокси-серверге қосылатын пайдаланушы есептік жазбасы (**Прокси-сервердегі аутентификация** жалаушасы қойылған болса, өріс қолжетімді болады).

- **Құпиясөз**

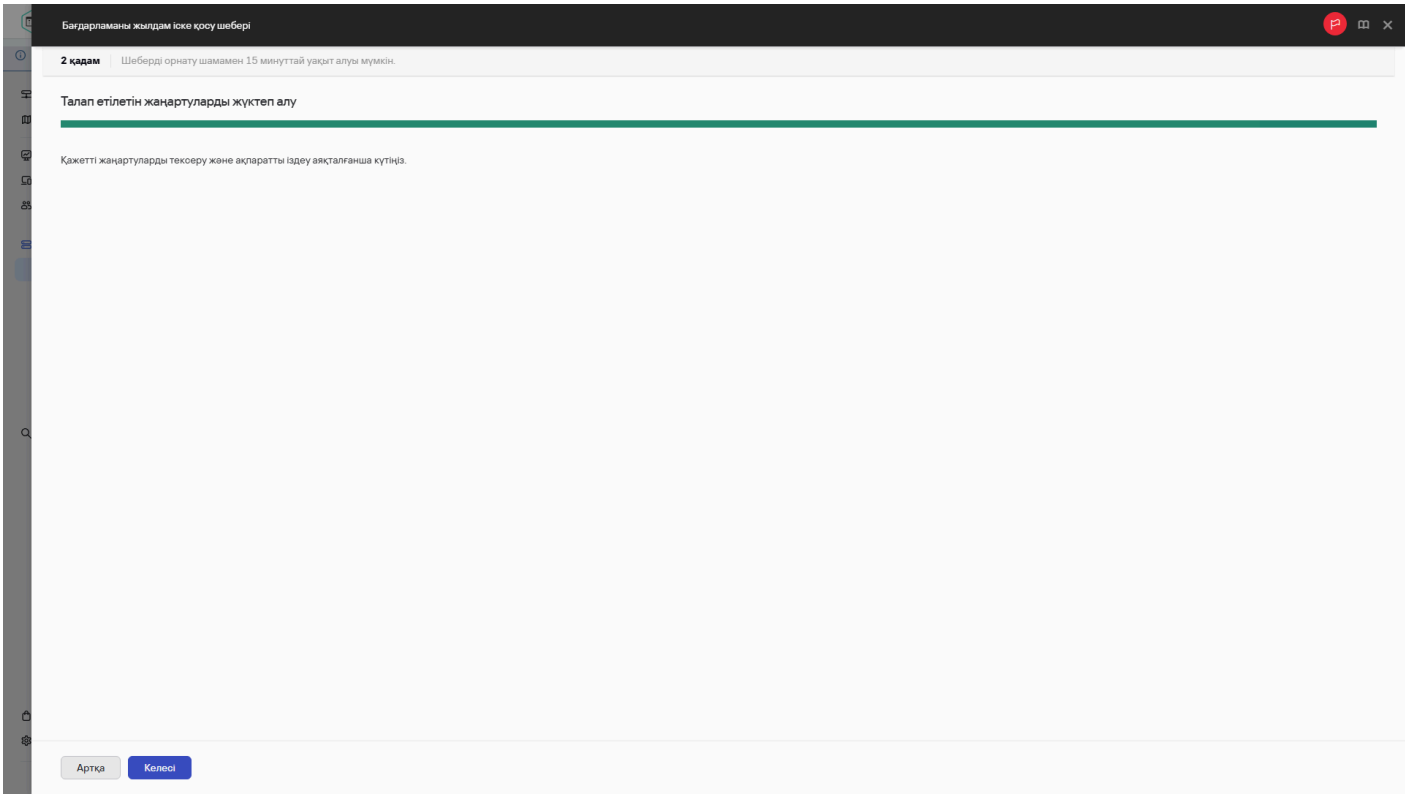
  Прокси-серверге қосылуға мүмкіндік беретін пайдаланушы құпиясөзі (**Прокси-сервердегі аутентификация** жалаушасы қойылған болса, өріс қолжетімді болады).

  Енгізілген құпиясөзді қарау үшін, **Көрсету** түймесін басып, оны қажетті уақыт бойы ұстап тұрыңыз.

Интернетке қатынасуды, бағдарламаны жылдам іске қосу шеберін іске қоспай-ақ, кейінірек конфигурациялай аласыз.

2-қадам. Талап етілетін жаңартуларды жүктеп алу

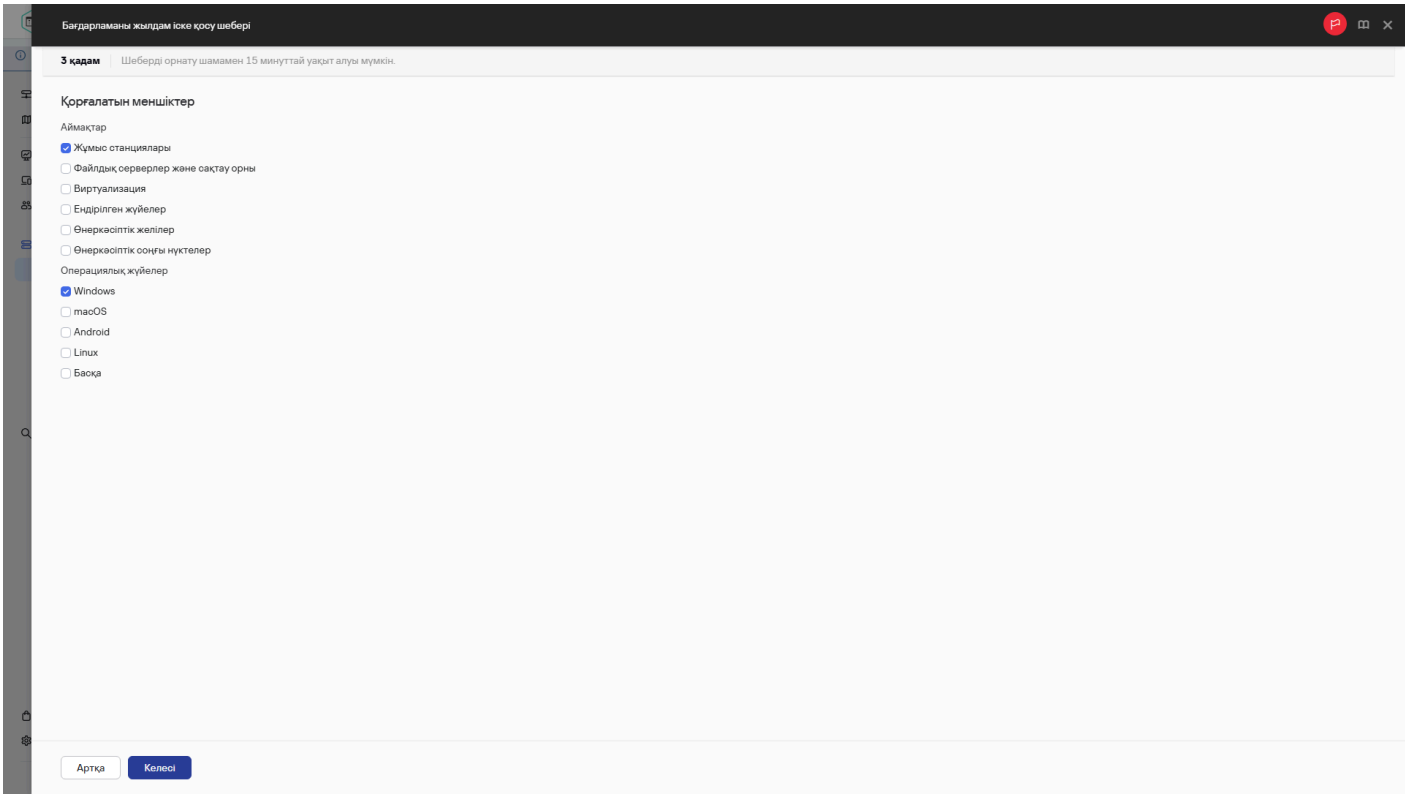
Қажетті жаңартулар Kaspersky серверлерінен автоматты түрде жүктеледі.



Талап етілетін жаңартуларды жүктеп алу

3-қадам. Қорғау үшін активтерді таңдау

Желіңізде қолданылатын қорғаныс аумақтары мен операциялық жүйелерді таңдаңыз. Осы параметрлерді таңдағанда, желіңіздегі клиент құрылғыларына орнату үшін жүктеуге болатын Kaspersky серверлеріндегі бағдарламаларды басқару плагиндері мен дистрибутивтеріне арналған сүзгілерді көрсетесіз.



Қорғау үшін активтерді таңдау

Келесі параметрлерді таңдаңыз:

- **Аймақтар**

  Сіз келесі қорғаныс аймақтарының бірін таңдай аласыз:

  - **Жұмыс станциялары**
  - **Файлдық серверлер және сақтау орны**
  - **Виртуалданды орталар**
  - **Банкоматтар және POS жүйелері**
  - **Өнеркәсіптік желілер**
  - **Өнеркәсіптік соңғы нүктелер**

- **Операциялық жүйелер**

  Сіз келесі платформалардың бірін таңдай аласыз:

  - Microsoft Windows
  - macOS
  - Android
  - Linux
  - Басқа

  Операциялық жүйелердің қолдау көрсетілетін нұсқалары туралы қосымша ақпаратты Kaspersky Security Center Web Console аппараттық және бағдарламалық талаптары бөлімінен қараңыз.

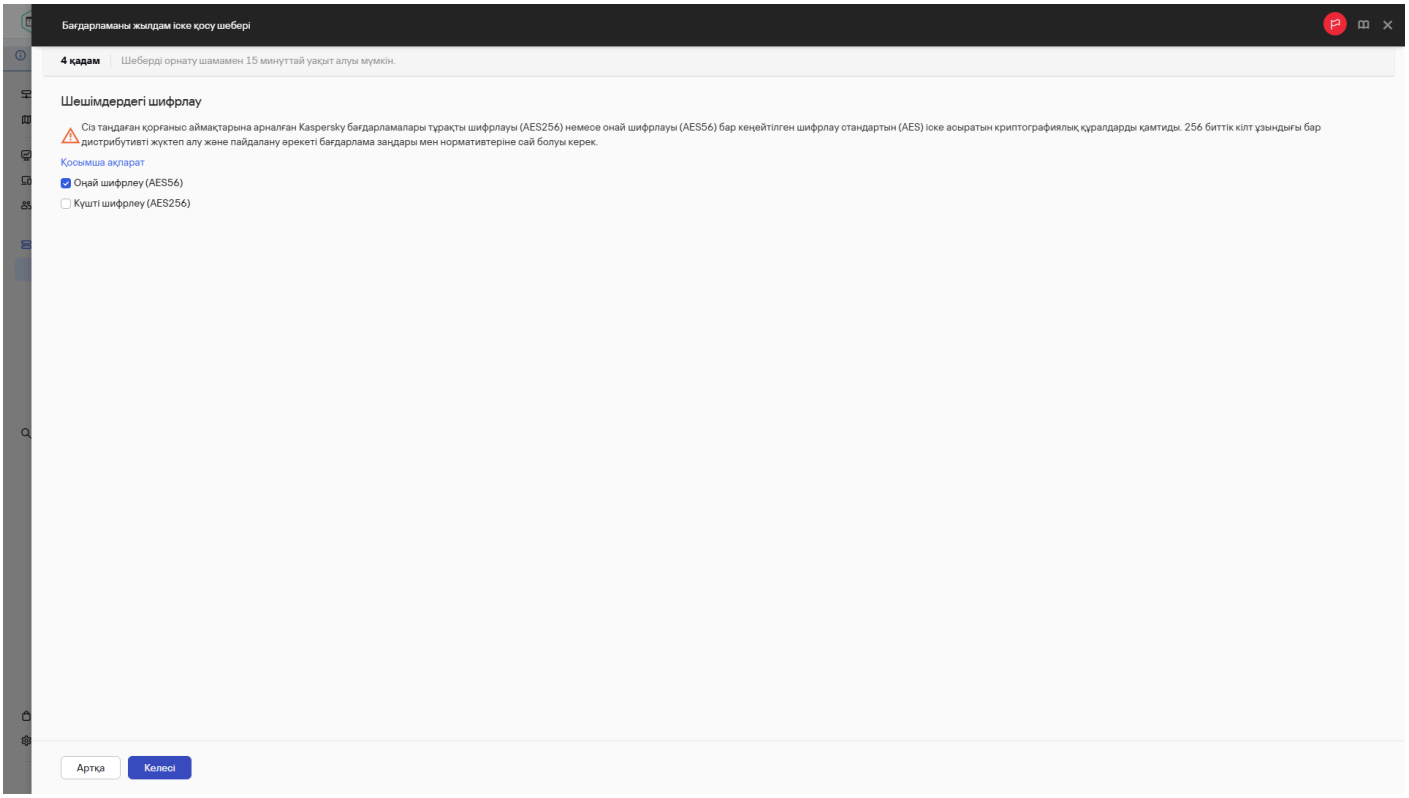
Бағдарламаны жылдам іске қосу шеберін іске қоспай-ақ, қолжетімді орнату пакеттерінің тізімінен Kaspersky бағдарламаларының орнату пакеттерін таңдауға болады. Қажетті орнату пакеттерін табуды жеңілдету үшін қолжетімді орнату пакеттерінің тізімін әртүрлі критерийлер бойынша сүзуге болады.

4-қадам. Шифрлауды таңдау

Шешімдердегі шифрлау терезесі, қорғаныс аумағы ретінде **Жұмыс станциялары** нұсқасы таңдалса ғана көрсетіледі.

Kaspersky Endpoint Security for Windows бағдарламасы, Windows операциялық жүйесі орнатылған клиент құрылғыларында сақталатын ақпаратты шифрлау аспаптарын қамтиды. Бұл шифрлау құралдарында, 256 биттік немесе 56 биттік кілттің ұзындығымен іске асырылған кеңейтілген шифрлау стандарты (AES) бар.

256 биттік кілт ұзындығы бар дистрибутивті жүктеу және пайдалану қолданыстағы заңдар мен ережелерге сәйкес жүзеге асырылуы керек. Ұйымыңыздың қажеттіліктері үшін жарамды Kaspersky Endpoint Security for Windows дистрибутивін жүктеп алу үшін ұйымыңыздың клиент құрылғылары орналасқан елдің заңнамасын қараңыз.



Шифрлауды таңдау

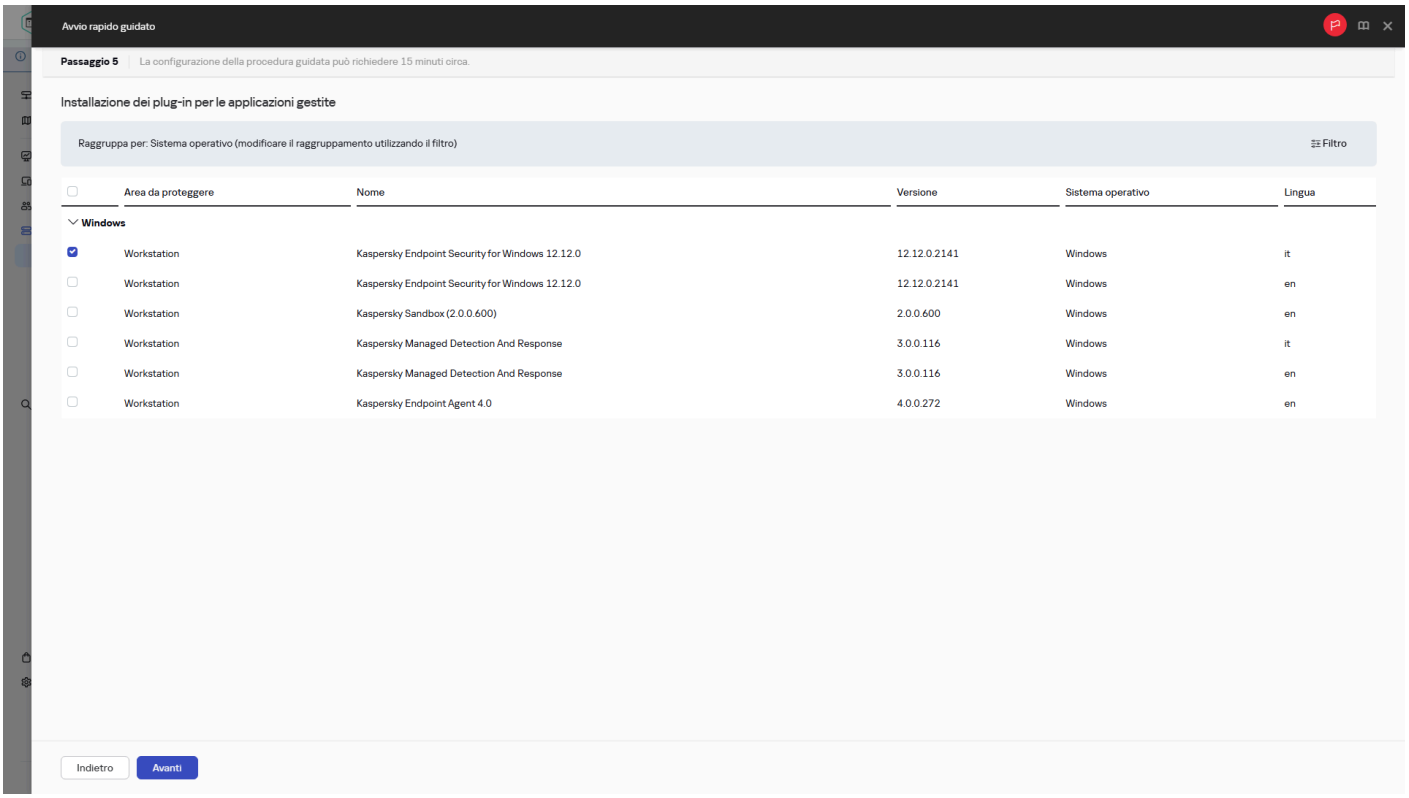
Шешімдердегі шифрлау терезесінде келесі шифрлау түрлерінің бірін таңдаңыз:

- Жылдам шифрлау. Осы шифрлау түрі үшін 56 разрядты кілт қолданылады.
- Тұрақты шифрлау. Осы шифрлау түрі үшін 256 разрядты кілт қолданылады.

Бағдарламаны жылдам іске қосу шеберін іске қоспай-ақ, қажетті шифрлау түрі бар Kaspersky Endpoint Security for Windows дистрибутивін кейінірек таңдауға болады.

5-қадам. Басқарылатын бағдарламалардың плагиндерін орнатуды конфигурациялау

Орнату үшін басқарылатын бағдарламалардың плагиндерін таңдаңыз. Kaspersky серверлерінде орналасқан плагиндер тізімі көрсетіледі. Тізім шебердің алдыңғы қадамында таңдалған параметрлерге сәйкес сүзгіленген. Әдепкі бойынша, барлық тілдердің плагиндері толық тізімге енгізілген. Таңдалған тілде тек плагинді көрсету үшін сүзгіні пайдаланыңыз.



Басқарылатын қолданбалардың плагиндерін орнату

Плагиндер тізімі келесі бағандарды қамтиды:

- **Қауіпсіз аймақ**

  Бұл бағаң қорғау үшін таңдалған аумақтарды көрсетеді.

- **Түрі**

  Бұл бағаң плагин түрлерін көрсетеді.

- **Атауы**

  Қосылатын модульдер, алдыңғы қадамда таңдалған қорғаныс аумақтары мен платформаларына байланысты таңдалды.

- **Нұсқа**

  Тізімге Kaspersky серверлерінде орналастырылған плагиндердің барлық нұсқалары қосылған. Әдепкі бойынша плагиндердің соңғы нұсқалары таңдалған.

- **Ең соңғы нұсқ**

  Бұл бағаң плагиннің соңғы нұсқасы екенін көрсетеді. Егер **true** мәні көрсетілсе, тиісті плагиннің соңғы нұсқасы бар. Егер **false** мәні көрсетілсе, тиісті плагиннің кейінгі нұсқасы бар.

- **ОЖ**

  Бұл бағаң операциялық жүйелердің плагиндерін көрсетеді.

- **Тіл**

  Әдепкі бойынша, плагинді локализациялау тілі, орнату кезінде таңдалған Kaspersky Security Center Linux тіліне байланысты. Басқа тілдерді **Басқару консолінің тілін көрсету немесе** ашылмалы тізімінен таңдауға болады.

Қосылатын модульдерді таңдау үшін, орнатуды бастау мақсатымен **Келесі** түймесін басыңыз.

Kaspersky бағдарламалары үшін басқару плагиндерін бағдарламаны жылдам іске қосу шеберін іске қоспай-ақ, кейінірек қолмен орнатуға болады.

Бағдарламаны жылдам іске қосу шебері таңдалған плагиндерді автоматты түрде орнатады. Кейбір плагиндерді орнату үшін сіз Лицензиялық келісімнің шарттарын қабылдауыңыз қажет. Экранда көрсетілетін Лицензиялық келісімнің мәтінімен танысып шығыңыз, **Kaspersky Security Network бағдарламасын пайдалану шарттарын қабылдаймын** жалаушасын қойыңыз және **Орнату** түймесін басыңыз. Лицензиялық келісімнің шарттарымен келіспесеңіз, плагин орнатылмайды.

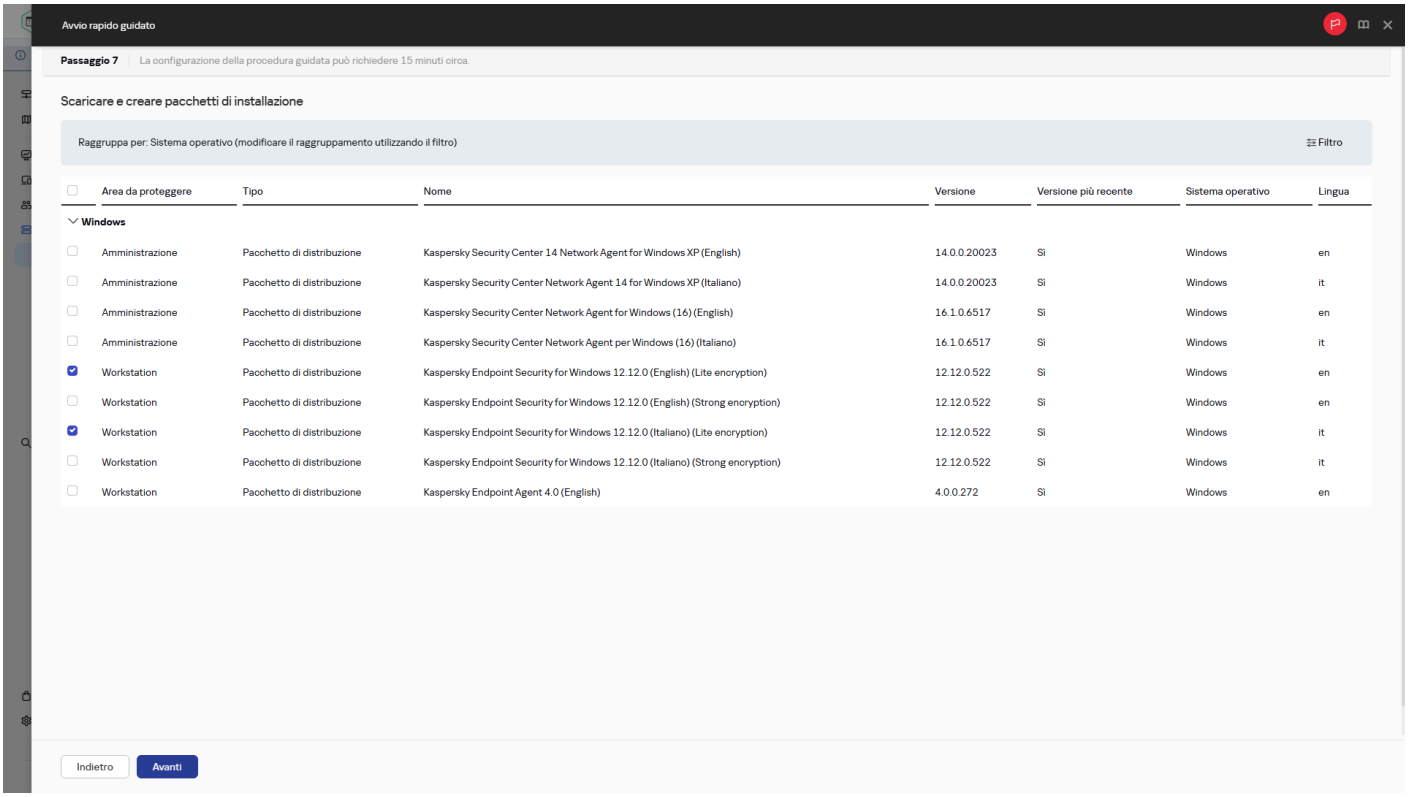
Барлық таңдалған плагиндер орнатылғаннан кейін, бағдарламаны жылдам іске қосу шебері автоматты түрде келесі қадамға өтеді.

6-қадам. Дистрибутивтерді жүктеу және орнату пакеттерін жасау

Жүктелетін дистрибутивті таңдаңыз.

Басқарылатын бағдарламалардың дистрибутивтері үшін Kaspersky Security Center Linux белгілі бір минималды нұсқасын орнату қажет болуы мүмкін.

Kaspersky Endpoint Security for Windows үшін шифрлау түрі таңдалғаннан кейін, екі шифрлау түрі үшін дистрибутивтер тізімі көрсетіледі. Тізімнен таңдалған шифрлау түрі бар дистрибутив таңдалады. Сіз кез келген шифрлау түрі үшін дистрибутивті таңдай аласыз. Дистрибутив тілі Kaspersky Security Center Linux тіліне сәйкес келеді. Kaspersky Security Center Linux тілі үшін бағдарлама дистрибутиві болмаса, ағылшын тіліндегі дистрибутив таңдалады.



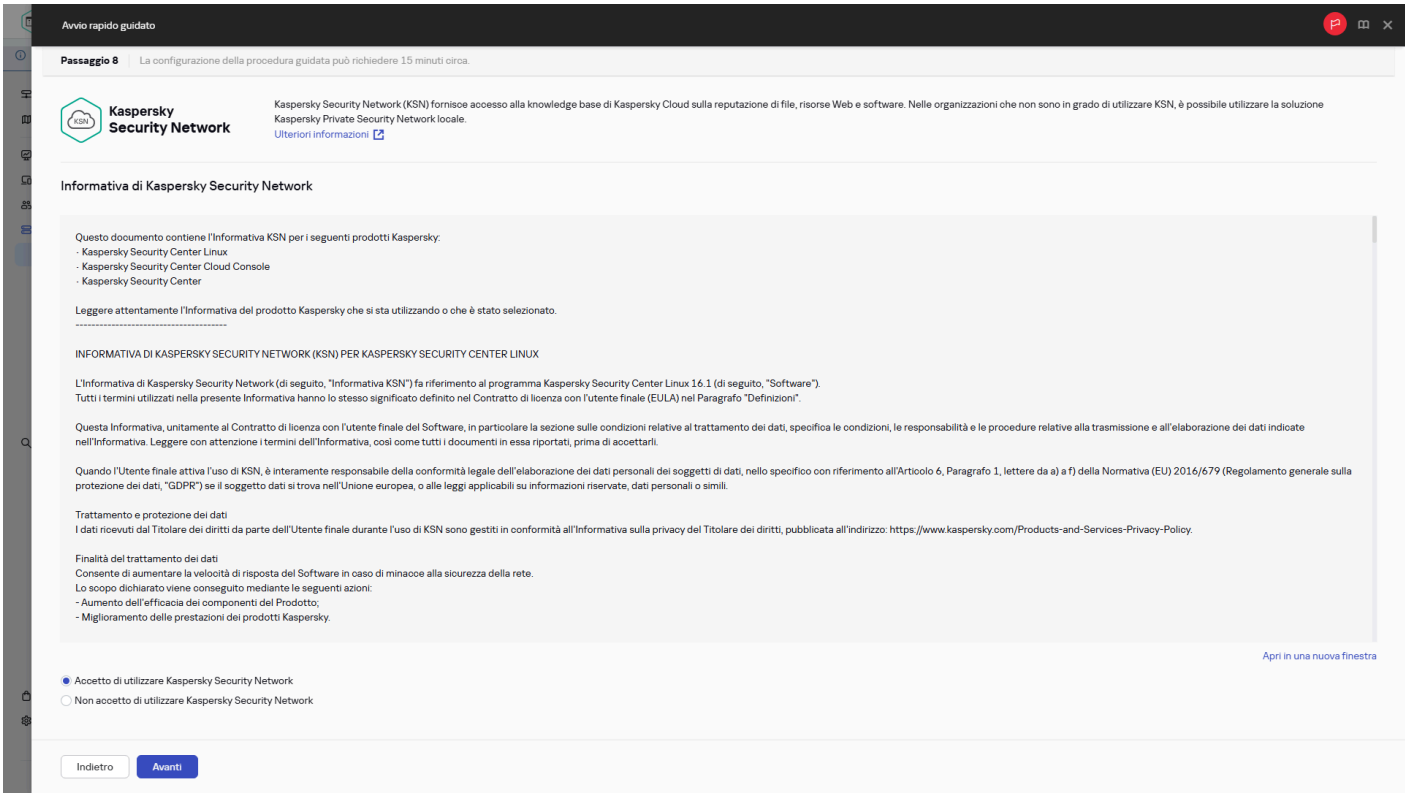
Дистрибутивтерді жүктеу және орнату пакеттерін жасау

Кейбір дистрибутивтерді жүктеуді аяқтау үшін сіз Лицензиялық келісімді қабылдауыңыз керек. **Қабылдау** түймесін басқан кезде Лицензиялық келісім мәтіні көрсетіледі. Шебердің келесі қадамына өту үшін сіз Лицензиялық келісімнің ережелері мен шарттарын, сондай-ақ Kaspersky Құпиялылық саясатының шарттарын қабылдауыңыз керек. Егер сіз ережелер мен шарттарды қабылдамасаңыз, пакетті жүктелмейді.

Лицензиялық келісімнің ережелері мен шарттарын, сондай-ақ Kaspersky Құпиялылық саясатының шарттарын қабылдағаннан кейін, дистрибутивтерді жүктеу жалғасады. Болашақта орнату пакеттерін клиент құрылғыларында Kaspersky бағдарламаларын орналастыру үшін пайдалануға болады.

7-қадам. Kaspersky Security Network конфигурациялау

Kaspersky Security Center Linux жұмысы туралы ақпаратты Kaspersky Security Network білім базасына беру параметрлерін конфигурациялаңыз.



Kaspersky Security Network конфигурациялау

Келесі нұсқалардың бірін таңдаңыз:

- **Kaspersky Security Network бағдарламасын пайдалану шарттарын қабылдаймын**

  Kaspersky Security Center Linux және клиент құрылғыларында орнатылған басқарылатын бағдарламалар, олардың жұмысы туралы ақпаратты Kaspersky Security Network қызметіне автоматты режимде жіберетін болады. Kaspersky Security Network-пен ынтымақтастық, вирустар мен қауіптер туралы дерекқорды барынша жылдам жаңартуды қамтамасыз ете отырып, туындаған қауіпсіздік қауіптеріне жауап беру жылдамдығын арттырады.

- **Kaspersky Security Network пайдалану шарттарын қабылдамаймын**

  Kaspersky Security Center Linux және басқарылатын бағдарламалар өз жұмысы туралы ақпаратты Kaspersky Security Network қызметіне жібермейді.

  Осы параметрді таңдасаңыз, Kaspersky Security Network қызметі өшіріледі.

Бағдарламаны жылдам іске қосу шеберін іске қоспай-ақ Kaspersky Security Network (KSN) жүйесіне қатынасуды кейінірек конфигурациялауға болады.

8-қадам. Бағдарламаны белсендіру тәсілін таңдау

Kaspersky Security Center Linux белсендірудің келесі нұсқаларының бірін таңдаңыз:

- **Белсендіру кодыңызды енгізіңіз**

  Белсендіру коды – жиырма латын әрпі мен санынан құралған бірегей бірізділік. Сіз Kaspersky Security Center Linux бағдарламасын белсендіретін кілтті қосу үшін белсендіру кодын енгізесіз. Белсендіру коды сізге Kaspersky Security Center сатып алу кезінде көрсетілген электрондық пошта мекенжайына жіберіледі.

  Бағдарламаны белсендіру кодының көмегімен белсендіру үшін, Kaspersky белсендіру серверлеріне қосылу мақсатында интернетке қатынасу талап етіледі.

  Бағдарламаны белсендірудің осы нұсқасын таңдаған болсаңыз, **Лицензиялық кілтті басқарылатын құрылғыларға автоматты түрде тарату** нұсқасын қосуға болады.

  Осы нұсқа таңдалса, лицензиялық кілт басқарылатын құрылғыларға таратылатын болады.

  Бұл нұсқа таңдалмаса, лицензиялық кілтті кейінірек басқарылатын құрылғыларға негізгі мәзірдің **Операциялар** → **Лицензиялау** → **Лицензиялар** бөлімінде таратуға болады.

- **Кілт файлын көрсетіңіз**

  Кілт файлы – Kaspersky сізге ұсынатын key кеңейтімі бар файл. Кілт файлы бағдарламаны белсендіретін кілтті қосуға арналған.

  Кілт файлы сізге Kaspersky Security Center сатып алу кезінде көрсетілген электрондық пошта мекенжайына жіберіледі.

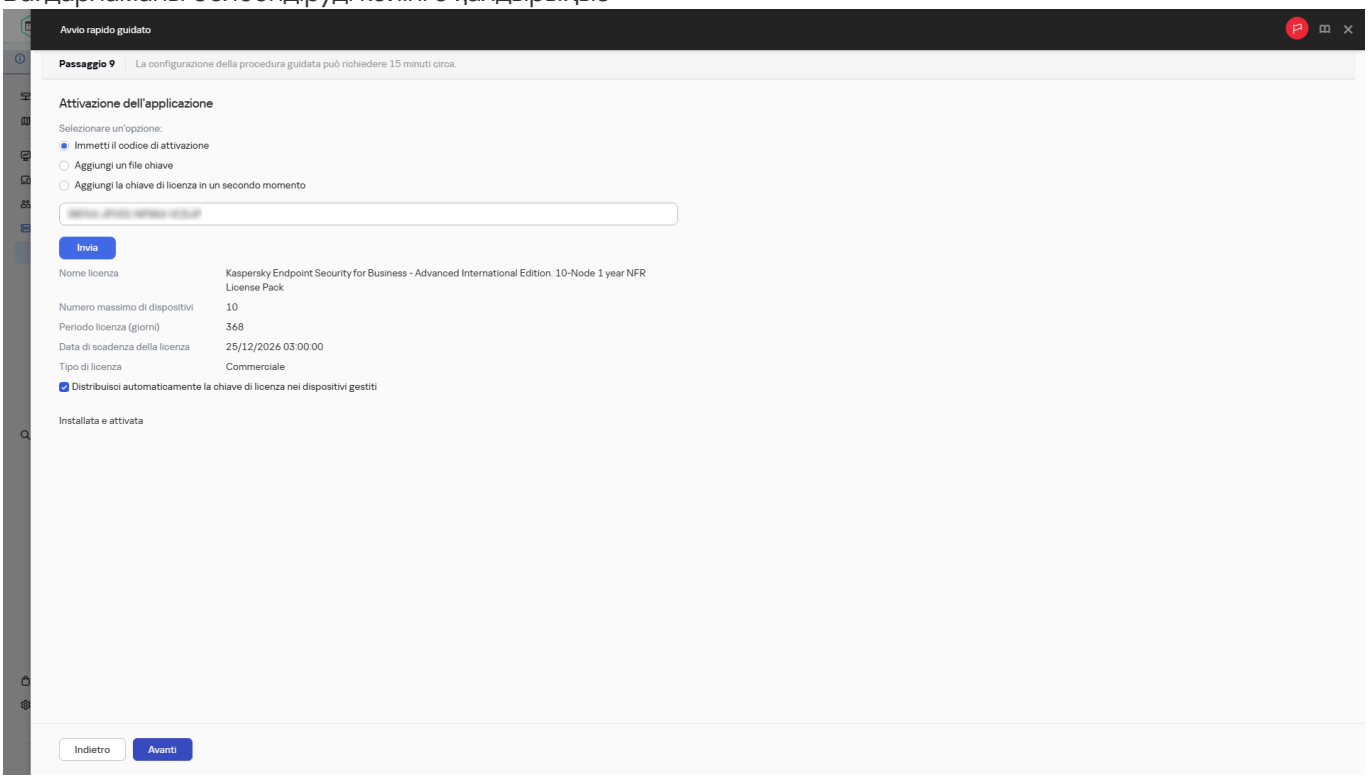
  Бағдарламаны кілт файлы арқылы белсендіру үшін Kaspersky белсендіру серверлеріне қосылудың қажет емес.

  Бағдарламаны белсендірудің осы нұсқасын таңдаған болсаңыз, **Лицензиялық кілтті басқарылатын құрылғыларға автоматты түрде тарату** нұсқасын қосуға болады.

  Осы нұсқа таңдалса, лицензиялық кілт басқарылатын құрылғыларға таратылатын болады.

  Бұл нұсқа таңдалмаса, лицензиялық кілтті кейінірек басқарылатын құрылғыларға негізгі мәзірдің **Операциялар** → **Лицензиялау** → **Лицензиялар** бөлімінде таратуға болады.

- Бағдарламаны белсендіруді кейінге қалдырыңыз



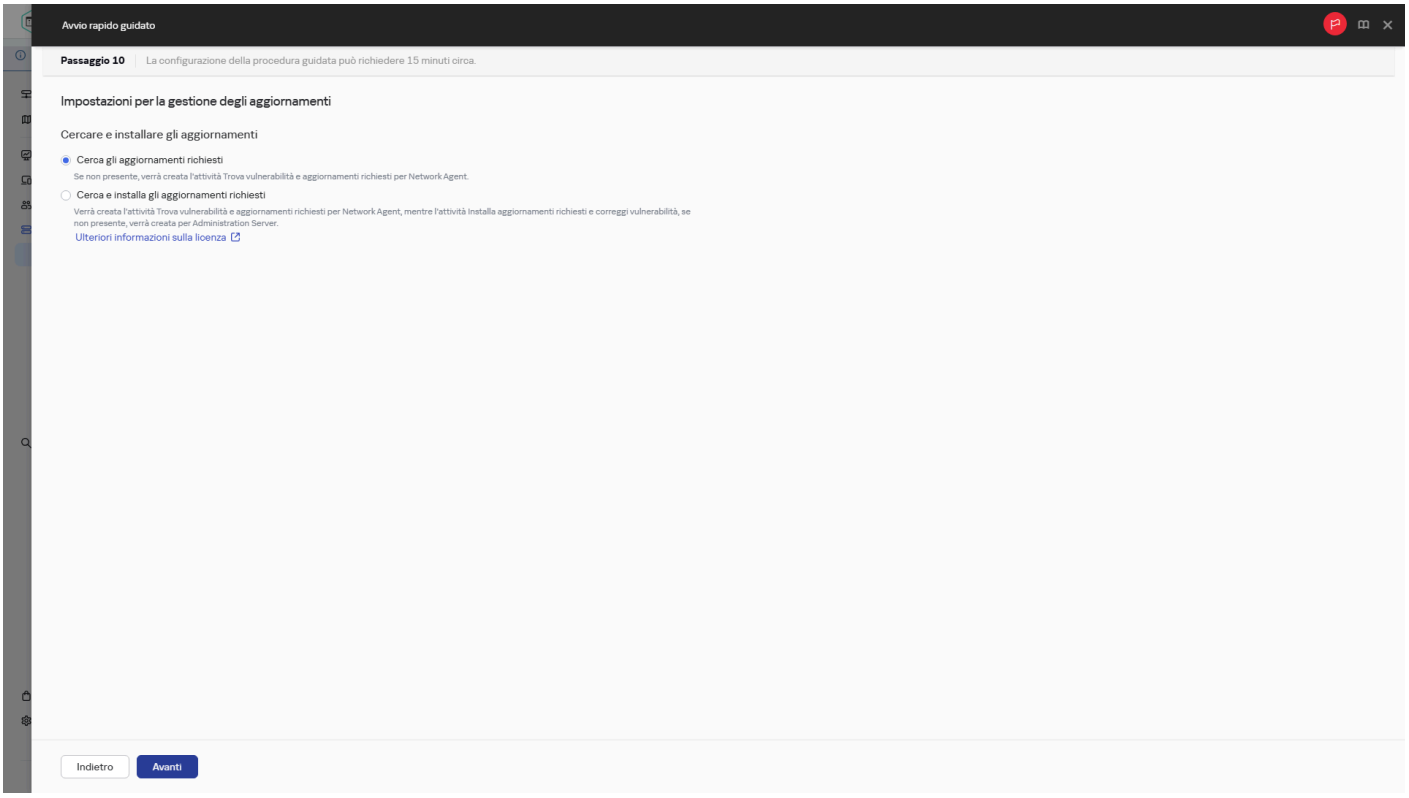
Бағдарламаны белсендіру тәсілін таңдау

Бағдарламаны белсендіруді кейінге қалдырсаңыз, **Операциялар** → **Лицензиялау** тармағын таңдап, кілтті кейін кез келген уақытта қоса аласыз.

AMI дайын кескінінен немесе SKU қолдану үшін ай сайынғы шоттарды қолдану арқылы орналастырылған Kaspersky Security Center бағдарламасымен жұмыс істеу кезінде, сіз кілт файлын көрсете алмайсыз немесе белсендіру кодын енгізе алмайсыз.

9-қадам. Үшінші тарап бағдарламаларының жаңартуларын басқару параметрлерін көрсету

Осалдықтар мен патчтарды басқару лицензиясы болмаса, ал *Осалдықтарды және қажетті жаңартуларды іздеу* бұрыннан бар болса, Бастапқы орнату шеберінің **Жаңартуларды басқару параметрлері** қадамы көрсетілмейді.



Үшінші тарап жаңартуларын басқару параметрлері

Үшінші тарап бағдарламаларын жаңарту үшін келесі нұсқалардың бірін таңдаңыз:

- **Қажетті жаңартуларды іздеу**

  Осалдықтарды және қажетті жаңартуларды іздеу тапсырмасы бұрын жасалмаған болса, автоматты түрде жасалады.

  Әдепкі бойынша, осы нұсқа таңдалады.

- **Қажетті жаңартуларды іздеу және орнату**

  Осалдықтарды және қажетті жаңартуларды іздеу және *Қажетті жаңартуларды орнату және осалдықтарды түзету* тапсырмалары бұған дейін жасалмаған болса, автоматты түрде жасалады.

  Бұл параметр Осалдықтар мен патчтарды басқару лицензиясы болған жағдайда қолжетімді.

Windows жаңарту орталығының жаңартулары үшін **Домен саясатында белгіленген жаңарту көздерін пайдалану** тармағын таңдаңыз.

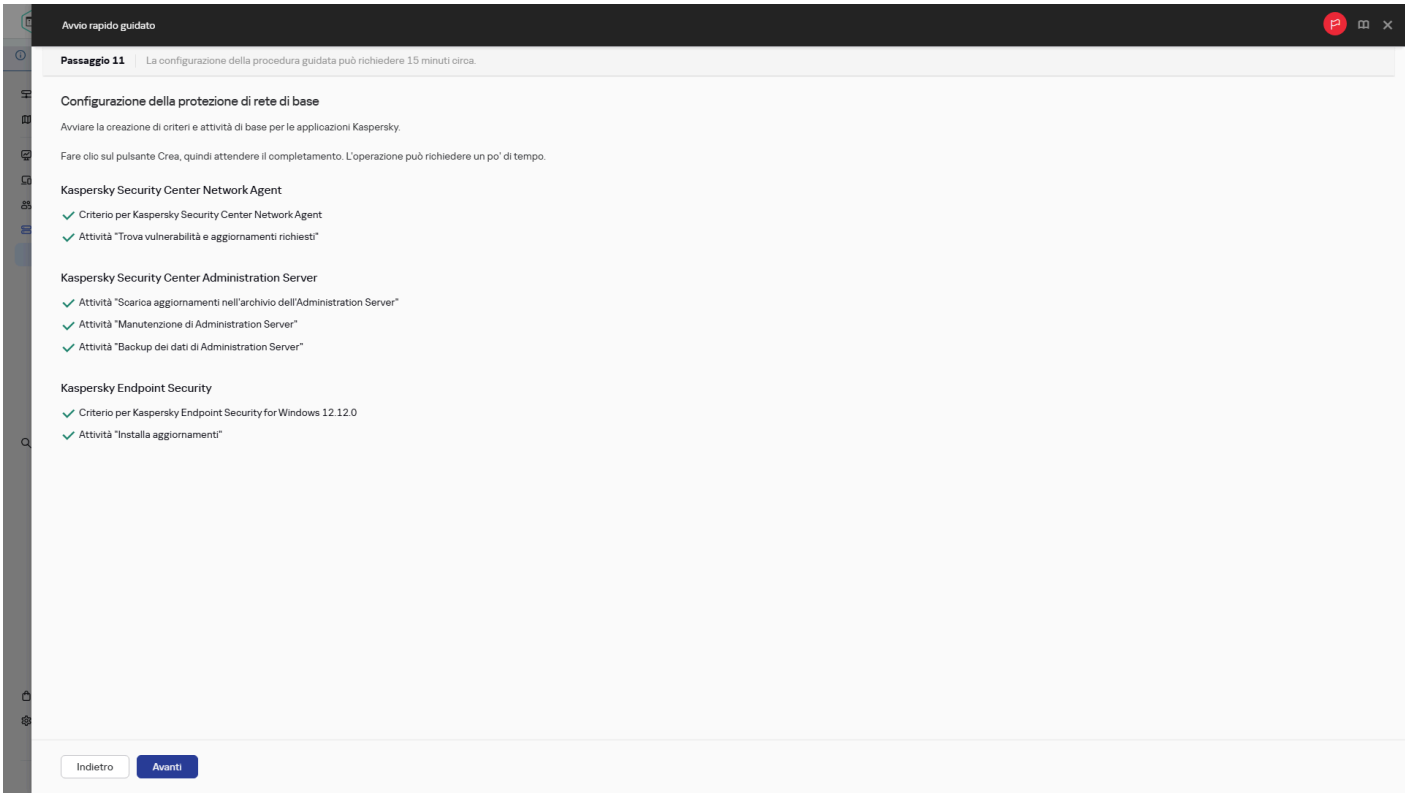
Windows Update жаңартулары клиент құрылғыларына домен саясаты параметрлеріне сай жүктеледі. Желілік агент саясаты бұрын жасалмаған болса, автоматты түрде жасалады.

Жылдам іске қосу шеберінен *Осалдықтарды және қажетті жаңартуларды іздеу* және *Қажетті жаңартуларды орнату және осалдықтарды түзету* тапсырмаларын бөлек жасауға болады.

10-қадам. Желі қорғанысының базалық конфигурациясын жасау

Сіз жасалған саясаттар мен тапсырмалардың тізімін тексере аласыз.

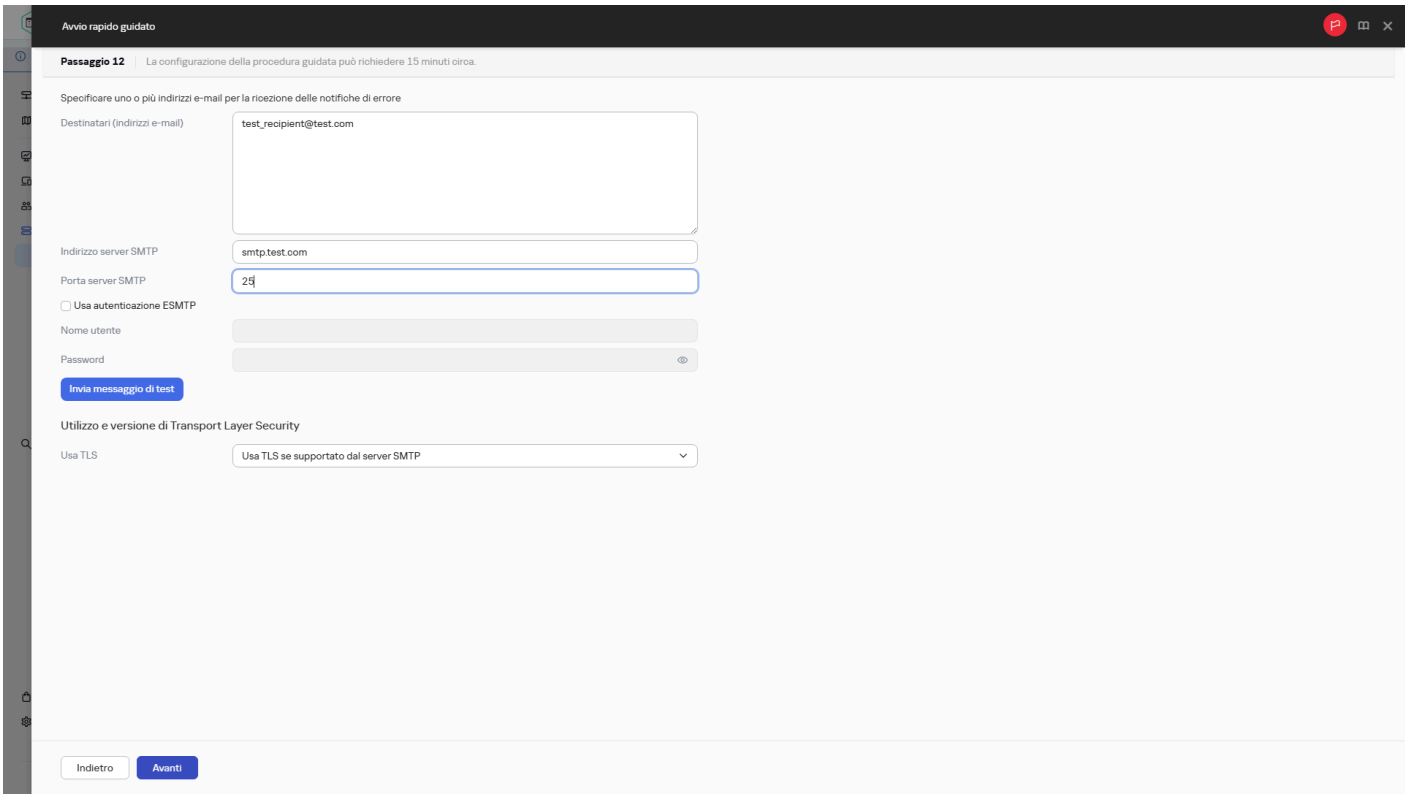
Шебердің келесі қадамына өту үшін саясаттар мен тапсырмалардың жасалуының аяқталуын күтіңіз.



Желі қорғанысының базалық конфигурациясын жасау

11-қадам. Электрондық пошта арқылы хабарландыруларды жіберу әдісін конфигурациялау

Клиент құрылғыларында Kaspersky бағдарламалары жұмыс істеген кезде тіркелетін оқиғалар туралы хабарландыру тарату параметрлерін конфигурациялаңыз. Бұл параметрлер бағдарламалардың саясаттарында әдепкі бойынша мәндер ретінде пайдаланылады.



Электрондық пошта арқылы хабарландыруларды жіберу әдісін конфигурациялау

Kaspersky бағдарламаларының туындайтын оқиғалары туралы хабарландырулар таратылымын конфигурациялау үшін келесі параметрлер қолжетімді:

- **Алушылар (электрондық пошта мекенжайлары)**

  Бағдарлама хабарландыру жіберетін пайдаланушылардың электрондық пошта мекенжайлары. Бір не бірнеше мекенжайды енгізуге болады; бірнеше мекенжай енгізілсе, оларды нүктелі үтірмен бөліңіз.

- **SMTP серверінің мекенжайы**

  Ұйымыңыздың пошта серверлерінің мекенжайы немесе мекенжайлары.

  Бірнеше мекенжайды көрсетсеңіз, оларды үтірлі нүктемен бөліңіз. Келесі параметр мәндерін пайдалануыңызға болады:

  - IPv4 мекенжайы немесе IPv6 мекенжайы;
  - SMTP сервері DNS атауы.

- **SMTP серверінің порты**

  SMTP серверінің коммуникациялық портының нөмірі. Бірнеше SMTP серверін қолдансаңыз, олармен қосылым көрсетілген коммуникациялық порт арқылы орнатылады. Әдепкі бойынша 25-порт орнатылған.

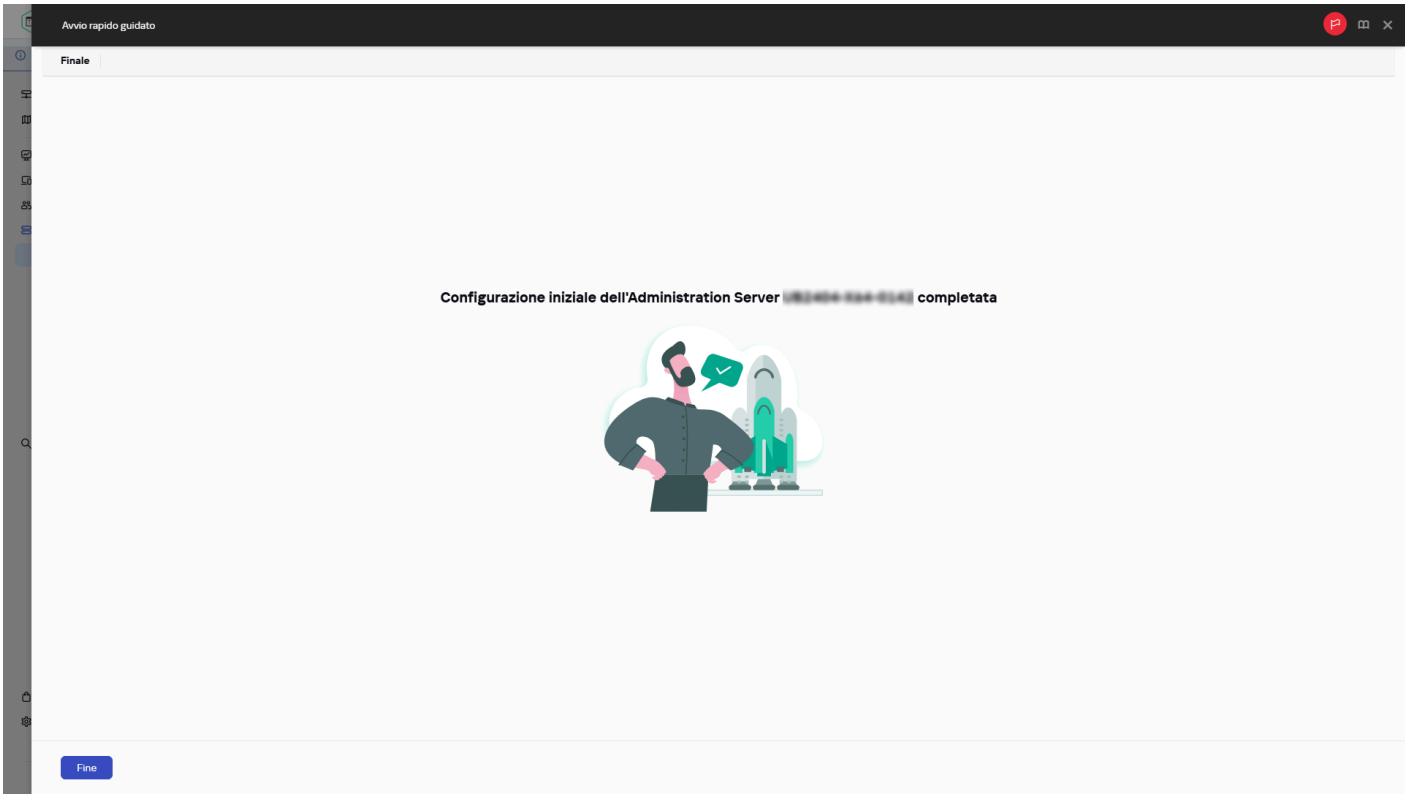
- **ESMTP аутентификациясын пайдалану**

  ESMTP аутентификациясын қолдауды қосу. Жалаушаны қойғаннан кейін, ESMTP аутентификациясы параметрлерін **Пайдаланушы аты** және **Құпиясөз** өрістерінде көрсетуге болады. Әдепкі бойынша, жалауша алынып тасталған.

Электрондық пошта хабарлары туралы хабарландыру параметрлерін **Тексеру хабарын жіберу** түймесі арқылы тексеруге болады.

12-қадам. Бағдарламаны жылдам іске қосу шеберінің жұмысын аяқтау

Шебердің жұмысын аяқтау үшін **Аяқтау** түймесін басыңыз.



Бастапқы орнату шеберінің соңғы қадамы

Бастапқы конфигурация шебері жұмысын аяқтағаннан кейін желіңіздегі құрылғыларда қауіпсіздік бағдарламаларын немесе Желілік агентті автоматты түрде орнату үшін қорғанысты орналастыру шеберін іске қосуға болады.

Қорғанысты орналастыру шебері

Kaspersky бағдарламаларын орнату үшін қорғанысты орналастыру шеберін пайдалануға болады. Қорғанысты орналастыру шебері бағдарламаларды арнайы жасалған орнату пакеттері арқылы және тікелей дистрибутивтерден қашықтан орнатуға мүмкіндік береді.

Қорғанысты орналастыру шебері келесі әрекеттерді орындайды:

- Бағдарламаны орнату үшін орнату пакетін жүктейді (егер ол бұрын жасалмаған болса). Орнату пакеті **Бағдарламалық жасақтаманы басқару** → **Орнату пакеттері** бөлімінде орналасқан. Бағдарламаны кейінірек орнату үшін осы орнату пакетін пайдалануға болады.
- Құрылғылар жиынтығы немесе басқару тобы үшін қашықтан орнату тапсырмасын жасайды және іске қосады. Құрылған қашықтан орнату тапсырмасы **Тапсырмалар** бөлімінде сақталады. Бұл тапсырманы кейінірек қолмен іске қосуға болады. Тапсырма түрі – **Бағдарламаны қашықтан орнату**.

SUSE Linux Enterprise Server 15 операциялық жүйесі бар құрылғыларға Желілік агентті орнатқыңыз келсе, алдымен Желілік агентті орнату үшін insserv-compat пакетін орнатыңыз.

1-қадам. Қорғанысты орналастыру шеберін іске қосу

Қорғанысты орналастыру шеберін қолмен іске қосуға болады.

Қорғанысты орналастыру шеберін қолмен іске қосу үшін,

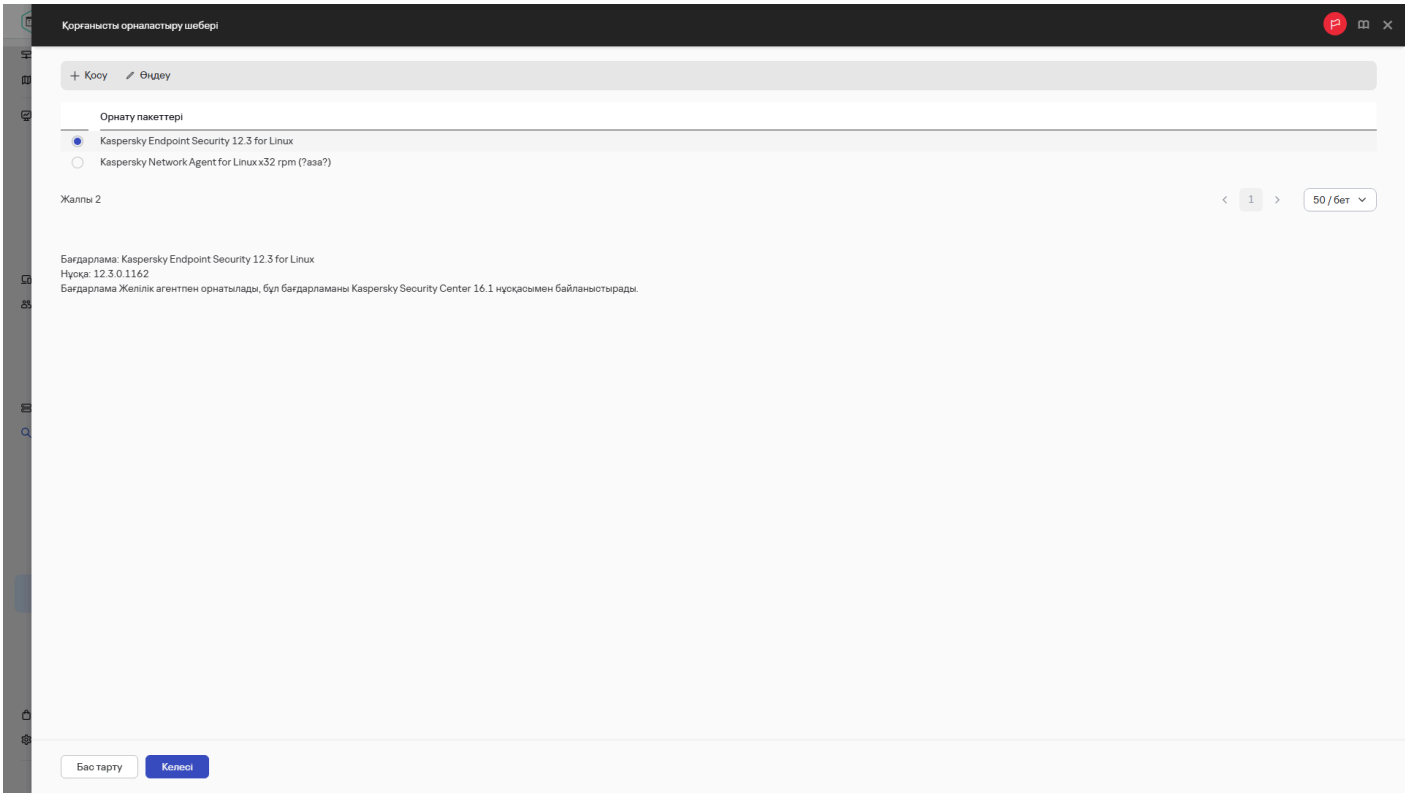
Бағдарламаның негізгі терезесінде **Табу және орналастыру** → **Орналастыру және тағайындау** → **Қорғанысты орналастыру шебері** бөліміне өтіңіз.

Қорғанысты орналастыру шебері іске қосылады. Шебердің жұмысын жалғастыру үшін **Келесі** түймесін басыңыз.

2-қадам. Орнату пакетін таңдау

Орнатқыңыз келетін бағдарламаның орнату пакетін таңдаңыз.

Қажетті бағдарламаның орнату пакеті тізімде болмаса, **Қосу** түймесін басып, тізімнен бағдарламаны таңдаңыз.



Орнату пакетін таңдау

3-қадам. Кілт файлын немесе белсендіру кодын тарату тәсілін таңдау

Кілт файлын немесе белсендіру кодын тарату тәсілін таңдаңыз:

- **Лицензиялық кілтті орнату пакетіне қоспау**

  Егер бұл нұсқа таңдалса, кілт автоматты түрде сәйкес келетін құрылғыларға таратылады:

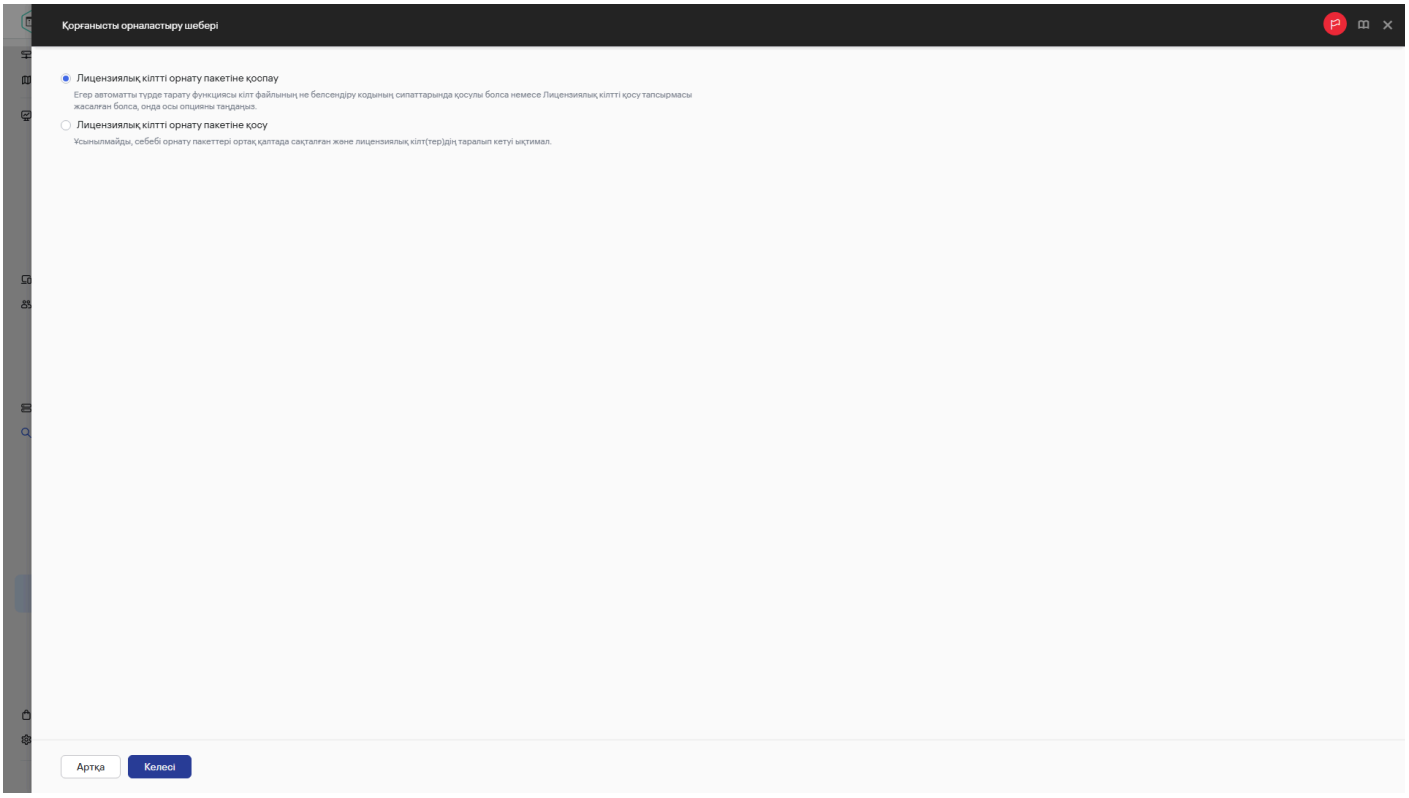
  - егер кілттің сипаттарында автоматты түрде тарату конфигурацияланған болса;
  - **Кілтті қосу** тапсырмасы жасалған болса.

- **Лицензиялық кілтті орнату пакетіне қосу**

  Кілт орнату пакетімен бірге құрылғыларға таралады.

  > Кілтті осылайша тарату ұсынылмайды, өйткені әдепкі бойынша орнату пакетінің қоймасы оқуға ортақ қатынасуға конфигурацияланған.

Егер орнату пакетінде кілт файлы немесе белсендіру коды болса, бұл терезе көрсетіледі, бірақ ол тек лицензиялық кілт туралы ақпаратты қамтиды.

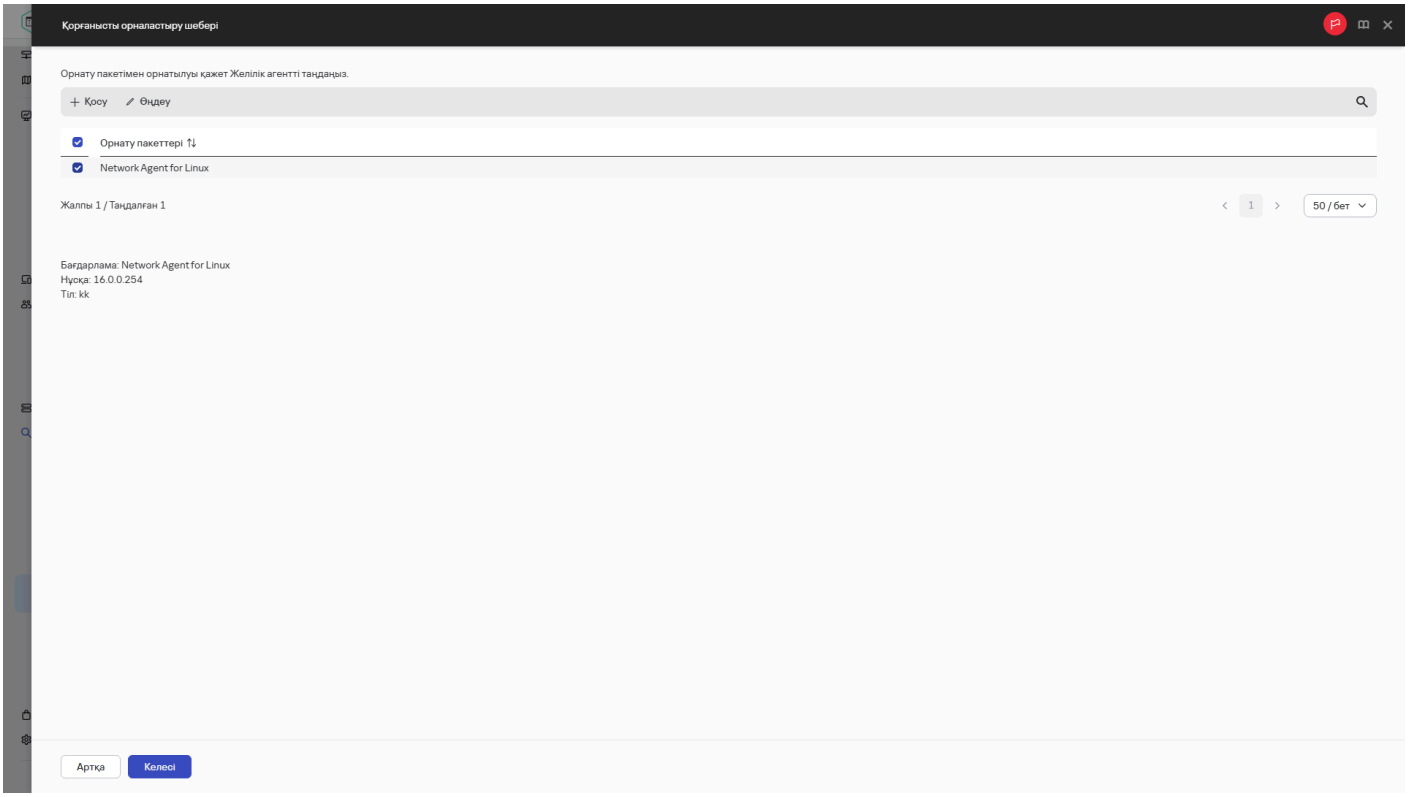


Кілт файлын немесе белсендіру кодын тарату әдісін таңдау

4-қадам. Желілік агенттің нұсқасын таңдау

Желілік агенттен басқа бағдарламаның орнату пакетін таңдаған болсаңыз, бағдарламаны Басқару серверіне қосу үшін Желілік агентті де орнату қажет.

Желілік агенттің соңғы нұсқасын таңдаңыз.



Желілік агент нұсқасын таңдау

5-қадам. Құрылғыларды таңдау

Бағдарламаны орнатуды қажет ететін құрылғылардың тізімін көрсетіңіз:

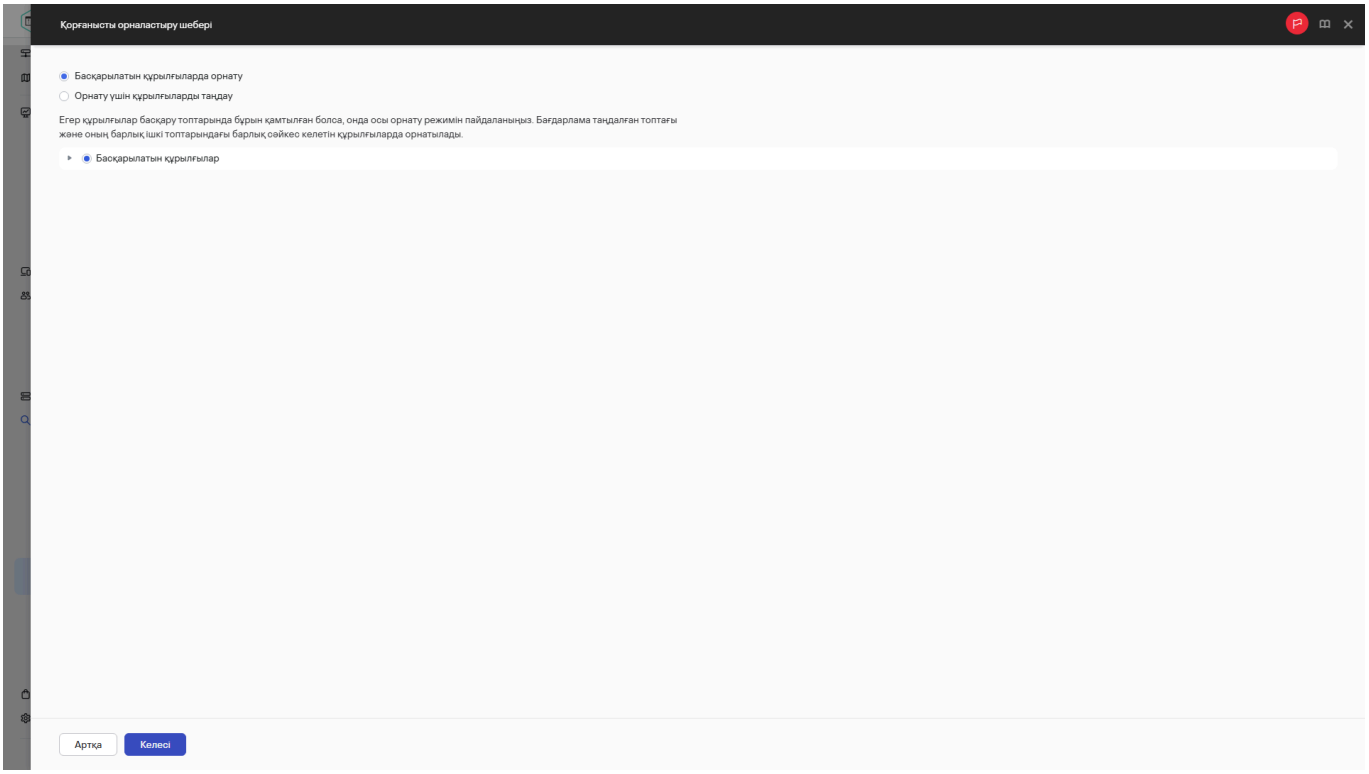
- **Басқарылатын құрылғыларда орнату**

  Егер бұл нұсқа таңдалса, құрылғылар тобы үшін бағдарламаны қашықтан орнату тапсырмасы жасалады.

- **Орнату үшін құрылғыларды таңдау**

  Тапсырма құрылғы таңдауларына кіретін құрылғыларға тағайындалады. Қолданыстағы таңдаулардың бірін көрсетуге болады.

Мысалы, операциялық жүйенің белгілі бір нұсқасы бар құрылғыларда тапсырманы іске қосу үшін осы параметрді пайдалануға болады.



Қолданба орнатылатын құрылғылар тізімін көрсету

6-қадам. Қашықтан орнату тапсырмасының параметрлерін орнату

"Қашықтан орнату" тапсырмасы параметрлері терезесінде бағдарламаны қашықтан орнату параметрлерін конфигурациялаңыз.

Орнату пакетін мәжбүрлеп жүктеп алу параметрлер блогында қолданбаны орнату үшін қажетті файлдарды клиент құрылғыларына жеткізу тәсілін таңдаңыз:

- **Желілік агенттің көмегімен**

  Егер бұл параметр қосылса, орнату пакеттерін клиент құрылғыларына жеткізуді клиент құрылғыларына орнатылған Желілік агент жүзеге асырады.

  Егер бұл параметр өшірулі болса, орнату пакеттері клиент құрылғысының операциялық жүйесі құралдарының көмегімен жеткізіледі.

  Егер тапсырма Желілік агенттер орнатылған құрылғыларға тағайындалса, бұл параметрді қосу ұсынылады.

  Әдепкі бойынша, параметр қосулы.

- **Тарату нүктелері арқылы операциялық жүйе ресурстарының көмегімен**

  Егер бұл параметр қосылса, орнату пакеттері тарату нүктелері арқылы операциялық жүйенің көмегімен клиент құрылғыларына беріледі. Егер желіде кем дегенде бір тарату нүктесі болса, бұл нұсқаны таңдауға болады.

  Желілік агент көмегімен параметрі қосылса, онда файлдар, операциялық жүйенің құралдарымен Желілік агент құралдарын пайдалану мүмкін болмаған жағдайда ғана жеткізіледі.

Әдепкі бойынша, параметр виртуалды Басқару серверінде жасалған қашықтан орнату тапсырмалары үшін қосылған.

Windows жүйесіне арналған бағдарламаны (Windows жүйесіне арналған Желілік агентті қоса) Желілік агент орнатылмаған құрылғыға орнатудың жалғыз жолы – бұл Windows операциялық жүйесі бар тарату нүктесін пайдалану болып табылады. Сондықтан Windows жүйесіне арналған бағдарламаны орнату кезінде:

- Осы параметрді таңдаңыз.
- Тарату нүктесі мақсатты клиенттік құрылғыларға тағайындалғанын көз жеткізіңіз.
- Тарату нүктесінде Windows операциялық жүйесі орнатылғанына көз жеткізіңіз.

- **Басқару сервері арқылы операциялық жүйе ресурстарының көмегімен**

  Бұл параметр қосылса, файлдар Басқару сервері көмегімен клиент құрылғыларының операциялық жүйесі арқылы клиент құрылғыларына жеткізіледі. Бұл параметрді клиент құрылғысында Желілік агент орнатылмаған, бірақ клиент құрылғысы Басқару серверімен бір желіде орналасқан кезде қосуға болады.

  Әдепкі бойынша, параметр қосулы.

Қосымша параметрді конфигурациялаңыз:

- **Бұрын орнатылып қойған жағдайда, бағдарламаны қайта орнатпау**

  Егер бұл параметр қосылса, таңдалған бағдарлама клиент құрылғысында орнатылған болса, қайта орнатылмайды.

  Егер бұл параметр өшірулі болса, бағдарлама кез келген жағдайда орнатылады.

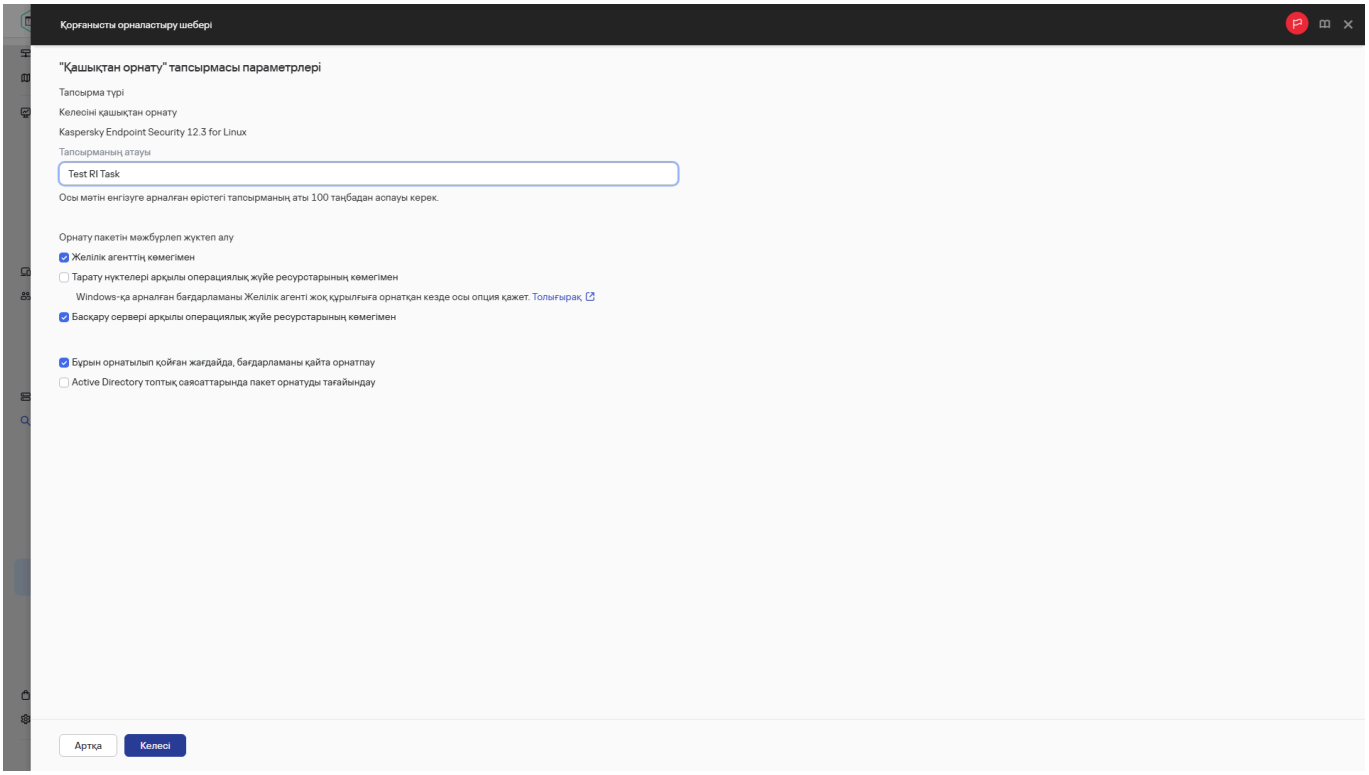
  Әдепкі бойынша, параметр қосулы.

- **Active Directory топтық саясаттарында пакет орнатуды тағайындау**

  Егер бұл параметр қосылса, орнату пакеті Active Directory топтық саясаттары арқылы орнатылады.

  Егер Желілік агенттің орнату пакеті таңдалса, параметр қолжетімді.

  Әдепкі бойынша, параметр өшірулі.



Қашықтан орнату тапсырмасының параметрлерін орнату

7-қадам. Өшіріп қайта қосуды басқару

Бағдарламаны орнату кезінде операциялық жүйені қайта іске қосу қажет болса, орындалатын әрекетті көрсетіңіз:

- **Құрылғыны қайта іске қоспау**

  Операция аяқталғаннан кейін, клиент құрылғылары автоматты түрде қайта жүктелмейді. Операцияны аяқтау үшін құрылғыны қайта қосу қажет (мысалы, қолмен немесе құрылғыны басқару тапсырмасы арқылы). Қайта жүктеу қажеттілігі туралы ақпарат тапсырманы орындау нәтижелерінде және құрылғы күйінде сақталады. Бұл нұсқа, үздіксіз жұмыс өте маңызды болып саналатын серверлердегі және басқа құрылғылардағы тапсырмалар үшін жарамды.

- **Құрылғыны қайта іске қосу**

  Бұл жағдайда, операцияны аяқтау үшін қайта жүктеу қажет болса, қайта жүктеу әрқашан автоматты түрде орындалады. Бұл нұсқа, мезгіл-мезгіл үзілістерге (өшіру, қайта жүктеу) рұқсат етілген құрылғылардағы тапсырмалар үшін жарамды.

- **Пайдаланушыдан әрекетті орындауды сұрау**

  Клиент құрылғысының экранында құрылғыны қолмен қайта жүктеу керек деген хабар пайда болады. Бұл нұсқа үшін қосымша параметрлерді конфигурациялауға болады: пайдаланушыға арналған хабар мәтіні, хабардың жиілігі, сондай-ақ қайта жүктеу мәжбүрлі түрде орындалатын уақыт (пайдаланушының растауынсыз). Бұл нұсқа жұмыс станциялары үшін оңтайлы болып табылады, сондықтан пайдаланушылар қайта жүктеудің ең қолайлы уақытын таңдай алады.

  Әдепкі бойынша, осы нұсқа таңдалған.

  - **Сұрауды қайталау жиілігі (мин)**

    Егер бұл нұсқа таңдалса, белгілі бір жиіліктегі бағдарлама пайдаланушыға операциялық жүйені қайта жүктеуді ұсынады.

    Әдепкі бойынша, параметр қосулы. Әдепкі бойынша аралық 5 минутты құрайды. Рұқсат етілген мәндер: 1-ден 1440 минутқа дейін.

    Егер параметр өшірулі болса, қайта жүктеу ұсынысы тек бір рет көрсетіледі.

  - **Келесі уақыттан кейін қайта іске қосу (мин)**

    Пайдаланушыға операциялық жүйені қайта жүктеуді ұсынғаннан кейін, бағдарлама көрсетілген уақыттан кейін мәжбүрлеп қайта жүктеуді орындайды.

    Әдепкі бойынша, параметр қосулы. Әдепкі бойынша уақыт аралығы 30 минутты құрайды. Рұқсат етілген мәндер: 1-ден 1440 минутқа дейін.

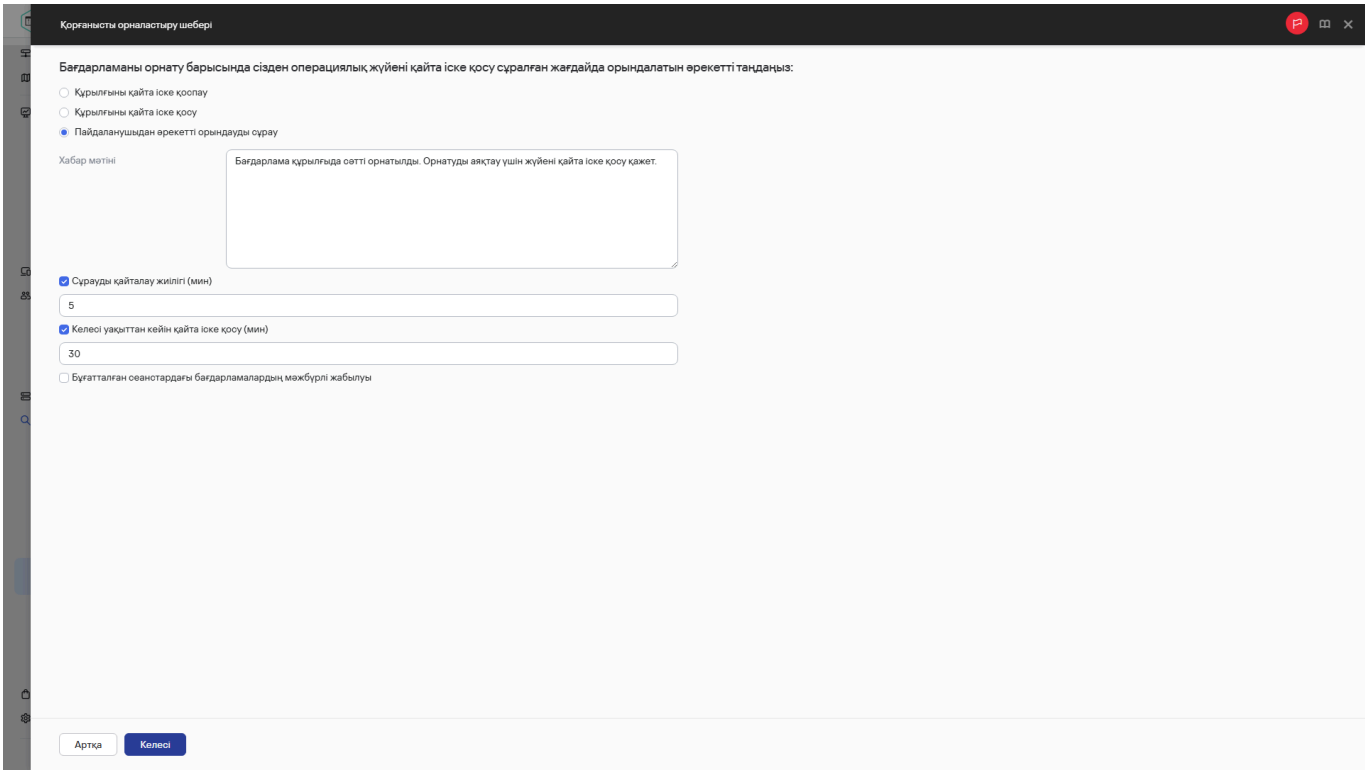
- **Бұғатталған сеанстардағы бағдарламалардың мәжбүрлі жабылуы**

  Іске қосылған қолданбалар клиент құрылғысын қайта жүктеуге мүмкіндік бермеуі мүмкін. Мысалы, егер мәтіндік редакторда құжатпен жұмыс жасалса және өзгертулер сақталмаса, бағдарлама құрылғыны қайта жүктеуге мүмкіндік бермейді.

  Егер бұл параметр қосулы болса, құрылғыны қайта іске қоспас бұрын бұғатталған құрылғылардағы мұндай бағдарламалар мәжбүрлі түрде жабылады. Нәтижесінде, пайдаланушылар сақталмаған жұмысын жоғалтуы мүмкін.

Егер бұл параметр өшірулі болса, бұғатталған құрылғы қайта жүктелмейді. Бұл құрылғыдағы тапсырманың күйі құрылғыны қайта іске қосу қажеттілігін көрсетеді. Пайдаланушылар бұғатталған құрылғыларда жұмыс істейтін барлық бағдарламаларды қолмен жауып, сол құрылғыларды қайта іске қосуы керек.

Әдепкі бойынша, параметр өшірулі.



Операциялық жүйені қайта іске қосу опциясын таңдау

8-қадам. Орнатудың алдында үйлесімді емес бағдарламаларды жою

Бұл қадам, сіз орналастыратын бағдарлама басқа бағдарламалармен үйлесімді болмаса ғана болады.

Kaspersky Security Center Linux бағдарламасы сіз орнатып жатқан бағдарламамен үйлесімді емес бағдарламаларды автоматты түрде жойғанын қаласаңыз, осы параметрді таңдаңыз.

Үйлесімді емес бағдарламалар тізімі көрсетіледі.

Егер бұл параметр таңдалмаса, бағдарлама тек үйлесімді емес бағдарламалары жоқ құрылғыларда орнатылады.

9-қадам. Құрылғыларды басқарылатын құрылғылар қалтасына жылжыту

Желілік агент орнатылғаннан кейін, құрылғыларды басқару тобына жылжыту керек пе екенін көрсетіңіз.

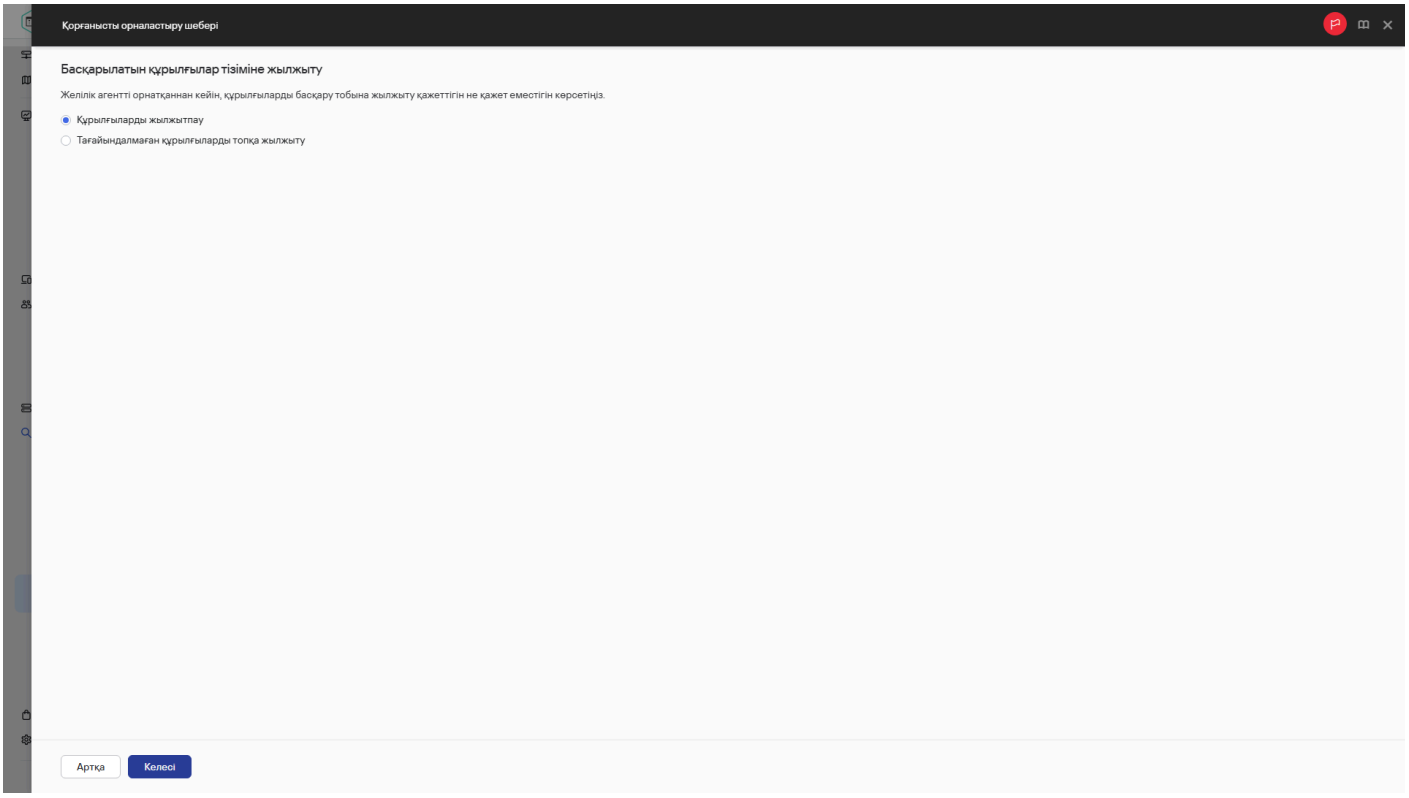
- **Құрылғыларды жылжытпау**

  Құрылғылар тиесілі болып саналатын топтарда қалады. Топтардың ешқайсысына жатпайтын құрылғылар таратылмаған болып қалады.

- **Тағайындалмаған құрылғыларды топқа жылжыту**

  Құрылғылар сіз таңдаған басқару тобына жылжытылады.

Әдепкі бойынша, **Құрылғыларды жылжытпау** нұсқасы таңдалған. Қауіпсіздік тұрғысынан, сіз құрылғыларды қолмен жылжытуды таңдай аласыз.



Құрылғыларды басқару тобына жылжыту опциясын таңдау

10-қадам. Құрылғыларға қатынасу үшін есептік жазбаларды таңдау

Қажет болса, қашықтан орнату тапсырмасын орындау үшін пайдаланылатын есептік жазбаларды қосыңыз:

- **Есептік жазба қажет емес (Желілік агент орнатылды)**

  Егер бұл нұсқа таңдалса, бағдарлама инсталляторын іске қосуға негіз болып саналатын есептік жазбаны көрсетудің қажеті жоқ. Тапсырма, Басқару сервері қызметі жұмыс істейтін есептік жазба астында іске қосылады.

  Желілік агент клиент құрылғыларында орнатылмаған болса, бұл нұсқа қолжетімді емес.

- **Есептік жазба қажет (Желілік агент пайдаланылмайды)**

  Егер сіз қашықтан орнату тапсырмасын тағайындайтын құрылғыларда Желілік агент орнатылмаған болса, осы нұсқаны таңдаңыз. Бұл жағдайда бағдарламаны орнату үшін пайдаланушы есептік жазбасын немесе SSH сертификатын көрсетуге болады.

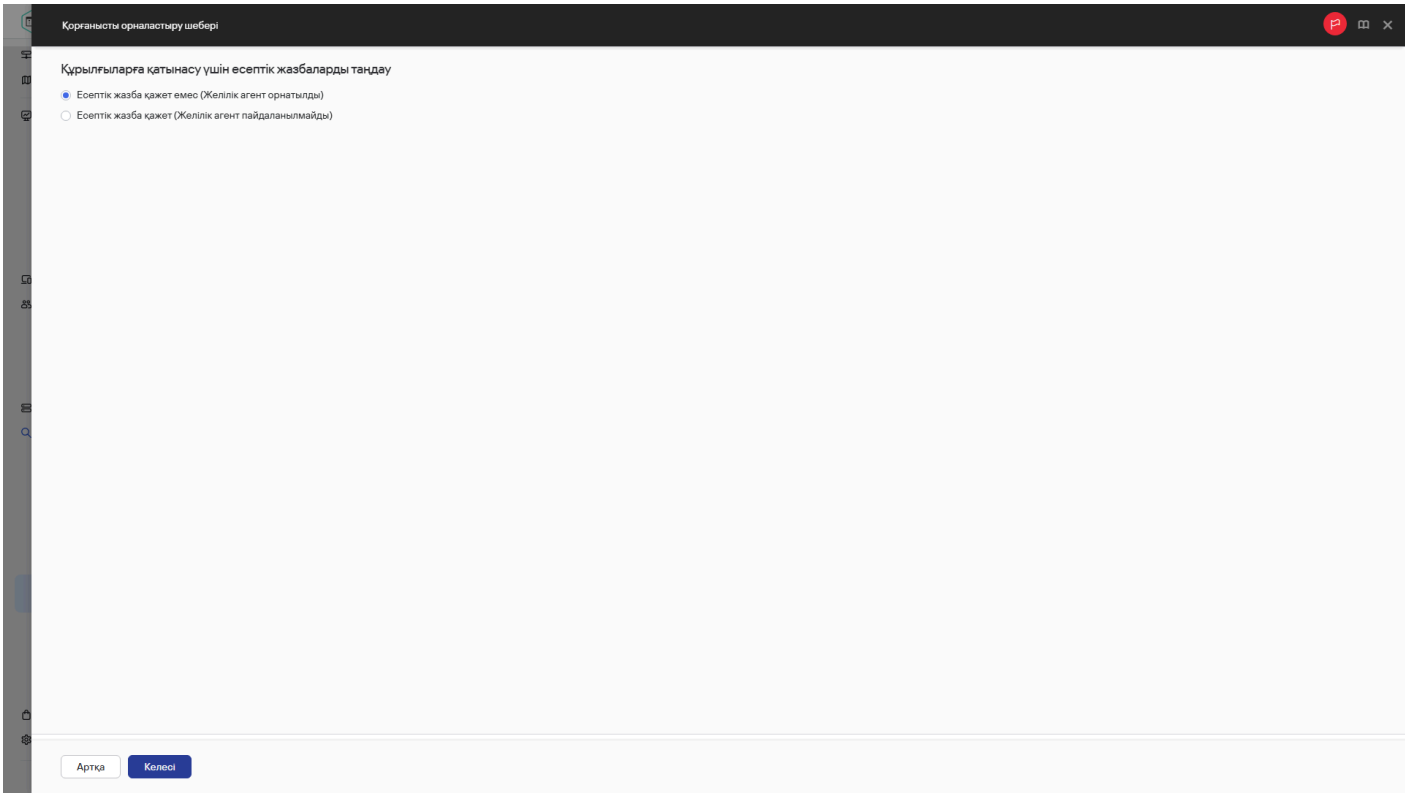
  - **Жергілікті немесе домен есептік жазбасы**. Егер бұл нұсқа таңдалса, бағдарлама инсталляторын іске қосуға негіз болатын есептік жазбаны көрсетіңіз. **Қосу** түймесін басыңыз, **Жергілікті немесе домен есептік жазбасы** опциясын таңдаңыз және пайдаланушының есептік жазбасының деректерін көрсетіңіз.

    Тапсырма тағайындалған барлық құрылғыларда олардың ешқайсысы қажетті құқықтарға ие болмаса, бірнеше есептік жазбаны көрсетуге болады. Бұл жағдайда, тапсырманы іске қосу үшін барлық қосылған есептік жазбалар бірізді түрде, жоғарыдан төменге қарай қолданылады.

  - **SSH сертификаты**. Бағдарламаны Linux басқаратын клиенттік құрылғыға орнатқыңыз келсе, пайдаланушы есептік жазбасының орнына SSH сертификатын көрсетуге болады. **Қосу** түймесін басыңыз, **SSH сертификаты** опциясын таңдаңыз және сертификаттың жеке және ашық кілттерін көрсетіңіз.

    Жеке кілт жасау үшін ssh-keygen утилитасын пайдалануға болады. Kaspersky Security Center Linux жеке кілттердің PEM форматына қолдау көрсететінін ескеріңіз, бірақ ssh-keygen утилитасы SSH кілттерін әдепкісінше OPENSSH форматында жасайды. OPENSSH форматына Kaspersky Security Center Linux қолдау көрсетпейді. PEM қолдау көрсетілетін пішімінде жабық кілт жасау үшін -m PEM параметрін ssh-keygen пәрменіне қосыңыз. Мысалы:

    ```
    ssh-keygen -m PEM -t rsa -b 4096 -C "< пайдаланушының электрондық поштасы >"
    ```



Құрылғыларға қатынасу үшін есептік жазбаларды таңдау

11-қадам. Орнатуды бастау

Бұл қадамның соңғы қадамы. Осы қадамда **Қашықтан орнату тапсырмасы** сәтті түрде жасалып, конфигурацияланды.

Әдепкі бойынша **Шебердің жұмысы аяқталғаннан кейін тапсырманы іске қосу** нұсқасы таңдалмаған. Осы параметрді таңдасаңыз, шебердің жұмысы аяқталғаннан кейін **Қашықтан орнату тапсырмасы** бірден басталады. Осы параметрді таңдамасаңыз, **Қашықтан орнату тапсырмасы** басталмайды. Бұл тапсырманы кейінірек қолмен іске қосуға болады.

Қорғанысты орналастыру шеберінің соңғы қадамын аяқтау үшін **OK** түймесін басыңыз.

Kaspersky Security Center Linux алдыңғы нұсқасын жаңарту

Басқару серверінің алдыңғы нұсқасы орнатылған құрылғыға басқару серверінің 16.3 нұсқасын орнатуға болады (13-нұсқадан бастап). 16.3 нұсқасына дейін жаңарту кезінде Басқару серверінің алдыңғы нұсқасының барлық деректері мен параметрлері сақталады.

Алдын ала талаптар

- Жаңартуды бастамас бұрын, Басқару сервері деректерінің сақтық көшірмесін жасау.
- Басқару серверін 16 немесе одан бұрынғы нұсқасынан 16.1 немесе одан кейінгі нұсқасына жаңартқан кезде екі факторлы аутентификация қосылады. Қосымша ақпарат алу үшін Есептік жазба үшін екі қадамдық тексеру туралы бөлімін қараңыз.

  Пайдаланушылардың конфигурацияланған екі факторлы аутентификация құпия кілттерін пайдаланып, Web Console веб-консоліне бар есептік жазбалармен кіре алатынына және OpenAPI автоматтандыру сценарийлерінің жаңартудан кейін жұмысын жалғастыратынына көз жеткізу үшін келесі қадамдарды орындауыңыз керек:

  - Барлық пайдаланушылар үшін екі факторлы аутентификацияны қосу
  - Әкімшілер өз есептік жазбалары үшін екі факторлы аутентификацияны конфигурациялауы керек
  - Талап етілетін есептік жазбаларды екі факторлы аутентификациядан алып тастау

    Қажет болса, OpenAPI арқылы сценарийлерді іске қосу үшін пайдаланылатын тұтастық есептік жазбаларын ерекшеліктер тізіміне қосыңыз.
- Басқару серверінің 16.3 нұсқасы қолдайтын операциялық жүйенің және ДҚБЖ нұсқаларын пайдаланып жатқаныңызға көз жеткізіңіз. Қажет болса, Басқару серверін операциялық жүйенің және ДҚБЖ кейінгі нұсқалары бар басқа құрылғыға тасымалдауға болады.
- Басқару серверін 15.4 немесе одан бұрынғы нұсқасынан 16 немесе одан кейінгі нұсқасына жаңартқан кезде, ДҚБЖ серверінде IAM үшін дерекқор жасаңыз. Дерекқор атауы Kaspersky Security Center Linux жүйесімен жұмыс істеу үшін орнатқан дерекқордан өзгеше болуы керек.

  - PostgreSQL үшін келесі пәрменді іске қосыңыз:

    ```
    sudo -i -u postgres psql -U postgres -c "CREATE DATABASE <iam_db_атауы>;"
    ```
  - MariaDB үшін келесі пәрменді іске қосыңыз:

    ```
    sudo mysql -u root -p -e "CREATE DATABASE <iam_db_атауы>;"
    ```

- Басқару серверін 15.4 немесе одан бұрынғы нұсқасынан 16 немесе одан кейінгі нұсқасына жаңартқан кезде, IAM үшін жаңа параметрлері бар жауап файлын дайындаңыз. Қажетті параметрлердің тізімі үшін мақаланы қараңыз: Kaspersky Security Center Linux жүйесін үнсіз режимде орнату. `KLAUTOANSWERS` орта айнымалысын қосыңыз және оның мәнін жауап файлының жолына орнатыңыз.

- OpenID қосу протоколының аутентификациясы үшін kliam процесі пайдаланатын портты қолжетімді етіңіз. Әдепкісінше — 4444. Келесі мақаладағы `trusted` параметр сипаттамасын қараңыз: Kaspersky Security Center Web Console орнату параметрлері.

Кезеңдер

1. **Басқару серверін жаңарту;**

   Басқару серверінің нұсқасын келесі әдістердің бірін пайдаланып жаңартуға болады:

   - Kaspersky Security Center Linux орнату файлын пайдалану.
   - Басқару сервері деректерінің сақтық көшірмесін жасау, Басқару серверінің жаңа нұсқасын орнату және сақтық көшірмеден Басқару сервері деректерін қалпына келтіру арқылы.

   > Жаңарту кезінде ДҚБЖ жүйесін Басқару сервері және басқа бағдарламамен ортақ пайдалануға жол берілмейді.

   Желіңізде бірнеше Басқару серверлері болса, әрбір Серверді қолмен жаңарту қажет. Kaspersky Security Center Linux орталықтандырылған жаңартуды қолдамайды.

2. **postinstall.pl скриптін іске қосу (міндетті емес қадам)**

   Жауап файлында IAM параметрлері болмаса немесе жауап файлы табылмаса, жаңарту кезінде терминалда postinstall.pl скриптісін іске қосуды сұрайтын хабар көрсетіледі.

   Сценарийдің осы қадамында келесі әрекеттерді орындаңыз:

   1. Басқару серверінің операциялық жүйесінде «kladmins» тобының мүшесі болуы тиіс артықшылықсыз «ksciam» пайдаланушы есептік жазбасын жасаңыз:

      ```
      adduser ksciam
      ```

      ```
      gpasswd -a ksciam kladmins
      ```

      ```
      usermod -g kladmins ksciam
      ```

   2. Жаңартылған басқару серверін конфигурациялау үшін /opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl скриптісін root артықшылықтары бар есептік жазбада іске қосыңыз. Сұрау көрсетілген кезде келесі параметрлерді енгізіңіз:

      1. IAM серверінің FQDN атауын енгізіңіз. Kaspersky Security Center Linux жүйесін орнату кезінде көрсетілген Басқару серверінің DNS атауын пайдалануыңыз керек.

      2. IAM қызметін іске қосу үшін есептік жазба атауын енгізіңіз. Есептік жазба көрсетілген қауіпсіздік тобының мүшесі болуы керек. Әдепкісінше ksciam есептік жазбасы пайдаланылады.

3. IAM қызметімен жұмыс істеу үшін орнатылған ДҚБЖ таңдаңыз:

   - MySQL немесе MariaDB орнатқан болсаңыз, 1 енгізіңіз.
   - PostgreSQL немесе Postgres Pro SQL орнатқан болсаңыз, 2 енгізіңіз.

4. IAM қызметі пайдаланатын IAM ДҚБЖ мекенжайын енгізіңіз.
5. IAM ДҚБЖ порт нөмірін енгізіңіз. Бұл порт IAM қызметімен байланысу үшін пайдаланылады. Әдепкі бойынша келесі порттар пайдаланылады:

   - MySQL немесе MariaDB үшін 3306 порты
   - PostgreSQL немесе Postgres Pro үшін 5432 порты

6. IAM қызметі пайдаланатын IAM дерекқор атауын енгізіңіз. IAM қызметі пайдаланатын дерекқордың атауы басқару сервері пайдаланатын дерекқордан өзгеше болуы керек.

3. **Сондай-ақ, Kaspersky Security Center Web Console веб-консолін жаңа нұсқаға дейін жаңарту қажет.**
4. **(Қосымша) Құрылғылардағы Желілік агентті жаңа нұсқаға жаңарту.**
5. **Екі факторлы аутентификацияға рұқсат беру тізімінде тек Басқару серверіне кіру мүмкіндігі болуы керек пайдаланушы есептік жазбалары ғана бар екеніне көз жеткізу.**

   Екі факторлы аутентификацияға рұқсат тізімін қарап шығыңыз және одан басқа аутентификация есептік жазбаларын алып тастаңыз.

Басқару серверін 16.3 нұсқасына жаңартсаңыз, желілік агенттің 15 немесе одан төмен нұсқасы үшін жаңа орнату пакеттерін жасай алмайтыныңызды ескеріңіз. Бұрын жасалған орнату пакеттері қолжетімді болады.

Kaspersky Security Center Linux бағдарламасының алдыңғы нұсқасын жаңарту кезінде Kaspersky қолдау көрсетілетін бағдарламаларының барлық орнатылған плагиндері сақталады. Басқару серверінің және Желілік агенттің плагиндері автоматты түрде жаңартылады.

Kaspersky Security Center Linux жүйесін 16 немесе одан кейінгі нұсқасынан жаңарту

Бұл бөлімде Kaspersky Security Center Linux жүйесін 16 немесе одан кейінгі нұсқасынан соңғы нұсқасына жаңартудың келесі нұсқалары сипатталған:

- Орнату файлын пайдаланып жаңарту
- Сақтық көшірме арқылы жаңарту
- Kaspersky Security Center Linux ақауларға төзімді кластерінде тораптарында жаңарту

Kaspersky Security Center Linux жүйесін 16 немесе одан кейінгі нұсқасынан орнату файлын пайдаланып жаңарту

Басқару серверін 16 немесе одан кейінгі нұсқадан соңғы нұсқаға дейін жаңарту үшін, Kaspersky Security Center Linux орнату файлын пайдаланып, алдыңғы нұсқаның үстіне жаңа нұсқаны орнатуға болады.

Kaspersky Security Center Linux жүйесін 16 немесе одан кейінгі нұсқасынан соңғы нұсқасына орнату файлын пайдаланып жаңарту:

1. Kaspersky сайтынан 16.3 нұсқасына арналған толық пакетімен Kaspersky Security Center Linux орнату файлын жүктеп алыңыз:

   - RPM негізіндегі операциялық жүйесі бар құрылғылар үшін: `ksc64-<version number>.x86_64.rpm`
   - Debian негізіндегі операциялық жүйесі бар құрылғылар үшін: `ksc64_<version number>_amd64.deb`

2. Kaspersky Security Center Linux нұсқасын жаңартуды бастау. Пәрмен жолы терминалында келесі пәрменді орындаңыз:

   - RPM негізіндегі операциялық жүйесі бар құрылғылар үшін:

     ```
     sudo yum install ./ksc64-<version number>.x86_64.rpm
     ```

   - Debian негізіндегі операциялық жүйесі бар құрылғылар үшін:

     ```
     sudo apt-get install ./ksc64_<version number>_amd64.deb
     ```

   Пәрменді сәтті орындағаннан кейін `/opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl` скрипті жасалады. Бұл туралы хабарлама терминалда көрсетіледі.

3. Жаңартылған Басқару серверін конфигурациялау үшін `/opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl` скриптін іске қосыңыз.

   ```
   sudo /opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl
   ```

4. Пәрмен жолы терминалында көрсетілетін Лицензиялық келісімді және Құпиялық саясатын оқыңыз. Лицензиялық келісімнің және Құпиялық саясатының барлық шарттарымен келіссеңіз:

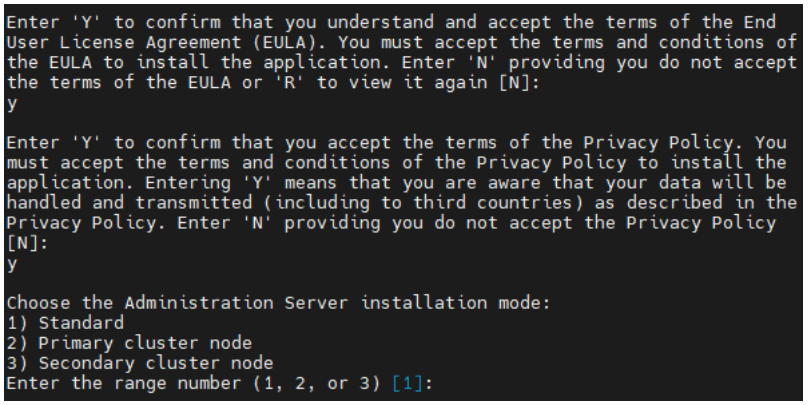
   a. Лицензиялық келісімнің талаптары мен шарттарын толығымен оқығаныңызды, түсінгеніңізді және қабылдағаныңызды растау үшін `Y` енгізіңіз.

   b. Деректерді өңдеуді сипаттайтын Құпиялық саясатын толық оқып, түсінгеніңізді және қабылдағаныңызды растау үшін `Y` тағы бір рет енгізіңіз.

   Бағдарламаны орнату `Y` әрпін екі рет енгізгеннен кейін жалғасады.

5. Басқару серверінің стандартты орнату режимін таңдау үшін `1` енгізіңіз.

Төмендегі суретте соңғы екі қадам көрсетілген.



Лицензиялық келісімнің және Құпиялық саясатының шарттарын қабылдау және пәрмен жолы терминалында Басқару серверінің стандартты орнату режимін таңдау

Әрі қарай, скрипт Басқару серверін жаңартуды конфигурациялайды және аяқтайды. Жаңарту кезінде жаңарту алдында өзгертілген Басқару серверінің параметрлерін өзгерте алмайсыз.

6. Сондай-ақ, Kaspersky Security Center Web Console веб-консолін жаңа нұсқаға дейін жаңарту қажет.

7. Алдыңғы нұсқаның Желілік агенті орнатылған құрылғылар үшін Желілік агенттің жаңа нұсқасын қашықтан орнату тапсырмасын жасаңыз және іске қосыңыз.

   Linux үшін Желілік агентті Kaspersky Security Center Linux нұсқасымен бірдей нұсқаға жаңарту ұсынылады.

   Қашықтан орнату тапсырмасын орындағаннан кейін Желілік агент нұсқасы жаңартылды.

   Енді қажет емес тәуелділіктерді жою үшін Linux негізіндегі активтерде келесі пәрмендерді орындаңыз:

   - Debian негізіндегі активтер үшін келесі пәрмендердің бірін іске қосыңыз:

     ```
     sudo apt-get -y autoremove
     ```

     ```
     sudo apt -y autoremove
     ```

   - RPM негізіндегі активтер үшін келесі пәрмендердің бірін іске қосыңыз:

     ```
     sudo dnf autoremove
     ```

     ```
     sudo yum autoremove
     ```

Kaspersky Security Center Linux жүйесін 16 немесе одан кейінгі нұсқасынан сақтық көшірме арқылы жаңарту

Басқару серверін 16 немесе одан кейінгі нұсқадан ең соңғы нұсқаға дейін жаңарту үшін, Басқару сервері деректерінің сақтық көшірмесін жасап, жаңа нұсқадағы Kaspersky Security Center Linux орнатылғаннан кейін осы деректерді қалпына келтіруге болады. Орнату кезінде қиындықтар туындаса, жаңарту алдында жасалған Сервер деректерінің сақтық көшірмесін пайдаланып Басқару серверінің алдыңғы нұсқасын қалпына келтіруге болады.

Kaspersky Security Center Linux жүйесін 16 немесе одан кейінгі нұсқасынан сақтық көшірме арқылы соңғы нұсқасына жаңарту:

1. Жаңарту алдында бағдарламаның ескі нұсқасының Басқару серверіндегі деректердің сақтық көшірмесін жасаңыз.

2. Kaspersky Security Center Linux жүйесінің ескі нұсқасын жойыңыз.

3. Kaspersky Security Center Linux бағдарламасының 16.3 нұсқасын бұған дейін Басқару сервері орнатылған құрылғыға орнатыңыз.

   Егер сақтық көшірмедегі дерекқор схемасы Басқару сервері немесе IAM қолданып отырғаннан өзгеше болса, деректер ағымдағы схемаға қалпына келтіріледі.

   Егер резервтік көшірмеде жалпыға қолжетімді схема пайдаланылса, келесі шарттар орындалуы керек:

   - Жалпыға қолжетімді дерекқор схемасы дерекқорда бар.
   - Дерекқорға кіру үшін Басқару сервері немесе IAM пайдаланатын ДҚБЖ тіркелгісінен жалпыға қолжетімді дерекқор схемасын өзгерте аласыз.

   Әйтпесе, деректерді қалпына келтіру қатемен аяқталады.

4. Жаңарту алдында жасалған деректердің сақтық көшірмесінен Басқару сервері деректерін қалпына келтіріңіз.

5. Kaspersky Security Center Web Console веб-консолін орнатыңыз.

   Kaspersky Security Center Web Console бұрын орнатылған болса, оны сол жауап файлымен қайта орнатыңыз.

   Әкімшінің ішкі пайдаланушы есептік жазбасы арқылы Kaspersky Security Center Web Console-ге кіріңіз.

   Деректерді жұмысқа дайындау процесі басқару серверінің деректерін қалпына келтіргеннен кейін әдетте 15 минутқа дейін созылады, бірақ уақыт аппараттық жасақтама өнімділігіне және басқару сервері деректерінің өлшеміне байланысты. Осы уақыт ішінде Kaspersky Security Center Web Console қосылмауы және қателерді көрсетуі мүмкін.

6. Алдыңғы нұсқаның Желілік агенті орнатылған құрылғылар үшін Желілік агенттің жаңа нұсқасын қашықтан орнату тапсырмасын жасаңыз және іске қосыңыз.

   > Linux үшін Желілік агентті Kaspersky Security Center Linux нұсқасымен бірдей нұсқаға жаңарту ұсынылады.

   Қашықтан орнату тапсырмасын орындағаннан кейін Желілік агент нұсқасы жаңартылды.

Енді қажет емес тәуелділіктерді жою үшін Linux негізіндегі активтерде келесі пәрмендерді орындаңыз:

- Debian негізіндегі активтер үшін келесі пәрмендердің бірін іске қосыңыз:

```
sudo apt-get -y autoremove
```

```
sudo apt -y autoremove
```

- RPM негізіндегі активтер үшін келесі пәрмендердің бірін іске қосыңыз:

```
sudo dnf autoremove
```

```
sudo yum autoremove
```

Kaspersky Security Center Linux бағдарламасын 16-нұсқадан немесе одан кейінгі нұсқадан Kaspersky Security Center Linux ақауларға төзімді кластер тораптарында жаңарту

Басқару серверінің 16 немесе одан кейінгі нұсқасы орнатылған әрбір Kaspersky Security Center Linux ақауларға төзімді кластер түйініне ең соңғы Басқару сервері нұсқасын орнатуға болады. Ең соңғы нұсқаға дейін жаңарту кезінде Басқару серверінің алдыңғы нұсқасының барлық деректері мен параметрлері сақталады.

Егер сіз бұрын құрылғыларға Kaspersky Security Center Linux-ті жергілікті түрде орнатқан болсаңыз, орнату файлын немесе сақтық көшірмені пайдаланып осы құрылғыларда Kaspersky Security Center Linux-ті жаңартуға болады.

Kaspersky Security Center Linux бағдарламасын 16-нұсқадан немесе одан кейінгі нұсқадан Kaspersky Security Center Linux ақауларға төзімді кластер тораптарында жаңарту үшін:

1. Kaspersky сайтынан 16.3 нұсқасына арналған толық пакетімен Kaspersky Security Center Linux орнату файлын жүктеп алыңыз:
   - RPM негізіндегі операциялық жүйесі бар құрылғылар үшін: `ksc64-<version number>-<build number>.x86_64.rpm`
   - Debian негізіндегі құрылғылар үшін: `ksc64_<version number>-<build number>_amd64.deb`
2. Кластерді тоқтату.
3. Жаңартуды іске қосу үшін кластердің белсенді торабында пәрмен жолы терминалында келесі пәрменді орындаңыз:
   - RPM негізіндегі операциялық жүйесі бар құрылғылар үшін:

```
sudo yum install ./ksc64-<version number>-<build number>.x86_64.rpm
```

- Debian негізіндегі операциялық жүйесі бар құрылғылар үшін:

```
sudo apt-get install ./ksc64_<version number>-<build number>_amd64.deb
```

Пәрменді сәтті орындағаннан кейін `/opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl` скрипті жасалады. Бұл туралы хабарлама терминалда көрсетіледі.

4. Жаңартылған Басқару серверін конфигурациялау үшін `/opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl` скриптін іске қосыңыз.

```
sudo /opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl
```

5. Пәрмен жолы терминалында көрсетілетін Лицензиялық келісімді және Құпиялық саясатын оқыңыз. Лицензиялық келісімнің және Құпиялық саясатының барлық шарттарымен келіссеңіз:

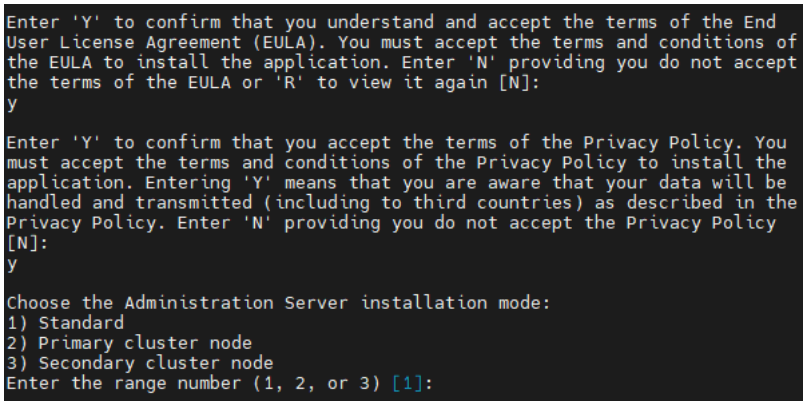
   a. Лицензиялық келісімнің талаптары мен шарттарын толығымен оқығаныңызды, түсінгеніңізді және қабылдағаныңызды растау үшін `Y` енгізіңіз.

   b. Деректерді өңдеуді сипаттайтын Құпиялық саясатын толық оқып, түсінгеніңізді және қабылдағаныңызды растау үшін `Y` тағы бір рет енгізіңіз.

   Бағдарламаны орнату `Y` әрпін екі рет енгізгеннен кейін жалғасады.

6. Жаңартып жатқан түйінді `2` енгізу арқылы таңдаңыз.

   Төмендегі суретте соңғы екі қадам көрсетілген.



Лицензиялық келісімнің және Құпиялық саясатының шарттарын қабылдау және пәрмен жолы терминалында орнату режимін таңдау

Әрі қарай, скрипт Басқару серверін жаңартуды конфигурациялайды және аяқтайды. Жаңарту кезінде жаңарту алдында өзгертілген Басқару серверінің параметрлерін өзгерте алмайсыз.

7. Пассивті түйінде 3–5 қадамдарды орындаңыз.

   6-қадамда түйінді таңдау үшін `3` енгізіңіз.

8. Кластерді іске қосу.

   Кез келген түйінде кластерді іске қосуға болады. Кластерді пассивті түйінде іске қоссаңыз, ол белсенді түйінге айналады.

9. Алдыңғы нұсқаның Желілік агенті орнатылған құрылғылар үшін Желілік агенттің жаңа нұсқасын қашықтан орнату тапсырмасын жасаңыз және іске қосыңыз.

Linux үшін Желілік агентті Kaspersky Security Center Linux нұсқасымен бірдей нұсқаға жаңарту ұсынылады.

Қашықтан орнату тапсырмасын орындағаннан кейін Желілік агент нұсқасы жаңартылды.

Енді қажет емес тәуелділіктерді жою үшін Linux негізіндегі активтерде келесі пәрмендерді орындаңыз:

- Debian негізіндегі активтер үшін келесі пәрмендердің бірін іске қосыңыз:

```
sudo apt-get -y autoremove
```

```
sudo apt -y autoremove
```

- RPM негізіндегі активтер үшін келесі пәрмендердің бірін іске қосыңыз:

```
sudo dnf autoremove
```

```
sudo yum autoremove
```

Нәтижесінде сіз ақауларға төзімді Kaspersky Security Center Linux кластерінің түйіндеріне басқару серверінің соңғы нұсқасын орнаттыңыз.

Kaspersky Security Center Linux 15.4 немесе одан алдыңғы нұсқасынан жаңарту

Бұл бөлімде Kaspersky Security Center Linux жүйесін 15.4 немесе одан бұрынғы нұсқасынан 16 немесе одан кейінгі нұсқасына жаңартудың келесі нұсқалары сипатталған:

- Орнату файлын пайдаланып жаңарту
- Сақтық көшірме арқылы жаңарту
- Kaspersky Security Center Linux ақауларға төзімді кластерінде тораптарында жаңарту

Kaspersky Security Center Linux жүйесін 15.4 немесе одан бұрынғы нұсқасынан 16 немесе одан кейінгі нұсқасына жаңартудың әрбір нұсқасы ДҚБЖ серверінде IAM дерекқорын жасау және конфигурациялау, IAM қызметін іске қосу үшін артықшылықсыз 'ksciam' есептік жазбасын жасау және бұл есептік жазбаны 'kladmins' қауіпсіздік тобына қосу қадамдарын қамтиды.

Kaspersky Security Center Linux жүйесін 15.4 немесе одан алдыңғы нұсқасынан орнату файлын пайдаланып жаңарту

Басқару серверін 13–15.4 нұсқаларынан 16 немесе одан кейінгі нұсқаға дейін жаңарту үшін, Kaspersky Security Center Linux орнату файлын пайдаланып, жаңа нұсқаны ескі нұсқаның үстінен орнатуға болады.

Бастамас бұрын, **арнайы сертификатқа қойылатын талаптарды тексеріңіз**.

Егер сіз өздігінен қол қойылған сертификаттың орнына арнайы сертификатты пайдалансаңыз, Kaspersky Security Center Linux жүйесін кейінгі нұсқасына жаңартпас бұрын, сертификатта Субъектінің балама атауы (SAN) бар екеніне көз жеткізуіңіз керек. Олай болмаса, Kaspersky Security Center Linux жүйесін жаңартпас бұрын сертификатты ауыстыру маңызды. Әйтпесе, жаңартудан кейін Web Console веб-консоліне кіре алмайсыз.

Сертификатта SAN бар екеніне көз жеткізу үшін:

1. Басқару сервер орнатылған құрылғыда келесі пәрменді орындаңыз:

   - Linux құрылғысы үшін:

     ```
     sudo openssl x509 -in /var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer -noout
     -ext subjectAltName
     ```

   - Windows құрылғысы үшін:

     ```
     certutil -dump %ProgramData%\KasperskyLab\adminkit\1093\cert\klserver.cer
     ```

2. Пәрмен шығысында Субъектінің балама атауының бар екеніне және Басқару сервері құрылғысының мекенжайын қамтитынына көз жеткізіңіз.

3. Егер Тақырыптың балама атауы болмаса, klsetsrvcert утилитасын пайдаланып, реттелетін сертификатыңызды талаптарға сай келетін сертификатпен ауыстырыңыз.

Kaspersky Security Center Linux жүйесін 15.4 немесе одан алдыңғы нұсқасынан соңғы нұсқасына орнату файлын пайдаланып жаңарту:

1. Kaspersky сайтынан 16.3 нұсқасына арналған толық пакетімен Kaspersky Security Center Linux орнату файлын жүктеп алыңыз:

   - RPM негізіндегі операциялық жүйесі бар құрылғылар үшін: `ksc64-<version number>.x86_64.rpm`
   - Debian негізіндегі операциялық жүйесі бар құрылғылар үшін: `ksc64_<version number>_amd64.deb`

2. ДҚБЖ серверінде IAM үшін дерекқор жасаңыз. IAM дерекқорының атауы басқару сервері пайдаланатын дерекқордан басқаша болуы керек.

   - PostgreSQL үшін келесі пәрменді іске қосыңыз:

     ```
     sudo -i -u postgres psql -U postgres -c "CREATE DATABASE <iam_db_атауы>;"
     ```

   - MariaDB үшін келесі пәрменді іске қосыңыз:

     ```
     sudo mysql -u root -p -e "CREATE DATABASE <iam_db_атауы>;"
     ```

3. Артықшылықсыз 'ksciam' есептік жазбасын жасаңыз, оны 'kladmins' қауіпсіздік тобына қосыңыз, содан кейін 'kladmins' тобын 'ksciam' есептік жазбасы үшін негізгі топ ретінде орнатыңыз. Ол үшін келесі пәрмендерді ретімен орындаңыз:

   ```
   sudo adduser ksciam
   sudo gpasswd -a ksciam kladmins
   sudo usermod -g kladmins ksciam
   ```

4. Kaspersky Security Center Linux нұсқасын жаңартуды бастау. Пәрмен жолы терминалында келесі пәрменді орындаңыз:

   - RPM негізіндегі операциялық жүйесі бар құрылғылар үшін:

     ```
     sudo yum install ./ksc64-<нұсқа нөмірі>.x86_64.rpm
     ```

   - Debian негізіндегі операциялық жүйесі бар құрылғылар үшін:

     ```
     sudo apt-get install ./ksc64_<нұсқа нөмірі>_amd64.deb
     ```

   Пәрменді сәтті орындағаннан кейін `/opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl` скрипті жасалады. Бұл туралы хабарлама терминалда көрсетіледі.

5. Жаңартылған Басқару серверін конфигурациялау үшін `/opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl` скриптін іске қосыңыз.

   ```
   sudo /opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl
   ```

6. Пәрмен жолы терминалында көрсетілетін Лицензиялық келісімді және Құпиялық саясатын оқыңыз. Лицензиялық келісімнің және Құпиялық саясатының барлық шарттарымен келіссеңіз:

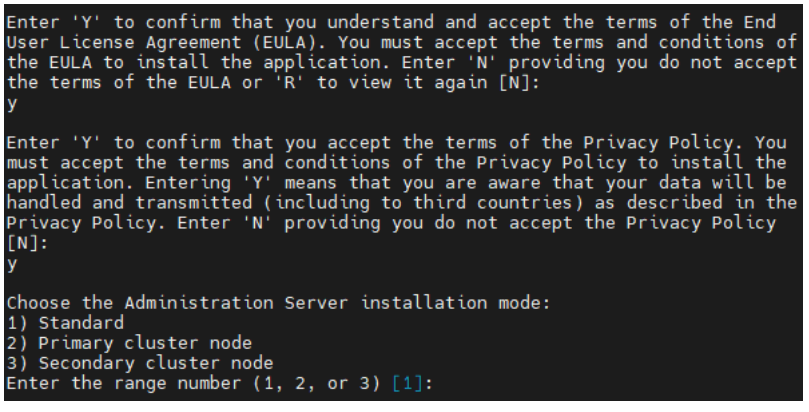
   a. Лицензиялық келісімнің талаптары мен шарттарын толығымен оқығаныңызды, түсінгеніңізді және қабылдағаныңызды растау үшін `Y` енгізіңіз.

   b. Деректерді өңдеуді сипаттайтын Құпиялық саясатын толық оқып, түсінгеніңізді және қабылдағаныңызды растау үшін `Y` тағы бір рет енгізіңіз.

   Бағдарламаны орнату `Y` әрпін екі рет енгізгеннен кейін жалғасады.

7. Басқару серверінің стандартты орнату режимін таңдау үшін `1` енгізіңіз.

   Төмендегі суретте соңғы екі қадам көрсетілген.



Лицензиялық келісімнің және Құпиялық саясатының шарттарын қабылдау және пәрмен жолы терминалында Басқару серверінің стандартты орнату режимін таңдау

8. Әрі қарай, скрипт Басқару серверін жаңартуды конфигурациялайды және аяқтайды. Жаңарту кезінде жаңарту алдында өзгертілген Басқару серверінің параметрлерін өзгерте алмайсыз. Сұрау көрсетілген кезде келесі параметрлерді енгізіңіз:

   a. IAM серверінің FQDN атауын енгізіңіз.

      Kaspersky Security Center Linux жүйесін орнату кезінде көрсетілген Басқару серверінің DNS атауын пайдалануыңыз керек.

   b. IAM қызметін іске қосу үшін есептік жазба атауын енгізіңіз. Есептік жазба көрсетілген қауіпсіздік тобының мүшесі болуы керек. Әдепкісінше ksciam есептік жазбасы пайдаланылады.

   c. IAM қызметімен жұмыс істеу үшін орнатылған ДҚБЖ таңдаңыз:

      - MySQL немесе MariaDB орнатқан болсаңыз, `1` енгізіңіз.
      - PostgreSQL немесе Postgres Pro SQL орнатқан болсаңыз, `2` енгізіңіз.

   d. IAM қызметі пайдаланатын IAM ДҚБЖ мекенжайын енгізіңіз.

   e. IAM ДҚБЖ порт нөмірін енгізіңіз. Бұл порт IAM қызметімен байланысу үшін пайдаланылады. Әдепкі бойынша келесі порттар пайдаланылады:

      - MySQL немесе MariaDB үшін 3306 порты
      - PostgreSQL немесе Postgres Pro үшін 5432 порты

   f. IAM қызметі пайдаланатын IAM дерекқор атауын енгізіңіз. IAM қызметі пайдаланатын дерекқордың атауы басқару сервері пайдаланатын дерекқордан өзгеше болуы керек.

   g. IAM сервисі пайдаланатын ДҚБЖ логині мен құпия сөзін енгізіңіз.

   h. Егер сіз PostgreSQL немесе Postgres Pro орнатқан болсаңыз, IAM пайдаланатын дерекқор схемасын көрсете аласыз. Ол үшін схема атауын көрсетіңіз.

      Егер сіз арнайы схеманы пайдаланғыңыз келмесе, `ENTER` пернесін басыңыз, сонда жалпы схема қолданылады.

      > Схема атауы регистрге сезімтал: тек кіші әріптерді пайдалану керек.
      > Резервтелген IAM схемаларының атауларын көрсетпеңіз: `client, iam, ksc, locker, pat, scope, voltron`.

9. Сондай-ақ, Kaspersky Security Center Web Console веб-консолін жаңа нұсқаға дейін жаңарту қажет.

10. Алдыңғы нұсқаның Желілік агенті орнатылған құрылғылар үшін Желілік агенттің жаңа нұсқасын қашықтан орнату тапсырмасын жасаңыз және іске қосыңыз.

    > Linux үшін Желілік агентті Kaspersky Security Center Linux нұсқасымен бірдей нұсқаға жаңарту ұсынылады.

    Қашықтан орнату тапсырмасын орындағаннан кейін Желілік агент нұсқасы жаңартылды.

Енді қажет емес тәуелділіктерді жою үшін Linux негізіндегі активтерде келесі пәрмендерді орындаңыз:

- Debian негізіндегі активтер үшін келесі пәрмендердің бірін іске қосыңыз:

```
sudo apt-get -y autoremove
```

```
sudo apt -y autoremove
```

- RPM негізіндегі активтер үшін келесі пәрмендердің бірін іске қосыңыз:

```
sudo dnf autoremove
```

```
sudo yum autoremove
```

Kaspersky Security Center Linux жүйесін 15.4 немесе одан алдыңғы нұсқасынан сақтық көшірме арқылы жаңарту

Басқару серверді 14.2—15.4 нұсқасынан 16 немесе одан кейінгі нұсқасына жаңарту үшін Басқару сервері деректерінің сақтық көшірмесін жасап, Kaspersky Security Center Linux бағдарламасының жаңа нұсқасын орнатқаннан кейін қалпына келтіре аласыз. Орнату кезінде қиындықтар туындаса, жаңарту алдында жасалған Сервер деректерінің сақтық көшірмесін пайдаланып Басқару серверінің алдыңғы нұсқасын қалпына келтіруге болады.

Алдын ала талаптар

1. **Арнайы сертификатқа қойылатын талаптарды тексеріңіз**.

   Егер сіз өздігінен қол қойылған сертификаттың орнына арнайы сертификатты пайдалансаңыз, Kaspersky Security Center Linux жүйесін кейінгі нұсқасына жаңартпас бұрын, сертификатта Субъектінің балама атауы (SAN) бар екеніне көз жеткізуіңіз керек. Олай болмаса, Kaspersky Security Center Linux жүйесін жаңартпас бұрын сертификатты ауыстыру маңызды. Әйтпесе, жаңартудан кейін Web Console веб-консоліне кіре алмайсыз.

   Сертификатта SAN бар екеніне көз жеткізу үшін:

   1. Басқару сервер орнатылған құрылғыда келесі пәрменді орындаңыз:

      - Linux құрылғысы үшін:

        ```
        sudo openssl x509 -in /var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer -noout -ext subjectAltName
        ```

      - Windows құрылғысы үшін:

        ```
        certutil -dump %ProgramData%\KasperskyLab\adminkit\1093\cert\klserver.cer
        ```

2. Пәрмен шығысында Субъектінің балама атауының бар екеніне және Басқару сервері құрылғысының мекенжайын қамтитынына көз жеткізіңіз.

3. Егер Тақырыптың балама атауы болмаса, klsetsrvcert утилитасын пайдаланып, реттелетін сертификатыңызды талаптарға сай келетін сертификатпен ауыстырыңыз.

2. Жаңарту алдында бағдарламаның ескі нұсқасының Басқару серверіндегі деректердің сақтық көшірмесін жасаңыз.

Жаңарту рәсімі

Kaspersky Security Center Linux жүйесін 15.4 немесе одан алдыңғы нұсқасынан сақтық көшірме арқылы соңғы нұсқасына жаңарту:

1. Kaspersky Security Center Linux жүйесінің ескі нұсқасын жойыңыз.

2. ДҚБЖ серверінде IAM үшін дерекқор жасаңыз. IAM дерекқорының атауы басқару сервері пайдаланатын дерекқордан басқаша болуы керек.

   - PostgreSQL үшін келесі пәрменді іске қосыңыз:

     ```
     sudo -i -u postgres psql -U postgres -c "CREATE DATABASE <iam_db_атауы>;"
     ```

   - MariaDB үшін келесі пәрменді іске қосыңыз:

     ```
     sudo mysql -u root -p -e "CREATE DATABASE <iam_db_атауы>;"
     ```

3. Артықшылықсыз 'ksciam' есептік жазбасын жасаңыз, оны 'kladmins' қауіпсіздік тобына қосыңыз, содан кейін 'kladmins' тобын 'ksciam' есептік жазбасы үшін негізгі топ ретінде орнатыңыз. Ол үшін келесі пәрмендерді ретімен орындаңыз:

   ```
   sudo adduser ksciam
   sudo gpasswd -a ksciam kladmins
   sudo usermod -g kladmins ksciam
   ```

4. Kaspersky Security Center Linux бағдарламасының 16.3 нұсқасын бұған дейін Басқару сервері орнатылған құрылғыға орнатыңыз.

   Егер сақтық көшірмедегі дерекқор схемасы Басқару сервері немесе IAM қолданып отырғаннан өзгеше болса, деректер ағымдағы схемаға қалпына келтіріледі.

   Егер резервтік көшірмеде жалпыға қолжетімді схема пайдаланылса, келесі шарттар орындалуы керек:

   - Жалпыға қолжетімді дерекқор схемасы дерекқорда бар.

   - Дерекқорға кіру үшін Басқару сервері немесе IAM пайдаланатын ДҚБЖ тіркелгісінен жалпыға қолжетімді дерекқор схемасын өзгерте аласыз.

   Әйтпесе, деректерді қалпына келтіру қатемен аяқталады.

5. Жаңарту алдында жасалған деректердің сақтық көшірмесінен Басқару сервері деректерін қалпына келтіріңіз.

6. Басқару сервері және IAM сервері арқылы сертификатты тексеруді конфигурациялаңыз.

7. Kaspersky Security Center Web Console веб-консолін орнатыңыз.

   Kaspersky Security Center Web Console бұрын орнатылған болса, оны сол жауап файлымен қайта орнатыңыз.

   Әкімшінің ішкі пайдаланушы есептік жазбасы арқылы Kaspersky Security Center Web Console-ге кіріңіз.

   Деректерді жұмысқа дайындау процесі басқару серверінің деректерін қалпына келтіргеннен кейін әдетте 15 минутқа дейін созылады, бірақ уақыт аппараттық жасақтама өнімділігіне және басқару сервері деректерінің өлшеміне байланысты. Осы уақыт ішінде Kaspersky Security Center Web Console қосылмауы және қателерді көрсетуі мүмкін.

8. Алдыңғы нұсқаның Желілік агенті орнатылған құрылғылар үшін Желілік агенттің жаңа нұсқасын қашықтан орнату тапсырмасын жасаңыз және іске қосыңыз.

   Linux үшін Желілік агентті Kaspersky Security Center Linux нұсқасымен бірдей нұсқаға жаңарту ұсынылады.

   Қашықтан орнату тапсырмасын орындағаннан кейін Желілік агент нұсқасы жаңартылды.

   Енді қажет емес тәуелділіктерді жою үшін Linux негізіндегі активтерде келесі пәрмендерді орындаңыз:

   - Debian негізіндегі активтер үшін келесі пәрмендердің бірін іске қосыңыз:

     ```
     sudo apt-get -y autoremove
     ```

     ```
     sudo apt -y autoremove
     ```

   - RPM негізіндегі активтер үшін келесі пәрмендердің бірін іске қосыңыз:

     ```
     sudo dnf autoremove
     ```

     ```
     sudo yum autoremove
     ```

Kaspersky Security Center Linux бағдарламасын 15.4-нұсқадан немесе одан алдыңғы нұсқадан Kaspersky Security Center Linux ақауларға төзімді кластер тораптарында жаңарту

Сіз Kaspersky Security Center Linux жүйесінің 16 немесе одан кейінгі нұсқасын 14–15.4 нұсқалары орнатылған әрбір Kaspersky Security Center ақауларға төзімді кластерінің кластер түйініне орната аласыз. Жаңарту кезінде Басқару серверінің алдыңғы нұсқасының барлық деректері мен параметрлері сақталады.

Бастамас бұрын, **арнайы сертификатқа қойылатын талаптарды тексеріңіз**.

Егер сіз өздігінен қол қойылған сертификаттың орнына арнайы сертификатты пайдалансаңыз, Kaspersky Security Center Linux жүйесін кейінгі нұсқасына жаңартпас бұрын, сертификатта Субъектінің балама атауы (SAN) бар екеніне көз жеткізуіңіз керек. Олай болмаса, Kaspersky Security Center Linux жүйесін жаңартпас бұрын сертификатты ауыстыру маңызды. Әйтпесе, жаңартудан кейін Web Console веб-консоліне кіре алмайсыз.

Сертификатта SAN бар екеніне көз жеткізу үшін:

1. Басқару сервер орнатылған құрылғыда келесі пәрменді орындаңыз:

   - Linux құрылғысы үшін:

     ```
     sudo openssl x509 -in /var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer -noout
     -ext subjectAltName
     ```

   - Windows құрылғысы үшін:

     ```
     certutil -dump %ProgramData%\KasperskyLab\adminkit\1093\cert\klserver.cer
     ```

2. Пәрмен шығысында Субъектінің балама атауының бар екеніне және Басқару сервері құрылғысының мекенжайын қамтитынына көз жеткізіңіз.

3. Егер Тақырыптың балама атауы болмаса, klsetsrvcert утилитасын пайдаланып, реттелетін сертификатыңызды талаптарға сай келетін сертификатпен ауыстырыңыз.

Егер сіз бұрын құрылғыларға Kaspersky Security Center Linux-ті жергілікті түрде орнатқан болсаңыз, орнату файлын немесе сақтық көшірмені пайдаланып осы құрылғыларда Kaspersky Security Center Linux-ті жаңартуға болады.

Kaspersky Security Center Linux бағдарламасын 15.4-нұсқадан немесе одан алдыңғы нұсқадан Kaspersky Security Center Linux ақауларға төзімді кластер тораптарында жаңарту үшін:

1. Kaspersky сайтынан 16.3 нұсқасына арналған толық пакетімен Kaspersky Security Center Linux орнату файлын жүктеп алыңыз:

   - RPM негізіндегі операциялық жүйесі бар құрылғылар үшін: `ksc64-<version number>-<build number>.x86_64.rpm`

   - Debian негізіндегі құрылғылар үшін: `ksc64_<version number>-<build number>_amd64.deb`

2. Кластерді тоқтату.

3. ДҚБЖ серверінде IAM үшін дерекқор жасаңыз. IAM дерекқорының атауы басқару сервері пайдаланатын дерекқордан басқаша болуы керек.

   - PostgreSQL үшін келесі пәрменді іске қосыңыз:

     ```
     sudo -i -u postgres psql -U postgres -c "CREATE DATABASE <iam_db_атауы>;"
     ```

   - MariaDB үшін келесі пәрменді іске қосыңыз:

     ```
     sudo mysql -u root -p -e "CREATE DATABASE <iam_db_атауы>;"
     ```

4. Артықшылықсыз 'ksciam' есептік жазбасын жасаңыз, оны 'kladmins' қауіпсіздік тобына қосыңыз, содан кейін 'kladmins' тобын 'ksciam' есептік жазбасы үшін негізгі топ ретінде орнатыңыз. Ол үшін келесі пәрмендерді ретімен орындаңыз:

```
sudo adduser ksciam
sudo gpasswd -a ksciam kladmins
sudo usermod -g kladmins ksciam
```

5. Кластердегі белсенді түйінде жаңартуды бастау үшін пәрмен жолы терминалында келесі командалардың бірін орындаңыз:

   - RPM негізіндегі операциялық жүйесі бар құрылғылар үшін:

     ```
     sudo yum install ./ksc64-<нұсқа нөмірі>-<құрастыру нөмірі>.x86_64.rpm
     ```

   - Debian негізіндегі операциялық жүйесі бар құрылғылар үшін:

     ```
     sudo apt-get install ./ksc64_<нұсқа нөмірі>-<құрастыру нөмірі>_amd64.deb
     ```

   Пәрменді сәтті орындағаннан кейін `/opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl` скрипті жасалады. Бұл туралы хабарлама терминалда көрсетіледі.

6. Жаңартылған Басқару серверін конфигурациялау үшін `/opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl` скриптін іске қосыңыз.

   ```
   sudo /opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl
   ```

7. Пәрмен жолы терминалында көрсетілетін Лицензиялық келісімді және Құпиялық саясатын оқыңыз. Лицензиялық келісімнің және Құпиялық саясатының барлық шарттарымен келіссеңіз:

   a. Лицензиялық келісімнің талаптары мен шарттарын толығымен оқығаныңызды, түсінгеніңізді және қабылдағаныңызды растау үшін `Y` енгізіңіз.

   b. Деректерді өңдеуді сипаттайтын Құпиялық саясатын толық оқып, түсінгеніңізді және қабылдағаныңызды растау үшін `Y` тағы бір рет енгізіңіз.

   Бағдарламаны орнату `Y` әрпін екі рет енгізгеннен кейін жалғасады.

8. Жаңартып жатқан түйінді `2` енгізу арқылы таңдаңыз.

Төмендегі суретте соңғы екі қадам көрсетілген.

```
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]:
```

Лицензиялық келісімнің және Құпиялық саясатының шарттарын қабылдау және пәрмен жолы терминалында орнату режимін таңдау

9. Әрі қарай, скрипт Басқару серверін жаңартуды конфигурациялайды және аяқтайды. Жаңарту кезінде жаңарту алдында өзгертілген Басқару серверінің параметрлерін өзгерте алмайсыз. Сұрау көрсетілген кезде келесі параметрлерді енгізіңіз:

   a. IAM серверінің FQDN атауын енгізіңіз.

   Kaspersky Security Center Linux жүйесін орнату кезінде көрсетілген Басқару серверінің DNS атауын пайдалануыңыз керек.

   b. IAM қызметін іске қосу үшін есептік жазба атауын енгізіңіз. Есептік жазба көрсетілген қауіпсіздік тобының мүшесі болуы керек. Әдепкісінше ksciam есептік жазбасы пайдаланылады.

   c. IAM қызметімен жұмыс істеу үшін орнатылған ДҚБЖ таңдаңыз:

   - MySQL немесе MariaDB орнатқан болсаңыз, `1` енгізіңіз.
   - PostgreSQL немесе Postgres Pro SQL орнатқан болсаңыз, `2` енгізіңіз.

   d. IAM қызметі пайдаланатын IAM ДҚБЖ мекенжайын енгізіңіз.

   e. IAM ДҚБЖ порт нөмірін енгізіңіз. Бұл порт IAM қызметімен байланысу үшін пайдаланылады. Әдепкі бойынша келесі порттар пайдаланылады:

   - MySQL немесе MariaDB үшін 3306 порты
   - PostgreSQL немесе Postgres Pro үшін 5432 порты

   f. IAM қызметі пайдаланатын IAM дерекқор атауын енгізіңіз. IAM қызметі пайдаланатын дерекқордың атауы басқару сервері пайдаланатын дерекқордан өзгеше болуы керек.

   g. IAM сервисі пайдаланатын ДҚБЖ логині мен құпия сөзін енгізіңіз.

10. Енжар түйінде 5-қадамды орындаңыз.

    6-қадамда түйінді таңдау үшін `3` енгізіңіз.

11. Кластерді іске қосу.

    Кез келген түйінде кластерді іске қосуға болады. Кластерді пассивті түйінде іске қоссаңыз, ол белсенді түйінге айналады.

12. Алдыңғы нұсқаның Желілік агенті орнатылған құрылғылар үшін Желілік агенттің жаңа нұсқасын қашықтан орнату тапсырмасын жасаңыз және іске қосыңыз.

    Linux үшін Желілік агентті Kaspersky Security Center Linux нұсқасымен бірдей нұсқаға жаңарту ұсынылады.

    Қашықтан орнату тапсырмасын орындағаннан кейін Желілік агент нұсқасы жаңартылды.

    Енді қажет емес тәуелділіктерді жою үшін Linux негізіндегі активтерде келесі пәрмендерді орындаңыз:

    - Debian негізіндегі активтер үшін келесі пәрмендердің бірін іске қосыңыз:

      ```
      sudo apt-get -y autoremove
      ```

      ```
      sudo apt -y autoremove
      ```

    - RPM негізіндегі активтер үшін келесі пәрмендердің бірін іске қосыңыз:

      ```
      sudo dnf autoremove
      ```

      ```
      sudo yum autoremove
      ```

    Нәтижесінде сіз ақауларға төзімді Kaspersky Security Center Linux кластерінің түйіндеріне басқару серверінің соңғы нұсқасын орнаттыңыз.

Kaspersky Security Center Web Console жаңарту

Бұл бөлімде Kaspersky Security Center Web Console Server серверін (бұдан әрі Kaspersky Security Center Web Console деп те аталады) қалай Linux операциялық жүйелері бар құрылғыларға жаңартуға болатыны сипатталған.

Astra Linux жүйесінде Kaspersky Security Center Web Console консолін жабық бағдарламалық орта режимінде жаңарту керек болса, Astra Linux нұсқауларын орындаңыз.

Құрылғыңызда орнатылған Linux дистрибутивіне сәйкес келетін келесі орнату файлдарының бірін пайдаланыңыз:

- Debian негізіндегі операциялық жүйелер үшін: ksc-web-console-<build_number>.x86_64.deb
- RPM негізіндегі операциялық жүйелер үшін: ksc-web-console-<құрастыру_нөмірі>.x86_64.rpm

Орнату файлын Kaspersky сайтынан жүктеу арқылы аласыз.

Kaspersky Security Center Web Console жаңарту үшін:

1. Kaspersky Security Center Web Console жаңартқыңыз келетін құрылғыда қолдау көрсетілетін Linux дистрибутивтерінің бірі жұмыс істейтініне көз жеткізіңіз.

2. Лицензиялық келісімді оқыңыз және қабылдаңыз. Kaspersky Security Center Linux дистрибутиві құрамына Лицензиялық келісім мәтіні бар TXT файлы кірмесе, бұл файлды Kaspersky сайтынан жүктеп алуға болады. Лицензиялық келісімнің шарттарын қабылдамасаңыз, орнату файлын пайдаланып Kaspersky Security Center Web Console веб-консолін жаңартпаңыз.

3. Kaspersky Security Center Web Console веб-консолін орнату алдында өзіңіз дайындаған жауап файлын пайдаланыңыз. Жауап файлының атауы — ksc-web-console-setup.json, ал файл орны — /etc/ksc-web-console-setup.json.

> Kaspersky Security Center Web Console орнату кезінде `webConsoleAccount`, `managementServiceAccount`, `serviceWebConsoleAccount`, `pluginAccount` және `natsMessageQueueAccount` параметрлерінің мәндерін көрсетсеңіз, осы параметрлердің барлығы жауап файлында көрсетілгенін тексеріңіз.

Жауап файлы жоқ болса, Kaspersky Security Center Web Console веб-консолін Басқару серверіне қосу параметрлерін қамтитын жаңа жауап файлын жасаңыз. Файлды ksc-web-console-setup.json деп атаңыз және оны /etc директориясында орналастырыңыз.

Параметрлердің ең аз жинағын қамтитын жауап файлының мысалы

Жауап файлының параметрлер жинағы Kaspersky Security Center Web Console қосылатын басқару серверінің нұсқасына байланысты:

- Басқару серверінің 16 және одан жоғары нұсқасы

  Басқару серверінің 16 немесе одан кейінгі нұсқасына кіруге арналған параметрлердің минималды жинағы бар жауап файлының мысалы:

```
{
    "address": "ksc-web-console.example.com",
    "port": 8080,
    "trusted":  {
        "Administration Server v16": {
            "iamHost": "ksc16.example.com",
            "iamOAuthPort": 4444,
            "iamProxyPort": 9050,
            "iamCertPath": "/var/opt/kaspersky/klnagent_srv/iam/main_certificate.pem",
            "iamPATPath": "/var/opt/kaspersky/klnagent_srv/iam/initial_token.txt",
            "kscPort": 13299,
            "kscCertPath": "/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer"
        }
    },
    "certDomain":"ksc-web-console.example.com",
    "acceptEula": true
}
```

- Басқару серверінің 15.4 немесе одан кейінгі нұсқасы

  Басқару серверінің 1.4 немесе одан кейінгі нұсқасына кіруге арналған параметрлердің минималды жинағы бар жауап файлының мысалы:

```
{
    "address": "ksc-web-console.example.com",
    "port": 8080,
    "trusted":  {
         "Administration Server v15.4": {
             "kscHost": "ksc.example.com",
             "kscPort": 13299,
             "kscCertPath": "/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer"
         }
    },
    "certDomain":"ksc-web-console.example.com",
    "acceptEula": true
}
```

Kaspersky Security Center Web Console-ді басқару серверімен бір құрылғыға немесе басқа құрылғыға орнатуға болады. Егер Kaspersky Security Center Web Console басқа құрылғыға орнатылған болса, Kaspersky Security Center Web Console-ның веб-мекенжайы (көрсетілген `address`) және Басқару серверінің веб-мекенжайы (көрсетілген `iamHost` немесе `kscHost`) ерекшеленеді. Егер Kaspersky Security Center Web Console Басқару серверімен бір құрылғыда орнатылған болса, бұл параметрлердің мәндері бірдей болады.

Басқару серверін орнату бағдарламасы кезінде көрсетілген IAM мекенжайына `iamHost` мәні сәйкес келуі керек. Көрсетілген IAM мекенжайын алу үшін Басқару сервері орнатылған құрылғыда келесі пәрменді орындаңыз:

```
grep "iam_address:" /var/opt/kaspersky/klnagent_srv/iam/iam_config.yaml
```

Толық ақпарат алу үшін Kaspersky Security Center Web Console орнату параметрлері мақаласын қараңыз.

Сенімді серверлер тізіміне әртүрлі нұсқалардың бірнеше басқару серверін қосуға болады. Бұл жағдайда серверлер әртүрлі аутентификация әдістерін қолдануы мүмкін.

Kaspersky Security Center Linux ақауларға төзімді кластерінің түйіндерінде орнатылған Басқару серверіне қосылған Kaspersky Security Center Web Console веб-консолі қолданбасын жаңартқыңыз келсе, Kaspersky Security Center Linux ақауларға төзімді кластеріне Kaspersky Security Center Web Console веб-консолінe қосылуға рұқсат беру үшін жауап файлында сенімді орнату параметрін көрсетіңіз.

`trusted` **орнату параметрінің** құрамдастары

SSO бар домен аутентификациясымен ақауларға төзімді Kaspersky Security Center Linux кластеріне қосылсаңыз, сенімді орнату параметрін келесідей көрсетіңіз: Kaspersky Security Center Web Console-ді басқару серверінің 16 немесе одан кейінгі нұсқасына қоссаңыз, Есептік деректер және қатынасу диспетчері (IAM) ұсынған бір рет кіру (SSO) мүмкіндігі бар домен аутентификациясы қолданылады. Бұл жағдайда `trusted` орнату параметрін келесідей көрсетіңіз:

```
"trusted":  {
  "<Басқару серверінің атауы>": {
    "iamHost": "ksc-iam.example.com",
    "iamOAuthPort": 4444,
    "iamProxyPort": 9050,
    "iamCertPath": "<ортақ деректер қалтасы>/iam/main_certificate.pem",
    "iamPATPath": "<ортақ деректер қалтасы>/iam/initial_token.txt",
    "kscPort": 13299,
    "kscCertPath": "<ортақ деректер қалтасы>/1093/cert/klserver.cer"
  }
}
```

мұндағы

- `< Басқару серверінің атауы >` — Kaspersky Security Center Web Console-іне кіру терезесінде көрсетілетін ақауларға төзімді Kaspersky Security Center Linux кластерінің атауы.

- `iamHost` — басқару сервері және IAM орнатылған құрылғының мекенжайы. Кластер түйіндерін дайындау кезінде қосалқы желі адаптерін жасасаңыз, адаптердің FQDN немесе хост атауын ақауларға төзімді Kaspersky Security Center Linux кластерінің мекенжайы ретінде пайдаланыңыз. Болмаса өзіңіз қолданатын үшінші тараптың жүктеме теңестіргішінің FQDN немесе хост атауын көрсетіңіз.

  Басқару серверін орнату бағдарламасы кезінде көрсетілген IAM мекенжайына `iamHost` мәні сәйкес келуі керек. Көрсетілген IAM мекенжайын алу үшін Басқару сервері хостында келесі пәрменді орындаңыз:

  `grep "iam_address:" /var/opt/kaspersky/klnagent_srv/iam/iam_config.yaml`

- `iamOAuthPort` – OpenID Connect аутентификация протоколы арқылы аутентификация токендерін алмастыру үшін пайдаланылатын порт (әдепкі мәні – 4444). Бұл порт Kaspersky Security Center Web Console Server мен басқару сервері арасындағы, сондай-ақ браузер (Kaspersky Security Center Web Console-мен пайдаланылады) мен басқару сервері арасындағы байланыс үшін де пайдаланылады.

- `iamProxyPort` – Kaspersky Security Center Web Console Server-ді басқару серверіне қосу үшін пайдаланылатын порт (әдепкі мән — 9050).

- `iamCertPath` — IAM сертификатының жолы. IAM сертификаты басқару серверін бірінші рет іске қосқанда автоматты түрде жасалады. Сертификат басқару сервері орнатылған құрылғыда орналасқан. Сертификаттың әдепкі жолы: `< ортақ деректер қалтасы >/iam/main_certificate.pem`. Сертификат ақауларға төзімді Kaspersky Security Center Linux кластерінің ортақ деректерді сақтау орнында орналасқан. Өздігінен қол қойылған IAM сертификаты автоматты түрде бұрылады.

- `iamPATPath` — IAM жүйесінде OAuth клиенті ретінде Kaspersky Security Center Web Console тіркеу үшін пайдаланылатын токен жолы. Бұл файл басқару серверін бірінші рет іске қосқан кезде жасалады. Токен басқару сервері орнатылған құрылғыда орналасқан. Токеннің әдепкі жолы: <ортақ деректер қалтасы>/iam/initial_token.txt. Сертификат ақауларға төзімді Kaspersky Security Center Linux кластерінің ортақ деректерді сақтау орнында орналасқан. Токен шексіз уақыт жарамды және бұруды қажет етпейді.

- `kscPort` — Security Center Web Console басқару серверіне қосылу үшін пайдаланатын OpenAPI порты (әдепкі мән — 13299).

- `kscCertPath` — ақауларға төзімді Kaspersky Security Center Linux кластерінің ортақ деректерді сақтау орнында орналасқан басқару серверінің сертификаты. Сертификат файлына әдепкі бойынша жол: `< ортақ деректер қалтасы >\1093\cert\klserver.cer`.

  > Басқару серверінің сертификат файлын (`kscCertPath` арқылы көрсетілген), IAM сертификат файлын (`iamCertPath` арқылы көрсетілген) және токен файлын (`iamPATPath` арқылы көрсетілген) ортақ деректерді сақтау орнынан Kaspersky Security Center Web Console орнататын құрылғыға көшіріңіз. Басқару серверінің сертификатына апаратын жергілікті жолды көрсетіңіз.

Kaspersky Security Center Web Console-ді басқару серверінің 15.4 немесе одан бұрынғы нұсқасына қоссаңыз, домен пайдаланушысының немесе ішкі пайдаланушының аты мен құпиясөзін көрсету арқылы аутентификациялау қолданылады. Бұл жағдайда сенімді орнату параметрін келесідей көрсетіңіз:

```
"trusted":  {
  "<Басқару серверінің атауы>": {
    "kscHost": "ksc.example.com",
    "kscPort": 13299,
    "kscCertPath": "<ортақ деректер қалтасы>/1093/cert/klserver.cer"
  }
}
```

мұндағы

- `< Басқару серверінің атауы >` — Kaspersky Security Center Web Console-іне кіру терезесінде көрсетілетін ақауларға төзімді Kaspersky Security Center Linux кластерінің атауы.

- `kscHost` — басқару серверінің мекенжайы (FQDN немесе хост атауы). Кластер түйіндерін дайындау кезінде қосалқы желі адаптерін жасасаңыз, адаптер мекенжайын ақауларға төзімді Kaspersky Security Center Linux кластерінің мекенжайы ретінде пайдаланыңыз. Болмаса өзіңіз пайдаланып жатқан үшінші тараптың жүктеме теңестіргішінің мекенжайын көрсетіңіз.

- `kscPort` — Kaspersky Security Center Web Console веб-консолі басқару серверіне қосылу үшін пайдаланатын OpenAPI порты (әдепкі мәні — 13299).

- `kscCertPath` — ақауларға төзімді Kaspersky Security Center Linux кластерінің ортақ деректерді сақтау орнында орналасқан басқару серверінің сертификаты. Сертификат файлына әдепкі бойынша жол: `<ортақ деректер қалтасы>\1093\cert\klserver.cer`. Сертификат файлын ортақ деректер қоймасынан Kaspersky Security Center Web Console орнатып жатқан құрылғыға көшіріңіз. Басқару серверінің сертификатына апаратын жергілікті жолды көрсетіңіз.

Kaspersky Security Center Web Console қолданбасын бірдей орнату файлының көмегімен жаңарту мүмкін емес. Егер сіз жауаптар файлының параметрлерін өзгерткіңіз келсе және осы файлды қолданбаны қайта орнату үшін пайдаланғыңыз келсе, алдымен қолданбаны жойып, содан кейін оны жаңа жауаптар файлымен қайта орнатуыңыз қажет.

4. root артықшылықты есептік жазбаның астында Linux дистрибутивіңізге байланысты .deb немесе .rpm кеңейтімі бар орнату файлын іске қосу үшін пәрмен жолын пайдаланыңыз.

   Kaspersky Security Center Web Console алдыңғы нұсқасын жаңарту үшін келесі пәрмендердің бірін орындаңыз:

   - RPM негізіндегі операциялық жүйесі бар құрылғылар үшін:
     ```
     sudo yum install ksc-web-console-<құрастыру_нөмірі>.x86_64.rpm
     ```

   - Debian негізіндегі операциялық жүйесі бар құрылғылар үшін:
     ```
     sudo apt-get install ksc-web-console-<құрастыру_нөмірі>.x86_64.deb
     ```

   Орнату файлын ашу басталады. Орнату аяқталғанша күте тұрыңыз.

5. Келесі пәрменді орындау арқылы Kaspersky Security Center Web Console барлық қызметтерін қайта іске қосыңыз:
   ```
   sudo systemctl restart KSC*
   ```

Жаңарту аяқталғаннан кейін, сіз Kaspersky Security Center Web Console веб-консолін ашып, жүйеге кіру үшін браузерді пайдалана аласыз.

Тұйық бағдарламалық орта режимінде Astra Linux-ке Kaspersky Security Center Web Console жаңарту

Бұл бөлімде Kaspersky Security Center Web Console Server серверін (бұдан әрі Kaspersky Security Center Web Console деп те аталады) қалай Astra Linux Special Edition операциялық жүйесі бар құрылғыларға жаңартуға болатыны сипатталған.

Kaspersky Security Center Web Console жаңарту үшін:

1. Kaspersky Security Center Web Console жаңартқыңыз келетін құрылғыда қолдау көрсетілетін Linux дистрибутивтерінің бірі жұмыс істейтініне көз жеткізіңіз.

2. Лицензиялық келісімді оқыңыз және қабылдаңыз. Kaspersky Security Center Linux дистрибутиві құрамына Лицензиялық келісім мәтіні бар TXT файлы кірмесе, бұл файлды Kaspersky сайтынан жүктеп алуға болады. Лицензиялық келісімнің шарттарын қабылдамасаңыз, орнату файлын пайдаланып Kaspersky Security Center Web Console веб-консолін жаңартпаңыз.

3. Kaspersky Security Center Web Console веб-консолін орнату алдында өзіңіз дайындаған жауап файлын пайдаланыңыз. Жауап файлының атауы — ksc-web-console-setup.json, ал файл орны — /etc/ksc-web-console-setup.json.

   Жауап файлы жоқ болса, Kaspersky Security Center Web Console веб-консолін Басқару серверіне қосу параметрлерін қамтитын жаңа жауап файлын жасаңыз. Файлды ksc-web-console-setup.json деп атаңыз және оны /etc директориясында орналастырыңыз.

   Параметрлердің ең аз жинағын қамтитын жауап файлының мысалы

   Жауап файлының параметрлер жинағы Kaspersky Security Center Web Console қосылатын басқару серверінің нұсқасына байланысты:

   - Басқару серверінің 16 және одан жоғары нұсқасы

     Басқару серверінің 16 немесе одан кейінгі нұсқасына кіруге арналған параметрлердің минималды жинағы бар жауап файлының мысалы:

     ```
     {
         "address": "ksc-web-console.example.com",
         "port": 8080,
         "trusted":  {
             "Administration Server v16": {
                 "iamHost": "ksc16.example.com",
                 "iamOAuthPort": 4444,
                 "iamProxyPort": 9050,
                 "iamCertPath": "/var/opt/kaspersky/klnagent_srv/iam/main_certificate.pem",
                 "iamPATPath": "/var/opt/kaspersky/klnagent_srv/iam/initial_token.txt",
                 "kscPort": 13299,
                 "kscCertPath": "/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer"
             }
         },
         "certDomain":"ksc-web-console.example.com",
         "acceptEula": true
     }
     ```

   - Басқару серверінің 15.4 немесе одан кейінгі нұсқасы

     Басқару серверінің 1.4 немесе одан кейінгі нұсқасына кіруге арналған параметрлердің минималды жинағы бар жауап файлының мысалы:

     ```
     {
         "address": "ksc-web-console.example.com",
         "port": 8080,
         "trusted":  {
              "Administration Server v15.4": {
                  "kscHost": "ksc.example.com",
                  "kscPort": 13299,
                  "kscCertPath": "/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer"
              }
         },
         "certDomain":"ksc-web-console.example.com",
         "acceptEula": true
     }
     ```

   Kaspersky Security Center Web Console-ді басқару серверімен бір құрылғыға немесе басқа құрылғыға орнатуға болады. Егер Kaspersky Security Center Web Console басқа құрылғыға орнатылған болса, Kaspersky Security Center Web Console-ның веб-мекенжайы (көрсетілген `address`) және Басқару серверінің веб-мекенжайы (көрсетілген `iamHost` немесе `kscHost`) ерекшеленеді. Егер Kaspersky Security Center Web Console Басқару серверімен бір құрылғыда орнатылған болса, бұл параметрлердің мәндері бірдей болады.

   Басқару серверін орнату бағдарламасы кезінде көрсетілген IAM мекенжайына `iamHost` мәні сәйкес келуі керек. Көрсетілген IAM мекенжайын алу үшін Басқару сервері орнатылған құрылғыда келесі пәрменді орындаңыз:

```
grep "iam_address:" /var/opt/kaspersky/klnagent_srv/iam/iam_config.yaml
```

Толық ақпарат алу үшін Kaspersky Security Center Web Console орнату параметрлері мақаласын қараңыз.

Сенімді серверлер тізіміне әртүрлі нұсқалардың бірнеше басқару серверін қосуға болады. Бұл жағдайда серверлер әртүрлі аутентификация әдістерін қолдануы мүмкін.

4. `/etc/digsig/digsig_initramfs.conf` файлында `DIGSIG_ELF_MODE` параметрінің төмендегідей көрсетілгеніне көз жеткізіңіз:

   ```
   DIGSIG_ELF_MODE=1
   ```

5. `astra-digsig-oldkeys` үйлесімділік пакетінің орнатылғанына көз жеткізіңіз.

   Бұл пакет орнатылмаған болса, келесі пәрменді орындаңыз:

   ```
   apt install astra-digsig-oldkeys
   ```

6. Қолданба кілті жоқ болса, ол үшін директория жасаңыз:

   ```
   mkdir -p /etc/digsig/keys/legacy/kaspersky/
   ```

7. /opt/kaspersky/ksc64/share/kaspersky_astra_pub_key.gpg бағдарлама кілтін алдыңғы қадамда жасалған каталогқа орналастырыңыз:

   ```
   cp kaspersky_astra_pub_key.gpg /etc/digsig/keys/legacy/kaspersky/
   ```

   > Егер Kaspersky Security Center Linux жеткізілім жинағында kaspersky_astra_pub_key.gpg кілті болмаса, бұл кілтті https://media.kaspersky.com/utilities/CorporateUtilities/kaspersky_astra_pub_key.gpg сілтемесінен жүктеп алуға болады.

8. Дискілердің жедел жадын жаңартыңыз:

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

   Жүйені қайта жүктеңіз.

9. root құқықтары бар тіркелгіде орнату файлын іске қосу үшін пәрмен жолын пайдаланыңыз. Орнату файлын Kaspersky сайтынан жүктеу арқылы аласыз.

   Kaspersky Security Center Web Console алдыңғы нұсқасын жаңарту үшін келесі пәрмендердің бірін орындаңыз:

   ```
   sudo apt-get install ksc-web-console-<құрастыру нөмірі>.x86_64.deb
   ```

   Орнату файлын ашу басталады. Орнату аяқталғанша күте тұрыңыз.

10. Келесі пәрменді орындау арқылы Kaspersky Security Center Web Console барлық қызметтерін қайта іске қосыңыз:

    ```
    sudo systemctl restart KSC*
    ```

Жаңарту аяқталғаннан кейін, сіз Kaspersky Security Center Web Console веб-консолін ашып, жүйеге кіру үшін браузерді пайдалана аласыз.

Kaspersky Security Center Linux бағдарламасына тасымалдау

Kaspersky Security Center Windows жүйесінен Kaspersky Security Center Linux жүйесіне көшіру Басқару сервері деректерінің сақтық көшірмесін (klbackup utility утилитасымен) және Тасымалдау шеберін пайдалану арқылы қолжетімді.

Төмендегі кесте басқару сервері деректерінің сақтық көшірмесін және тасымалдау шеберін пайдалану арқылы көшірудің негізгі мүмкіндіктері мен шектеулерін салыстыруға, қай тәсіл ұйымыңыз үшін қолайлы екенін шешуге мүмкіндік береді.

Параметрлер	Басқару сервері деректерін сақтық көшірмелеу	Тасымалдау шебері
Көшіру процесі	Kaspersky Security Center Windows басқару сервері деректерінің толық сақтық көшірмесін жасау және оны Kaspersky Security Center Linux басқару серверінде қалпына келтіру	Көшіру үшін басқару сервері деректерін таңдау және экспорттау, бұл деректерді Kaspersky Security Center Linux басқару серверіне импорттау және Kaspersky Security Center Linux басқаратын құрылғыларды ауыстыру
Көшіру әдісінің мүмкіндіктері	• Барлық басқару сервері дерегін көшіру • Басқарылатын құрылғылардың кез келген санын көшіру • Kaspersky Security Center Windows басқару сервері деректерінің толық көшірмесін алу және оны Kaspersky Security Center Linux басқару серверіне тасымалдау үшін пайдаланылады	• Басқару сервері деректерін ішінара көшіру • Көшіру үшін нысандарды таңдау қолжетімді • Көшірілетін басқару тобы немесе ішкі топ 10000 құрылғыдан аспауы керек • Басқару сервері деректерін, соның ішінде тек көшіру ауқымындағы топтық нысандарды ішінара тасымалдау үшін пайдаланылады; көшіру ауқымынан тыс топтық нысандар қолмен қалпына келтірілуі керек
Көшіру ауқымы	Басқарылатын құрылғылардың шектеусіз санымен басқару сервері деректерін толық тасымалдау	• Басқару тобының құрылымы • Басқару топтарына қосылған басқарылатын құрылғылар (**10000 құрылғыдан аспайды**) • Көшіру құрылғыларына тағайындалған тегтер • Желілік агенттің жаһандық тапсырмалары және басқарылатын қолданбалар (басқару серверіне арналмаған) • Желілік агент пен басқарылатын қолданбалардың топтық тапсырмалары • Басқарылатын қолданбалардың саясаттары • Есеп үлгілері • Пайдаланушы рөлдері • Ішкі пайдаланушылар және қауіпсіздік топтары • Қолмен қосылған мазмұны бар арнаулы қолданба санаттары • Пайдаланушылық құрылғы таңдаулары
Көшірілмеген ауқым	—	• Басқару серверінің жаһандық тапсырмалары • Басқару серверінде сақталған оқиғалар • Қашықтан орнатуға арналған қолданбалар дистрибутивтерінің қоймасы • Басқару сервері сертификаты • Басқару сервері және басқарылатын қолданбалар пайдаланатын лицензия кілттері • Виртуалды Басқару серверлері • Желілік агент саясатының параметрлері • Құрылғыны жылжыту ережелері • Құрылғыларға автоматты түрде тәг енгізу ережелері • Тарату нүктелері • Басқару серверінде сақталған Kaspersky қолданба параметрлері
Көшіруді қолдайтын Kaspersky Security Center нұсқалары	• Kaspersky Security Center Windows жүйесінің кез келген қолдау көрсетілетін нұсқасы • Kaspersky Security Center Linux 15.2 немесе одан кейінгі нұсқасы	• Kaspersky Security Center Windows 14.2 немесе одан кейінгі нұсқасы • Kaspersky Security Center Linux 15 немесе одан кейінгі нұсқасы
Көшіруге болатын ДҚБЖ-лар	• Microsoft SQL Server → MySQL, MariaDB • Microsoft SQL Server → PostgreSQL, Postgres Pro (тек Kaspersky Security Center Windows 14.2 немесе одан кейінгі нұсқасынан орнатылған патчпен Kaspersky Security Center Linux 15.3 немесе одан кейінгі нұсқасына көшіру) • MySQL → MySQL, MariaDB • MariaDB → MySQL, MariaDB • PostgreSQL → PostgreSQL Postgres Pro → Postgres Pro (тек Kaspersky Security Center Windows 15.1 немесе одан кейінгі нұсқасынан Kaspersky Security Center Linux 16 немесе одан кейінгі нұсқасына көшіру үшін)	Қолдау көрсетілетін ДҚБЖ-лар арасында шектеусіз көшіру

Басқару сервері деректерінің сақтық көшірмесін пайдалану арқылы Kaspersky Security Center Linux жүйесіне көшіру

Kaspersky Security Center Linux-ке Kaspersky Security Center Windows басқару серверінің деректерін жылжыту үшін деректердің сақтық көшірмесін пайдалануға болады. Тасымалдау алдында Kaspersky Security Center Windows жүйесінің қажетті мүмкіндіктеріне Kaspersky Security Center Linux жүйесінде қолдау көрсетілетініне көз жеткізіңіз.

Түсінікті болуы үшін, басқару сервері деректерін сақтық көшірме жасау арқылы Kaspersky Security Center Linux жүйесіне көшіру жолы туралы оқулық бейне қолжетімді.

Шектеулер

- Келесі ДҚБЖ-лар арасында тасымалдауға болады:
  - Microsoft SQL Server → MySQL, MariaDB
  - Microsoft SQL Server → PostgreSQL, Postgres Pro
  - MySQL → MySQL, MariaDB
  - MariaDB → MySQL, MariaDB
  - PostgreSQL → PostgreSQL
  - Postgres Pro → Postgres Pro
- Microsoft SQL Server, MySQL немесе MariaDB дерекқорында сақталған басқару сервері деректерін MySQL немесе MariaDB жүйесіне көшіруге Kaspersky Security Center Windows жүйесінің кез келген қолдау көрсетілетін нұсқасынан Kaspersky Security Center Linux 15.2 немесе одан кейінгі нұсқасына тасымалдауға қолдау көрсетіледі.
- PostgreSQL дерекқорында сақталған басқару сервері деректерін PostgreSQL жүйесіне немесе Postgres Pro деректерін Postgres Pro жүйесіне көшіруге Kaspersky Security Center Windows 15.1 немесе одан кейінгі нұсқасынан Kaspersky Security Center Linux 16 немесе одан кейінгі нұсқасына көшіруге қолдау көрсетіледі.
- Microsoft SQL Server дерекқорында сақталған басқару сервері деректерін PostgreSQL немесе Postgres Pro жүйесіне көшіруге Kaspersky Security Center Windows 14.2 немесе одан кейінгі нұсқасынан Kaspersky Security Center Linux 15.3 немесе одан кейінгі нұсқасына көшіруге қолдау көрсетіледі.

PostgreSQL немесе Postgres Pro жүйесіне көшіруге қолдау көрсету үшін Kaspersky техникалық қолдау қызметіне сұрау салып, келесі патчтардың бірін орнатуыңыз керек:

- Kaspersky Security Center 14.2 Windows үшін: 14.2.0.26967-pf5
- Kaspersky Security Center 14.2 Windows негізіндегі Kaspersky Secure Mobility Management үшін: 14.2.0.48079-pf5
- Kaspersky Security Center 15.1 Windows үшін: 15.1.0.20748-pf2

  PostgreSQL немесе Postgres Pro жүйесіне көшіру Kaspersky Security Center Windows жүйесін 15.1.0.22239 нұсқасына жаңартқаннан кейін де қолжетімді болады.

- Kaspersky Security Center Windows және Kaspersky Security Center Linux үшін ДҚБЖ ретінде MySQL немесе MariaDB жүйесін пайдалансаңыз, `lower_case_table_names` параметрі ағымдағы және жаңа ДҚБЖ үшін сәйкес келуі керек.

  Деректердің сақтық көшірмесін жасамай тұрып, `lower_case_table_names` параметрін тексеріңіз. Содан кейін Kaspersky Security Center Linux үшін MySQL немесе MariaDB орнатқан кезде, бұл параметрді Windows жүйесіне арналған осы параметр үшін көрсетілген мәнге орнатуыңыз керек.

Алдын ала талаптар

Бастамас бұрын, **арнайы сертификатқа қойылатын талаптарды тексеріңіз**.

Егер сіз өздігінен қол қойылған сертификаттың орнына арнайы сертификатты пайдалансаңыз, Kaspersky Security Center Linux жүйесін кейінгі нұсқасына жаңартпас бұрын, сертификатта Субъектінің балама атауы (SAN) бар екеніне көз жеткізуіңіз керек. Олай болмаса, Kaspersky Security Center Linux жүйесін жаңартпас бұрын сертификатты ауыстыру маңызды. Әйтпесе, жаңартудан кейін Web Console веб-консоліне кіре алмайсыз.

Сертификатта SAN бар екеніне көз жеткізу үшін:

1. Басқару сервер орнатылған құрылғыда келесі пәрменді орындаңыз:

   - Linux құрылғысы үшін:

     ```
     sudo openssl x509 -in /var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer -noout
     -ext subjectAltName
     ```

   - Windows құрылғысы үшін:

     ```
     certutil -dump %ProgramData%\KasperskyLab\adminkit\1093\cert\klserver.cer
     ```

2. Пәрмен шығысында Субъектінің балама атауының бар екеніне және Басқару сервері құрылғысының мекенжайын қамтитынына көз жеткізіңіз.

3. Егер Тақырыптың балама атауы болмаса, klsetsrvcert утилитасын пайдаланып, реттелетін сертификатыңызды талаптарға сай келетін сертификатпен ауыстырыңыз.

Кезеңдер

Басқару сервері деректерінің сақтық көшірмесін пайдалану арқылы тасымалдау кезең-кезеңімен жүзеге асырылады:

1. **Басқару серверіне кіруге болатын әкімшінің ішкі пайдаланушы есептік жазбасы бар екенін тексеру**

   Әкімшінің есептік жазбасы Kaspersky Security Center Linux басқару серверіне кіру үшін пайдаланылады. Сізде бұл есептік жазба болмаса және тек жергілікті Windows есептік жазбасымен немесе домен есептік жазбасымен кірсеңіз, сақтық көшірмені қалпына келтіргеннен кейін Kaspersky Security Center Linux басқару серверіне кіре алмайсыз. Kaspersky Security Center Linux басқару сервері жергілікті Windows есептік жазбасын пайдалану арқылы жүйеге кіруге қолдау көрсетпейді. Домен есептік жазбасы арқылы кіруге болады, бірақ ол үшін басқару серверінің қосымша конфигурациясы қажет болуы мүмкін.

   Сізде әкімшінің есептік жазбасы болмаса, kladduser утилитасын пайдалану арқылы сақтық көшірмені қалпына келтіргеннен кейін осы есептік жазбаны жасау керек болады.

2. **Kaspersky Security Center Windows басқару сервері деректерінің жаңартылған сақтық көшірмесін жасау**

   Kaspersky Security Center Windows және Kaspersky Security Center Linux үшін пайдаланылатын ДҚБЖ түріне байланысты келесі әрекеттердің бірін орындаңыз:

   - MySQL немесе MariaDB жүйесін MySQL немесе MariaDB-ге көшіру үшін: klbackup утилитасын пайдаланып, сақтық көшірме жасаңыз немесе басқару сервері орнатылған құрылғыда деректердің сақтық көшірмесін жасау тапсырмасын орындаңыз.

   - PostgreSQL-ден PostgreSQL-ге және Postgres Pro-дан Postgres Pro-ға: klbackup утилитасын пайдалану арқылы сақтық көшірме немесе Басқару сервері орнатылған құрылғыда деректердің сақтық көшірмесін жасау тапсырмасын жасаңыз.

   - Microsoft SQL серверін MySQL немесе MariaDB жүйесіне тасымалдау үшін: klbackup утилитасы көмегімен сақтық көшірме жасаңыз, **MySQL/MariaDB пішіміне көшіру** опциясы қосылып тұруы керек.

   - Microsoft SQL серверін PostgreSQL немесе Postgres Pro жүйесіне көшіру үшін:

     1. PostgreSQL және Postgres Pro жүйесіне көшіруді қолдау үшін басқару серверіне арналған патчты орнатыңыз. Бұл патчты алу үшін Kaspersky техникалық қолдау қызметіне хабарласыңыз.

        Kaspersky Security Center 15.1 Windows жүйесінде патчты орнатудың орнына 15.1.0.22239 нұсқасына жаңартуға болады.

     2. klbackup утилитасын пайдалану арқылы сақтық көшірме жасаңыз.

        Егер пәрмен жолынан klbackup іске қоссаңыз, `-migrate postgres` пайдаланыңыз жалаушасын пайдаланыңыз.

        Klbackup интерфейсін пайдалансаңыз, **Postgres-ке көшіру форматы** опциясын қосыңыз.

   Сақтық көшірмені жасағаннан кейін Kaspersky Security Center Windows басқару серверін желіден ажыратыңыз.

3. **Kaspersky Security Center Linux орнату үшін жаңа құрылғыны дайындау**

Сценарийдің осы қадамында келесі әрекеттерді орындаңыз:

1. Басқару сервері орнатылатын жаңа құрылғыны таңдаңыз. Бұл құрылғы аппараттық және бағдарламалық жасақтама талаптарына сай болуы керек. Басқару серверінде қолданылатын порттардың қолжетімді екеніне көз жеткізіңіз.

2. Жаңа құрылғыға сол мекенжайды тағайындаңыз.

   Жаңа басқару серверіне NetBIOS атауын, FQDN және статикалық IP мекенжайын тағайындауға болады. Бұл желілік агенттер орналастырылған кезде желілік агенттің орнату бумасында басқару серверінің қандай мекенжайы орнатылғанына байланысты. Сондай-ақ желілік агент қосылатын басқару серверін анықтайтын қосылым мекенжайын пайдалануға болады (бұл мекенжайды klnagchk утилитасын қолданып, басқарылатын құрылғыларда алуға болады).

4 ДҚБЖ орнату және конфигурациялау

Сценарийдің осы қадамында келесі әрекеттерді орындаңыз:

1. Оңтайлы өнімділікті қамтамасыз ететін ДҚБЖ түрін таңдаңыз. Желіге қосылған құрылғылардың санын, желі топологиясын және желідегі жұмыс жүктемесін ескеріңіз. Кез келген қолдау көрсетілетін ДҚБЖ таңдай аласыз.

2. Сақтық көшірме жасау кезінде таңдалған ДҚБЖ түріне сәйкес ДҚБЖ орнатыңыз. Таңдалған ДҚБЖ жүйесін қалай орнату керектігі туралы мәліметтер оның құжаттамасында келтірілген.

   IAM үшін дерекқорды қолмен жасаңыз.

   > Дерекқордың жаңа нұсқасы ағымдағы нұсқадан төмен болмауы керек.

3. Kaspersky Security Center Linux-пен жұмыс істеу үшін ДҚБЖ-ны конфигурациялаңыз:

   - Kaspersky Security Center Linux нұсқасымен жұмыс істеу үшін MariaDB x64 серверінің конфигурациясы
   - Kaspersky Security Center Linux бағдарламасымен жұмыс істеу үшін PostgreSQL немесе Postgres Pro серверін конфигурациялау
   - Kaspersky Security Center Linux нұсқасымен жұмыс істеу үшін MySQL x64 серверінің конфигурациясы

5 Kaspersky Security Center Linux орнату

Kaspersky Security Center Linux жүйесін жаңа құрылғыға орнатыңыз.

Орнату кезінде жасалған әкімшінің ішкі пайдаланушы есептік жазбасы, сондай-ақ сақтық көшірмеден басқару серверінің деректерін қалпына келтірмей тұрып жасалған басқа нысандар (топтар, саясаттар, тапсырмалар, пайдаланушылар) қалпына келтіргеннен кейін жоғалады. Бұл нысандар сақтық көшірмеде қамтылған нысандармен ауыстырылады.

6 Сақтық көшірмеден басқару сервер деректерін қалпына келтіру

Сценарийдің осы қадамында келесі әрекеттерді орындаңыз:

1. klbackup утилитасын пайдалану арқылы жаңа құрылғыда басқару сервері деректерін қалпына келтіріңіз.

   > PostgreSQL шектеулеріне байланысты басқару сервері ДҚБЖ-ға қосылу үшін пайдаланатын есептік жазбаға PostgreSQL суперпайдаланушы артықшылықтарын уақытша беруіңіз қажет.

2. Сізде Kaspersky Security Center Windows басқару серверіне кірген әкімшінің ішкі пайдаланушы есептік жазбасы болмаса және жергілікті Windows есептік жазбасын немесе домен есептік жазбасын

пайдалансаңыз, kladduser утилитасын пайдаланып, әкімші есептік жазбасын келесідей жасаңыз:

`/opt/kaspersky/ksc64/sbin/kladduser -n kscadmin -p <құпиясөз>`

мұндағы <құпиясөз> параметрі келесі талаптарға сәйкес келеді:

- Пайдаланушының құпиясөзі 8 таңбадан кем немесе 256 таңбадан аспауы керек.
- Құпиясөзде төмендегі тізімдегі кемінде үш топтың таңбалары болуы керек:
  - Бас әріптер (A-Z)
  - Кіші әріптер (a-z)
  - Сандар (0-9)
  - Арнайы таңбалар (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)

7. **Басқару сервері және IAM сервері арқылы сертификатты тексеруді конфигурациялау.**

8. **Kaspersky Security Center Web Console орнату және басқару серверін конфигурациялау**

   Сценарийдің осы қадамында келесі әрекеттерді орындаңыз:

   1. Kaspersky Security Center Web Console веб-консолін орнатыңыз.

      Kaspersky Security Center Web Console бұрын орнатылған болса, оны сол жауап файлымен қайта орнатыңыз.

      Әкімшінің ішкі пайдаланушы есептік жазбасы арқылы Kaspersky Security Center Web Console-ге кіріңіз.

      Деректерді жұмысқа дайындау процесі басқару серверінің деректерін қалпына келтіргеннен кейін әдетте 15 минутқа дейін созылады, бірақ уақыт аппараттық жасақтама өнімділігіне және басқару сервері деректерінің өлшеміне байланысты. Осы уақыт ішінде Kaspersky Security Center Web Console қосылмауы және қателерді көрсетуі мүмкін.

   2. Дерекқордағы деректерді жұмысқа дайындау аяқталған кезде, басқару серверінің негізгі мүмкіндіктерінің жұмыс істейтінін тексеріңіз. Басқару сервері басқарылатын құрылғылармен синхрондалатынын және басқару сервері деректерінің қалпына келтірілгенін тексеріңіз.

   3. Домен құрылымы, пайдаланушы есептік жазбалары, қауіпсіздік топтары және домендерге қосылған құрылғылардың DNS атаулары туралы ақпаратты қалпына келтіру үшін домен контроллерлеріне сауалнама жүргізіңіз.

   4. Көшірілген тапсырмаларды қарап шығыңыз. Егер олардың кез келген параметрі Windows файл жолын қамтыса, оны тиісті Linux файл жолымен ауыстырыңыз.

   5. Қажет болса, алдыңғы құрылғыдан басқару сервері мен дерекқор серверін жойыңыз.

      Бір желіде бірдей қосылым мекенжайын және басқару сервер сертификатын ортақ пайдаланатын бірнеше басқару сервері болмауы керек.

Әкімші Kaspersky Security Center Linux жүйесінде қолдау көрсетілетін функцияларды ескере отырып, Kaspersky Security Center Windows жүйесінде болған басқарылатын құрылғыларға және басқару серверінің деректеріне қол жеткізе алады.

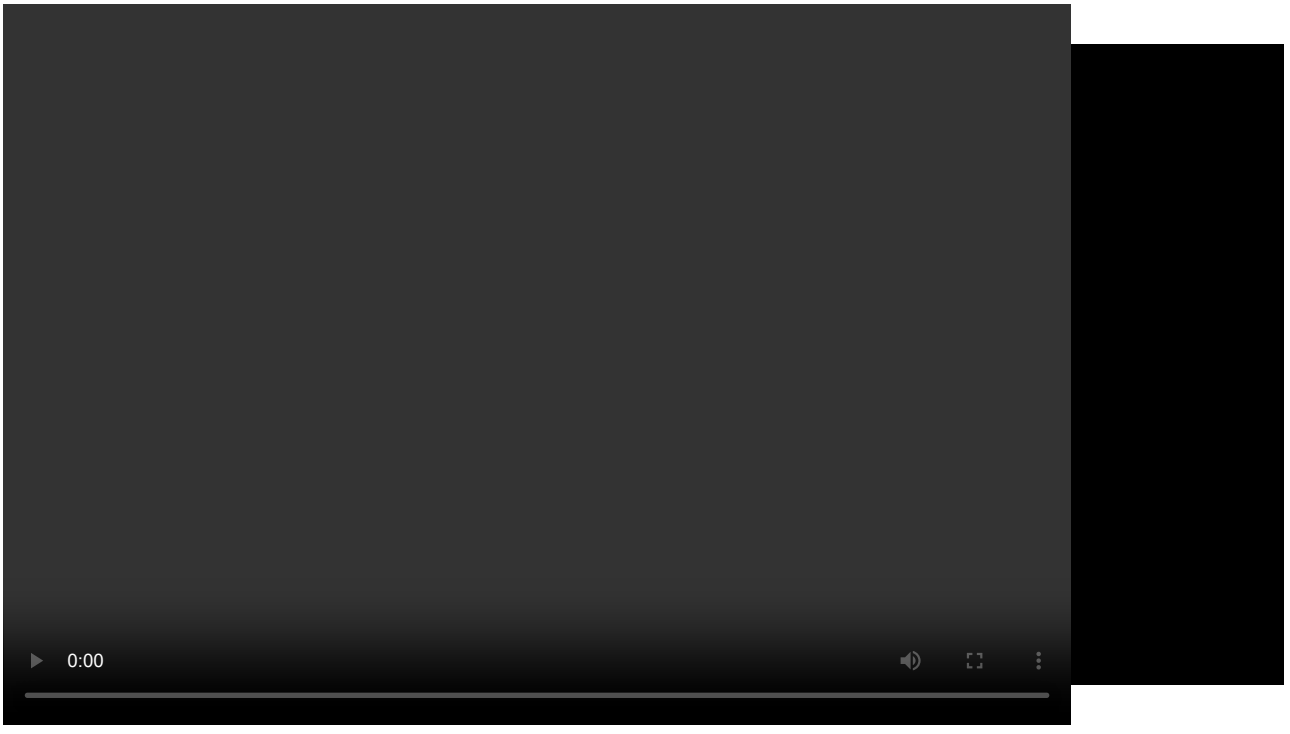
Оқулық бейне: басқару сервері деректерінің сақтық көшірмесін жасау арқылы Kaspersky Security Center Linux жүйесіне көшіру

Басқару сервері деректерінің сақтық көшірмесін (klbackup утилитасымен) пайдалану арқылы Kaspersky Security Center Windows басқару серверінің деректерін Kaspersky Security Center Linux жүйесіне көшіру жолын білу үшін бейнені көріңіз.

PostgreSQL немесе Postgres Pro жүйесіне көшіруге қолдау көрсету үшін Kaspersky техникалық қолдау қызметіне сұрау салып, келесі патчтардың бірін орнатуыңыз керек:

- Kaspersky Security Center 14.2 Windows үшін: 14.2.0.26967-pf5
- Kaspersky Security Center 14.2 Windows негізіндегі Kaspersky Secure Mobility Management үшін: 14.2.0.48079-pf5
- Kaspersky Security Center 15.1 Windows үшін: 15.1.0.20748-pf2

PostgreSQL немесе Postgres Pro жүйесіне көшіру Kaspersky Security Center Windows жүйесін 15.1.0.22239 нұсқасына жаңартқаннан кейін де қолжетімді болады.



Басқару сервері деректерінің сақтық көшірмесін жасау арқылы Kaspersky Security Center Linux жүйесіне көшіру Бейне

Kaspersky Security Center Linux серверіне тасымалдау шеберімен тасымалдау

Осы сценарий арқылы басқару тобының құрылымын, сонымен қатар басқарылатын құрылғыларды және топтың басқа нысандарын (саясаттарды, тапсырмаларды, жаһандық тапсырмаларды, тегтерді және құрылғы таңдауларын) Kaspersky Security Center Windows жүйесінен Kaspersky Security Center Linux басқаруына тасымалдауға болады.

Шектеулер:

- Деректерді тек Kaspersky Security Center Windows 14.2 және одан жоғары нұсқасынан Kaspersky Security Center Linux 15 және одан жоғары нұсқасына тасымалдауға болады.
- Бұл сценарийді тек Kaspersky Security Center Web Console көмегімен орындауға болады.

Бастамай тұрып, Kaspersky Security Center Linux функциялары мен шектеулері туралы қосымша ақпарат алыңыз:

- Kaspersky Security Center Windows және Kaspersky Security Center Linux екеуінің функционалды айырмашылықтары
- Kaspersky бағдарламаларының Kaspersky Security Center Linux қолдау көрсететін тізімі

Кезеңдер

Деректерді тасымалдау сценарийі келесі қадамдардан тұрады:

1. **Деректерді тасымалдау әдісін таңдаңыз**

   Деректерді Kaspersky Security Center Linux серверіне деректерді тасымалдау шеберімен тасымалдап жатырсыз. Деректерді тасымалдау шеберінің әрекеттері Kaspersky Security Center Windows және Kaspersky Security Center Linux басқару серверлері иерархияға реттелгеніне байланысты:

   - Басқару серверлерінің иерархиясы арқылы деректерді тасымалдау

     Kaspersky Security Center Windows Басқару сервері Kaspersky Security Center Linux Басқару серверіне бағынышты болса, осы параметрді таңдаңыз. Сіз деректерді тасымалдау процесін басқарасыз және Kaspersky Security Center Web Console веб-консолінің бір үлгісі шеңберінде Серверлер арасында ауысасыз. Бұл нұсқаны артық көрсеңіз, деректерді тасымалдау рәсімін жеңілдету үшін Басқару серверлерін иерархия түрінде ұйымдастыра аласыз. Мұны істеу үшін деректерді тасымалдауды бастамас бұрын иерархияны жасаңыз.

   - Деректерді экспорттау файлы (ZIP мұрағаты) арқылы тасымалдау

     Kaspersky Security Center Windows және Kaspersky Security Center Linux басқару серверлері иерархияда реттелмеген болса, осы параметрді таңдаңыз. Сіз деректерді тасымалдау процесін Kaspersky Security Center Web Console екі данасын, Kaspersky Security Center Windows жүйесінің бір данасын және Kaspersky Security Center Linux басқа данасын пайдалану арқылы басқарасыз. Бұл жағдайда сіз Kaspersky Security Center Windows жүйесінен экспорттау кезінде жасаған және жүктеп алған экспорттау файлын пайдаланасыз және бұл файлды Kaspersky Security Center Linux жүйесіне импорттайсыз.

2. **Kaspersky Security Center Windows Басқару серверінің сертификаты мен жеке кілтінің сақтық көшірмесін жасау (қосымша қадам)**

   Сақтық көшірмеден Басқару серверінің сертификаты мен жеке кілтін қалпына келтіру арқылы басқарылатын құрылғыларды Kaspersky Security Center Linux Басқару серверінің басқаруына орналастырғыңыз келуі мүмкін. Бұл жағдайда Kaspersky Security Center Windows басқару серверінің сертификаты мен жеке кілтінің сақтық көшірмесін жасаңыз. Содан кейін, 6-қадамда сертификат пен жеке кілтті қалпына келтіру керек.

3. **Kaspersky Security Center Windows жүйесінен деректерді экспорттау**

   Kaspersky Security Center Windows жүйесін ашып, деректерді тасымалдау шеберін іске қосыңыз.

4. **Деректерді Kaspersky Security Center Linux бағдарламасына импорттау**

   Экспортталған деректерді Kaspersky Security Center Linux жүйесіне импорттау үшін деректерді тасымалдау шеберімен жұмыс істеуді жалғастырыңыз. Серверлер иерархияға ұйымдастырылған болса, импорттау сол шеберде сәтті экспорттаудан кейін автоматты түрде басталады. Серверлер иерархияда орналаспаса, Kaspersky Security Center Linux жүйесіне ауысқаннан кейін, деректерді тасымалдау шеберімен жұмыс істеуді жалғастырасыз.

5. **Kaspersky Security Center Windows жүйесінен Kaspersky Security Center Linux жүйесіне нысандар мен параметрлерді қолмен тасымалдау үшін қосымша қадамдарды орындау (қосымша қадам)**

   Сондай-ақ деректерді тасымалдау шебері арқылы тасымалдау мүмкін емес нысандар мен параметрлерді тасымалдауға болады. Мысалы, қосымша келесі әрекеттерді орындауға болады:

   - Басқару сервері және басқарылатын қолданбалар пайдаланатын лицензия кілттерін тасымалдаңыз
   - Басқару серверінің жаһандық тапсырмаларын конфигурациялау
   - Желілік агент саясаты параметрлерін конфигурациялау
   - Бағдарламаларды орнату пакеттерін жасау
   - Виртуалды басқару серверлерін жасау
   - Құрылғыларды жылжыту ережелерін конфигурациялау
   - Құрылғыларға автоматты түрде тег қою ережелерін конфигурациялау
   - Бағдарламалар санаттарын жасау
   - Тарату нүктелерін тағайындау және конфигурациялау

     Тарату нүктесі ретінде әрекет ететін құрылғыны басқа басқару серверіне жылжытсаңыз, тарату нүктесінің аумағына кіретін құрылғылар автоматты түрде жылжытылмайды. Әрбір құрылғыны жеке жылжыту керек. Тарату нүктесі шлюз ретінде әрекет етсе, тарату нүктесі енді шлюз ретінде қызмет етпеуі үшін, `# /opt/kaspersky/klnagent64/bin/setup/postinstall.pl` сценарийін іске қосу керек.

6. **Импортталған басқарылатын құрылғыларды Kaspersky Security Center Linux басқаруына жылжыту**

   Деректерді тасымалдауды аяқтаңыз, импортталған басқарылатын құрылғыларды Kaspersky Security Center Linux басқаруына жылжытыңыз. Келесі әдістердің бірін пайдалана аласыз:

   - klmover утилитасын пайдалану арқылы

     klmover утилитасын пайдаланыңыз және жаңа басқару сервері үшін қосылым параметрлерін көрсетіңіз.

- *Басқару серверін өзгерту* тапсырманың көмегімен

  Басқару серверін өзгерту тапсырмасын жасап, импортталған басқарылатын құрылғыларды, жаңа Басқару серверін және басқа тапсырма параметрлерін көрсетіңіз. Содан кейін басқарылатын құрылғыларды Kaspersky Security Center Linux Басқару серверінің басқаруына орналастыру тапсырмасын орындаңыз.

- Жою (егер орнатылған болса), содан кейін басқарылатын құрылғыларда Желілік агентін орнату арқылы

  Желілік агентті орнату пакетін жасаңыз және орнату пакетінің сипаттарында жаңа басқару сервері үшін қосылым параметрлерін көрсетіңіз. Импортталған басқарылатын құрылғыларда Network Agent бағдарламасын жойыңыз, содан кейін қашықтан орнату тапсырмасын пайдаланып, осы құрылғыларға желілік агентті орнату үшін орнату бумасын пайдаланыңыз. Сондай-ақ желілік агентті жергілікті түрде орнату үшін автономды орнату бумасын жасауға және пайдалануға болады. Толық ақпаратты Kaspersky Security Center Linux басқаруындағы басқарылатын құрылғыларды ауыстыру бөлімінен қараңыз.

- Сертификатты және басқару серверінің жеке кілтін сақтық көшірмеден қалпына келтіру арқылы (тек Kaspersky Security Center Linux 15.1 және одан кейінгі нұсқасына тасымалдау үшін)

  Kaspersky Security Center Linux басқару сервері бар құрылғыға Kaspersky Security Center Windows басқару серверінікімен бірдей желі мекенжайын тағайындаңыз. Басқару сервері сертификатын және 2-қадамда сақталған сақтық көшірмеден жеке кілтті қалпына келтіру үшін klbackup утилитасын `-cert_only` параметрімен іске қосыңыз. Пәрмен жолында келесі пәрменді орындаңыз: `/opt/kaspersky/ksc64/sbin/klbackup -path <басқару сервері сертификатының сақтық көшірме жолы> -restore -cert_only`. Қосымша ақпарат алу үшін Басқа басқару серверінің басқаруымен басқарылатын құрылғыларды ауыстыру үшін klbackup утилитасын пайдалану бөлімін қараңыз.

7. **Желілік агентті соңғы нұсқаға жаңартыңыз**

   Linux үшін желілік агентті Kaspersky Security Center нұсқасымен бірдей нұсқаға жаңарту ұсынылады.

8. **Басқарылатын құрылғылардың жаңа басқару серверінде көрінетініне көз жеткізіңіз**

   Kaspersky Security Center Linux Басқару серверінде басқарылатын құрылғылар тізімін ашыңыз (**Активтерді басқару** → **Активтер (құрылғылар)**) және **Көзге көрінетін**, **Желілік агент орнатылған** және **Басқару серверіне соңғы қосылу уақыты** бағандарындағы мәндерді тексеріңіз.

Деректерді тасымалдаудың басқа әдістері

Тасымалдау шеберінен басқа, ағымдағы нысандарды тасымалдаудың басқа да әдістері бар, бірақ бұл әдістер тек саясаттар мен тапсырмаларды тасымалдауға мүмкіндік береді.

- Тапсырмаларды Kaspersky Security Center Windows жүйесінен экспорттаңыз, содан кейін Kaspersky Security Center Linux жүйесіне импорттаңыз.

- Белгілі бір саясаттарды Kaspersky Security Center Windows жүйесінен экспорттаңыз, содан кейін саясаттарды Kaspersky Security Center Linux жүйесіне импорттаңыз. Байланыстырылған саясат профильдері таңдалған саясаттармен бірге экспортталады және импортталады.

Kaspersky Security Center Windows жүйесінен топтық нысандарды экспорттау

Басқарылатын құрылғыларды және басқа топ нысандарын қамтитын басқару тобының құрылымын Kaspersky Security Center Windows жүйесінен Kaspersky Security Center Linux жүйесіне тасымалдау үшін алдымен экспортталатын деректерді таңдап, экспорттау файлын жасау керек. Экспорттау файлы тасымалдағыңыз келетін барлық топ нысандары туралы ақпаратты қамтиды. Экспорттау файлы Kaspersky Security Center Linux жүйесіне кейіннен импорттау үшін пайдаланылады.

Сіз келесі нысандарды экспорттай аласыз:

- Басқарылатын бағдарламалардың тапсырмалары мен саясаттары
- Глобалдық тапсырмалар
- Пайдаланушылық құрылғы таңдаулары
- Басқару топтары құрылымы және оған кіретін құрылғылар
- Деректер жылжытылатын құрылғыларға тағайындалған тегтер

Экспорттауды бастау алдында Kaspersky Security Center Linux жүйесіне деректерді тасымалдау туралы жалпы ақпаратты оқыңыз. Деректерді тасымалдау тәсілін таңдаңыз: Kaspersky Security Center Windows және Kaspersky Security Center Linux Басқару серверлері иерархиясын пайдаланып немесе пайдаланбай.

Деректерді тасымалдау шебері арқылы басқарылатын құрылғылар мен байланыстырылған топтық нысандарды экспорттау үшін:

1. Kaspersky Security Center Windows және Kaspersky Security Center Linux басқару серверлері иерархияда реттелгеніне қарай, келесі әрекеттердің бірін орындаңыз:
   - Серверлер иерархияда орналасса, Kaspersky Security Center Web Console веб-консолін ашып, Kaspersky Security Center Windows Басқару серверіне ауысыңыз.
   - Серверлер иерархияда реттелмесе, Kaspersky Security Center Windows жүйесіне қосылған Kaspersky Security Center Web Console веб-консолін ашыңыз.
2. Бағдарламаның негізгі терезесінде **Операциялар** → **Тасымалдау** бөліміне өтіңіз.
3. Шеберді іске қосу үшін **Kaspersky Security Center Linux немесе Open Single Management Platform платформасына көшіру** тармағын таңдап, оның қадамдарын орындаңыз.
4. Экспорттағыңыз келетін басқару тобын немесе ішкі тобын таңдаңыз. Таңдалған басқару тобында немесе ішкі тобында 10 000-нан аспайтын құрылғы болуы керек екенін ескеріңіз.

5. Тапсырмалары мен саясаттары экспортталатын басқарылатын бағдарламаларды таңдаңыз. Тек Kaspersky Security Center Linux қолдайтын бағдарламаларды таңдаңыз. Қолдау көрсетілмейтін бағдарламалардың нысандары әлі де экспортталады, бірақ жұмыс істемейді.

6. Глобалдық тапсырмаларды, құрылғы таңдауларын және экспорттау есептерін таңдау үшін сол жақтағы сілтемелерді пайдаланыңыз. **Топ нысандары** сілтемесі пайдаланушылардың, ішкі пайдаланушылардың және қауіпсіздік топтарының рөлдерін, сондай-ақ бағдарламалардың пайдаланушы санаттарын экспорттаудан алып тастауға мүмкіндік береді.

Экспорттау файлы (ZIP мұрағаты) жасалды. Басқару сервері иерархиясын қолдау арқылы деректерді тасымалдайтыныңызға байланысты экспорттау файлы келесідей сақталады:

- Серверлер иерархияда реттелген болса, экспорттау файлы Kaspersky Security Center Web Console серверіндегі уақытша қалтаға сақталады.

- Серверлер иерархияда ұйымдастырылмаған болса, экспорттау файлы құрылғыңызға жүктеледі.

Басқару сервері иерархиясын қолдау арқылы деректерді тасымалдаған кезде, импорттау сәтті экспорттаудан кейін автоматты түрде басталады. Басқару сервері иерархиясының қолдауынсыз деректерді тасымалдаған кезде, сақталған экспорттау файлын Kaspersky Security Center Linux жүйесіне қолмен импорттауға болады.

Экспорттық файлын Kaspersky Security Center Linux жүйесіне импорттау

Kaspersky Security Center Windows жүйесінен экспорттаған басқарылатын құрылғылар, нысандар және олардың параметрлері туралы ақпаратты тасымалдау үшін оны Kaspersky Security Center Linux немесе Kaspersky кеңейтілген анықтау және әрекет ету сарапшысы қолданбасына импорттау қажет.

Деректерді тасымалдау шебері арқылы басқарылатын құрылғылар мен топтың байланыстырылған нысандарын импорттау үшін:

1. Kaspersky Security Center Windows және Kaspersky Security Center Linux басқару серверлері иерархияда реттелгеніне қарай, келесі әрекеттердің бірін орындаңыз:

   - Серверлер иерархияға реттелген болса, экспорттауды аяқтағаннан кейін деректерді тасымалдау шеберінің келесі қадамына өтіңіз. Бұл шеберде сәтті экспорттаудан кейін импорт автоматты түрде басталады (осы нұсқадың 2-қадамын қараңыз).

   - Серверлер иерархияға реттелмесе:

     a. Kaspersky Security Center Linux немесе Kaspersky кеңейтілген анықтау және әрекет ету сарапшысы қолданбасына қосылған Kaspersky Security Center Web Console ашыңыз.

     b. Бағдарламаның негізгі терезесінде **Операциялар** → **Тасымалдау** бөліміне өтіңіз.

     c. Kaspersky Security Center Windows жүйесінен экспорттау кезінде жасаған және жүктеп алған экспорттау файлын (ZIP мұрағаты) таңдаңыз. Экспорттау файлы жүктеле бастайды.

2. Экспорттау файлы сәтті жүктелгеннен кейін, импорттауды жалғастыра аласыз. Экспортталатын басқа файлды көрсеткіңіз келсе, **Өзгерту** сілтемесін басып, қажетті файлды таңдаңыз.

3. Kaspersky Security Center Linux басқару топтардың бүкіл иерархиясы көрсетіледі.

   Экспортталған басқару топтың нысандарын (басқарылатын құрылғылар, саясаттар, тапсырмалар және басқа топ нысандары) қалпына келтіргіңіз келетін мақсатты басқару топтың жанындағы жалаушаны белгілеңіз.

4. Топтық нысандарды импорттау басталады. Импорттау кезінде деректерді тасымалдау шеберін жия алмайсыз немесе кез келген әрекеттерді бірге орындай алмайсыз. Нысандар тізіміндегі барлық тармақтардың жанындағы белгішелер (🔄) жасыл жалаушаларға (✓) ауысқанын және импорттау аяқталғанын күтіңіз.

5. Импорттау аяқталған кезде, экспортталған басқару топтың құрылымы, соның ішінде құрылғылар туралы ақпарат таңдалған мақсатты басқару топта пайда болады. Қалпына келтірілетін нысанның атауы бар нысанның атымен бірдей болса, қалпына келтірілген нысанға қосымша жұрнақ қосылады.

> Егер кейінге қалдырылған тапсырмада іске қосылатын есептік жазбаның деректері көрсетілсе, импорттау аяқталғаннан кейін тапсырманы ашып, құпиясөзді қайта енгізу қажет болады.

Импорттау сәтсіз болса, келесі әрекеттердің бірін орындауға болады:

- Басқару сервер иерархиясының қолдауы арқылы деректерді тасымалдау үшін экспорттық файлды қайта импорттауға болады.
- Басқару сервер иерархиясының қолдауынсыз деректерді тасымалдау үшін басқа экспорттау файлын таңдау мақсатында деректерді тасымалдау шеберін іске қосып, оны қайтадан импорттауға болады.

Экспорттау ауқымына кіретін топ нысандарының Kaspersky Security Center Linux жүйесіне сәтті импортталғанын тексеруге болады. Ол үшін **Активтерді басқару** бөліміне өтіп, импортталған нысандардың сәйкес бөлімшелерде көрсетілгеніне көз жеткізіңіз.

Импортталған басқарылатын құрылғылар **Басқарылатын құрылғылар** бөлімшесінде көрсетілетінін, бірақ олар желіде көрінбейтінін және желілік агент орнатылмағанын ескеріңіз (**Көзге көрінетін**, **Желілік агент орнатылған** бағандарындағы **Желілік агент іске қосулы** *Жоқ* мәні).

Деректерді тасымалдауды аяқтау үшін Kaspersky Security Center Linux басқаруындағы басқарылатын құрылғыларды ауыстыру қажет.

Kaspersky Security Center Linux басқаруындағы басқарылатын құрылғыларды ауыстыру

Басқарылатын құрылғылар, нысандар және олардың параметрлері туралы ақпаратты Kaspersky Security Center Linux жүйесіне сәтті импорттағаннан кейін, деректерді тасымалдауды аяқтау үшін Kaspersky Security Center Linux басқаруындағы басқарылатын құрылғыларды ауыстыру қажет.

Басқарылатын құрылғыларды Kaspersky Security Center Linux басқаруымен келесі жолдардың бірімен жылжытуға болады:

- klmover утилитасын пайдалану арқылы.
- *Басқару серверін өзгерту* тапсырмасын пайдалану.

- Сертификатты және Басқару сервердің жеке кілтін сақтық көшірмеден қалпына келтіру арқылы (тек Kaspersky Security Center Linux 15.1 және одан жоғары нұсқасына деректерді тасымалдау үшін).

  Қосымша ақпаратты деректерді тасымалдаудың негізгі сценарийінің 6-қадамынан қараңыз.

- Қашықтан орнату тапсырмасы көмегімен басқарылатын құрылғыларға желілік агентті орнату арқылы.

Желілік агентті орнату арқылы Kaspersky Security Center Linux басқаруындағы басқарылатын құрылғыларды ауыстыру үшін:

1. Kaspersky Security Center Linux басқаруына ауыстырылатын импортталған басқарылатын құрылғылардан Желілік агентті жойыңыз.

2. Kaspersky Security Center Windows Басқару серверіне ауысыңыз.

3. **Бағдарламалық жасақтаманы басқару** → **Орнату пакеттері** бөліміне өтіңіз және бар Желілік агентті орнату пакетінің сипаттарын ашыңыз.

   Желілік агентті орнату бумасы бумалар тізімінде болмаса, жаңасын жүктеп алыңыз.

   Сондай-ақ желілік агентті жергілікті түрде орнату үшін автономды орнату бумасын жасауға және пайдалануға болады.

4. **Параметрлер** қойыншасында **Қосылым** бөлімін таңдаңыз. Kaspersky Security Center Linux Басқару сервері үшін қосылым параметрлерін көрсетіңіз.

5. Импортталған басқарылатын құрылғылар үшін қашықтан орнату тапсырмасын жасаңыз, содан кейін қайта орнатылған желілік агентті орнату бумасын көрсетіңіз.

   Желілік агентті Kaspersky Security Center Windows Басқару серверін немесе тарату нүктесі ретінде әрекет ететін Windows жүйесімен жұмыс істейтін құрылғыны пайдаланып орнатуға болады. Басқару серверін пайдаланып жатсаңыз, **Басқару сервері арқылы операциялық жүйе ресурстарының көмегімен** параметрін қосыңыз. Тарату нүктесін пайдаланып жатсаңыз, **Тарату нүктелері арқылы операциялық жүйе ресурстарының көмегімен** параметрін қосыңыз.

6. Бағдарламаны қашықтан орнату тапсырмасын іске қосыңыз.

Қашықтан орнату тапсырмасын сәтті орындағаннан кейін, Kaspersky Security Center Linux Басқару серверіне өтіп, басқарылатын құрылғылар желіде көрінетініне және оларда желілік агент орнатылғанына және жұмыс істеп тұрғанына көз жеткізіңіз (**Көзге көрінетін**, **Желілік агент орнатылған** және **Желілік агент іске қосулы** бағандарындағы *Иә* мәні).

Басқару серверін конфигурациялау

Бұл бөлімде Басқару серверін конфигурациялау процесі мен сипаттары сипатталған.

Басқару серверінің қосылу мекенжайын конфигурациялау

Басқару серверінің қосылу мекенжайы — келесі мақсаттарда қолданылатын желі мекенжайы:

- Желілік агенттің орнату пакеттерін жасаған кездегі әдепкі мекенжай

  Желілік агентті орнатқаннан кейін, басқарылатын құрылғылар басқару серверіне осы мекенжайда қосылады.

- KSN прокси-серверінің мекенжайы ретінде

  Басқарылатын құрылғылар KSN прокси-серверіне осы мекенжай арқылы қосылады.

Басқару серверінің қосылу мекенжайын конфигурациялау үшін:

1. Негізгі мәзірдегі басқару серверінің атауын басыңыз.

   Басқару серверінің сипаттары терезесі ашылады.

2. **Жалпы** қойыншасында **Жалпы** бөлімін таңдаңыз.

3. Ашылған терезедегі **Басқару серверінің қосылу мекенжайы** өрісінде жаңа басқару серверінің қосылу мекенжайын көрсетіңіз.

   Қосылу мекенжайының максималды ұзындығы — 255 таңба.

   Басқару серверінің қосылу мекенжайын NetBIOS атауы, FQDN немесе басқару серверінің IP мекенжайы ретінде көрсетуге болады.

4. **Сақтау** түймесін басыңыз.

Көрсетілген мекенжай басқару серверінің мекенжайы және KSN прокси-серверінің мекенжайы ретінде қолданылады.

Kaspersky Security Center Web Console веб-консолін Басқару серверіне қосу параметрлерін конфигурациялау

Kaspersky Security Center Web Console-дің басқару серверіне қосылуын басқару серверінің сипаттары немесе басқару сервері саясатының параметрлері арқылы конфигурациялауға болады.

Басқару серверінің сипаттары арқылы қосылым порттарын орнату үшін:

1. Негізгі мәзірдегі басқару серверінің атауын басыңыз.

   Басқару серверінің сипаттары терезесі ашылады.

2. **Жалпы** қойыншасында **Қосылу порттары** бөлімін таңдаңыз.

3. Қажет болса, **Web Console-ге арналған SSL порты** параметрін немесе басқару серверінің басқа қосылым порттарын көрсетіңіз.

Таңдалған сервердің негізгі қосылым параметрлері көрсетілген.

Басқару серверінің саясат параметрлері арқылы қосылым порттарын орнату үшін:

1. Қолданбаның негізгі терезесінде **Активтерді басқару** → **Саясаттар** бөліміне өтіңіз.

2. Басқару сервері саясатының атауын басыңыз, содан кейін **Бағдарлама параметрлері** қойындысына өтіңіз.

3. Қажет болса, **Web Console-ге арналған SSL порты** параметрін немесе басқару серверінің басқа қосылым порттарын көрсетіңіз.

   Web Console-ге арналған ашық порт опциясын өшірсеңіз және бұл саясат параметрі құрылғыға қолданылса, Kaspersky Security Center Web Console арқылы басқару серверіне қосылу мүмкін болмайды. Бұл жағдайда қосылым тоқтатылады. Бұл саясат қолданылмайтын басқару сервері болса, бұл басқару серверіне Kaspersky Security Center Web Console арқылы қайта қосылуға болады.

Таңдалған сервердің негізгі қосылым параметрлері көрсетілген.

Kaspersky Security Center Linux бағдарламасына кіру үшін IP мекенжайларының рұқсат тізімін конфигурациялау

Әдепкісінше Kaspersky Security Center Linux жүйесіне кез келген құрылғыдан қосылуға рұқсат етіледі. Мысалы, Kaspersky Security Center Web Console Server-ді талаптарға сай кез келген құрылғыға орнатуға болады және Kaspersky Security Center Web Console Server жүйесі Kaspersky Security Center Linux-пен байланысады. Дегенмен басқару серверін қосылымдарға сіз көрсеткен IP мекенжайлары бар құрылғылардан ғана рұқсат етілетіндей етіп конфигурациялауға болады. Бұл жағдайда қаскүнем рұқсат тізіміне кірмейтін құрылғыға орнатылған Kaspersky Security Center Web Console Server арқылы Kaspersky Security Center Linux жүйесіне қосылуға әрекеттенсе, ол Kaspersky Security Center Linux жүйесіне кіре алмайды.

IP мекенжайы пайдаланушы Kaspersky Security Center Linux қолданбасына кіргенде немесе Kaspersky Security Center Linux OpenAPI арқылы басқару серверімен өзара әрекеттесетін қолданбаны іске қосқанда тексеріледі. Бұл кезде құрылғыдағы қолданба басқару серверімен байланыс орнатуға тырысады. Құрылғының IP мекенжайы рұқсат етілгендер тізімінде болмаса, түпнұсқалық растама қатесі туындайды және KLAUD_EV_SERVERCONNECT оқиғасы Басқару серверімен қосылымның орнатылмағаны туралы хабарлайды.

Рұқсат етілген IP мекенжайлары тізіміне қойылатын талаптар

IP мекенжайлары келесі бағдарламалардың Басқару серверіне қосылу әрекеті кезінде ғана тексеріледі:

- Kaspersky Security Center Web Console Server сервері

  Kaspersky Security Center Linux жүйесіне Kaspersky Security Center Web Console арқылы кірсеңіз, операциялық жүйенің штаттық құралдары арқылы Kaspersky Security Center Web Console Server сервері орнатылған құрылғыдағы желілік экранды конфигурациялауға болады. Содан кейін, Kaspersky Security Center Web Console Server сервері басқа құрылғыда орнатылған кезде біреу бір құрылғыда Kaspersky Security Center Linux жүйесіне кіруге әрекеттенсе, желілік экран зиянкестердің араласуын болдырмауға көмектеседі.

- klakaut автоматтандыру нысандары арқылы Басқару серверімен өзара әрекеттесетін бағдарламалар.

- Kaspersky мақсатты шабуылдардан қорғау платформасы немесе Kaspersky Security for Virtualization сияқты OpenAPI арқылы Басқару серверімен өзара әрекеттесетін бағдарламалар.

Сондықтан, жоғарыда аталған бағдарламалар орнатылған құрылғылардың мекенжайларын көрсетіңіз.

Сіз IPv4 мекенжайлары мен IPv6 мекенжайларын орната аласыз. IP мекенжайлары ауқымдарын көрсетуге болмайды.

Рұқсат етілген IP мекенжайлары тізімін қалай жасауға болады

Егер сіз рұқсат етілген тізімді әлі орнатпаған болсаңыз, төмендегі нұсқауларды орындаңыз.

Kaspersky Security Center Linux бағдарламасына кіру үшін рұқсат етілген IP мекенжайларының тізімін жасау үшін:

1. Басқару сервері құрылғысында әкімші құқықтары бар есептік жазбамен пәрмен жолын іске қосыңыз.

2. Ағымдағы қалтаны Kaspersky Security Center Linux орнату қалтасына өзгертіңіз (әдетте /opt/kaspersky/ksc64/sbin).

3. root есептік жазбасында келесі пәрменді енгізіңіз:
   `klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "<IP addresses>" -t s`

   Жоғарыда аталған талаптарға сәйкес келетін IP мекенжайларын көрсетіңіз. Бірнеше IP мекенжайларын нүктелі үтірмен бөлу керек.

   Басқару серверіне тек бір құрылғының қосылуына рұқсат беру мысалы:

   `klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "192.0.2.0" -t s`

   Бірнеше құрылғыға Басқару серверіне қосылуға рұқсат беру мысалы:

   `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. Басқару сервері қызметін қайта іске қосыңыз.

Рұқсат етілген IP мекенжайларының тізімі сәтті конфигурацияланғанын Басқару серверіндегі Syslog Event Log журналынан білуге болады.

Рұқсат етілген IP мекенжайлары тізімін қалай өзгертуге болады

Сіз рұқсат етілген тізімді, оны жасау кезіндегідей өзгерте аласыз. Бұл үшін, дәл сол пәрменді орындаңыз және рұқсат етілгендердің жаңа тізімін көрсетіңіз:

```
klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "<IP
addresses>" -t s
```

Егер сіз рұқсат етілгендер тізімнен кейбір IP мекенжайларын жойғыңыз келсе, оны қайта жазыңыз. Мысалы, рұқсат етілгендер тізіміне келесі IP мекенжайлары кіреді: 192.0.2.0; 198.51.100.0; 203.0.113.0. 198.51.100.0 IP мекенжайын жойғыңыз келсе. Бұл үшін, пәрмен жолына келесі пәрменді енгізіңіз:

```
klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "192.0.2.0;
203.0.113.0" -t s
```

Басқару серверін қызметін қайта іске қосуды ұмытпаңыз.

Рұқсат етілген IP мекенжайларының конфигурацияланған тізімін қалай бастапқы мәнге келтіруге болады

Рұқсат етілген IP мекенжайларының конфигурацияланған тізімін бастапқы мәнге келтіру үшін:

1. root есептік жазбасында пәрмен жолына келесі пәрменді енгізіңіз:
   `klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "" -t s`
2. Басқару сервері қызметін қайта іске қосыңыз.

Осыдан кейін, IP мекенжайлары енді тексерілмейді.

Басқару серверінің интернетке қатынасу параметрлерін конфигурациялау

Kaspersky Security Network пайдалану, сондай-ақ Kaspersky Security Center Linux және Kaspersky басқарылатын қолданбалары үшін антивирустық дерекқорлар жаңартуларын жүктеу үшін интернетке қатынасуды конфигурациялау қажет.

Басқару серверінің интернетке қатынасу параметрлерін көрсету үшін:

1. Негізгі мәзірдегі басқару серверінің атауын басыңыз.

   Басқару серверінің сипаттары терезесі ашылады.

2. **Жалпы** қойыншасында **Интернет желісіне қатынасу параметрлері** бөлімін таңдаңыз.

3. Интернетке қосу үшін прокси-серверді қолдану керек болса, **Прокси-серверді пайдалану** параметрін қосыңыз. Параметр қосулы болса, параметрлерді енгізу өрістері қолжетімді болады. Прокси-серверге қосылудың келесі параметрлерін конфигурациялаңыз:

   - **Прокси-сервердің мекенжайы**

     Kaspersky Security Center Linux-ті интернетке қосу үшін прокси-сервер мекенжайы.

   - **Порт нөмірі**

     Kaspersky Security Center Linux прокси-қосылымы орнатылатын порт нөмірі.

   - **Жергілікті мекенжайларға арналған прокси-серверді айналып өту**

     Жергілікті желідегі құрылғыларға қосылған кезде прокси-сервер қолданылмайды.

   - **Прокси-сервердегі аутентификация**

     Жалауша қойылған болса, енгізу өрістерінде прокси-сервердегі түпнұсқалық растама үшін есептік деректерді көрсетуге болады.

     Прокси-серверді пайдалану жалаушасы қойылған болса, енгізу өрісі қолжетімді.

   - **Пайдаланушы аты**

     Прокси-серверге қосылатын пайдаланушы есептік жазбасы (**Прокси-сервердегі аутентификация** жалаушасы қойылған болса, өріс қолжетімді болады).

   - **Құпиясөз**

     Прокси-серверге қосылуға мүмкіндік беретін пайдаланушы құпиясөзі (**Прокси-сервердегі аутентификация** жалаушасы қойылған болса, өріс қолжетімді болады).

     Енгізілген құпиясөзді қарау үшін, **Көрсету** түймесін басып, оны қажетті уақыт бойы ұстап тұрыңыз.

Сондай-ақ, бағдарламаны жылдам іске қосу шебері арқылы интернетке қатынасуды конфигурациялуға болады.

Басқару серверлерінің иерархиясы

Кейбір клиенттік компаниялар, мысалы, MSP клиенттері бірнеше Басқару серверлерін пайдалана алады. Бірнеше шашыраңқы Серверлерді басқару ыңғайсыз, сондықтан оларды иерархияға біріктірген жөн. Linux операциялық жүйесі бар Басқару сервері Сервер иерархиясында Басты сервер ретінде де, Қосалқы сервер ретінде де жұмыс істей алады. Linux операциялық жүйесі бар Басты сервер Linux және Windows операциялық жүйелері бар Қосалқы серверлерді басқара алады. Windows операциялық жүйесінде жұмыс істейтін негізгі сервер Linux операциялық жүйесінде жұмыс істейтін қосалқы серверді басқара алады.

Екі Басқару сервері арасындағы "негізгі – қосалқы" өзара іс-қимылы келесі мүмкіндіктер ұсынады:

- Қосалқы Басқару сервер саясаттарды, тапсырмаларды, пайдаланушы рөлдерін және орнату пакеттерін негізгі Басқару серверден алады, параметрлердің қайталануы жойылады.
- Басқару сервердегі құрылғыны таңдауларға қосалқы Басқару серверлердегі құрылғылар қосылуы мүмкін.
- Басты Басқару сервердегі есептерге қосалқы Басқару серверлердегі деректер (соның ішінде егжей-тегжейлі) қосылуы мүмкін.
- Негізгі Басқару серверін Қосалқы Басқару сервері үшін жаңарту көзі ретінде пайдалануға болады.

Негізгі Басқару сервері жоғарыда берілген параметрлер аясында деректерді виртуалды емес, тәуелді басқару серверлерінен ғана алады. Бұл шектеулер негізгі басқару серверімен бір дерекқорды пайдаланатын виртуалды басқару серверлеріне қолданылмайды.

Басқару серверлерінің иерархиясы көптиістілік режиміне қолдау көрсетеді. Бұл режим негізгі әкімшіге бірнеше клиентті орталықтан дербес басқаруға мүмкіндік береді. Әрбір клиент ұйымы немесе кеңсе басқалардан оқшауланған және клиент деп аталады. Бірнеше басқарылатын құрылғыны байланыстырылған деректермен, параметрлермен, саясаттармен және тапсырмалармен бірге тенантқа бөлуге және пайдаланушы құқықтарын тенант арқылы конфигурациялауға болады.

Негізгі ұйымның инфрақұрылымына орнатылған негізгі басқару сервері негізгі тенант ретінде әрекет етеді. Негізгі басқару сервері қосалқы немесе виртуалдық басқару серверлеріне, оның оқшауланған тенанттарына өз оқиғаларын дербес қабылдауға және өңдеуге, сондай-ақ өз ресурстарымен, қызметтерімен және конфигурацияларымен жұмыс істеуге мүмкіндік береді.

Бірнеше клиент ұйымы бар қызмет провайдері әрбір клиент ұйымына дабылдарды біріктіру және жауап беру әрекеттерін қамтитын Kaspersky Security Center Linux функцияларын дербес қамтамасыз ете алады. Бұған қол жеткізу үшін қызмет провайдері әрбір клиент ұйымы үшін тенанттар ретінде қосалқы немесе виртуалдық басқару серверлерін қосады. Қызмет провайдері өз қызметкерлері мен ресурстары көмегімен қызметтерді жеткізеді.

Басқару серверлерінің иерархиясын жасау: қосалқы Басқару серверін қосу

Linux операциялық жүйесі бар Басқару сервері Сервер иерархиясында Басты сервер ретінде де, Қосалқы сервер ретінде де жұмыс істей алады. Linux операциялық жүйесі бар Басты сервер Linux және Windows операциялық жүйелері бар Қосалқы серверлерді басқара алады. Windows операциялық жүйесінде жұмыс істейтін негізгі сервер Linux операциялық жүйесінде жұмыс істейтін қосалқы серверді басқара алады.

Қосалқы Басқару серверін қосу (болашақ негізгі Басқару серверімен бірге орындалады)

Басқару серверін қосалқы Сервер ретінде қосып, осылайша "басты Сервер – қосалқы Сервер" иерархиясының қатынасын орнатуға болады.

Kaspersky Security Center Web Console арқылы қосылуға болатын Басқару серверін қосалқы Сервер ретінде қосу үшін:

1. Болашақ негізгі Басқару серверінің 13000 портының қолжетімді екеніне көз жеткізіңіз.

   Бұл порт иерархияны құрғаннан кейін негізгі және қосымша Басқару серверлері арасындағы өзара әрекеттесу үшін пайдаланылады.

2. Болашақ негізгі басқару серверінің сипаттарына өтіңіз.

   a. Негізгі мәзірден бөлім таңдаңыз (**Marketplace**, **Консольді шарлау** және **Параметрлер** бөлімдерінен басқа), содан кейін беттің жоғарғы жағындағы **Иерархияны көрсету** түймесін басыңыз.

   b. Ашылатын навигация панелінде тінтуір курсорын қажетті басқару серверінің үстіне апарып, параметрлер белгішесін (⚙) басыңыз.

      Сонымен қатар басқару серверінің атауын басуға болады, содан кейін негізгі мәзірде атауы көрсетілген кезде, сервер сипаттары терезесін ашу үшін оны негізгі мәзірде басыңыз.

3. Ашылған сипаттар терезесіндегі **Басқару серверлері** қойындысын басыңыз.

4. Басқару серверін қосқыңыз келетін басқару тобы атауының жанындағы жалаушаны қойыңыз.

5. Мәзірден **Қосалқы Басқару серверіне қосылу** тармағын таңдаңыз.

   Қосалқы Басқару серверін қосу шебері іске қосылады. Шебердің жұмысын жалғастыру үшін **Келесі** түймесін басыңыз.

6. Келесі өрістерді толтырыңыз:

   - **Қосалқы Басқару серверінің көрсетілетін атауы**

     Серверлер иерархиясында көрсетілетін қосалқы Басқару серверінің атауы. Сіз IP мекенжайын атау ретінде енгізе аласыз немесе мысалы, "1-топқа арналған қосалқы Сервер" сияқты атауды қолдана аласыз.

   - **Қосалқы Басқару серверінің мекенжайы (міндетті емес)**

     Қосалқы Басқару серверінің IP мекенжайын немесе домен атауын көрсетіңіз.

     Бұл параметр **Демилитаризацияланған аймақтағы негізгі Серверді қосалқы Серверге қосу** параметрі қосылған болса қажет.

   - **Басқару сервері SSL порты**

     Иерархияны құрғаннан кейін негізгі және қосалқы Басқару серверлері арасындағы өзара әрекеттесу үшін пайдаланылатын SSL портының нөмірін көрсетіңіз. Әдепкі бойынша 13000-порт орнатылған.

   - **Басқару сервері API порты**

     Web Console OpenAPI арқылы қосалқы Басқару серверінен қосылымдарды алу үшін пайдаланатын порттың нөмірі. Әдепкі бойынша 13299-порт орнатылған.

     Иерархияны құру кезінде Web Console болашақ қосалқы Басқару серверіне қосылады, тіркелгі деректерін сұрайды, ашық сертификатты алады және бастапқы орнатуды орындайды.

     Басқару серверінің иерархиясы құрылғаннан кейін, 13299 порты енді пайдаланылмайды. Басқару серверлері 13000 порты арқылы өзара әрекеттеседі.

   - **DMZ режимінде негізгі Басқару серверін қосалқы Басқару серверіне қосу**

     Қосалқы Басқару сервері демилитаризацияланған аймақта (DMZ) болса, осы параметрді таңдаңыз.

     Егер бұл параметр таңдалса, негізгі Басқару сервері қосалқы Басқару серверіне қосылуды бастайды. Әйтпесе, қосалқы Басқару сервері негізгі Басқару серверіне қосылуды бастайды.

   - **Прокси-серверді пайдалану**

     Қосалқы Басқару серверіне қосылу үшін прокси-серверді пайдаланып жатсаңыз, осы параметрді таңдаңыз.

     Бұл жағдайда прокси-сервердің келесі параметрлерін де көрсетуге болады:

     - **Прокси-сервердің мекенжайы**
     - **Пайдаланушы аты**
     - **Құпиясөз**

7. Қосылым параметрлерін белгілеңіз:

   - Болашақ негізгі Басқару серверінің мекенжайын енгізіңіз.
   - Егер болашақ қосалқы Басқару сервері прокси-серверді пайдаланса, прокси-серверге қосылу үшін прокси-сервер мекенжайын және пайдаланушы есептік деректерін енгізіңіз.

8. Болашақ қосалқы Басқару серверіне кіру құқығы бар пайдаланушының есептік деректерін енгізіңіз.

   Шебер аяқталды, болашақ қосалқы Басқару серверімен байланыс орнатылды және "негізгі/қосалқы" иерархиясы құрылды.

Негізгі және қосалқы Басқару серверлері арасындағы байланыс 13000-порт арқылы орнатылады. Негізгі Басқару серверінің тапсырмалары мен саясаттары алынды және қолданылды. Қосалқы Басқару сервері негізгі Басқару серверінде, ол қосылған басқару тобында көрсетіледі.

Қосылым келесі жағдайларда сәтсіз аяқталады:

- Қосылым параметрлері дұрыс емес.

  Параметрлерді тексеру немесе болашақ қосалқы Басқару серверінің сертификатын қолмен көрсету керек.

- Болашақ қосалқы Басқару сервері Kaspersky Security Center Linux автоматты түрде жасаған өзі қол қойған сертификат арқылы түпнұсқалығын растайды. Нәтижесінде, браузер өзігінен қол қойған сертификатты жүктеуге тыйым салуы мүмкін.

  Сіз келесі әрекеттердің бірін орындай аласыз:

  - Болашақ қосалқы Сервер үшін сіздің инфрақұрылымыңызда сенімді болып саналатын және пайдаланушы сертификаттарына қойылатын талаптарға сәйкес келетін сертификат жасаңыз.
  - Сенімді браузер сертификаттарының тізіміне болашақ қосалқы Сервердің өздігінен қол қойған сертификатын қосыңыз. Бұл параметрді пайдаланушы сертификатын жасай алмаған жағдайда ғана пайдалану ұсынылады. Сертификатты сенімді сертификаттар тізіміне қосу туралы ақпаратты браузеріңіздің құжаттамасынан қараңыз.

Қосалқы Басқару серверін қосу (болашақ қосалқы Басқару серверімен бірге орындалады)

Болашақ Қосалқы Басқару серверіне қосыла алмасаңыз (мысалы, ол уақытша өшірілген, қолжетімсіз немесе Қосалқы Басқару серверінің сертификат файлы өздігінен қол қойылғандықтан), Қосалқы Басқару серверін әлі де қосуға болады.

Kaspersky Security Center Web Console арқылы қосылуға қолжетімді емес Басқару серверін қосалқы Сервер ретінде қосу үшін:

1. Болашақ негізгі Басқару сервері сертификатының файлын болашақ қосалқы Басқару сервері орналасқан кеңсенің жүйелік әкімшісіне жіберіңіз. (Мысалы, файлды сыртқы құрылғыға жазуға немесе электрондық пошта арқылы жіберуге болады.)

   Сертификат файлы болашақ негізгі Басқару серверінде орналасқан, /var/opt/kaspersky/klnagent_srv/1093/cert/.

2. Болашақ қосалқы Басқару серверіне жауапты жүйелік әкімшіге мыналарды ұсыныңыз:

   a. Басқару серверінің атауын басыңыз.

   b. Ашылған сипаттар бетінде **Жалпы** қойыншасындағы **Басқару серверлерінің иерархиясы** бөліміне өтіңіз.

   c. **Бұл Басқару сервері иерархияда қосымша** параметрін таңдаңыз.

   d. **Негізгі Басқару серверінің мекенжайы** өрісінде болашақ негізгі Басқару серверінің желілік атауын енгізіңіз.

   e. **Шолу** түймесін басу арқылы болашақ негізгі Сервердің бұған дейін сақталған сертификат файлын таңдаңыз.

   f. Қажет болса, **DMZ режимінде негізгі Басқару серверін қосалқы Басқару серверіне қосу** белгішесін қойыңыз.

   g. Егер болашақ негізгі Басқару серверіне қосылу прокси-сервер арқылы орындалса, **Прокси-серверді пайдалану** параметрін таңдап, қосылым параметрлерін белгілеңіз.

   h. **Сақтау** түймесін басыңыз.

"Басты Сервер – қосалқы Сервер" қатынасы орнатылады. Басты Сервер 13000-портты пайдаланып қосалқы Серверден қосылымды қабылдай бастайды. Негізгі Басқару серверінің тапсырмалары мен саясаттары алынды және қолданылды. Қосалқы Басқару сервері негізгі Басқару серверінде, ол қосылған басқару тобында көрсетіледі.

Қосалқы Басқару серверлері тізімін қарау

Басқару серверлерінің (соның ішінде виртуалды) тізімін көру үшін:

1. Негізгі мәзірден бөлім таңдаңыз (**Marketplace**, **Консольді шарлау** және **Параметрлер** бөлімдерінен басқа).

2. Беттің жоғарғы жағындағы **Иерархияны көрсету** түймесін басыңыз.

Ашылатын навигация панелінде қосалқы (соның ішінде виртуалды) басқару серверлерінің тізімі көрсетіледі. Осы Басқару серверлерінің кез келгеніне оның атын басу арқылы өтуге болады.

Навигация панелін **IP ауқымдары** және **Жойылған нысандар** бөлімдерінен ашсаңыз, виртуалды басқару серверлеріне өте алмайсыз.
Басқару топтары да көрсетіледі. Навигация панелін келесі бөлімдерден ашсаңыз, топтар басқаруға қолжетімді болады: **Активтер (құрылғылар)**, **Саясаттар**, **Тапсырмалар** және **Тарату нүктелері**. Әйтпесе топтар сұр түсті болады.

Егер сіз Kaspersky Security Center Web Console веб-консоліндегі негізгі Басқару серверіне қосылған болсаңыз және қосалқы Басқару сервері басқаратын виртуалды Басқару серверіне қосыла алмасаңыз, келесі тәсілдердің бірін пайдалана аласыз:

- **Сенімді Басқару серверлері тізіміне қосалқы Серверді қосу арқылы қолданыстағы Kaspersky Security Center Web Console орнатуын өзгертіңіз**. Осыдан кейін, сіз виртуалды Басқару серверіне Kaspersky Security Center Web Console веб-консоліне қосыла аласыз.

  1. Kaspersky Security Center Web Console қолданбасы орнатылған құрылғыда әкімші құқықтары бар тіркелгі бойынша құрылғыңызда орнатылған Linux дистрибутивіне сәйкес келетін Kaspersky Security Center Web Console орнату файлын іске қосыңыз.

     Қолданбаның орнату шебері іске қосылады. Шебердің жұмысын жалғастыру үшін **Келесі** түймесін басыңыз.

  2. **Жаңарту** параметрін таңдаңыз.

  3. **Өзгеріс түрі** бетінде **Қосылым параметрлерін өзгерту** параметрін таңдаңыз.

  4. **Сенімді Басқару серверлері** қадамында қажетті қосалқы Басқару серверлерін қосыңыз.

  5. Соңғы қадамда, жаңа параметрлерді қолдану үшін **Өзгерту** түймесін басыңыз.

  6. Бағдарламаны орнату сәтті аяқталғаннан кейін **Дайын** түймесін басыңыз.

- Виртуалды Сервер құрылған қосалқы Басқару серверіне тікелей қосылу үшін Kaspersky Security Center Web Console пайдаланыңыз. Осыдан кейін, сіз Kaspersky Security Center Web Console веб-консолінде виртуалды Басқару серверіне ауыса аласыз.

Виртуалды Басқару серверлерін басқару

Бұл бөлімде виртуалды Басқару серверлерін қалай басқаруға болатындығы сипатталған:

- Виртуалды Басқару серверлерін жасау
- Виртуалды Басқару серверлерін қосу және өшіру
- Виртуалды Басқару сервері әкімшісін тағайындау
- Клиент құрылғылары үшін Басқару серверін ауыстыру
- Виртуалды Басқару серверлерін жою

Виртуалды Басқару серверін жасау

Виртуалды Басқару серверлерін жасауға және оларды басқару топтарына қосуға болады.

Виртуалды Басқару серверін құру кезінде, ол пайдаланушылар тізімін және негізгі Басқару серверінің барлық пайдаланушы құқықтарын иеленеді. Егер пайдаланушының басты Серверге қатынасу құқығы болса, онда бұл пайдаланушының виртуалды Серверге қатынасу құқығы да бар. Жасалғаннан кейін, серверлерге қол жеткізу құқықтарын өзіңіз конфигурациялайсыз.

Виртуалды Басқару серверін жасау және қосу үшін:

1. Негізгі мәзірдегі басқару серверінің атауын басыңыз.

2. Ашылған бетте **Басқару серверлері** қойыншасына өтіңіз.

3. Виртуалды Басқару серверін қосқыңыз келетін басқару тобын таңдаңыз.
   Виртуалды Басқару сервері құрылғыларды таңдалған топтан (оның ішінде ішкі топтардан) басқарады.

4. Мәзірден **Жаңа виртуалды Басқару сервері** тармағын таңдаңыз.

5. Ашылған бетте жаңа виртуалды Басқару серверінің сипаттарын белгілеңіз:

   - **Виртуалды Басқару серверінің атауы**.

   - **Басқару серверінің қосылу мекенжайы**

     Басқару серверінің атын немесе IP мекенжайын көрсетуге болады.

6. Пайдаланушылар тізімінен виртуалды Басқару сервері әкімшісін таңдаңыз. Қажет болса, қолданыстағы есептік жазбаны әкімші рөлін тағайындамас бұрын өзгертуге болады; жаңа есептік жазба да жасалуы мүмкін.

   Қажет болса, kladduser утилитасын пайдалану арқылы виртуалды басқару сервері әкімшісі ретінде әрекет ететін жаңа есептік жазбаны жасауға болады. Ол үшін келесі пәрменді пайдаланыңыз:

   `kladduser -n <пайдаланушы_атауы> -p <құпиясөз> -vs <виртуалды_сервер_атауы>`

   бұл жерде `виртуалды_сервер_атауы` — виртуалды басқару серверінің атауы.

7. **Сақтау** түймесін басыңыз.

Жаңа виртуалды Басқару сервері жасалды, басқару тобына қосылды және **Басқару серверлері** қойыншасында көрсетіледі.

Егер сіз Kaspersky Security Center Web Console веб-консоліндегі негізгі Басқару серверіне қосылған болсаңыз және қосалқы Басқару сервері басқаратын виртуалды Басқару серверіне қосыла алмасаңыз, келесі тәсілдердің бірін пайдалана аласыз:

- **Сенімді Басқару серверлері тізіміне қосалқы Серверді қосу арқылы қолданыстағы Kaspersky Security Center Web Console орнатуын өзгертіңіз**. Осыдан кейін, сіз виртуалды Басқару серверіне Kaspersky Security Center Web Console веб-консоліне қосыла аласыз.

  1. Kaspersky Security Center Web Console қолданбасы орнатылған құрылғыда әкімші құқықтары бар тіркелгі бойынша құрылғыңызда орнатылған Linux дистрибутивіне сәйкес келетін Kaspersky Security Center Web Console орнату файлын іске қосыңыз.

     Қолданбаның орнату шебері іске қосылады. Шебердің жұмысын жалғастыру үшін **Келесі** түймесін басыңыз.

  2. **Жаңарту** параметрін таңдаңыз.

  3. **Өзгеріс түрі** бетінде **Қосылым параметрлерін өзгерту** параметрін таңдаңыз.

  4. **Сенімді Басқару серверлері** қадамында қажетті қосалқы Басқару серверлерін қосыңыз.

5. Соңғы қадамда, жаңа параметрлерді қолдану үшін **Өзгерту** түймесін басыңыз.

6. Бағдарламаны орнату сәтті аяқталғаннан кейін **Дайын** түймесін басыңыз.

- Виртуалды Сервер құрылған қосалқы Басқару серверіне тікелей қосылу үшін Kaspersky Security Center Web Console пайдаланыңыз. Осыдан кейін, сіз Kaspersky Security Center Web Console веб-консолінде виртуалды Басқару серверіне ауыса аласыз.

Виртуалды Басқару серверін қосу және өшіру

Виртуалды Басқару серверін жасаған кезде, ол әдепкі бойынша қосылады. Оны кез келген уақытта өшіруге немесе қайта қосуға болады. Виртуалды Басқару серверін өшіру немесе қосу физикалық Басқару серверін өшіруге немесе қосуға тең.

Виртуалды Басқару серверін қосу немесе өшіру үшін:

1. Негізгі мәзірдегі басқару серверінің атауын басыңыз.

2. Ашылған бетте **Басқару серверлері** қойыншасына өтіңіз.

3. Қосқыңыз немесе өшіргіңіз келетін виртуалды Басқару серверін таңдаңыз.

4. Мәзірде **Виртуалды Басқару серверін қосу / өшіру** түймесін басыңыз.

Виртуалды Басқару серверінің күйі оның алдыңғы күйіне байланысты қосулы немесе өшірулі болып өзгереді. Жаңартылған күй Басқару сервері атауының жанында көрсетіледі.

Виртуалды Басқару сервері әкімшісін тағайындау

Ұйымыңызда виртуалды Басқару серверлерін пайдалансаңыз, әрбір виртуалды Басқару сервері үшін бөлек әкімші тағайындау қажет болуы мүмкін. Мысалы, бұл сіздің ұйымыңыздың жеке кеңселерін немесе бөлімдерін басқару үшін виртуалды Басқару серверлерін құрған кезде немесе сіз провайдер (MSP) болсаңыз және виртуалды Басқару серверлері арқылы клиенттеріңізді басқарсаңыз пайдалы болуы мүмкін.

Виртуалды Басқару серверін құру кезінде, ол пайдаланушылар тізімін және негізгі Басқару серверінің барлық пайдаланушы құқықтарын иеленеді. Егер пайдаланушының басты Серверге қатынасу құқығы болса, онда бұл пайдаланушының виртуалды Серверге қатынасу құқығы да бар. Жасалғаннан кейін, сіз Серверлерге қатынасу құқығын өзіңіз конфигурациялайсыз. Егер сіз тек виртуалды Басқару серверіне әкімші тағайындағыңыз келсе, әкімшінің негізгі Басқару серверінде қатынасу құқығы жоқ екеніне көз жеткізіңіз.

Сіз виртуалды Басқару серверіне әкімші рұқсаттарын беру арқылы виртуалды Басқару сервері әкімшісін тағайындайсыз. Сіз келесі жолдардың бірімен қажетті қатынасу құқықтарын бере аласыз:

- Әкімші үшін қатынасу құқықтарын қолмен конфигурациялаңыз.

- Әкімшіге бір немесе бірнеше пайдаланушы рөлдерін тағайындаңыз.

Kaspersky Security Center Web Console серверіне кіру үшін виртуалды Басқару серверінің әкімшісі виртуалды Басқару серверінің атауын, пайдаланушы атын және құпиясөзді көрсетеді. Kaspersky Security Center Web Console сервері әкімшінің түпнұсқалық растамасын орындайды және әкімшінің қатынасу құқығы бар виртуалды Басқару серверін ашады. Әкімші Басқару серверлері арасында ауыса алмайды.

Алдын ала талаптар

Келесі шарттардың орындалғанына көз жеткізіңіз:

- Виртуалды Басқару сервері жасалды.
- Негізгі Басқару серверінде, сізде виртуалды Басқару серверіне тағайындағыңыз келетін әкімші үшін есептік жазба жасалған.
- Сізде **Жалпы функционал** → **Пайдаланушы рұқсаттары** функционалдық аймағында **Нысан ACL параметрлерін өзгерту** құқығыңыз бар.

Қатынасу құқықтарын қолмен конфигурациялау

Виртуалды Басқару сервері әкімшісін тағайындау үшін:

1. Қажетті виртуалды басқару серверіне ауысу:

   a. Негізгі мәзірден бөлім таңдаңыз (**Marketplace**, **Консольді шарлау** және **Параметрлер** бөлімдерінен басқа), содан кейін беттің жоғарғы жағындағы **Иерархияны көрсету** түймесін басыңыз.

   b. Ашылатын навигация панелінде қажетті виртуалды басқару серверінің атауын басыңыз.

   > **IP ауқымдары** мен **Жойылған нысандар** бөлімдерінен виртуалды басқару серверіне ауысу мүмкін емес.

   Негізгі мәзірде басқару сервері сіз таңдағанға өзгереді.

2. Басқару серверінің атауын негізгі мәзірде басып, оның сипаттарына өтіңіз.

   Навигация панелінде тінтуір курсорын қажетті виртуалды басқару серверінің атауына апарыңыз, содан кейін параметрлер белгішесін (⚙) басыңыз.

   Басқару серверінің сипаттары терезесі ашылады.

3. **Қатынасу құқықтары** қойыншасында **Қосу** түймесін басыңыз.

   Негізгі Басқару сервері мен ағымдағы виртуалды Басқару сервері пайдаланушыларының бірыңғай тізімі ашылады.

4. Пайдаланушылар тізімінен виртуалды Басқару серверіне тағайындағыңыз келетін әкімші есептік жазбасын таңдап, **OK** түймесін басыңыз.

   Бағдарлама таңдалған пайдаланушыны пайдаланушылар тізіміне, **Қатынасу құқықтары** қойыншасына қосады.

5. Қосылған есептік жазбаның жанына жалаушаны қойып, **Қатынасу құқықтары** түймесін басыңыз.

6. Виртуалды Басқару серверінде әкімші құқықтарын конфигурациялаңыз.

Сәтті түпнұсқалық растамаүшін әкімшінің келесі құқықтары болуы керек:

- **Оқу** → **Жалпы функционал** функционалдық аймағындағы **Базалық функционалдылық** құқығы.
- **Оқу** → **Жалпы функционал** функционалдық аймағындағы **Виртуалды Басқару серверлері** құқығы.

Бағдарлама өзгертілген пайдаланушы құқықтарын әкімші есептік жазбасында сақтайды.

Бірнеше виртуалды Басқару серверлері әкімшісін тағайындау үшін:

1. Негізгі мәзірдегі басты Басқару серверінің атауын басыңыз.
2. Ашылған бетте « **Қатынасу құқықтары** қойындысына өтіп, **«Тағайындау»** түймесін басыңыз.

   Ашылған **Пайдаланушыларды немесе топтарды қосу** терезесінде әкімші ретінде тағайындағыңыз келетін пайдаланушының жанындағы құсбелгіні қойыңыз.
3. Пайдаланушы топтарын таңдау үшін **Топтар** қойындысына ауыса аласыз.
4. **Келесі** түймесін басыңыз.
5. Әкімші тағайындағыңыз келетін серверлерді таңдап, **«Келесі»** түймесін басыңыз.
6. Қажет болса, пайдаланушы үшін орнатқыңыз келетін әкімші рөлдерін таңдаңыз.

   Егер пайдаланушы үшін ағымдағы Басқару сервері үшін реттелетін рөлдерді орнатқыңыз келсе, қажетті басқару серверінің қасиеттеріне өтіп, **«Рөлдерді орнату»** түймесін басып, реттелетін рөлдерді таңдаңыз.
7. Өзгерістерді қолдану үшін **Аяқтау** түймесін басыңыз.

Таңдалған рөлдері бар әкімші енді бірнеше виртуалды Басқару серверлеріне тағайындалады.

Әкімшінің қатынасу құқықтарын қайтарып алу үшін:

1. Қажетті Басқару серверіне ауысу.
2. Негізгі мәзірдегі басқару серверінің атауын басыңыз.
3. Ашылған бетте **Қатынасу құқықтары** қойыншасына өтіңіз.
4. қатынасу құқықтарын қайтарып алғыңыз келетін пайдаланушының жанындағы құсбелгіні қойыңыз.
5. **Қайтарып алу** түймесін басып, әрекетіңізді растаңыз.

Таңдалған пайдаланушының қатынасу құқықтары қайтарып алынады.

Пайдаланушы рөлдерін тағайындау арқылы қатынасу құқығын конфигурациялау

Сондай-ақ, сіз виртуалды Басқару сервері әкімшісіне пайдаланушы рөлі арқылы қатынасу құқығын бере аласыз. Мысалы, егер сіз бір виртуалды Басқару серверіне бірнеше әкімші тағайындағыңыз келсе, бұл пайдалы болуы мүмкін. Бұл жағдайда, сіз бірнеше әкімші үшін бірдей құқықтарды конфигурациялаудың орнына әкімші есептік жазбаларына бір немесе бірнеше пайдаланушы рөлдерін тағайындай аласыз.

Виртуалды Басқару сервері әкімшісін тағайындау мақсатында оған пайдаланушы рөлдерін тағайындау үшін:

1. Негізгі Басқару серверінде пайдаланушы рөлін жасаңыз және виртуалды Басқару серверінде әкімші ие болуы тиісті барлық қажетті қатынасу құқықтарын көрсетіңіз. Сіз бірнеше рөлдерді жасай аласыз, мысалы, әртүрлі функционалды аймақтарға қатынасуды бөлгіңіз келсе.

2. Қажетті виртуалды басқару серверіне ауысу:

   a. Негізгі мәзірден бөлім таңдаңыз (**Marketplace**, **Консольді шарлау** және **Параметрлер** бөлімдерінен басқа), содан кейін беттің жоғарғы жағындағы **Иерархияны көрсету** түймесін басыңыз.

   b. Ашылатын навигация панелінде қажетті виртуалды басқару серверінің атауын басыңыз.

   > **IP ауқымдары** мен **Жойылған нысандар** бөлімдерінен виртуалды басқару серверіне ауысу мүмкін емес.

   Негізгі мәзірде басқару сервері сіз таңдағанға өзгереді.

3. Әкімші есептік жазбаның жаңа рөлін немесе бірнеше рөлдерін тағайындаңыз.

Бағдарлама әкімші есептік жазбасының рөлін тағайындайды.

Нысан деңгейінде қатынасу құқықтарын конфигурациялау

Функционалды аймақ деңгейінде қатынасу құқықтарын тағайындаудан басқа, сіз виртуалды Басқару серверіндегі белгілі бір нысандарға, мысалы, белгілі бір басқару тобына немесе тапсырмаға қатынасуды конфигурациялай аласыз. Ол үшін, виртуалды Басқару серверіне ауысыңыз, содан кейін нысан сипаттарындағы қатынасу құқықтарын конфигурациялаңыз.

Клиент құрылғылары үшін Басқару серверін ауыстыру

Басқару серверін ауыстыру тапсырмасы көмегімен клиент құрылғыларын басқаратын басқару серверін басқа серверге ауыстыруға болады. Тапсырма аяқталғаннан кейін, таңдалған клиент құрылғылары көрсетілген Басқару серверінің басқаруында болады.

> Басқару серверіне қосылым шлюздері арқылы қосылған клиент құрылғыларында *Басқару серверін ауыстыру* тапсырмасын пайдалану мүмкін емес. Мұндай құрылғылар үшін Желілік агентті қайта конфигурациялау немесе желілік агентті қайта орнату және қосылым шлюзін көрсету керек.

Клиент құрылғылары жұмыс істейтін Басқару серверін басқа Сервермен ауыстыру үшін:

1. Бағдарламаның негізгі терезесінде **Тапсырмалар** бөліміне өтіңіз.

2. **Қосу** түймесін басыңыз.

   Жаңа тапсырма жасау шебері іске қосылады. Шебердің жұмысын жалғастыру үшін **Келесі** түймесін басыңыз.

3. Шебердің **Жаңа тапсырма параметрлері** қадамында келесі параметрлерді көрсетіңіз:

   a. **Бағдарлама** ашылмалы тізімінде **Kaspersky Security Center** опциясын таңдаңыз.

   b. **Тапсырма түрі** өрісінде **Басқару серверін ауыстыру** опциясын таңдаңыз.

   c. **Тапсырманың атауы** өрісінде жасап жатқан тапсырма атауын көрсетіңіз.

   Тапсырма атауы 100 таңбадан асуы және арнайы таңбаларды ("*<>?\:|) қамтуы мүмкін емес.

   d. Тапсырма тағайындалатын құрылғыларды таңдаңыз.

   - **Басқару тобына тапсырманы белгілеу**

     Тапсырма бұрын жасалған басқару тобына кіретін құрылғыларға тағайындалады. Бар топтардың бірін көрсетуге немесе жаңа топ құруға болады.

     Мысалы, хабар белгілі бір басқару тобындағы құрылғыларға арналған болса, пайдаланушыларға хабар жіберу тапсырмасын іске қосу үшін осы параметрді пайдалануға болады.

     Тапсырма Басқару тобына тағайындалса, **Қауіпсіздік** қойындысы тапсырма сипаттары терезесінде көрсетілмейді, себебі топтық тапсырмалар олар тиесілі болып саналатын қауіпсіздік топтарының параметрлеріне бағынады.

   - **Құрылғының мекенжайларын қолмен белгілеу немесе тізімнен импорттау**

     Сіз DNS атауларын, IP мекенжайларын, сондай-ақ тапсырманы тағайындауды қажет ететін құрылғылардың IP мекенжайы ауқымдарын белгілей аласыз.

     Бұл параметрді белгіленген ішкі желі үшін тапсырманы орындау үшін пайдалануға болады. Мысалы, сіз бухгалтерлердің құрылғыларына белгілі бір бағдарламаны орната аласыз немесе вирус жұқтыруы мүмкін ішкі желідегі құрылғыларды тексере аласыз.

   - **Құрылғы таңдауына тапсырманы белгілеу**

     Тапсырма құрылғы таңдауларына кіретін құрылғыларға тағайындалады. Қолданыстағы таңдаулардың бірін көрсетуге болады.

     Мысалы, операциялық жүйенің белгілі бір нұсқасы бар құрылғыларда тапсырманы іске қосу үшін осы параметрді пайдалануға болады.

4. Шебердің **Тапсырма ауқымы** қадамында басқару тобын, нақты мекенжайлары бар құрылғыларды немесе құрылғы таңдауын көрсетіңіз.

5. Шебердің келесі қадамында клиент құрылғыларына арналған басқару серверін өзгерту шарттарына келісетініңізді растаңыз.

6. Шебердің келесі қадамында таңдалған құрылғыларды басқару үшін қолданғыңыз келетін басқару серверін таңдаңыз:

   - **Басқа негізгі Басқару серверіне өзгертіңіз**

     Клиент құрылғыларын басқа негізгі басқару серверіне жылжыту үшін келесі басқару серверінің қосылым параметрлерін көрсетіңіз:

     1. **Басқару серверінің мекенжайы** өрісінде жаңа негізгі басқару серверінің мекенжайын көрсетіңіз.

     2. **Порт нөмірі** өрісінде басқару серверіне қосылу үшін порт нөмірін көрсетіңіз.

     Әдепкі бойынша 14000-порт орнатылған.

3. **SSL порты** өрісінде негізгі басқару серверінің SSL портының нөмірін көрсетіңіз.

   Әдепкі бойынша 13000-порт орнатылған.

4. Қажет болса, **Прокси-серверді пайдалану** опциясын қосыңыз.

   Бұл опция өшірілсе, құрылғыны басқару серверіне қосу үшін тікелей қосылым қолданылады.

   Бұл параметр қосылса, прокси сервер параметрлерін көрсетіңіз:

   - **Прокси-сервердің мекенжайы**
   - **Прокси-сервердің порты**

   Прокси-серверге аутентификация қажет болса, прокси-сервер қосылымы орнатылатын есептік жазбаның **Пайдаланушы аты** және **Құпиясөз** өрістерінде есептік жазбаның кіру деректерін көрсетіңіз. Прокси-сервердегі түпнұсқалық растама үшін ғана талап етілетін ең аз құқықтарға ие есептік жазба деректерін беру ұсынылады.

5. Қажет болса, жаңа басқару сервері сертификатын жүктеп салыңыз.

- **Осы негізгі сервердегі басқа виртуалды Басқару серверіне өзгертіңіз**

  Клиент құрылғыларын ағымдағы негізгі басқару серверіндегі виртуалды басқару серверіне жылжыту үшін осы опцияны таңдаңыз. Ол үшін **Виртуалды Басқару серверінің атауы** ашылмалы тізімінде қажетті виртуалды басқару серверін таңдаңыз.

7. Шебердің **Тапсырманы іске қосу үшін есептік жазбаны таңдау** қадамында есептік жазба параметрлерін көрсетіңіз:

   - **Әдепкі есептік жазба**

     Тапсырма, сол тапсырманы орындайтын бағдарлама орнатылған және іске қосылған сол есептік жазбамен іске қосылады.

     Әдепкі бойынша, осы нұсқа таңдалған.

   - **Есептік жазбаны көрсету**

     Есептік жазба және **Құпиясөз** өрістерінде тапсырма іске қосылуы тиісті есептік жазба деректерін көрсетіңіз. Есептік жазбада тапсырманы орындау үшін қажетті құқықтар болуы керек.

     - **Есептік жазба**

       Тапсырманы іске қосатын есептік жазба.

     - **Құпиясөз**

       Тапсырманы іске қосатын есептік жазбаның құпиясөзі.

8. Әдепкі тапсырма параметрлерін өзгерткіңіз келсе, шебердің **Тапсырманы жасауды аяқтау** қадамында **Жасап болған соң, тапсырма туралы мәліметтерді ашу** опциясын қосыңыз.

   Егер сіз бұл параметрді қоспасаңыз, тапсырма әдепкі бойынша белгіленген параметр мәндерімен жасалады. Әдепкі параметрлерді кез келген уақытта өзгертуге болады.

9. **Аяқтау** түймесін басыңыз.

   Тапсырма жасалып, тапсырмалар тізімінде көрсетіледі.

10. Тапсырма сипаттары терезесін ашу үшін жасалған тапсырманың атын басыңыз.

11. Әдепкі тапсырма параметрлерін өзгерткіңіз келсе, тапсырма сипаттары терезесінде қажеттіліктеріңізге сәйкес жалпы тапсырма параметрлерін көрсетіңіз.

12. **Сақтау** түймесін басыңыз.

    Тапсырма жасалды және конфигурацияланды.

13. Жасалған тапсырманы іске қосыңыз.

Тапсырма аяқталғаннан кейін, ол жасалған клиент құрылғылары тапсырма параметрлерінде көрсетілген басқару серверінің басқаруына өтеді.

Виртуалды Басқару серверін жою

Виртуалды Басқару сервері жойылған кезде, Басқару серверінде жасалған барлық нысандар, соның ішінде саясаттар мен тапсырмалар да жойылады. Виртуалды Басқару сервері басқарған басқару топтарынан басқарылатын құрылғылар басқару топтарынан жойылады. Құрылғыларды Kaspersky Security Center Linux басқаруына қайтару үшін желі сауалнамасын орындаңыз, содан кейін табылған құрылғыларды Тағайындалмаған құрылғылар тобынан басқару топтарына жылжытыңыз.

Виртуалды Басқару серверін жою үшін:

1. Жойылатын виртуалды Басқару сервері тиесілі негізгі физикалық Басқару серверіне ауысыңыз:

   a. Негізгі мәзірде кез келген бөлімді (**Marketplace**, **Консольді шарлау** және **Параметрлерден** басқа) таңдап, беттің жоғарғы жағындағы **Иерархияны көрсету** түймесін басыңыз.

   b. Ашылатын навигация панелінде негізгі физикалық Басқару серверінің атауын басыңыз.

      Негізгі мәзірде басқару сервері сіз таңдағанға өзгереді.

2. Негізгі физикалық Басқару серверінің сипаттарына келесі жолдардың бірімен өтіңіз:

   - Навигация панелінде тінтуір курсорын қажетті Басқару серверінің атауына апарыңыз, содан кейін параметрлер белгішесін (⚙) басыңыз.

   - Негізгі мәзірдегі басқару серверінің атауын басыңыз.

3. Ашылған сипаттар терезесінде **Басқару серверлері** қойындысына өтіңіз.

4. Жойғыңыз келетін виртуалды Басқару серверін таңдаңыз.

5. Мәзірде **Жою** түймесін басыңыз.

Виртуалды Басқару сервері жойылды.

Басқару серверіне қосылу оқиғасының журналын реттеу

Басқару серверінің жұмысы барысында, оған қосылымдар мен қосылым әрекеттері тарихын журнал файлына сақтауға болады. Файлдағы ақпарат желі инфрақұрылымы ішіндегі қосылымдарды ғана емес, серверлерге рұқсатсыз қатынасу әрекеттерін де қадағалауға мүмкіндік береді.

Басқару серверіне қосылым оқиғаларын тіркеуді конфигурациялау үшін:

1. Негізгі мәзірдегі басқару серверінің атауын басыңыз.

   Басқару серверінің сипаттары терезесі ашылады.

2. **Жалпы** қойыншасында **Қосылу порттары** бөлімін таңдаңыз.

3. **Басқару серверінің байланыс оқиғаларын журналға тіркеу** параметрін қосыңыз.

Басқару серверіне кіріс қосылымдарының барлық кейінгі оқиғалары, түпнұсқалық растама нәтижелері және SSL қателері /var/opt/kaspersky/klnagent_srv/logs/sc.syslog файлына жазылатын болады.

Оқиғалар қоймасындағы оқиғалар санын конфигурациялау

Басқару сервері сипаттары терезесінің **Оқиғалар қоймасы** бөлімінде Басқару серверінің дерекқорында оқиғаларды сақтау параметрлерін конфигурациялауға болады: оқиғалар туралы жазбалар санын және жазбаларды сақтау уақытын шектеу. Оқиғалардың ең көп санын көрсеткенде, бағдарламалар оқиғалардың көрсетілген санын сақтау үшін диск кеңістігінің долбарлы өлшемін есептейді. Сіз бұл есептеуді дерекқордың толып кетуіне жол бермеу үшін бос диск кеңістігінің жеткілікті ме екенін бағалау үшін пайдалана аласыз. Әдепкі бойынша, Басқару сервері дерекқорының сыйымдылығы 400 000 оқиғаны құрайды. Дерекқордың ұсынылған ең жоғары сыйымдылығы 45 000 000 оқиғаны құрайды.

Бағдарлама дерекқорды 10 минут сайын тексереді. Оқиғалар саны көрсетілген максималды мәннен 10 000 артық болса, бағдарлама оқиғалардың көрсетілген ең көп саны ғана қалуы үшін ең ескі оқиғаларды жояды.

Басқару сервері ескі оқиғаларды жойған кезде, ол жаңа оқиғаларды дерекқорға сақтай алмайды. Осы кезең ішінде қабылданбаған оқиғалар туралы ақпарат операциялық жүйенің оқиғалар журналына жазылады. Жаңа оқиғалар кезекке қойылады, содан соң жою операциясы аяқталғаннан кейін, дерекқорда сақталады. Әдепкі бойынша, оқиға кезегі 20 000 оқиғамен шектеледі. KLEVP_MAX_POSTPONED_CNT жалаушаның мәнін өзгерту арқылы кезек шегін конфигурациялауға болады.

Басқару серверіндегі оқиғалар қоймасында сақтауға болатын оқиғалар санын шектеу үшін:

1. Негізгі мәзірдегі басқару серверінің атауын басыңыз.

   Басқару серверінің сипаттары терезесі ашылады.

2. **Жалпы** қойыншасында **Оқиғалар қоймасы** бөлімін таңдаңыз. Дерекқорда сақталатын оқиғалардың максималды санын көрсетіңіз.

3. **Сақтау** түймесін басыңыз.

Сондай-ақ келесі әрекеттерді орындауға болады:

- Тапсырманы орындау барысына қатысты оқиғаларды сақтау немесе тек тапсырманы орындау нәтижелерін сақтау үшін кез келген тапсырманың параметрлерін өзгертуге болады.
- Басқарылатын құрылғыларда орнатылған басқару сервері, желілік агент және Kaspersky қолданбаларының оқиғалары үшін сақтау мерзімін азайтуға немесе өшіруге болады.

Осылайша, сіз дерекқордағы оқиғалардың санын азайтасыз, дерекқордағы оқиғалар кестесін талдаумен байланысты сценарийлердің жұмыс жылдамдығын арттырасыз және критикалық оқиғаларды оқиғалардың көп санымен ығыстыру қаупін азайтасыз.

Басқару серверін басқа құрылғыға тасымалдау

Егер сізге жаңа құрылғыда Басқару серверін пайдалану қажет болса, оны келесі тәсілдердің бірімен тасымалдауға болады:

- Басқару серверін және дерекқор серверін жаңа құрылғыға жылжытыңыз (дерекқор серверін жаңа құрылғыға басқару серверімен бірге немесе басқа құрылғыға орнатуға болады).
- Дерекқор серверін ескі құрылғыда қалдыру және жаңа құрылғыға тек Басқару серверін тасымалдау.

Басқару серверін мен дерекқор серверін жаңа құрылғыға жылжыту үшін:

1. Алдыңғы құрылғыда Басқару сервері деректерінің сақтық көшірмесін жасаңыз.

   Бұл үшін, Kaspersky Security Center Web Console көмегімен деректерді сақтық көшірмелеу тапсырмасын іске қосыңыз немесе klbackup утилитасын іске қосыңыз.

2. Алдыңғы құрылғыда басқару серверін желіден ажыратыңыз.

3. Басқару сервері орнатылатын жаңа құрылғыны таңдаңыз. Таңдалған құрылғыдағы аппараттық және бағдарламалық жасақтама Басқару серверіне, Kaspersky Security Center Web Console серверіне және Желілік агентке қойылатын талаптарға сәйкес келетініне көз жеткізіңіз. Басқару серверінде қолданылатын порттардың қолжетімді екеніне көз жеткізіңіз.

4. Жаңа құрылғыға сол мекенжайды тағайындаңыз.

   Жаңа басқару серверіне NetBIOS атауын, FQDN және статикалық IP мекенжайын тағайындауға болады. Бұл желілік агенттер орналастырылған кезде желілік агенттің орнату бумасында басқару серверінің қандай мекенжайы орнатылғанына байланысты. Сондай-ақ желілік агент қосылатын басқару серверін анықтайтын қосылым мекенжайын пайдалануға болады (бұл мекенжайды klnagchk қызметтік бағдарламасын қолданып, басқарылатын құрылғыларда алуға болады).

5. Қажет болса, жаңа құрылғыда басқару сервері пайдаланатын дерекқорларды басқару жүйесін (ДҚБЖ) орнатыңыз.

   Дерекқорды басқару серверімен бірге жаңа құрылғыға немесе басқа құрылғыға орнатуға болады. Таңдалған құрылғы аппараттық және бағдарламалық талаптарға сәйкес келетініне көз жеткізіңіз. ДҚБЖ таңдау кезінде Басқару сервері қызмет көрсететін құрылғылардың санын ескеріңіз.

6. Басқару серверін жаңа құрылғыға орнатыңыз.

   Дерекқор серверін жаңа құрылғыға тасымалдайтын болсаңыз, жергілікті мекенжайды дерекқор орнатылған құрылғының IP мекенжайы ретінде көрсету керек екенін ескеріңіз (Kaspersky Security Center Linux орнату нұсқаулығының "h" тармағы). Дерекқор серверін алдыңғы құрылғыда сақтау қажет болса, Kaspersky Security Center Linux орнату нұсқаулығының "h" тармағында алдыңғы құрылғының IP мекенжайын енгізіңіз.

7. Орнату аяқталғаннан кейін, klbackup утилитасын көмегімен жаңа құрылғыдағы Басқару сервері деректерін қалпына келтіріңіз.

8. Kaspersky Security Center Web Console бағдарламасын ашып, Басқару серверіне қосылыңыз.

9. Барлық басқарылатын құрылғылар басқару серверіне қосылғанына көз жеткізіңіз.

10. Алдыңғы құрылғыдан Басқару сервері мен дерекқорлар серверін жойыңыз.

Басқару серверінің атауын өзгерту

Сервер атауын өзгерту қадамдары ортаңызға байланысты өзгеруі мүмкін. Сервер атауын өзгерту үшін келесі сценарийлердің бірін таңдауға болады:

- Жаңа DNS жазбасын қосу арқылы қосылымдарды сақтау.
- IP мекенжайына негізделген қосылымға ауысу арқылы қосылымдарды сақтау.
- Сервер атауын өзгерткеннен кейін үзілген қосылымдарды қалпына келтіру.

Егер сервер атауын өзгертуде қиындықтар туындаса, Техникалық қолдау қызметіне хабарласыңыз.

Жаңа DNS жазбасын қосу арқылы қосылымдарды сақтау

Бұл сценарийде басқарылатын құрылғылар және Kaspersky Security Center Web Console Басқару серверінің атауын өзгерткеннен кейін ескі Басқару серверінің мекенжайына қосылуды жалғастырады. Мұны конфигурациялау үшін келесі DNS жазба түрлерінің бірін қосыңыз:

- Ескі Басқару серверінің мекенжайы туралы жазба жаңа Басқару серверінің IP мекенжайына нұсқайды.
- CNAME жазбасы ескі Басқару сервері атауын жаңа Басқару сервері атауымен байланыстырады.

  Қажетті жазбаларды конфигурациялау туралы қосымша ақпарат алу үшін DNS сервер құжаттамасын қараңыз.

Жаңа DNS жазбасын қосу арқылы қосылымдарды сақтау үшін:

1. **Тег атауын өзгертіңіз**.

   Орнату кезінде компоненттердің конфигурациялануына байланысты, Басқару серверін қайта орнатпай, Басқару серверінің атауын өзгерту мүмкін емес.

   Сервер атауын өзгерту үшін:

   1. klbackup утилитасын пайдаланып Басқару серверінің жаңа сақтық көшірмесін жасаңыз.
   2. Барлық әкімшінің жұмыс станцияларынан Kaspersky Security Center Linux ОЖ-н және Kaspersky Security Center Web Console ОЖ-ін жойыңыз.
   3. Басқару серверінің Басқару серверідерекқорын және IAM дерекқорын қолмен жойыңыз. Басқару сервері оларды жою кезінде автоматты түрде жоймайды.

4. ОС құжаттамасына сәйкес, Басқару серверінің операциялық жүйесіндегі құрылғының атын өзгертіңіз.

5. Kaspersky Security Center Linux Басқару серверін Басқару серверінің жаңа FQDN мекенжайын пайдаланып орнатыңыз.

6. Орнатқаннан кейін бұрын дайындалған Басқару серверінің сақтық көшірмесін қалпына келтіріңіз.

7. IAM серверінің конфигурациясын тексеріңіз және қажет болған жағдайда IAM серверінің конфигурация файлына Басқару серверінің мекенжайын қосыңыз.

8. Жауап файлында Басқару серверінің жаңа FQDN мекенжайын көрсету арқылы барлық әкімшінің жұмыс станцияларына Web Console орнатыңыз.

2. Ескі Басқару серверінің мекенжайы үшін жаңа DNS жазбасын қосыңыз.

3. Kaspersky Security Center Web Console ішіндегі Басқару серверінің параметрлерінде жаңа мекенжайды көрсетіңіз.

4. Басқару сервері тікелей көрінетін құрылғыларда **Басқару серверін ауыстыру** тапсырмасын орындаңыз. Осыдан кейін басқарылатын құрылғылар Басқару серверіне жаңа атауды пайдаланып қосыла алады.

   Сервер тікелей көрінбейтін құрылғыларда тапсырманы орындамаңыз, әйтпесе олар Басқару серверімен және қосылым шлюздерімен қосылымын жоғалтады.

   Қосылым шлюздері арқылы қосылған басқарылатын құрылғылар Басқару серверінің атауын тексермейді. Сондықтан, олар үшін қосымша әрекет қажет емес. Басқару серверінің мекенжайы туралы ақпарат klnagchk диагностикалық командасының шығысында жаңартылмайды.

Басқару серверіне қосылым сервер атауы өзгертілгеннен кейін сақталады.

Сервер атауы өзгертілгеннен кейін сертификаттар туралы ақпарат ескіреді. Бұл компоненттердің жұмысына әсер етпейтіндіктен, өздігінен қол қойылған сертификаттарды кестеден тыс ауыстыруды ұсынбаймыз. Бұл сертификаттар Kaspersky Security Center орнату кезінде жасалады және сервермен автоматты түрде жаңартылады. Олар келесі автоматты сертификатты ауыстыру кезінде жаңа Басқару сервері атауымен қайта шығарылады.

Қайта орнату кезінде IAM сервері мен Web Console сервері үшін жаңа сертификаттар беріледі. Қажет болған жағдайда, оларды жаңа Басқару сервер атауы үшін Сертификаттау орталығыңыз берген арнайы сертификаттармен ауыстырыңыз. Толығырақ ақпарат алу үшін келесі мақаланы қараңыз: Kaspersky Security Center Linux сертификаттары туралы.

IP мекенжайына негізделген қосылымға ауысу арқылы қосылымдарды сақтау

Бұл сценарийде басқарылатын құрылғылардың Басқару серверіне қосылу тәсілі өзгереді. Құрылғылар Басқару сервері атауының орнына Басқару серверінің IP мекенжайын пайдаланып қосылады. Барлық басқарылатын құрылғыларды ауыстыру құрылғылар санына және олардың Басқару серверімен желіде қаншалықты жиі пайда болатынына байланысты уақытты алуы мүмкін.

IP мекенжайына негізделген қосылымға ауысу арқылы қосылымдарды сақтау үшін:

1. **Басқару серверінің атауын өзгертпес бұрын Kaspersky Security Center инфрақұрылымын дайындаңыз**.

   1. Басқарылатын құрылғыларды Басқару серверіне IP мекенжайын пайдаланып қосыңыз. Басқару серверінің атауын өзгерткеннен кейін, қосылым атауы ретінде оның атауын пайдаланатын Құрылғылар серверден ажыратылады. IP мекенжайы арқылы қосылу үшін Басқару сервері тікелей көрінетін құрылғыларда, соның ішінде қосылым шлюздері ретінде әрекет ететін құрылғыларда "Басқару серверін өзгерту" тапсырмасын орындаңыз.

      Сервер тікелей көрінбейтін құрылғыларда тапсырманы орындамаңыз, әйтпесе олар Басқару серверімен және қосылым шлюздерімен қосылымын жоғалтады.

      Қосылым шлюздері арқылы қосылған басқарылатын құрылғылар Басқару серверінің атауын тексермейді. Сондықтан, олар үшін қосымша әрекет қажет емес. Басқару серверінің мекенжайы туралы ақпарат klnagchk диагностикалық командасының шығысында жаңартылмайды.

   2. Барлық басқарылатын құрылғылардың Басқару серверіне IP мекенжайы арқылы қосылғанына көз жеткізіңіз. Бұл үшін келесі әрекеттерді орындаңыз:

      - Басқару сервері тікелей көрінетін басқарылатын құрылғылардағы Басқару сервері мекенжай жолындағы klnagchk диагностикалық командасының нәтижелері.
      - Құрылғыларға орнату кезіндегі Желілік агент орнату пакетінің қасиеттері туралы ақпарат.

        Желілік агент бастапқыда Басқару серверіне IP мекенжайын пайдаланып қосылу үшін конфигурациялануы керек.

        Егер сіз Желілік агентті алдымен жоймай, бар орнатудың үстіне орнатсаңыз, Желілік агент конфигурациясында көрсетілген Басқару серверінің қосылым мекенжайы мен сертификаты жаңартылмайды.

   3. Бар Басқару серверінің қосылым профильдерінде жаңа атауды көрсетіңіз.

   4. Егер сіз Ұялы құрылғыларды басқару рөлін пайдалансаңыз (Android және iOS құрылғыларын басқарсаңыз), MDM немесе KSMM рөлімен Kaspersky Endpoint Security for Android пайдаланатын басқарылатын құрылғыларда Басқару серверінің мекенжайын қалай өзгерту керек нұсқауларын орындаңыз.

2. **Тег атауын өзгертіңіз**.

   Орнату кезінде компоненттердің конфигурациялануына байланысты, Басқару серверін қайта орнатпай, Басқару серверінің атауын өзгерту мүмкін емес.

   Сервер атауын өзгерту үшін:

   1. klbackup утилитасын пайдаланып Басқару серверінің жаңа сақтық көшірмесін жасаңыз.

   2. Барлық әкімшінің жұмыс станцияларынан Kaspersky Security Center Linux ОЖ-н және Kaspersky Security Center Web Console ОЖ-ін жойыңыз.

   3. Басқару серверінің Басқару серверідерекқорын және IAM дерекқорын қолмен жойыңыз. Басқару сервері оларды жою кезінде автоматты түрде жоймайды.

4. ОС құжаттамасына сәйкес, Басқару серверінің операциялық жүйесіндегі құрылғының атын өзгертіңіз.

5. Kaspersky Security Center Linux Басқару серверін Басқару серверінің жаңа FQDN мекенжайын пайдаланып орнатыңыз.

6. Орнатқаннан кейін бұрын дайындалған Басқару серверінің сақтық көшірмесін қалпына келтіріңіз.

7. IAM серверінің конфигурациясын тексеріңіз және қажет болған жағдайда IAM серверінің конфигурация файлына Басқару серверінің мекенжайын қосыңыз.

8. Жауап файлында Басқару серверінің жаңа FQDN мекенжайын көрсету арқылы барлық әкімшінің жұмыс станцияларына Web Console орнатыңыз.

3. **Басқару серверінің параметрлерінде Басқару серверінің мекенжайын жаңартыңыз**.

   Басқару серверінің атауын өзгерткеннен кейін, Kaspersky Security Center Web Console-дағы Басқару серверінің параметрлерінде жаңа FQDN мекенжайын көрсетіңіз. Ол үшін келесі параметрлердің әрқайсысында FQDN мекенжайын тексеріп, жаңартыңыз:

   - Kaspersky Security Network прокси-сервері мекенжайы
   - Веб-сервер
   - Желілік агенттің орнату пакетінің параметрлері
   - Қауіпсіздік коды эмитентінің атауы (2FA)

   Сонымен қатар, келесі әрекеттерді орындаңыз:

   - Басқа Kaspersky қолданбаларының саясаты мен параметрлерінде жаңа сервер атауын көрсетіңіз.
   - Әрбір жарияланған автономды пакетті және мобильді құрылғы пакетін қайта жариялаңыз.
   - Егер сіз Басқару серверлерінің иерархиясын пайдалансаңыз және серверлер IP мекенжайы бойынша емес, қосылым атауы бойынша қосылған болса, қосалқы Басқару серверлерін қайта қосыңыз.

4. Басқарылатын құрылғылардағы қосылым мекенжайын жаңа Басқару сервері атауына өзгерту үшін Басқару сервері тікелей көрінетін құрылғыларда «Басқару серверін **Басқару серверін ауыстыру** тапсырмасын орындаңыз.

Басқару серверіне қосылым сервер атауы өзгертілгеннен кейін сақталады.

Сервер атауы өзгертілгеннен кейін сертификаттар туралы ақпарат ескіреді. Бұл компоненттердің жұмысына әсер етпейтіндіктен, өздігінен қол қойылған сертификаттарды кестеден тыс ауыстыруды ұсынбаймыз. Бұл сертификаттар Kaspersky Security Center орнату кезінде жасалады және сервермен автоматты түрде жаңартылады. Олар келесі автоматты сертификатты ауыстыру кезінде жаңа Басқару сервері атауымен қайта шығарылады.

Қайта орнату кезінде IAM сервері мен Web Console сервері үшін жаңа сертификаттар беріледі. Қажет болған жағдайда, оларды жаңа Басқару сервер атауы үшін Сертификаттау орталығыңыз берген арнайы сертификаттармен ауыстырыңыз. Толығырақ ақпарат алу үшін келесі мақаланы қараңыз: Kaspersky Security Center Linux сертификаттары туралы.

Сервер атауын өзгерткеннен кейін үзілген қосылымдарды қалпына келтіру

Бұл сценарий келесі жағдайларда өзекті:

- Егер сіз Басқару сервері құрылғысының домен атауына иелік ету құқығынан айырылсаңыз, бірақ Басқару серверіне әлі де қол жеткізе алсаңыз.
- Егер Басқару сервері басқарылатын құрылғыларды басқармаса.
- Егер басқа себептермен ескі Kaspersky Security Center Linux мекенжайына DNS жазбаларын қосу мүмкін болмаса.

Сервер атауын өзгерткеннен кейін үзілген қосылымдарды қалпына келтіру үшін:

1. **Тег атауын өзгертіңіз**.

   Орнату кезінде компоненттердің конфигурациялануына байланысты, Басқару серверін қайта орнатпай, Басқару серверінің атауын өзгерту мүмкін емес.

   Сервер атауын өзгерту үшін:

   1. klbackup утилитасын пайдаланып Басқару серверінің жаңа сақтық көшірмесін жасаңыз.
   2. Барлық әкімшінің жұмыс станцияларынан Kaspersky Security Center Linux ОЖ-н және Kaspersky Security Center Web Console ОЖ-ін жойыңыз.
   3. Басқару серверінің Басқару серверідерекқорын және IAM дерекқорын қолмен жойыңыз. Басқару сервері оларды жою кезінде автоматты түрде жоймайды.
   4. ОС құжаттамасына сәйкес, Басқару серверінің операциялық жүйесіндегі құрылғының атын өзгертіңіз.
   5. Kaspersky Security Center Linux Басқару серверін Басқару серверінің жаңа FQDN мекенжайын пайдаланып орнатыңыз.
   6. Орнатқаннан кейін бұрын дайындалған Басқару серверінің сақтық көшірмесін қалпына келтіріңіз.
   7. IAM серверінің конфигурациясын тексеріңіз және қажет болған жағдайда IAM серверінің конфигурация файлына Басқару серверінің мекенжайын қосыңыз.
   8. Жауап файлында Басқару серверінің жаңа FQDN мекенжайын көрсету арқылы барлық әкімшінің жұмыс станцияларына Web Console орнатыңыз.

2. **Басқару серверінің параметрлерінде Басқару серверінің мекенжайын жаңартыңыз**.

   Басқару серверінің атауын өзгерткеннен кейін, Kaspersky Security Center Web Console-дағы Басқару серверінің параметрлерінде жаңа FQDN мекенжайын көрсетіңіз. Ол үшін келесі параметрлердің әрқайсысында FQDN мекенжайын тексеріп, жаңартыңыз:

   - Kaspersky Security Network прокси-сервері мекенжайы
   - Веб-сервер

- Желілік агенттің орнату пакетінің параметрлері
- Қауіпсіздік коды эмитентінің атауы (2FA)

Сонымен қатар, келесі әрекеттерді орындаңыз:

- Басқа Kaspersky қолданбаларының саясаты мен параметрлерінде жаңа сервер атауын көрсетіңіз.
- Әрбір жарияланған автономды пакетті және мобильді құрылғы пакетін қайта жариялаңыз.
- Егер сіз Басқару серверлерінің иерархиясын пайдалансаңыз және серверлер IP мекенжайы бойынша емес, қосылым атауы бойынша қосылған болса, қосалқы Басқару серверлерін қайта қосыңыз.

3. Бұрын басқарылған құрылғыларда Басқару серверіне қосылымды қалпына келтіріңіз:

- Басқару серверіне тікелей көрінетін құрылғыларда жаңа Басқару сервері атауымен қосылым мекенжайын көрсету үшін klmover утилитасын пайдаланыңыз. Толығырақ ақпарат алу үшін келесі мақаланы қараңыз: klmover утилитасын пайдаланып Желілік агенттерді Басқару серверіне қосу.
- Қосылым шлюздері ретінде әрекет ететін құрылғыларда Желілік агентті қайта орнатыңыз және қосылым шлюзінің рөлін қайта конфигурациялаңыз. Толығырақ ақпарат алу үшін келесі мақаланы қараңыз: DMZ-ге қосылым шлюзін тарату нүктесі ретінде қосу.
- Қосылым шлюздері арқылы қосылған құрылғылар қосылым шлюздері қалпына келтірілгеннен кейін автоматты түрде қайта қосылады. Желілік агент қосылым шлюздеріне қосылған кезде Басқару сервері атауын пайдаланбайды.

  Қосылым шлюздері арқылы қосылған құрылғыларда klmover утилитасын пайдаланбаңыз. Толығырақ ақпарат алу үшін келесі мақаланы қараңыз: Басқару серверіне қосылған құрылғыларды қосылым шлюздері арқылы басқа Басқару серверіне жылжыту.

Басқару серверіне қосылым сервер атауы өзгертілгеннен кейін қалпына келтіріледі.

Сервер атауы өзгертілгеннен кейін сертификаттар туралы ақпарат ескіреді. Бұл компоненттердің жұмысына әсер етпейтіндіктен, өздігінен қол қойылған сертификаттарды кестеден тыс ауыстыруды ұсынбаймыз. Бұл сертификаттар Kaspersky Security Center орнату кезінде жасалады және сервермен автоматты түрде жаңартылады. Олар келесі автоматты сертификатты ауыстыру кезінде жаңа Басқару сервері атауымен қайта шығарылады.

Қайта орнату кезінде IAM сервері мен Web Console сервері үшін жаңа сертификаттар беріледі. Қажет болған жағдайда, оларды жаңа Басқару сервер атауы үшін Сертификаттау орталығыңыз берген арнайы сертификаттармен ауыстырыңыз. Толығырақ ақпарат алу үшін келесі мақаланы қараңыз: Kaspersky Security Center Linux сертификаттары туралы.

ДҚБЖ есептік деректерін өзгерту

Кейде ДҚБЖ есептік деректерін өзгерту қажет болуы мүмкін, мысалы, қауіпсіздік мақсатында есептік деректердің ротациясын орындау үшін.

Басқару серверінің дерекқордың кіру деректерін өзгерту

Linux ортасында Басқару сервері мен IAM дерекқорының тіркелгі деректерін өзгерту үшін:

1. Басқару серверін тоқтатыңыз. Kaspersky Security Center Linux орналастыру түріне байланысты, root тіркелгісінен келесі пәрмендердің бірін орындаңыз:

   - Kaspersky Security Center Linux ақаулықтарға төзімді кластері үшін:

     Белсенді түйінде келесі пәрменді орындаңыз:

     ```
     /opt/kaspersky/ksc64/sbin/klfoc -stopcluster --stp klfoc
     ```

   - Географиялық таратылған Kaspersky Security Center Linux ақаулықтарға төзімді кластері үшін:

     Екі түйінде де келесі пәрменді орындаңыз:

     ```
     crm node standby
     ```

   - Кластерлік емес Басқару серверін орналастыру үшін:

     Келесі пәрмендерді орындаңыз:

     ```
     systemctl stop kladminserver_srv.service
     systemctl stop kliam_srv.service
     ```

2. ДҚБЖ суперпайдаланушысының құқықтарымен Басқару серверінің дерекқорына қосылыңыз және келесі пәрменді орындаңыз:

   ```
   REASSIGN OWNED BY <old_kscdbadmin> TO <new_kscdbadmin>;
   ```

   Мұндағы `<old_kscdbadmin>` — Басқару сервері өз дерекқорына қосылу үшін пайдаланған бұрынғы ДҚБЖ тіркелгісі, ал `<new_kscdbadmin>` — жаңа ДҚБЖ тіркелгілері.

3. ДҚБЖ суперпайдаланушысының құқықтарымен IAM дерекқорына қосылыңыз және келесі пәрменді орындаңыз:

   ```
   REASSIGN OWNED BY <old_iamdbadmin> TO <new_iamdbadmin>;
   ```

   Мұндағы `<old_iamdbadmin>` — Басқару сервері өз дерекқорына қосылу үшін пайдаланған бұрынғы ДҚБЖ тіркелгісі, ал `<new_iamdbadmin>` — жаңа ДҚБЖ тіркелгілері.

4. IAM конфигурация файлын табыңыз: /var/opt/kaspersky/klnagent_srv/iam/iam_config.yaml

5. `dbms_iam` бөлімінде пайдаланушы және құпиясөз өрістерінде жаңа есептік деректерін көрсетіңіз. Тіркелгінің ДҚБЖ-де бар екеніне және IAM дерекқорының иесі ретінде көрсетілгеніне көз жеткізіңіз.

6. Басқару серверін іске қосыңыз. Kaspersky Security Center Linux орналастыру түріне байланысты, root тіркелгісінен келесі пәрмендердің бірін орындаңыз:

   - Kaspersky Security Center Linux ақаулықтарға төзімді кластері үшін:

     Белсенді түйінде келесі пәрменді орындаңыз:

     ```
     /opt/kaspersky/ksc64/sbin/klfoc -startcluster --stp klfoc
     ```

   - Географиялық таратылған Kaspersky Security Center Linux ақаулықтарға төзімді кластері үшін:

     Екі түйінде де келесі пәрменді орындаңыз:

     ```
     crm node online
     ```

   - Кластерлік емес Басқару серверін орналастыру үшін:

     Келесі пәрмендерді орындаңыз:

     ```
     systemctl start kladminserver_srv.service
     systemctl start kliam_srv.service
     ```

7. klsrvconfig утилитасын іске қосыңыз:

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

8. Есептік жазбаның жаңа атауын көрсетіңіз. ДҚБЖ-да бұрыннан бар есептік жазбаның есептік деректерін көрсетуіңіз керек.

9. Жаңа құпиясөзді енгізіңіз.

10. Растау үшін осы жаңа құпиясөзді көрсетіңіз.

11. Басқару сервері жұмысын қайта бастағанша және белсенді түйінде Басқару серверінің графикалық интерфейс операцияларына дайын екенін көрсететін syslog журналының жазбасы пайда болғанша күтіңіз.

Басқару серверінің дерекқорының есептік деректері өзгертілді.

Басқару сервері деректерін сақтық көшірмелеу және қалпына келтіру

Деректердің сақтық көшірмесі Басқару серверін бір құрылғыдан екіншісіне ақпаратты жоғалтпай тасымалдауға мүмкіндік береді. Сақтық көшірмелеу арқылы, Басқару серверінің ақпараттық дерекқорын басқа құрылғыға тасымалдаған кезде немесе Kaspersky Security Center бағдарламасының ең соңғы нұсқасына көшкен кезде деректерді қалпына келтіруге болады. Сондай-ақ Kaspersky Security Center Linux басқаруындағы Kaspersky Security Center Windows жүйесінен басқару сервері деректерін жылжыту үшін деректердің сақтық көшірмесін пайдалануға болады (деректерді Kaspersky Security Center Linux жүйесінен Kaspersky Security Center Windows жүйесіне жылжытуға қолдау көрсетілмейді).

Орнатылған басқару плагиндерінің сақтық көшірмелері сақталмайтынын ескеріңіз. Сақтық көшірмеден Басқару сервері деректерін қалпына келтіргеннен кейін, басқарылатын бағдарлама плагиндерін жүктеп, қайта орнату қажет.

Басқару серверінің деректерінің сақтық көшірмесін жасамас бұрын, келесі әрекеттерді орындаңыз:

- **Басқару сервері 16 немесе одан бұрынғы нұсқасында сақтық көшірме жасау және оны 16.1 немесе одан кейінгі нұсқасында қалпына келтіру талаптарын орындаңыз**

  - Егер сіз Басқару сервері 16 немесе одан бұрынғы нұсқасында деректердің сақтық көшірмесін жасап, оны Басқару сервері 16.1 немесе одан кейінгі нұсқасында қалпына келтірсеңіз, екі факторлы аутентификация қосылған. Қосымша ақпарат алу үшін Есептік жазба үшін екі факторлы аутентификация туралы бөлімін қараңыз.

    Пайдаланушылардың конфигурацияланған екі факторлы аутентификация құпия кілттерін пайдаланып, Web Console веб-консоліне бар есептік жазбалармен кіре алатынына және OpenAPI автоматтандыру сценарийлерінің қалпына келтіруден кейін жұмысын жалғастыратынына көз жеткізу үшін келесі қадамдарды орындауыңыз керек:

    - Барлық пайдаланушылар үшін екі факторлы аутентификацияны қосу
    - Әкімшілер өз есептік жазбалары үшін екі факторлы аутентификацияны конфигурациялауы керек
    - Талап етілетін есептік жазбаларды екі факторлы аутентификациядан алып тастау

      Қажет болса, OpenAPI арқылы сценарийлерді іске қосу үшін пайдаланылатын тұтастық есептік жазбаларын ерекшеліктер тізіміне қосыңыз.

  Егер сақтық көшірмені жасамас бұрын екі факторлы аутентификацияны конфигурациялау мүмкін болмаса, пайдаланушы есептік жазбалары екі факторлы аутентификацияға рұқсат беру тізіміне қосылады және Web Console веб-консоліне кірген кезде екі факторлы аутентификацияны конфигурациялай алады. Тіркелгіні рұқсат ету тізіміне қосудың егжей-тегжейлі шарттары Пайдаланушыларға екі факторлы аутентификацияны конфигурациялауға рұқсат беру тақырыбында сипатталған.

- Виртуалды Басқару серверінің әкімшілік тобына қосылғанын тексеріңіз. Сақтық көшірме жасау алдында виртуалды Басқару сервер қосылса, осы виртуалды серверге әкімші тағайындалғанын тексеріңіз. Сақтық көшірмеден кейін виртуалды Басқару серверге әкімші құқықтарын бере алмайсыз. Әкімшінің тіркелгі деректері жоғалса, виртуалды әкімші серверіне жаңа әкімші тағайындай алмайтыныңызды ескеріңіз.

- Kaspersky Security Center Linux ақауларға төзімді кластерінің сақтық көшірмесін жасау немесе қалпына келтіру қажет болса, бүкіл кластерді техникалық қызмет көрсету үшін тоқтатып, сақтық көшірме жасау немесе қалпына келтіру аяқталғаннан кейін оны қайта бастау керек.

Басқару серверді деректерінің сақтық көшірмесін келесі тәсілдердің бірімен жасауға болады:

- Kaspersky Security Center Web Console арқылы деректердің сақтық көшірмесін жасау тапсырмасын жасау және іске қосу.

- Басқару сервері орнатылған құрылғыда klbackup утилитасын іске қосу. Утилита Kaspersky Security Center жеткізу жиынтығының құрамына кіреді. Басқару сервері орнатылғаннан кейін бағдарламаны орнату кезінде көрсетілген тағайындалған қалтаның түбірінде орналасады (әдетте /opt/kaspersky/ksc64/sbin/klbackup).

Басқару сервері деректерінің сақтық көшірмесінде келесі деректер сақталады:

- Басқару серверінің дерекқоры (оқиғаның Басқару серверінде сақталған саясаттар, тапсырмалар, бағдарлама параметрлері).

- Басқару топтары құрылымы және клиент құрылғылары туралы конфигурациялық ақпарат.

- Қашықтан орнатуға арналған бағдарлама дистрибутивтері қоймасы.

- Басқару сервері сертификаты.

- Пайдаланушы есептік жазбалары үшін конфигурацияланған екі факторлы аутентификацияның құпия кілттері.

- Екі факторлы аутентификациядан шығарылған пайдаланушы есептік жазбаларының тізімі.

Басқару сервері деректерінің сақтық көшірмесін жасау тапсырмасын құрып және іске қосу арқылы немесе klbackup утилитасын пайдалану арқылы жасай аласыз. Басқару сервері деректерін тек klbackup утилитасының көмегімен қалпына келтіруге болады. Жаңа ғана орнатылған және сақтық көшірме жасалған нұсқамен бірдей (немесе одан кейінгі) басқару серверінің жұмыс істейтін данасында ғана қалпына келтіруге болады. Сақтық көшірме жасау немесе қалпына келтіру үшін үшінші тарап құралдарын пайдаланбаңыз және мүмкін болса, конфигурация мен деректерді беру толығымен аяқталғанша алдыңғы Kaspersky Security Center Linux орнатуын жоймаңыз.

Басқару серверінің деректерін сақтық көшірмелеу тапсырмасын жасау

Сақтық көшірмелеу тапсырмасы Басқару серверінің тапсырмасы болып табылады және оны бағдарламаны жылдам іске қосу шебері жасайды. Бағдарламаны жылдам іске қосу шебері жасаған сақтық көшірмелеу тапсырмасы жойылса, оны қолмен жасауға болады.

Басқару сервері деректерінің резервтік қоймасы тапсырмасын тек бір үлгіде ғана жасауға болады. Басқару сервері деректерін сақтық көшірмелеу тапсырмасы Басқару сервері үшін жасалған болса, онда ол тапсырма жасау шеберінің таңдау терезесінде көрсетілмейді.

Басқару серверінің деректерін сақтық көшірмелеу тапсырмасын жасау үшін:

1. Бағдарламаның негізгі терезесінде **Тапсырмалар** бөліміне өтіңіз.
2. **Қосу** түймесін басыңыз.

   Жаңа тапсырма жасау шебері іске қосылады. Шебердің жұмысын жалғастыру үшін **Келесі** түймесін басыңыз.
3. **Бағдарлама** тізімінде **Kaspersky Security Center 16.3** тармағын және **Тапсырма түрі** тізімінде **Басқару сервері деректерінің сақтық көшірмесін жасау** тармағын таңдаңыз.
4. Тиісті қадамда келесі ақпаратты көрсетіңіз:
   - сақтық көшірмелерді сақтауға арналған қалта;
   - сақтық көшірмеге арналған құпиясөз (міндетті емес);
   - сақталған сақтық көшірмелердің максималды саны.
5. **Тапсырманы жасауды аяқтау** қадамында **Жасап болған соң, тапсырма туралы мәліметтерді ашу** параметрін қоссаңыз, әдепкі бойынша белгіленген тапсырма параметрлері мәндерін өзгерте аласыз. Егер сіз бұл параметрді қоспасаңыз, тапсырма әдепкі бойынша белгіленген параметр мәндерімен жасалады. Әдепкі бойынша параметр мәндерін кейінірек кез келген уақытта өзгертуге болады.
6. **Аяқтау** түймесін басыңыз.

Тапсырма жасалып, тапсырмалар тізімінде көрсетіледі.

Деректердің сақтық көшірмесін жасау және қалпына келтіру үшін klbackup утилитасын пайдалану

Kaspersky Security Center дистрибутивінің құрамына кіретін klbackup утилитасы арқылы сақтық көшірмелеу және кейіннен қалпына келтіру үшін Басқару сервері деректерін көшіруге болады.

Қалпына келтіру әрекеті орындалатын басқару серверінің данасында бір түрдегі ДҚБЖ қолданылуы керек. Басқару серверінің нұсқасы сондай (ұқсас немесе барынша жаңа патчпен) немесе барынша жаңа болуы мүмкін.

Егер сіз MariaDB ДҚБЖ бұрынғы нұсқасын пайдаланып Kaspersky Security Center Linux 15 немесе одан бұрынға нұсқаның құрамына кіретін Басқару сервері деректерінің сақтық көшірмесін жасаған болсаңыз, содан кейін MariaDB кейінгі нұсқасы бар құрылғыдағы деректерді қалпына келтірсеңіз, қате орын алуы мүмкін. Қосымша ақпаратты Бұрынғы ДҚБЖ нұсқасында жасалған сақтық көшірмеден басқару сервері деректерін қалпына келтіру жолы бөлімінен қараңыз.

klbackup утилитасын пайдаланған кезде, желілік агент жалаушалары қалпына келтірілмейді. Желілік агент жалаушаларын қолмен конфигурациялау қажет.

Деректерді сақтық көшірмелеу немесе Басқару сервері деректерін тыныш режимде қалпына келтіру үшін,

Басқару сервері орнатылған құрылғының пәрмен жолында klbackup утилитасын қажетті кілттер жиынтығымен іске қосыңыз.

Утилитаның пәрмен жолының синтаксисі:

```
klbackup -path <сақтық көшірме жолы> [-linux_path <dbms сақтық көшірме жолы>-node_cert
<сертификат жолы>] [-logfile <журнал файлы> [-use_ts]|[-restore] [-password
<құпиясөз>] [-cert_only]
```

Егер сіз klbackup утилитасының пәрмен жолында құпиясөзді белгілемесеңіз, утилита оны интерактивті түрде енгізуді сұрайды.

Кілттердің сипаттамалары:

- `-path <сақтық көшірме жолы>` — сақтық көшірме қалтасындағы ақпаратты сақтаңыз немесе қалпына келтіру үшін сақтық көшірме қалтасындағы деректерді пайдаланыңыз (міндетті параметр).
- `-linux_path <dbms сақтық көшірме жолы>` — ДҚБЖ сақтық көшірме деректері бар жергілікті жол.

  Дерекқор серверінің есептік жазбасы және klbackup утилитасы ДҚБЖ сақтық көшірме қалтасындағы деректерді өзгерту құқығына ие болуы керек.
- `-node_cert <сертификат жолы>` — қалпына келтіруден кейін белсенді емес ақауларға төзімді түйінді конфигурациялауға арналған сервер сертификатының файлы. Параметр көрсетілмесе, ол серверден автоматты түрде алынады.
- `-logfile <журнал файлы>` — басқару сервері деректерінің сақтық көшірмесін жасау немесе қалпына келтіру туралы есепті сақтау.

  Дерекқор серверінің есептік жазбасы және klbackup утилитасы сақтық көшірме қалтасындағы деректерді өзгерту құқығына ие болуы керек.
- `-use_ts` — деректерді сақтаған кезде, ақпаратты сақтық көшірме қалтасына, `klbackup YYYY-MM-DD # HH-MM-SS` форматымен аталатын ішкі қалтаға көшіріңіз. Онда ағымдағы күн мен операция уақыты (UTC) қамтылған. Кілт көрсетілмеген болса, ақпарат сақтық көшірме қалтасының түбірінде сақталады.

  Ақпаратты сақтық көшірмесі бар қалтаға сақтауға тырысқанда, қате туралы хабар пайда болады. Ақпарат жаңартылмайды.

`-use_ts` кілтінің болуы арқасында Басқару сервері деректері мұрағатын жүргізуге болады. Мысалы, `-path` кілті `/tmp/KLBackups`, `klbackup 2022/6/19 # 11-30-18` қалтасын білдірсе, басқару серверінің 2022 жылғы 19 маусым, 11:30:18-дегі күйі туралы ақпаратты сақтайды.

- `-restore` – Басқару сервері деректерін қалпына келтіруді орындау. Деректерді қалпына келтіру сақтық көшірме қалтасында ұсынылған ақпарат негізінде жүзеге асырылады. Кілт болмаса, сақтық көшірме қалтасына деректердің сақтық көшірмесі жасалады.

- `-password <құпиясөз>` — құпия деректерді қорғауға арналған құпиясөз.

  Ұмытылған құпиясөзді қалпына келтіру мүмкін емес. Құпиясөзге қойылатын талаптар жоқ. Құпиясөздің ұзындығы шектелмейді, сондай-ақ құпиясөздің нөлдік ұзындығы да болуы мүмкін (яғни құпиясөзсіз).

  Деректерді қалпына келтіру кезінде, сақтық көшірмелеу барысында енгізілген құпиясөзді көрсету қажет. Сақтық көшірмелеуден кейін ортақ қатынасы бар қалтаға апаратын жол өзгерсе, қалпына келтірілген деректерді пайдаланатын тапсырмалардың жұмысын тексеріңіз (қалпына келтіру тапсырмалары және қашықтан орнату тапсырмалары). Қажет болса, осы тапсырмалардың параметрлерін өңдеңіз. Деректер сақтық көшірме файлынан қалпына келтіріліп жатқанда, ешкім Басқару серверінің ортақ қатынасы бар қалтасына кіре алмайды. klbackup утилитасы іске қосылатын есептік жазба ортақ қатынасы бар қалтаға толық қатынасу мүмкіндігіне ие болуы керек. Басқару сервер деректерін сақтық көшірмеден қалпына келтіру үшін утилитаны жаңадан орнатылған Басқару серверінде іске қосу ұсынылады.

- `-cert_only` – Басқару серверінің сертификаты мен жеке кілтін ғана сақтау немесе қалпына келтіру.

  Бұл жалауша Kaspersky Security Center Windows басқару серверінен Kaspersky Security Center Linux бсқару серверіне тасымалдау әрекетін орындаған кезде пайдалы болуы мүмкін. Сондай-ақ Kaspersky Security Center Linux басқару серверлері, сонымен қатар Kaspersky Security Center Windows басқару серверлері арасында басқарылатын құрылғыларды тасымалдауға болады.

Kaspersky Security Center Linux арқылы басқарылатын Kaspersky Security Center Windows басқару серверінің деректерін жылжыту үшін деректердің сақтық көшірмесін пайдалануға болады.
Kaspersky Security Center Windows және Kaspersky Security Center Linux үшін ДҚБЖ ретінде MySQL немесе MariaDB жүйесін пайдалансаңыз, `lower_case_table_names` параметрі ағымдағы және жаңа ДҚБЖ үшін сәйкес келуі керек.
Деректердің сақтық көшірмесін жасамай тұрып, `lower_case_table_names` параметрін тексеріңіз. Содан кейін Kaspersky Security Center Linux жүйесіне арналған MySQL немесе MariaDB орнату кезінде Windows жүйесіне арналған осы параметр үшін көрсетілген мәнге `lower_case_table_names` параметрін орнату керек.

Қалпына келтіру кезінде Басқару серверінің жалпы сертификаты сақтық көшірмеден басқа сертификатпен ауыстырылса, дұрыс жұмыс істеуін қамтамасыз ету үшін келесі қадамдарды орындаңыз:
1. Келесі қатені болдырмау үшін веб-консольді қайта орнатыңыз:
Басқару сервері сенімсіз сертификатты пайдаланады. Қолданбаны жарамды сертификатты көрсету арқылы қайта конфигурациялаңыз немесе негізгі әкімшіге хабарласыңыз.
2. IAM серверінің конфигурациясын тексеріңіз және қажет болған жағдайда IAM серверінің конфигурация файлына Басқару серверінің мекенжайын қосыңыз.

Басқа басқару серверінің басқаруымен басқарылатын құрылғыларды ауыстыру үшін klbackup утилитасын пайдалану

klbackup утилитасы басқа басқару серверінің басқаруындағы басқарылатын құрылғыларды ауыстыруға мүмкіндік береді. Тасымалдау әрекетін орындаған кезде, Kaspersky Security Center Windows басқару серверін Kaspersky Security Center Linux басқару серверіне klbackup утилитасы көмегімен өзгертуге болады. Сондай-ақ басқарылатын құрылғыларды Kaspersky Security Center Linux басқару серверлері, сондай-ақ Kaspersky Security Center Windows басқару серверлері арасында тасымалдауға болады.

Бастамас бұрын, **арнайы сертификатқа қойылатын талаптарды тексеріңіз**.

Егер сіз өздігінен қол қойылған сертификаттың орнына арнайы сертификатты пайдалансаңыз, Kaspersky Security Center Linux жүйесін кейінгі нұсқасына жаңартпас бұрын, сертификатта Субъектінің балама атауы (SAN) бар екеніне көз жеткізуіңіз керек. Олай болмаса, Kaspersky Security Center Linux жүйесін жаңартпас бұрын сертификатты ауыстыру маңызды. Әйтпесе, жаңартудан кейін Web Console веб-консоліне кіре алмайсыз.

Сертификатта SAN бар екеніне көз жеткізу үшін:

1. Басқару сервер орнатылған құрылғыда келесі пәрменді орындаңыз:

   - Linux құрылғысы үшін:

     ```
     sudo openssl x509 -in /var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer -noout
     -ext subjectAltName
     ```

   - Windows құрылғысы үшін:

     ```
     certutil -dump %ProgramData%\KasperskyLab\adminkit\1093\cert\klserver.cer
     ```

2. Пәрмен шығысында Субъектінің балама атауының бар екеніне және Басқару сервері құрылғысының мекенжайын қамтитынына көз жеткізіңіз.

3. Егер Тақырыптың балама атауы болмаса, klsetsrvcert утилитасын пайдаланып, реттелетін сертификатыңызды талаптарға сай келетін сертификатпен ауыстырыңыз.

klbackup утилитасы көмегімен басқа басқару серверінің басқаруындағы басқарылатын құрылғыларды ауыстыру үшін:

1. Алдыңғы құрылғыда басқару серверінің сертификаты мен жеке кілтінің сақтық көшірмесін жасаңыз.

   Сақтық көшірмені келесі жолдардың бірімен жасауға болады:

   - klbackup утилитасының интерфейсін пайдалану арқылы (тек Kaspersky Security Center Windows басқару сервері үшін)

     Kaspersky Security Center орнату қалтасындағы klbackup утилитасын іске қосыңыз, содан кейін **Тек Басқару серверінің сертификатын сақтық көшірмелеу немесе қалпына келтіру** опциясы көмегімен сақтық көшірме жасаңыз.

   - Пәрмен нұсқауын пайдалану арқылы (Kaspersky Security Center Windows және Kaspersky Security Center Linux басқару серверлерінің 15.1 немесе одан кейінгі нұсқасы үшін)

     Басқару серверінің сертификаты мен жеке кілтінің сақтық көшірмесін жасау үшін пәрмен жолындағы `-cert_only` кілтімен klbackup утилитасын іске қосыңыз.

```
klbackup -path <басқару сервері сертификатының сақтық көшірмесіне апаратын жол> -
cert_only
```

2. Алдыңғы құрылғыда басқару серверін желіден ажыратыңыз.

3. Құрылғыға басқа басқару серверіндегідей домендік атауды тағайындаңыз.

   Жаңа басқару серверіне NetBIOS атауын, FQDN және статикалық IP мекенжайын тағайындауға болады. Бұл желілік агенттер орналастырылған кезде желілік агенттің орнату бумасында басқару серверінің қандай мекенжайы орнатылғанына байланысты. Сондай-ақ желілік агент қосылатын басқару серверін анықтайтын қосылым мекенжайын пайдалануға болады (бұл мекенжайды klnagchk утилитасын қолданып, басқарылатын құрылғыларда алуға болады).

   Құрылғыға басқа басқару серверімен бірдей мекенжайды тағайындау мүмкін болмаса, жаңа басқару сервері сертификатын жасап, IAM конфигурация файлында осы сертификатты көрсету керек. Басқару серверін орнатқаннан кейін, желілік агенттерді жаңа басқару серверіне қолмен ауыстыру қажет.

4. Басқа басқару сервері бар құрылғыда сақтық көшірмеден басқару серверінің сертификатын және жеке кілтті қалпына келтіріңіз.

   Сақтық көшірмені келесі жолдардың бірімен қалпына келтіруге болады:

   - klbackup утилитасының интерфейсін пайдалану арқылы (тек Kaspersky Security Center Windows басқару сервері үшін)

     klbackup утилитасын іске қосыңыз, содан кейін **Тек Басқару серверінің сертификатын сақтық көшірмелеу немесе қалпына келтіру** опциясы көмегімен сақтық көшірмені қалпына келтіріңіз.

   - Пәрмен нұсқауын пайдалану арқылы (Kaspersky Security Center Windows және Kaspersky Security Center Linux басқару серверлерінің 15.1 немесе одан кейінгі нұсқасы үшін)

     Басқару серверінің сертификаты мен жеке кілтінің сақтық көшірмесін қалпына келтіру үшін пәрмен жолындағы `-cert_only` кілтімен klbackup утилитасын іске қосыңыз.

     ```
     klbackup -path <басқару сервері сертификатының сақтық көшірмесіне апаратын жол> -
     restore -cert_only
     ```

5. Басқару сервері және IAM сервері арқылы сертификатты тексеруді конфигурациялаңыз.

Басқарылатын құрылғылар басқа басқару серверінің басқаруына тапсырылады. Осы басқару серверіне өтіп, басқарылатын құрылғылардың желіде көрінетініне және желілік агент орнатылып, оларда жұмыс істейтініне көз жеткізуге болады (**Көзге көрінетін** опциясындағы *Иә* мәні, **Желілік агент орнатылған** және **Желілік агент іске қосулы** бағандары).

MySQL немесе MariaDB пайдалану кезінде басқару сервері деректерінің сақтық көшірмесін жасау және қалпына келтіру

Басқару сервері деректерін Kaspersky Security Center Linux басқаруындағы Kaspersky Security Center Windows жүйесінен тасымалдау үшін деректердің сақтық көшірмесін пайдалануға болады. Басқару сервері деректерінің сақтық көшірмесін пайдалану арқылы тасымалдау әрекетіне Kaspersky Security Center Windows жүйесінің кез келген қолдау көрсетілетін нұсқасынан Kaspersky Security Center Linux 15.2 немесе одан кейінгі нұсқасына тасымалдау арқылы ғана қолдау көрсетіледі.

Kaspersky Security Center Windows және Kaspersky Security Center Linux үшін ДҚБЖ ретінде MySQL немесе MariaDB жүйесін пайдалансаңыз, `lower_case_table_names` параметрі ағымдағы және жаңа ДҚБЖ үшін сәйкес келуі керек. Әйтпесе басқару серверінің деректері қате тасымалданады.

Kaspersky Security Center Windows жүйесінде басқару серверінің деректерінің сақтық көшірмесін жасамай тұрып, `lower_case_table_names` параметрінің мәнін тексеріңіз. ДҚБЖ орнату кезінде бұл параметрді бұрын көрсетпесеңіз, әдепкі параметр мәні пайдаланылады. Windows жүйесіне арналған `lower_case_table_names` параметрінің әдепкі мәні — `1`.

Kaspersky Security Center Linux жүйесіне арналған MySQL немесе MariaDB орнату кезінде MySQL веб-сайтындағы нұсқауды пайдаланып, `lower_case_table_names` параметрін Windows жүйесіне арналған осы параметр үшін көрсетілген мәнге орнатыңыз. Бұл параметрді көрсетпесеңіз, әдепкі параметр мәні пайдаланылады. Linux негізіндегі операциялық жүйелер үшін `lower_case_table_names` параметрінің әдепкі мәні Windows жүйесіне арналған әдепкі мәннен өзгеше.

MySQL 8.0 орнатқыңыз келсе, осы нұсқауға сәйкес `lower_case_table_names` параметрін көрсету жұмыс істемеуі мүмкін. Бұл жағдайда алдымен MySQL 5.7 орнатуыңыз керек, нұсқауды пайдаланып, `lower_case_table_names` параметрін көрсетіңіз, содан кейін MySQL 5.7 нұсқасын MySQL 8.0 нұсқасына жаңартыңыз. `lower_case_table_names` параметрі ағымдағы және жаңа ДҚБЖ-ларға сәйкес келмесе, басқару серверінің деректері дұрыс қалпына келтірілмейді.

Басқару серверіне техникалық қызмет көрсету

Басқару серверіне техникалық қызмет көрсету, Басқару сервері қалтасында орынды босатуға және қажет емес нысандарды жою арқылы дерекқордың өлшемін азайтуға мүмкіндік береді. Бұл қолданбаның өнімділігі мен сенімділігін жақсартуға көмектеседі. Басқару серверіне аптасына бір реттен сиретпей техникалық қызмет көрсету ұсынылады.

Басқару серверіне техникалық қызмет көрсету тиісті тапсырманың көмегімен орындалады. Басқару серверіне техникалық қызмет көрсету барысында бағдарлама келесі әрекеттерді орындайды:

- Сақтау қалтасынан қажет емес қалталар мен файлдарды жояды.
- Кестелерден қажет емес жазбаларды жояды («аспалы көрсеткіштер» деп те аталады).
- Кэшті тазартады.
- Дерекқорды сақтайды (ДҚБЖ ретінде PostgreSQL пайдалансаңыз):
  - дерекқордың индекстерін қайта құрады;
  - дерекқордың статистикасын жаңартады;
  - дерекқорды қысады (қажет болса).

Басқару серверіне техникалық қызмет көрсету тапсырмасы MariaDB 10.3 және одан жоғары нұсқасын қолдайды. MariaDB 10.2 немесе одан кейінгі нұсқасын пайдалансаңыз, әкімшілер дерекқорға өздері қызмет көрсетуі керек.

Басқару серверіне техникалық қызмет көрсету тапсырмасы Kaspersky Security Center Linux жүйесін орнату кезінде автоматты түрде жасалады. Басқару серверіне техникалық қызмет көрсету тапсырмасы жойылған, сіз оны қолмен жасай аласыз.

Басқару серверіне техникалық қызмет көрсету тапсырмасын жасау үшін:

1. Бағдарламаның негізгі терезесінде **Тапсырмалар** бөліміне өтіңіз.
2. **Қосу** түймесін басыңыз.

   Жаңа тапсырма жасау шебері іске қосылады.
3. Шебердің **Жаңа тапсырма параметрлері** терезесінде **Басқару серверіне техникалық қызмет көрсету** тапсырма түрін таңдап, **Келесі** түймесін басыңыз.
4. Шебердің келесі қадамдарын орындаңыз.

Нәтижесінде, жасалған тапсырма тапсырмалар тізімінде көрсетіледі. Бір Басқару сервері үшін бір Басқару серверіне техникалық қызмет көрсету тапсырмасы ғана орындалуы мүмкін. Басқару серверіне техникалық қызмет көрсету тапсырмасы Басқару сервері үшін әлдеқашан жасалған болса, басқа Басқару серверіне техникалық қызмет көрсету тапсырмасын жасау мүмкін емес.

Басқару серверлерінің иерархиясын жою

Егер сізге бұдан былай Басқару сервері иерархиясы қажет болмаса, оларды осы иерархиядан ажыратуға болады.

Басқару сервері иерархиясын жою үшін:

1. Негізгі мәзірдегі басқару серверінің атауын басыңыз.
2. Ашылған бетте **Басқару серверлері** қойыншасына өтіңіз.
3. Қосалқы Басқару серверін жойғыңыз келетін басқару тобында қосалқы Басқару серверін таңдаңыз.
4. Мәзірден **Жою** тармағын таңдаңыз.
5. Ашылған терезеде қосалқы Басқару серверін жоюды растау үшін **OK** түймесін басыңыз.

Бұрынғы негізгі Басқару сервері және бұрынғы қосалқы Басқару сервері енді бір-бірінен тәуелсіз. Серверлер иерархиясы енді жоқ.

Жалпыға қолжетімді DNS серверлеріне қатынасу

Жүйелік DNS арқылы Kaspersky серверлеріне қатынасу мүмкін болмаса, Kaspersky Security Center Linux жалпыға қолжетімді DNS серверлерін келесі ретпен пайдалана алады:

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).

Қолданба DNS серверімен TCP/UDP қосылымын орнатқандықтан, DNS серверлеріне сұрауларда домен мекенжайлары мен Басқару серверінің жалпыға қолжетімді IP мекенжайы болуы мүмкін. Kaspersky Security Center Linux жалпыға қолжетімді DNS серверін пайдаланса, деректерді өңдеу тиісті сервистің құпиялылық саясатымен реттеледі.

klscflag утилитасын пайдаланып жалпы DNS пайдалануды орнату үшін:

1. Пәрмен жолын іске қосыңыз және ағымдағы каталогты klscflag утилитасы бар каталогке өзгертіңіз. Klscflag утилитасы Басқару сервер орнатылған каталогте орналасқан. Әдепкі бойынша жол - /opt/kaspersky/ksc64/sbin.

2. Қоғамдық DNS пайдалануды өшіру үшін root есептік жазбасында келесі пәрменді орындаңыз:

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

3. Қоғамдық DNS пайдалануды қосу үшін root есептік жазбасында келесі пәрменді орындаңыз:

   ```
   klscflag -fset -pv ".core/.independent" -s Transport -n ForceUseSystemDNS -t d -v 0
   ```

Интерфейсті конфигурациялау

Сіз Kaspersky Security Center Web Console интерфейсін пайдаланылатын функцияларға байланысты интерфейс бөлімдері мен элементтерін көрсетуге және жасыруға конфигурациялай аласыз.

Kaspersky Security Center Web Console интерфейсін қазіргі уақытта қолданылатын функциялар жиынтығына сай конфигурациялау үшін:

1. Негізгі мәзірдегі **Параметрлер** → **Интерфейс опциялары** бөліміне өтіңіз.

2. Қажетті параметрлерді қосыңыз немесе өшіріңіз:

   - **Деректерді шифрлау және қорғау опциясын көрсету**
   - **MDR функцияларын көрсету**
   - **EDR дабылдарын көрсету**

3. **Сақтау** түймесін басыңыз.

Қажетті параметрлерді қосқаннан кейін, консоль негізгі мәзірде тиісті бөлімдерді көрсетеді. Мысалы **EDR дабылдарын көрсету** опциясын қоссаңыз, **Мониторинг** → **Дабылдар** бөлімі басты мәзірде пайда болады.

Басқару серверіне қорғалған қосылым

Клиент құрылғылары мен басқару сервері арасындағы дерек алмасу TLS (Transport Layer Security) протоколы арқылы жүзеге асырылуы мүмкін. TLS протоколы, қосылған кезде өзара әрекеттесетін тараптарды анықтауға, жіберілетін деректерді шифрлауға және оларды тасымалдау кезінде өзгерістерден қорғауға мүмкіндік береді. TLS протоколының негізінде өзара әрекеттесетін тараптардың түпнұсқалық растамасы және жалпыға ортақ кілт әдісі бойынша деректерді шифрлау жатыр.

Клиент құрылғысын Басқару серверіне алғаш рет қосқан кезде құрылғыдағы Желілік агент Басқару сервері сертификатының көшірмесін алады және оны жергілікті түрде сақтайды.

Желілік агентті құрылғыға жергілікті түрде орнатқан кезде Басқару сервері сертификатын қолмен таңдауға болады.

Сертификаттың алынған көшірмесі негізінде Басқару серверінің құқықтары мен өкілеттіктері келесі қосылымдар кезінде тексеріледі.

Болашақта, құрылғыны Басқару серверіне қосқан сайын Желілік агент Басқару серверінің сертификатын сұрайды және оны жергілікті көшірмемен салыстырады. Олар бір-біріне сәйкес келмесе, Басқару серверіне құрылғыға қатынасуға рұқсат етілмейді.

TLS қосылымын шифрлау

Ұйымыңыздың желісіндегі осалдықтарды түзету үшін TLS протоколымен трафикті шифрлауды қосуға болады. Басқару серверде TLS шифрлау протоколдарын және қолдау көрсетілетін шифр жиынтықтарын қосуға болады. Kaspersky Security Center Linux жүйесі TLS протоколының 1.0, 1.1, 1.2 және 1.3 нұсқаларына қолдау көрсетеді. Сіз қажетті шифрлау протоколы мен шифрлау жиынтықтарын таңдай аласыз.

Kaspersky Security Center Linux бағдарламасы өздігінен қол қойылатын сертификаттарды қолданады. Сондай-ақ, сіз өзіңіздің сертификаттарыңызды да қолдана аласыз. Сенімді сертификаттау орталығы қол қойған сертификаттарды қолдану ұсынылады.

Басқару серверінде рұқсат етілген шифрлау протоколдары мен шифрлау жиынтықтарын конфигурациялау үшін:

1. Пәрмен жолын іске қосыңыз және ағымдағы каталогты klscflag утилитасы бар каталогке өзгертіңіз. Klscflag утилитасы Басқару сервер орнатылған каталогте орналасқан. Әдепкі бойынша жол - /opt/kaspersky/ksc64/sbin.

2. Әкімшілік серверде рұқсат етілген шифрлау протоколдары мен шифрлау жиынтықтарын орнату үшін SrvUseStrictSslSettings жалаушасын қолданыңыз. root есептік жазбасындағы пәрмен жолында келесі пәрменді іске қосыңыз:

   ```
   ./klscflag -fset -pv ".core/.independent" -s Transport -n SrvUseStrictSslSettings -v <мән> -t d
   ```

   SrvUseStrictSslSettings жалаушасының <мән> параметрін көрсетіңіз:

   - 4 – TLS протоколдарының тек 1.2 және 1.3 нұсқалары қосылған. Сондай-ақ TLS_RSA_WITH_AES_256_GCM_SHA384 бар шифрлау жиынтығы қосылған (бұл шифрлау жиынтықтары Kaspersky Security Center Linux алдыңғы нұсқаларымен кері үйлесімділік үшін қажет). Бұл әдепкі бойынша мәні.

     TLS 1.2 протоколы қолдау көрсететін шифрлау жиынтықтары:

     - ECDHE-RSA-AES256-GCM-SHA384
     - ECDHE-RSA-AES256-SHA384
     - ECDHE-RSA-CHACHA20-POLY1305
     - AES256-GCM-SHA384 (TLS_RSA_WITH_AES_256_GCM_SHA384 шифр жинағымен)

- ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-RSA-AES128-SHA256

TLS 1.3 протоколы қолдау көрсететін шифрлау жиынтықтары:

- TLS_AES_256_GCM_SHA384
- TLS_CHACHA20_POLY1305_SHA256
- TLS_AES_128_GCM_SHA256
- TLS_AES_128_CCM_SHA256

- 5 – TLS протоколдарының тек 1.2 және 1.3 нұсқалары қосылған. TLS протоколының 1.2 және 1.3 нұсқалары төменде берілген арнайы шифрлау жиынтықтарына қолдау көрсетеді.

  TLS 1.2 протоколы қолдау көрсететін шифрлау жиынтықтары:

  - ECDHE-RSA-AES256-GCM-SHA384
  - ECDHE-RSA-AES256-SHA384
  - ECDHE-RSA-CHACHA20-POLY1305
  - ECDHE-RSA-AES128-GCM-SHA256
  - ECDHE-RSA-AES128-SHA256

  TLS 1.3 протоколы қолдау көрсететін шифрлау жиынтықтары:

  - TLS_AES_256_GCM_SHA384
  - TLS_CHACHA20_POLY1305_SHA256
  - TLS_AES_128_GCM_SHA256
  - TLS_AES_128_CCM_SHA256

SrvUseStrictSslSettings жалауша параметрінің мәндері үшін 0, 1, 2 немесе 3 мәндерін пайдалану ұсынылмайды. Бұл параметр мәндері TLS протоколының қауіпті нұсқаларына (TLS 1.0 және TLS 1.1) және қауіпті шифрлау жиынтықтарына сәйкес келеді және Kaspersky Security Center бағдарламасының бұрынғы нұсқаларымен кері үйлесімділік үшін ғана пайдаланылады.

3. Kaspersky Security Center Linux келесі қызметтерін қайта іске қосыңыз:

- Басқару сервері
- Веб-сервер
- Прокси-серверді белсендіру қызметі

Нәтижесінде TLS протоколы арқылы трафикті шифрлау қосылады.

KLTR_TLS12_ENABLED және KLTR_TLS13_ENABLED жалаушаларын сәйкесінше TLS 1.2 және 1.3 протоколдарына қолдау көрсетуді қосу үшін пайдалануға болады. Бұл жалаушалар әдепкі бойынша қосылады.

TLS 1.2 және 1.3 протоколдарына қолдау көрсетуді қосу немесе өшіру үшін:

1. klscflag утилитасын іске қосыңыз.

   Пәрмен жолын іске қосыңыз және ағымдағы каталогты klscflag утилитасы бар каталогке өзгертіңіз. Klscflag утилитасы Басқару сервер орнатылған каталогте орналасқан. Әдепкі бойынша жол - /opt/kaspersky/ksc64/sbin.

2. root есептік жазбасында пәрмен жолында келесі пәрмендердің бірін іске қосыңыз:

   - TLS 1.2 протоколының қолдауын қосу немесе өшіру үшін осы пәрменді пайдаланыңыз:

     ```
     ./klscflag -fset -pv ".core/.independent" -s Transport -n KLTR_TLS12_ENABLED -v <мән> -t d
     ```

   - TLS 1.3 протоколының қолдауын қосу немесе өшіру үшін осы пәрменді пайдаланыңыз:

     ```
     ./klscflag -fset -pv ".core/.independent" -s Transport -n KLTR_TLS13_ENABLED -v <мән> -t d
     ```

   Жалаушаның <мән> параметрін көрсетіңіз:

   - `1` – TLS протоколының қолдауын қосу үшін.
   - `0` – TLS протоколының қолдауын өшіру үшін.

Сыртқы қызметтермен әрекеттесуге арналған желі параметрлері

Kaspersky Security Center Linux жүйесі сыртқы қызметтермен әрекеттесу үшін келесі желі параметрлерін пайдаланады.

Желі параметрлері	Мекенжай	Сипаттамасы
Порт: 443 Протокол: HTTPS	`https://activation-v2.kaspersky.com`	Бағдарламаны белсендіру.

Порт: 443
Протокол: 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`
		Kaspersky дерекқорлары, бағдарламалық жасақтама модульдеріне мен бағдарламаларын арналған жаңартулар.

Порт: 443 Протокол: HTTPS	`https://downloads.upd.kaspersky.com`	• Kaspersky дерекқорлары, бағдарламалық жасақтама модульдеріне мен бағдарламаларын арналған жаңартулар. • Kaspersky серверлерінің қолжетімділігін тексеру. Kaspersky Security Center Linux бағдарламасы Kaspersky дерекқорлары мен бағдарламалық модульдерін жүктемес бұрын Kaspersky серверлерінің қолжетімділігін тексереді. Жүйелік DNS арқылы серверлерге қатынасу мүмкін болмаса, бағдарлама жалпыға ортақ DNS серверлерін пайдаланады.

Желі параметрлері	Мекенжай	Сипаттамасы
Порт: 80 Протокол: HTTP	http://p00.upd.kaspersky.com http://p01.upd.kaspersky.com http://p02.upd.kaspersky.com http://p03.upd.kaspersky.com http://p04.upd.kaspersky.com http://p05.upd.kaspersky.com http://p06.upd.kaspersky.com http://p07.upd.kaspersky.com http://p08.upd.kaspersky.com http://p09.upd.kaspersky.com http://p10.upd.kaspersky.com http://p11.upd.kaspersky.com http://p12.upd.kaspersky.com http://p13.upd.kaspersky.com http://p14.upd.kaspersky.com http://p15.upd.kaspersky.com http://p16.upd.kaspersky.com http://p17.upd.kaspersky.com http://p18.upd.kaspersky.com http://p19.upd.kaspersky.com http://downloads0.kaspersky-labs.com http://downloads1.kaspersky-labs.com http://downloads2.kaspersky-labs.com http://downloads3.kaspersky-labs.com http://downloads4.kaspersky-labs.com http://downloads5.kaspersky-labs.com http://downloads6.kaspersky-labs.com http://downloads7.kaspersky-labs.com http://downloads8.kaspersky-labs.com http://downloads9.kaspersky-labs.com http://downloads.kaspersky-labs.com http://cm.k.kaspersky-labs.com	Kaspersky дерекқорлары, бағдарламалық жасақтама модульдеріне мен бағдарламаларын арналған жаңартулар.
Порт: 443 Протокол: HTTPS	https://ds.kaspersky.com https://dc1.ksn.kaspersky-labs.com https://dc1-file.ksn.kaspersky-labs.com https://dc1-pp.ksn.kaspersky-labs.com https://dc1-st.ksn.kaspersky-labs.com/ https://dc1-cert.ksn.kaspersky-labs.com https://dc1-cf.ksn.kaspersky-labs.com https://dc1-file.ksn.kaspersky-labs.com https://dc1-kas.ksn.kaspersky-labs.com https://dc1-ml.ksn.kaspersky-labs.com https://dc1-pp.ksn.kaspersky-labs.com https://dc1-st.ksn.kaspersky-labs.com https://dc1.ksn.kaspersky-labs.com	Kaspersky Security Network қолдану.

Желі параметрлері	Мекенжай	Сипаттамасы
Порт: 443, 1443 Протокол: HTTPS	https://ksn-file-geo.kaspersky-labs.com https://ksn-verdict-geo.kaspersky-labs.com https://ksn-url-geo.kaspersky-labs.com https://ksn-a-p2p-geo.kaspersky-labs.com https://ksn-info-geo.kaspersky-labs.com https://ksn-cinfo-geo.kaspersky-labs.com	Kaspersky Security Network қолдану.
Порт: 443, 1443 Протокол: KSN	ksn://ksn-a-p2p-geo.kaspersky-labs.com ksn://ksn-a-stat-geo.kaspersky-labs.com ksn://ksn-ca-geo.kaspersky-labs.com ksn://ksn-cinfo-geo.kaspersky-labs.com ksn://ksn-crypto-catm-geo.kaspersky-labs.com ksn://ksn-crypto-dnscheck-geo.kaspersky-labs.com ksn://ksn-crypto-hash-geo.kaspersky-labs.com ksn://ksn-crypto-ipm-geo.kaspersky-labs.com ksn://ksn-crypto-whocalls-geo.kaspersky-labs.com ksn://ksn-crypto-wifiplus-geo.kaspersky-labs.com ksn://ksn-eu-stat-kmp.kaspersky-labs.com ksn://ksn-file-geo.kaspersky-labs.com ksn://ksn-his-geo.kaspersky-labs.com ksn://ksn-info-geo.kaspersky-labs.com ksn://ksn-kas-geo.kaspersky-labs.com ksn://ksn-kddi.kaspersky-labs.com ksn://ksn-ml-geo.kaspersky-labs.com ksn://ksn-oui-geo.kaspersky-labs.com ksn://ksn-pp.kaspersky-labs.com ksn://ksn-src.kaspersky-labs.com ksn://ksn-stat-geo.kaspersky-labs.com ksn://ksn-tcert-geo.kaspersky-labs.com ksn://ksn-url-geo.kaspersky-labs.com ksn://ksn-verdict-geo.kaspersky-labs.com ksn://mdr.ksn.kaspersky-labs.com ksn://stat-eu.ksn.kaspersky-labs.com ksn://stat-hq.ksn.kaspersky-labs.com ksn://stat-ru.ksn.kaspersky-labs.com ksn://stat-sa.ksn.kaspersky-labs.com ksn://stat-sbr.ksn.kaspersky-labs.com	Kaspersky Security Network қолдану.
Порт: 443 Протокол: HTTPS	https://click.kaspersky.com https://redirect.kaspersky.com	Интерфейстегі сілтемелерге өту.

Желі параметрлері	Мекенжай	Сипаттамасы
Порт: 80 Протокол: HTTP	`http://crl.kaspersky.com` `http://ocsp.kaspersky.com`	Бұл серверлер ашық кілттер инфрақұрылымының (PKI) бөлігі болып табылады және Kaspersky сандық қолтаңбасы сертификаттарының жарамдылық күйін тексеру үшін қажет. CRL – кері қайтарып алынған сертификаттар тізімі болып табылады. OCSP нақты уақыт режимінде нақты сертификаттың күйін сұрауға мүмкіндік береді. Бұл қызметтер сандық сертификаттармен қауіпсіз өзара әрекетті қамтамасыз етуге және ықтимал шабуылдардан қорғауға көмектеседі.
Порт: 443 Протокол: HTTPS	`https://ipm-klca.kaspersky.com`	Жарнамалық хабарландырулар.
Порт: 443 Протокол: HTTPS	`https://tip.kaspersky.com`	Kaspersky Threat Intelligence Portal арқылы қауіптерге жауап беру (Kaspersky Security: Бизнеске арналған Кәсіби функциясын пайдаланған кезде).
Порт: 443 Протокол: HTTPS	Мекенжайлардың толық тізімін көру үшін Мекенжай және домен құрылымын қараңыз.	Kaspersky Automated Security Awareness Platform арқылы қауіптерге жауап беру (Kaspersky Security: Бизнеске арналған Кәсіби функциясын пайдаланған кезде).

Kaspersky Security Center Linux жүйесінің сыртқы қызметтермен дұрыс әрекеттесуін қамтамасыз ету үшін келесі ұсыныстарды орындаңыз:
- Ұйымыңыздың желілік жабдығы мен прокси серверіндегі 443 және 1443 порттарында шифрланбаған желілік трафикке рұқсат етілуі керек.
- Басқару сервер Kaspersky жаңарту серверлерімен және Kaspersky Security Network серверлерімен әрекеттескенде, сертификатты ауыстыру арқылы желілік трафикті (MITM шабуылдары) ұстап қалуға жол бермеу керек.

klscflag утилитасын пайдаланып, HTTP немесе HTTPS протоколы арқылы жаңартуларды жүктеп алу үшін:

1. Пәрмен жолын іске қосыңыз және ағымдағы каталогты klscflag утилитасы бар каталогке өзгертіңіз. Klscflag утилитасы Басқару сервер орнатылған каталогте орналасқан. Әдепкі бойынша жол - /opt/kaspersky/ksc64/sbin.

2. Жаңартуларды HTTP протоколы арқылы жүктеп алғыңыз келсе, келесі пәрмендердің бірін root есептік жазбасымен іске қосыңыз:

   - Басқару сервер орнатылған құрылғыда:

     ```
     klscflag -fset -pv klserver -s Updater -n DisableKLHttps -t d -v 1
     ```

   - Тарату нүктесіне:

     ```
     klscflag -fset -pv klnagent -s Updater -n DisableKLHttps -t d -v 1
     ```

   Жаңартуларды HTTPS протоколы арқылы жүктеп алғыңыз келсе, келесі пәрмендердің бірін root есептік жазбасымен іске қосыңыз:

   - Басқару сервер орнатылған құрылғыда:

     ```
     klscflag -fset -pv klserver -s Updater -n DisableKLHttps -t d -v 0
     ```

   - Тарату нүктесіне:

     ```
     klscflag -fset -pv klnagent -s Updater -n DisableKLHttps -t d -v 0
     ```

Глобалды қосалқы желілердің тізімі

Сіз пайдаланатын әрбір басқару сервері үшін желіңіздің ішкі желілері туралы ақпаратты сақтау үшін ішкі желілердің ғаламдық тізімін орнатуға болады. Бұл тізім филиалдардың кеңселері сияқты физикалық бірліктер мен жұптарды (IP мекенжайы, бүркеніш) салғастыруға мүмкіндік береді. Сіз желілік ережелер мен параметрлердегі тізімнен ішкі желілерді қолдана аласыз.

Глобалды қосалқы желілердің тізіміне ішкі желіні қосу үшін:

1. Негізгі мәзірдегі басқару серверінің атауын басыңыз.

   Басқару серверінің сипаттары терезесі ашылады.

2. **Жалпы** қойындысындағы **Глобалды ішкі желілер** бөлімін таңдаңыз.

3. **Қосу** түймесін басыңыз.

   Жаңа ішкі желі терезесі ашылады.

4. Келесі өрістерді толтырыңыз:

   - **Атауы**
   - **Ішкі желінің мекенжайы**
   - **Ішкі желі маскасы**
   - **Сипаттама**

5. **Сақтау** түймесін басыңыз.

Терезе жабылады және ішкі желі ішкі желілер тізімінде пайда болады.

Қажет болса, жаһандық ішкі желілер тізімінде келесі әрекеттерді орындауға болады:

- Қажетті ішкі желіні таңдап, **Жою** түймесін басу арқылы тізімнен ішкі желілерді жою.
- Қажетті ішкі желі атауы бар сілтемені басу арқылы ішкі желілердің сипаттарын өзгерту, содан кейін 4-5-қадамдарда сипатталған әрекеттерді орындау.

klscmodchk және integrity_checker утилиталарын пайдалану арқылы модульдердің тұтастығын тексеру

Kaspersky Security Center Linux құрамында динамикалық түрде байланысқан кітапханалар, орындалатын файлдар, конфигурация файлдары және интерфейс файлдары түріндегі бірнеше екілік модуль бар. Зиянкестер бір немесе бірнеше орындалатын модульді немесе қолданба файлдарын зиянды кодты қамтитын басқа файлдармен ауыстыруы мүмкін. Модуль мен файлдарды ауыстыруға жол бермеу үшін Kaspersky Security Center Linux жүйесі klscmodchk және integrity_checker утилиталарын пайдалану арқылы құрамдас тұтастығының тексерісін қамтамасыз етеді. Бұл утилиталар модульдер мен файлдарда рұқсат етілмеген өзгерістер мен зақымның бар-жоғын тексереді. Модульде немесе қолданба файлында қате тексеру сомасы болса, ол зақымдалған болып саналады.

Klscmodchk утилитасы келесі Kaspersky Security Center Linux құрамдастарының тұтастығын тексереді:

- Басқару сервері
- Желілік агент

Integrity_checker утилитасы келесі Kaspersky Security Center Linux құрамдастарының тұтастығын тексереді:

- Басқару сервері
- Желілік агент
- Kaspersky Security Center Web Console

Екі утилита да Kaspersky Security Center Linux құрылымының бір бөлігі болатын және орнату қалтасында орналасқан kl_file_integrity_manifest.xml манифест файлының негізінде модуль тұтастығын тексереді. Құрамдастың манифест файлында тұтастығы Kaspersky Security Center Linux құрамдасының дұрыс жұмыс істеуі үшін маңызды файлдар бар. Манифест файлдарының тұтастығы да тексеріледі.

Kl_file_integrity_manifest.xml манифест файлын өзгерту ұсынылмайды, себебі бұл сандық қолтаңбаны жарамсыз қылады және тұтастықты тексеру сәтсіз аяқталады.

Kaspersky Security Center Linux құрамдасының тұтастығын тексеру үшін келесі пәрмендердің бірін орындаңыз:

- `$ klscmodchk [ параметрлер ]`

  Klscmodchk утилитасы integrity_checker утилитасын `--verbose` параметрімен іске қосады және модульдердің тұтастығын тексереді.

  Klscmodchk утилитасының параметрлері:

  - `-logfile < журнал_файлының_жолы >`: журналға жазу үшін дискідегі файл жолын көрсетіңіз. Әдепкісінше ақпарат консольге шығарылады.
  - `-verbose`: тұтастықты тексеру кезінде кеңейтілген ақпаратты шығару.

- `$ integrity_checker [ параметрлер ] < manifest_file_path >`

Integrity_checker утилитасының параметрлері:

- `--help`: integrity_checker утилитасының анықтамасын көрсету.
- `--version`: integrity_checker утилитасының нұсқасын көрсету.
- `--verbose`: утилитаның жұмысы туралы ақпаратты көрсету. Тұтастығын тексеру кезінде пәрменде осы параметрді пайдалану жеткілікті.

Әрбір манифест файлын тексеру нәтижесі манифест файлы атауының жанында келесі форматта көрсетіледі:

- SUCCEEDED: файлдың тұтастығы расталды (қайтару коды: 0).
- FAILED: файлдың тұтастығы расталмады (нөлге тең емес емес қайтару коды).

Сондай-ақ қолданбаны іске қосқан кезде автоматты түрде іске қосылуы үшін, тұтастық тексерістерін конфигурациялауға болады. Тұтастықты автоматты түрде тексеру әдепкісінше өшірілген болады.

Тұтастықты автоматты түрде тексеруді қосу үшін:

1. Басқару сервері орнатылған құрылғыда пәрмен жолына келесі пәрменді енгізіңіз:

   ```
   ./klscflag -fset -pv klserver -n KLMODCHK_ENABLE_CHECKING -t d -v 1
   ```

2. Құрылғыны өшіріп қосыңыз.

Тұтастықты автоматты түрде тексеру қосылды.

Kaspersky Security Center келесіде іске қосылғанда, klscmodchk утилитасы басқару серверімен бірге іске қосылады және модульдердің тұтастығын тексеруді бастайды. Тұтастықты тексеру нәтижесі Kaspersky Event журналына жазылады.

Желідегі құрылғыларды табу

Бұл бөлімде құрылғыларды іздеу және желі сауалнамасы сипатталған.

Kaspersky Security Center Linux белгіленген критерийлер негізінде құрылғыларды іздеуге мүмкіндік береді. Іздеу нәтижелерін мәтіндік файлға сақтауға болады.

Іздеу функциясы келесі құрылғыларды табуға мүмкіндік береді:

- Басқару сервері және оның қосалқы Серверлері топтарындағы басқарылатын құрылғылары;
- Басқару сервері мен оның бағынышты Басқару серверлері басқаратын тағайындалмаған құрылғылар.

Сценарий: Желілік құрылғыларды табу

Қауіпсіздік бағдарламаларын орнатпас бұрын құрылғыларды іздеу керек. Егер желілік құрылғылар табылса, олар туралы ақпарат алуға және оларды саясат арқылы басқаруға болады. Жаңа құрылғылардың пайда болуын және желіде бұрын табылған құрылғылардың болуын тексеру үшін үнемі желілік сауалнамалар өткізіп тұру қажет.

Желілік құрылғыларды анықтау келесі кезеңдерден тұрады:

1. **Құрылғыларды бастапқы табу**

   Бағдарламаны жылдам іске қосу шебері жұмысын аяқтағаннан кейін құрылғыларды табу үшін желіде сауалнаманы қолмен орындаңыз.

2. **Болашақ сауалнамаларды конфигурациялау**

   Бұл IP-ауқымдарының сауалнамасы қосылғанына және сауалнама кестесі сіздің ұйымыңыздың талаптарына сәйкес келетініне көз жеткізіңіз. Сауалнама кестесін орнатқан кезде желі сауалнамасының жиілігіне арналған ұсыныстарға сүйеніңіз.

   Сондай-ақ, желіңізде IPv6 құрылғылары болса, Zeroconf сауалнамасын қосуға болады.

   Егер желілік құрылғылар доменге қосылса, домен контроллері сұрауын пайдалану ұсынылады.

   Windows желілеріне сауалнама жүргізу үшін Windows негізіндегі тарату нүктелерін пайдаланыңыз.

3. **Табылған құрылғыларды басқару топтарына қосу ережелерін орнату (қажет болса)**

   Желіде жаңа құрылғылар пайда болса, олар әдеттегі сауалнамалар кезінде табылып, **Тағайындалмаған құрылғылар** тобына автоматты түрде қосылады. Қажет болса, осы құрылғыларды **Басқарылатын құрылғылар** тобына автоматты түрде жылжыту ережелерін конфигурациялауға болады. Сондай-ақ, сақтау ережелерін конфигурациялауға болады.

   Егер сіз ережелер белгіленген кезеңді өткізіп алсаңыз, барлық жаңа құрылғылар **Тағайындалмаған құрылғылар** тобына орналастырылады. Сіз осы құрылғыларды **Басқарылатын құрылғылар** тобына қолмен жылжыта аласыз. Құрылғыларды **Басқарылатын құрылғылар** тобына қолмен жылжытқан болсаңыз, онда сіз құрылғылардың әрқайсысы туралы ақпаратты талдап, оны басқару тобына және қайсысына жылжыту керектігін шеше аласыз.

Нәтижелер

Сценарийдің аяқталуы арқасында:

- Kaspersky Security Center Linux Басқару сервері желідегі құрылғыларды анықтайды және олар туралы ақпарат береді.
- Желінің болашақ сауалнамалары және оларды іске қосу кестесі конфигурацияланды.

Жаңадан табылған құрылғылар конфигурацияланған ережелерге сәйкес орналастырылады. (Болмаса ережелер конфигурацияланбаса, құрылғылар **Тағайындалмаған құрылғылар** тобында қалады).

Windows желісінің сауалнамасы

Windows желісінің сауалнамасы туралы

Kaspersky Security Center басқару сервері Linux Windows желісінің сауалнамасына қолдау көрсетпейді. Windows желілеріне сауалнама жүргізу үшін Windows негізіндегі тарату нүктелерін пайдаланыңыз.

Жылдам сауалнама кезінде тарату нүктелері желінің барлық домені мен жұмыс тобы құрылғыларының NetBIOS атаулары тізімі туралы ақпаратты ғана алады. Толық сауалнама барысында, әрбір клиент құрылғысынан келесі ақпарат сұралады:

- Операциялық жүйенің аты
- IP мекенжайы
- DNS атауы
- NetBIOS атауы

Жылдам сауалнама кезінде де, толық сауалнама кезінде де керегі:

- UDP 137/138, TCP 139, UDP 445, TCP 445 ашық порттары.
- Қосулы SMB протоколы.
- Microsoft Computer Browser қызметі қолданылуы тиіс, ал негізгі браузер рөлін атқаратын құрылғы Басқару серверінде қолжетімді болуы керек;
- Microsoft Computer Browser қызметі қолданылуы тиіс, ал негізгі браузер рөлін атқаратын құрылғы клиент құрылғысында қолжетімді болуы керек:
  - Желілік құрылғылардың саны 32-ден аспаса, кемінде бір құрылғының болуы.
  - Әрбір 32 желілік құрылғыға кемінде бір құрылғының болуы.

Желінің толық сауалнамасы, егер жылдам сауалнама кемінде бір рет іске қосылған болса ғана іске қосылуы тиіс.

IP ауқымдарының сауалнамасы

Kaspersky Security Center Linux бағдарламасы атауды кері түрлендіруді: көрсетілген ауқымдағы әрбір IPv4 мекенжайы үшін стандартты DNS сұраулары арқылы DNS атауын түрлендіруді орындауға тырысады. Осы операция сәтті аяқталса, сервер `ICMP ECHO REQUEST` (ping пәрменінің баламасы) сұрауын алынған атауға жібереді. Егер құрылғы жауап берсе, бұл құрылғы туралы ақпарат Kaspersky Security Center Linux дерекқорына қосылады. Атауды кері түрлендіру, IP мекенжайлары болуы мүмкін, бірақ желілік принтерлер немесе роутерлер сияқты компьютерлер болып саналмайтын желілік құрылғыларды алып тастау үшін қажет.

Бұл сауалнама тәсілі дұрыс конфигурацияланған жергілікті DNS қызметіне негізделеді. Оны пайдалану үшін DNS кері қарау аймағы конфигурациялануы керек. Бұл аймақ конфигурацияланған болмаса, IP ішкі желісіне жүргізілген сауалнаманың нәтижесі болмайды.

Бастапқыда Kaspersky Security Center Linux бағдарламасы өзі орнатылған құрылғының желілік параметрлерінен сауалнама өткізу үшін IP ауқымдарын алады. Құрылғы мекенжайы 192.168.0.1, ал ішкі желі бүркеніші 255.255.255.0 болса, онда Kaspersky Security Center Linux бағдарламасы автоматты түрде 192.168.0.0/24 желісін сауалнамаға арналған мекенжайлар тізіміне қосады. Kaspersky Security Center Linux бағдарламасы 192.168.0.1 және 192.168.0.254 аралығындағы барлық мекенжайларда сауалнама өткізеді.

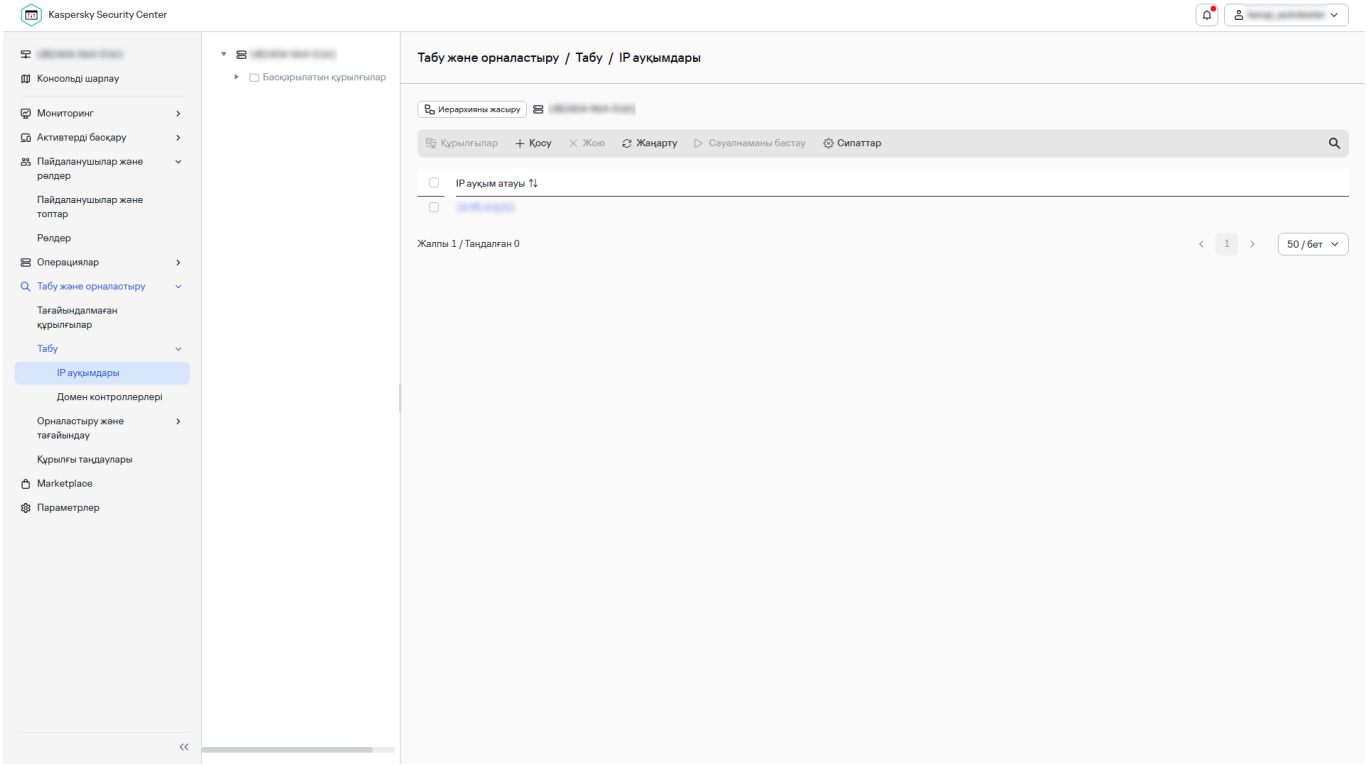
Тек IP ауқымдарын сұрау қосулы болса, Kaspersky Security Center Linux тек IPv4 мекенжайлары бар құрылғыларды анықтайды. Желіңізде IPv6 құрылғылары болса, құрылғылардың Zeroconf сауалнамасын іске қосыңыз.

Microsoft Active Directory, Samba, FreeIPA немесе ALD Pro домен контроллері ішіндегі барлық Linux негізіндегі хост үшін `/etc/samba/smb.conf` файлындағы `netbios name` және `workgroup` параметрлерін көрсетіңіз. Әйтпесе сауалнама нәтижелері қайталанатын хосттарды қамтуы мүмкін.

IP ауқымдарының сауалнамасы параметрлерін көру және өзгерту

IP ауқымдарының сауалнамасы параметрлерін көру және өзгерту үшін:

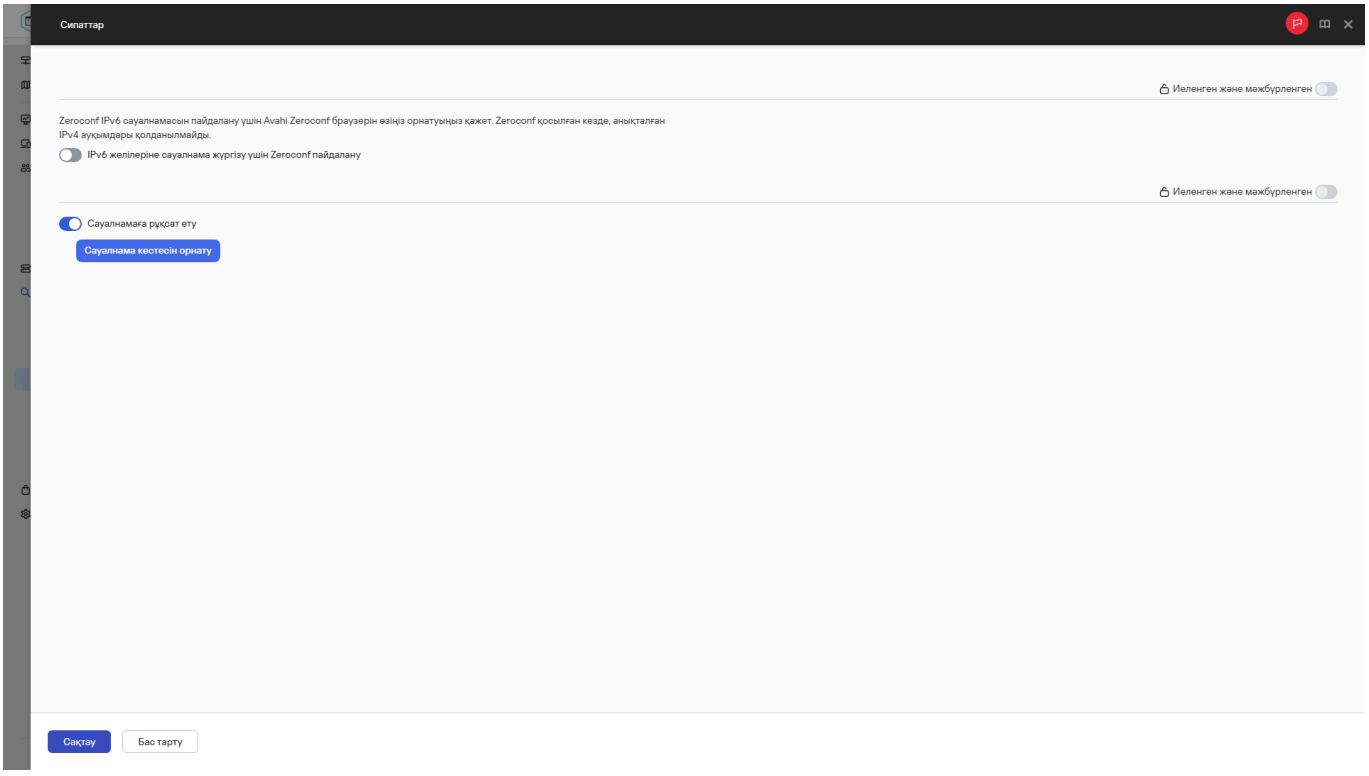
1. Бағдарламаның негізгі терезесінде **Табу және орналастыру → Табу → IP ауқымдары** бөліміне өтіңіз.



IP ауқымдарының тізімі

2. **Сипаттар** түймесін басыңыз.

   IP ауқымдарының сауалнамасы сипаттары терезесі ашылады.



IP ауқымдарын сұрау параметрлері

3. **Сауалнамаға рұқсат ету** ауыстырып-қосқышын қолдану арқылы IP ауқымдарының сауалнамасын қосыңыз немесе өшіріңіз.

4. Сауалнама кестесін конфигурациялаңыз. Әдепкі бойынша, IP ауқымдарының сауалнамасы 420 минут (жеті сағат) сайын іске қосылады.

   Сауалнама аралығын көрсеткен кезде, оның мәні IP мекенжайының әрекет ету уақыты параметрінің мәнінен аспайтынына көз жеткізіңіз. IP мекенжайы IP мекенжайының әрекет ету уақыты ішінде сауалнама өткізу кезінде расталмаса, ол сауалнама нәтижелерінен автоматты түрде жойылады. Әдепкі бойынша, сұраулардың қызмет ету мерзімі 24 сағатты құрайды, өйткені DHCP (Dynamic Host Configuration Protocol – желілік түйіннің динамикалық конфигурациясы протоколы) арқылы тағайындалған динамикалық IP мекенжайлары 24 сағат сайын өзгереді.

   Сауалнама кестесінің нұсқалары:

   - **N күн сайын**

     Сауалнама белгіленген күн мен уақыттан бастап, көрсетілген күндер аралығымен жүйелі түрде жүргізіледі.

     Әдепкі бойынша, сауалнама ағымдағы жүйелік күн мен уақыттан бастап алты сағат сайын іске қосылып тұрады.

   - **N минут сайын**

     Сауалнама көрсетілген уақыттан бастап, белгіленген минуттар аралығымен жүйелі түрде жүргізіледі.

   - **Апта күндері бойынша**

     Сауалнама жүйелі түрде, аптаның көрсетілген күндерінде, көрсетілген уақытта орындалады.

   - **Таңдалған апта күні ай сайын**

     Сауалнама жүйелі түрде, әр айдың көрсетілген күндерінде, көрсетілген уақытта орындалады.

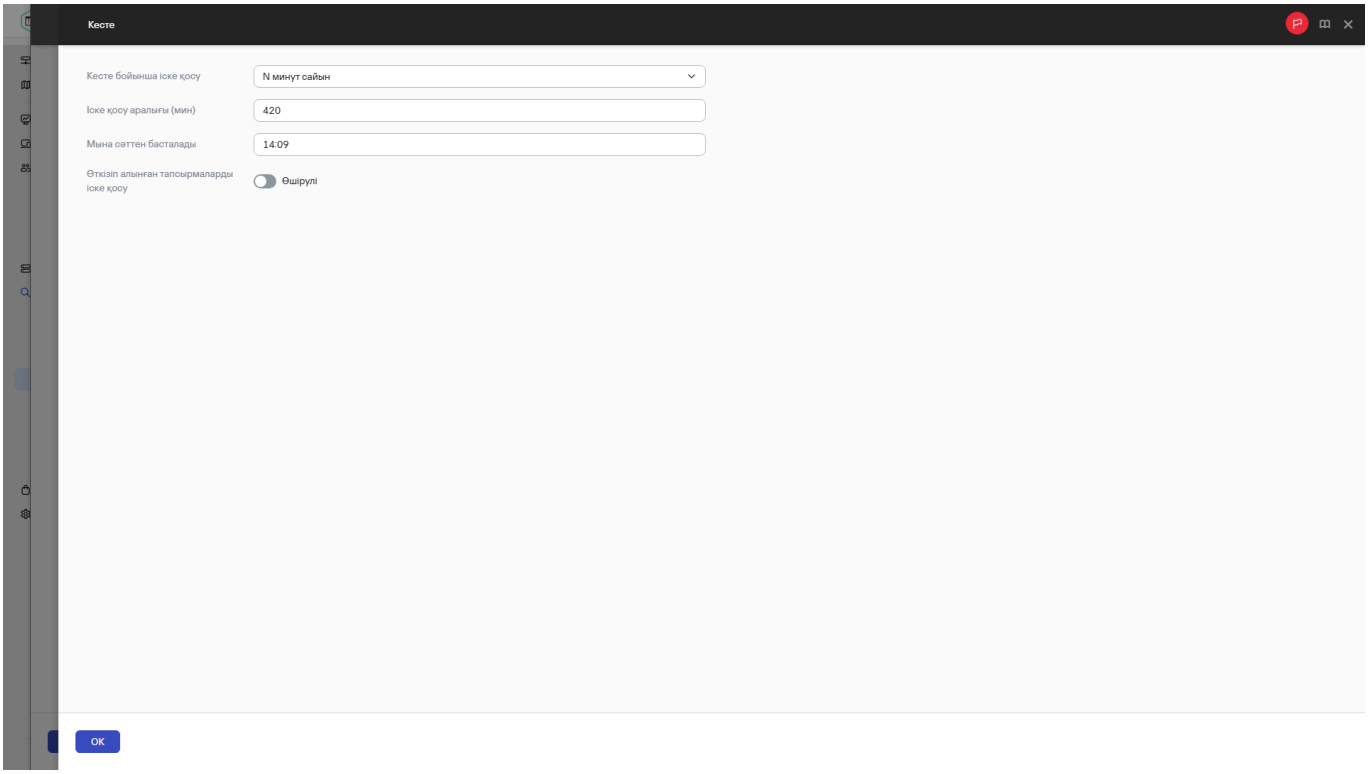
   - **Өткізіп алынған тапсырмаларды іске қосу**

     Басқару сервері өшірулі болса немесе сауалнама жоспарланған уақыт ішінде қолжетімді болмаса, Басқару сервері сауалнаманы қосқаннан кейін бірден бастай алады немесе келесі жоспарланған сауалнаманы күте алады.

     Егер бұл параметр қосулы болса, Басқару сервері сауалнаманы қосқаннан кейін бірден бастайды.

     Егер бұл параметр өшірулі болса, Басқару сервері келесі жоспарланған сауалнаманы күтеді.

Әдепкі бойынша, параметр өшірулі.



Сауалнама кестесін конфигурациялау

5. **Сақтау** түймесін басыңыз.

Параметрлер сақталады және барлық IP ауқымдарына қатысты қолданылады.

Сауалнаманы қолмен іске қосу

Тексеруді дереу іске қосу үшін,

Сауалнаманы бастау түймесін басыңыз.

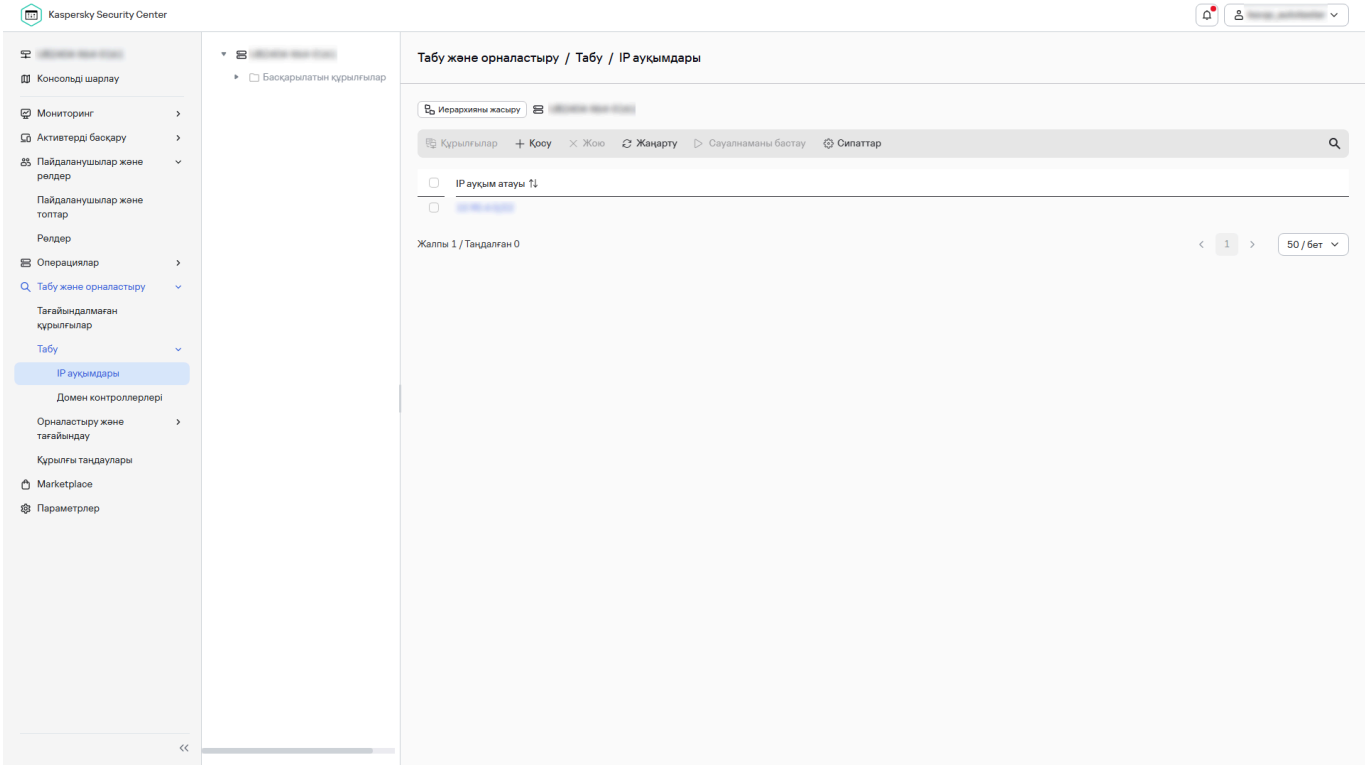
IP ауқымын қосу және өзгерту

Бастапқыда Kaspersky Security Center Linux бағдарламасы өзі орнатылған құрылғының желілік параметрлерінен сауалнама өткізу үшін IP ауқымдарын алады. Құрылғы мекенжайы 192.168.0.1, ал ішкі желі бүркеніші 255.255.255.0 болса, онда Kaspersky Security Center Linux бағдарламасы автоматты түрде 192.168.0.0/24 желісін сауалнамаға арналған мекенжайлар тізіміне қосады. Kaspersky Security Center Linux бағдарламасы 192.168.0.1 және 192.168.0.254 аралығындағы барлық мекенжайларда сауалнама өткізеді. Сіз автоматты түрде анықталған IP ауқымдарын өзгерте аласыз немесе өзіндік IP ауқымдарын қоса аласыз.

Ауқымды IPv4 мекенжайлары үшін ғана жасай аласыз. Zeroconf сауалнамасын қоссаңыз, Kaspersky Security Center Linux бағдарламасы бүкіл желіде сауалнама өткізетін болады.

Жаңа IP ауқымын қосу үшін:

1. Бағдарламаның негізгі терезесінде **Табу және орналастыру → Табу → IP ауқымдары** бөліміне өтіңіз.



IP ауқымдарының тізімі

2. IP ауқымын қосу үшін **Қосу** түймесін басыңыз.

3. Ашылған терезеде келесі параметрлерді конфигурациялаңыз:

   - **IP ауқым атауы**

     IP ауқым атауы. Сіз IP ауқымын атауы бойынша көрсете аласыз, мысалы, 192.168.0.0/24.

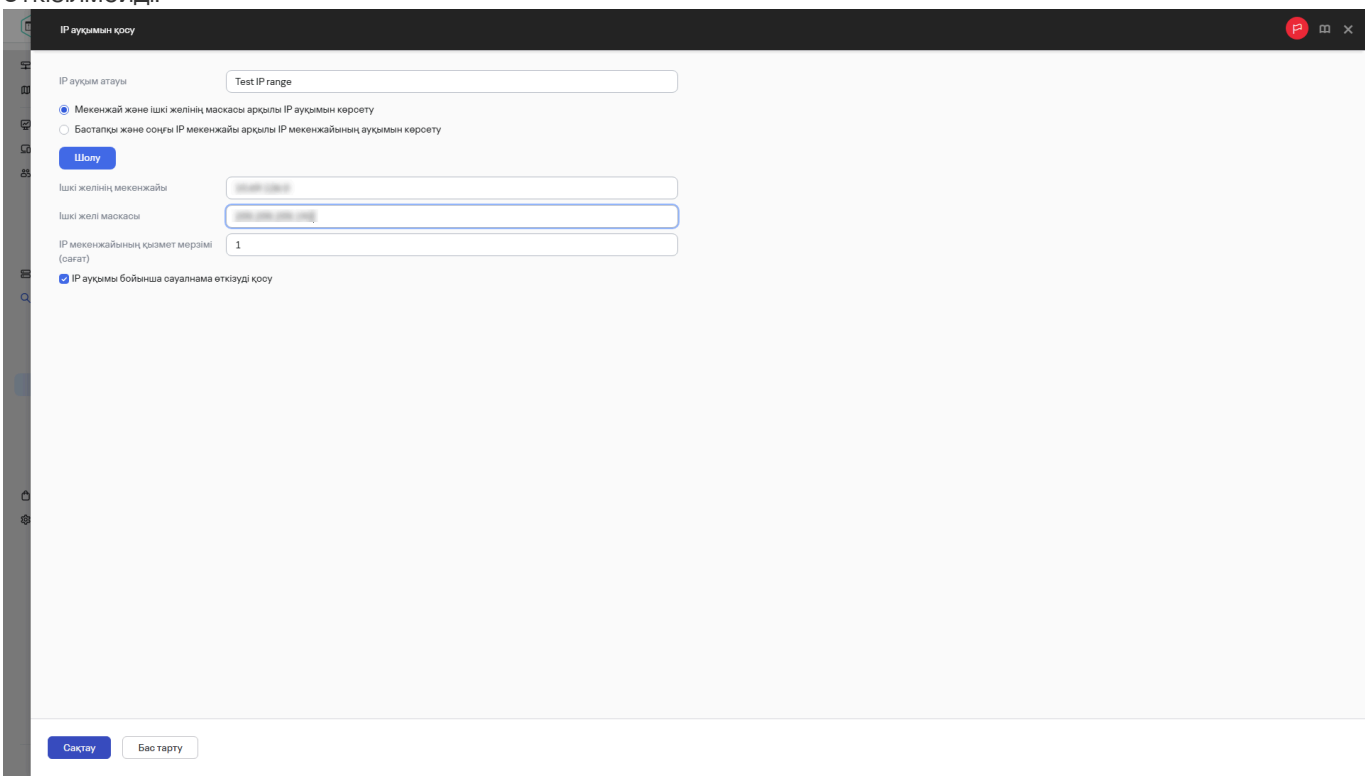
   - **IP аралығы немесе мекенжайы және ішкі желі бүркеніші**

     Бастапқы және соңғы IP мекенжайларын немесе ішкі желі мекенжайын және ішкі желі бүркенішін көрсету арқылы IP ауқымын белгілеңіз. **Шолу** түймесін басып, қолданыстағы IP мекенжайы ауқымдарының бірін де таңдай аласыз.

   - **IP мекенжайының қызмет мерзімі (сағат)**

     Осы параметрді белгілеу кезінде, ол сауалнама кестесінде белгіленген сауалнама аралығының мәнінен асатынына көз жеткізіңіз. IP мекенжайы IP мекенжайының әрекет ету уақыты ішінде сауалнама өткізу кезінде расталмаса, ол сауалнама нәтижелерінен автоматты түрде жойылады. Әдепкі бойынша, сұраулардың қызмет ету мерзімі 24 сағатты құрайды, өйткені DHCP (Dynamic Host Configuration Protocol – желілік түйіннің динамикалық конфигурациясы протоколы) арқылы тағайындалған динамикалық IP мекенжайлары 24 сағат сайын өзгереді.

4. Егер сіз ішкі желіде немесе сіз көрсеткен аралықта сауалнама өткізгіңіз келсе, **IP ауқымы бойынша сауалнама өткізуді қосу** тармағын таңдаңыз. Әйтпесе, сіз қосқан ішкі желі немесе аралықта сауалнама өткізілмейді.



IP ауқымының параметрлерін көрсету

5. **Сақтау** түймесін басыңыз.

IP ауқымы IP ауқымдарының тізіміне қосылды.

Сауалнаманы бастау түймесін пайдаланып, әр IP ауқымы үшін бөлек сауалнама жүргізе аласыз. Әдепкі бойынша, сауалнама нәтижелерінің жарамдылық мерзімі 24 сағатты құрайды және IP мекенжайының әрекет ету уақытына тең келеді.

Қолданыстағы IP ауқымына ішкі желіні қосу үшін:

1. Бағдарламаның негізгі терезесінде **Табу және орналастыру** → **Табу** → **IP ауқымдары** бөліміне өтіңіз.

2. Ішкі желіні қосқыңыз келетін IP ауқымының атауын басыңыз.

3. Пайда болған терезеде **Қосу** түймесін басыңыз.

4. Ішкі желіні оның мекенжайы мен бүркеніші арқылы немесе IP ауқымындағы бірінші және соңғы IP мекенжайларын белгілеу арқылы көрсетіңіз. Не болмаса, **Шолу** түймесін басып, қолданыстағы ішкі желіні қосыңыз.

5. **Сақтау** түймесін басыңыз.

   Ішкі желі IP ауқымына қосылған.

6. **Сақтау** түймесін басыңыз.

IP ауқымы параметрлері сақталған.

Ішкі желілердің қалаған санын қоса аласыз. Аталған IP ауқымдары бір-бірімен қиылыспауы керек, бірақ IP ауқымдары ішіндегі атаусыз ішкі желілерге бұл шектеу қолданылмайды. Әрбір IP ауқымы үшін сауалнаманы дербес түрде қосуға немесе өшіруге болады.

Zeroconf сауалнамасы

Сауалнаманың бұл түріне тек Linux операциялық жүйелері бар тарату нүктелері үшін қолдау көрсетіледі.

Kaspersky Security Center Linux IPv6 мекенжайы бар құрылғыларға ие желілерді сұрастыра алады. Бұл жағдайда, IP ауқымдары көрсетілмейді, ал Kaspersky Security Center Linux нөлдік конфигурациясы бар желіні (бұдан әрі *Zeroconf* деп те аталады) қолдану арқылы бүкіл желіде сауалнама жүргізеді. Zeroconf пайдалануды бастау үшін avahi-browse утилитасын желілерде сауалнама жүргізетін Linux құрылғысында, яғни Басқару серверінде немесе тарату нүктесінде орнату қажет.

Zeroconf сауалнамасын қосу үшін:

1. Бағдарламаның негізгі терезесінде **Табу және орналастыру → Табу → IP ауқымдары** бөліміне өтіңіз.
2. **Сипаттар** түймесін басыңыз.
3. Ашылған терезеде **IPv6 желілеріне сауалнама жүргізу үшін Zeroconf пайдалану** қосқышты қосыңыз.

Осыдан кейін Kaspersky Security Center Linux сіздің желіңізге сауалнама жүргізуді бастайды. Бұл жағдайда, көрсетілген IP ауқымдары еленбейді.

Домен контроллері сауалнамасы

Kaspersky Security Center Linux келесі домен контроллері түрлеріне сауалнама жүргізуге қолдау көрсетеді:

- Microsoft Active Directory
- Samba
- FreeIPA
- ALD Pro

Samba домен контроллерлері үшін Active Directory домен контроллерлері ретінде Samba 4 пайдаланылады.

Домен контроллерін сұрау кезінде Басқару сервер немесе тарату нүктесі домен құрылымы, пайдаланушы тіркелгілері, қауіпсіздік топтары және доменге кіретін құрылғылардың DNS атаулары туралы ақпаратты алады.

Барлық желілік құрылғылар домен мүшелері болса, домен контроллерлері сұрауын пайдалану ұсынылады. Кейбір желілік құрылғылар доменге қосылмаған болса, бұл құрылғыларды домен контроллерлерін сұрау арқылы табу мүмкін емес.

Алдын ала талаптар

Домен контроллеріне сұрау салмас бұрын желілік экран немесе прокси-сервер арқылы домен контроллеріне қосылуға рұқсат бергеніңізге көз жеткізіңіз. Сондай-ақ, домен контроллерінде келесі протоколдардың қосылғанын тексеріңіз:

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

  Бұл протокол домен контроллері қосылымы SASL аутентификациясы арқылы орнатылған кезде пайдаланылады. Басқару сервері және тарату нүктелері тек DIGEST-MD5 механизмін қолдайды.
- Ақпаратты қорғау протоколы (LDAPS) арқылы Lightweight Directory Access Protocol

  Бұл протокол домен контроллеріне шифрланған қосылым арқылы қосылуыңыз қажет болған жағдайда пайдаланылады.

Домен контроллері құрылғысында келесі порттардың қолжетімді екеніне көз жеткізіңіз:

- LDAP протоколы және Simple Authentication (SASL қоса алғанда) үшін 389
- LDAPS протоколы үшін 636

FreeIPA және ALD Pro үшін LDAP және LDAPS хаттамалары тек домендік сауалнама үшін қолданылады. Kaspersky Security Center Linux жүйесі FreeIPA есептік жазбаларының LDAP(S) арқылы аутентификациясын қолдамайды. FreeIPA және ALD Pro пайдаланушыларына Web Console веб-консоліне кіруге мүмкіндік беру үшін IAM қызметі арқылы Kerberos аутентификациясын конфигурациялау керек.

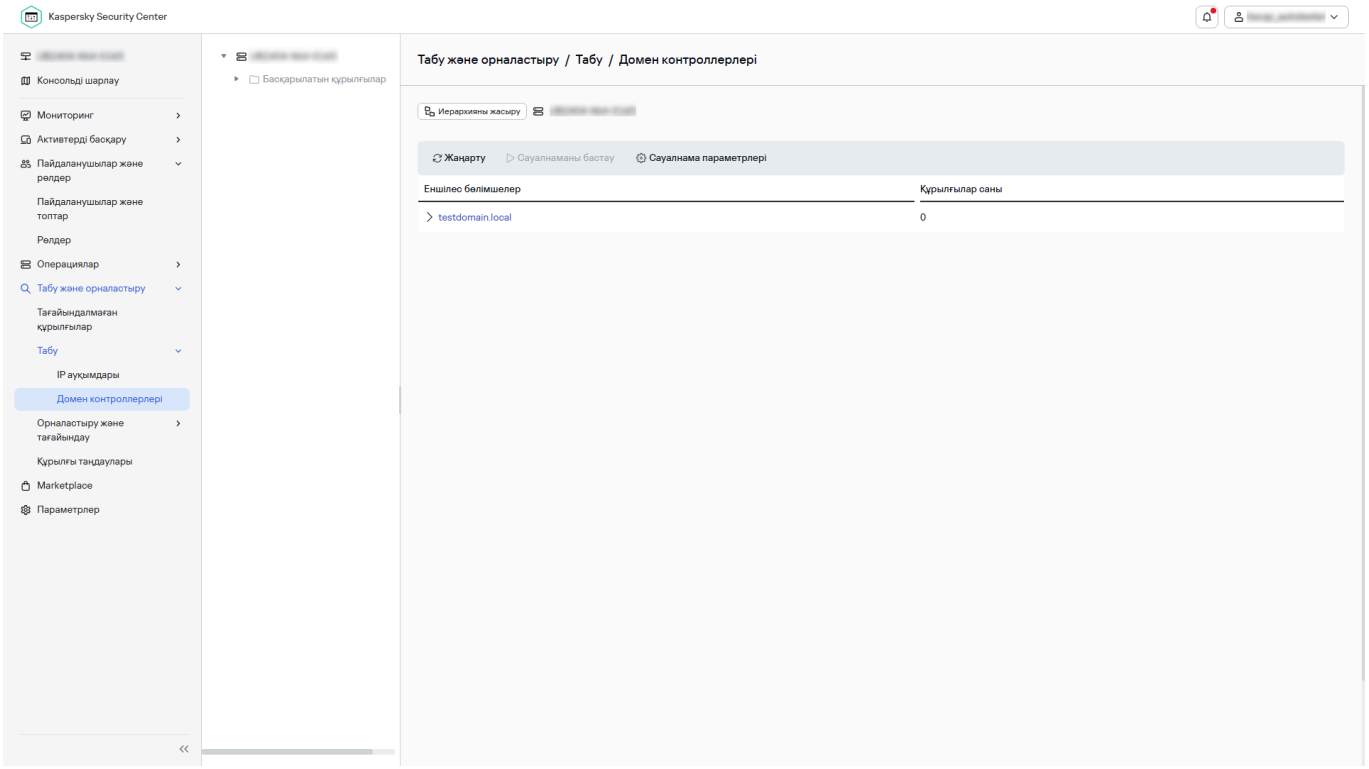
Microsoft Active Directory, Samba, FreeIPA немесе ALD Pro домен контроллері ішіндегі барлық Linux негізіндегі хост үшін `/etc/samba/smb.conf` файлындағы `netbios name` және `workgroup` параметрлерін көрсетуіңіз қажет. Әйтпесе сауалнама нәтижелері қайталанатын хосттарды қамтуы мүмкін.

Егер Microsoft Active Directory доменінде бірнеше домен контроллері болса, доменді сұрау кезінде белгілі бір контроллерді таңдауға қолдау көрсетілмейді. Байланыс бірінші анықталған домен контроллерімен орнатылады. Microsoft Active Directory доменімен дұрыс аутентификацияны қамтамасыз ету үшін сертификаттың Subject Alternative Name (SAN) өрісі осы доменге енгізілген домен контроллерлерінің барлық мекенжайларын, сондай-ақ Microsoft Active Directory доменінің NetBIOS атауын қамтуы керек.

Басқару сервер көмегімен домен контроллерлерін сұрау

Басқару сервер арқылы домен контроллерлерін сұрау үшін:

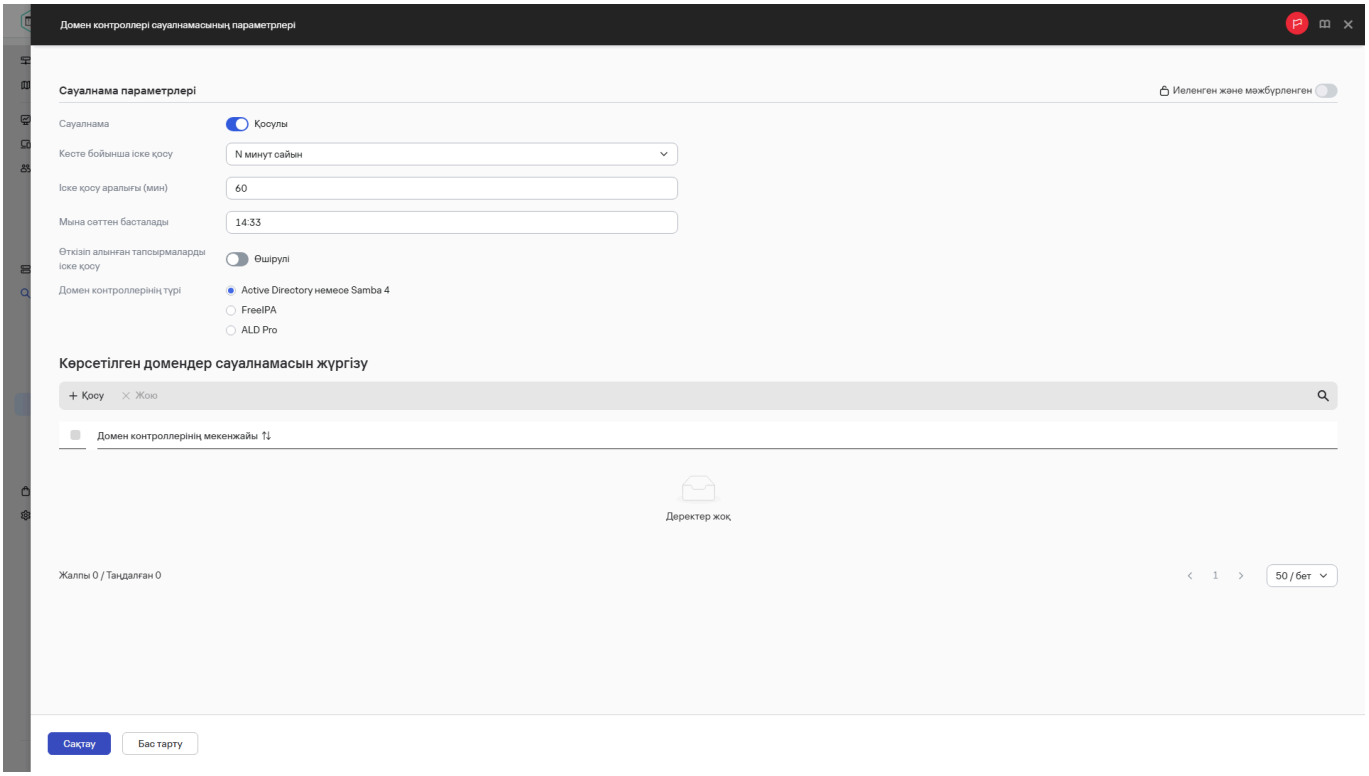
1. Қолданбаның негізгі терезесінде **Табу және орналастыру** → **Табу** → **Домен контроллерлері** бөліміне өтіңіз.



Домен контроллері сауалнамасы терезесі

2. **Сауалнама параметрлерін конфигурациялау** түймесін басыңыз.

Домен контроллері сауалнамасының параметрлері терезесі ашылады.



Домен контроллері сауалнамасы параметрлері

3. **Сауалнама** өрісінде ауыстырып-қосқыш түймесін **Қосулы** күйіне ауыстырыңыз.

4. **Көрсетілген домендер сауалнамасын жүргізу** бөлімінде **Қосу** түймесін басыңыз, домен контроллерлерінің мекенжайын және пайдаланушының тіркелгі деректерін көрсетіңіз.

5. **Домен контроллері сауалнамасының параметрлері** терезесінде келесі әрекеттерді орындаңыз:

   - Сауалнама жасалатын домен контроллерінің түрін таңдаңыз: **Active Directory немесе Samba 4**, **FreeIPA**, **ALD Pro**.

   - Қажет болса, сауалнама кестесін реттеңіз. Әдепкі бойынша, сауалнама кезеңі бір сағатты құрайды. Әрбір кейінгі сауалнама кезінде алынған деректер алдыңғы деректерді толығымен алмастырады.

     Желіде сауалнама өткізу кестесінің келесі нұсқалары қолжетімді:

     - **N күн сайын**

       Сауалнама белгіленген күн мен уақыттан бастап, көрсетілген күндер аралығымен жүйелі түрде жүргізіледі.

       Әдепкі бойынша, сауалнама ағымдағы жүйелік күн мен уақыттан бастап алты сағат сайын іске қосылып тұрады.

     - **N минут сайын**

       Сауалнама көрсетілген уақыттан бастап, белгіленген минуттар аралығымен жүйелі түрде жүргізіледі.

     - **Апта күндері бойынша**

       Сауалнама жүйелі түрде, аптаның көрсетілген күндерінде, көрсетілген уақытта орындалады.

     - **Таңдалған апта күні ай сайын**

       Сауалнама жүйелі түрде, әр айдың көрсетілген күндерінде, көрсетілген уақытта орындалады.

- **Өткізіп алынған тапсырмаларды іске қосу**

  Басқару сервері өшірулі болса немесе сауалнама жоспарланған уақыт ішінде қолжетімді болмаса, Басқару сервері сауалнаманы қосқаннан кейін бірден бастай алады немесе келесі жоспарланған сауалнаманы күте алады.

  Егер бұл параметр қосулы болса, Басқару сервері сауалнаманы қосқаннан кейін бірден бастайды.

  Егер бұл параметр өшірулі болса, Басқару сервері келесі жоспарланған сауалнаманы күтеді.

  Әдепкі бойынша, параметр өшірулі.

Доменнің қауіпсіздік тобындағы пайдаланушы тіркелгілерін өзгертсеңіз, бұл өзгерістер домен контроллерлері сауалнамасынан соң бір сағаттан кейін Kaspersky Security Center Linux жүйесінде көрсетіледі.

6. Өзгерістерді қолдану үшін **Сақтау** түймесін басыңыз.

7. Желіде сауалнама өткізуді бірден іске қосу қажет болса, **Сауалнаманы бастау** түймесін басыңыз.

Тарату нүктесі көмегімен домен контроллерлерін сұрау

Сондай-ақ тарату нүктесі арқылы домен контроллерлерін сұрауға болады. Windows немесе Linux жүйесімен басқарылатын құрылғы тарату нүктесі ретінде әрекет ете алады.

Linux тарату нүктесі үшін домен контроллерлерінің барлық түрлеріне сауалнама жүргізуге қолдау көрсетіледі.
Windows тарату нүктесі үшін тек Microsoft Active Directory домен контроллеріне сауалнама жүргізуге ғана қолдау көрсетіледі.
Mac тарату нүктесімен сауалнама жүргізуге қолдау көрсетілмейді.

Тарату нүктесі көмегімен домен контроллерлерінің сауалнамасын конфигурациялау үшін:

1. Тарату нүктесінің сипаттарын ашыңыз.

2. **Домен контроллерінің сауалнамасы** бөлімін таңдаңыз.

3. **Сауалнама** өрісінде ауыстырып-қосқыш түймесін **Қосулы** күйіне ауыстырыңыз.

4. Linux тарату нүктесін пайдалансаңыз, сауалнама жүргізілетін домен контроллерінің түрін таңдаңыз: **Active Directory немесе Samba 4**, **FreeIPA**, **ALD Pro**.

   Тарату нүктесін пайдалану және басқару серверін пайдалану арқылы сауалнаманы конфигурациялау кезінде бірдей домен контроллерінің түрін көрсету қажет емес.

5. Сауалнама жүргізгіңіз келетін домен контроллерлерін таңдаңыз.

   Linux операциялық жүйесі бар тарату нүктесін пайдалансаңыз, **Көрсетілген домендер сауалнамасын жүргізу** бөлімінде **Қосу** түймесін басып, домен контроллерлерінің мекенжайы мен пайдаланушының тіркелгі деректерін көрсетіңіз.

Windows операциялық жүйесі бар тарату нүктесін пайдалансаңыз, келесі нұсқалардың бірін таңдауға болады:

- **Ағымдағы домен сауалнамасын жүргізу**
- **Бүкіл домендер тобының сауалнамасын жүргізу**
- **Көрсетілген домендер сауалнамасын жүргізу**

6. Қажет болса, сауалнама кестесінің параметрлерін көрсету үшін **Сауалнама кестесін орнату** түймесін басыңыз.

   Сауалнама кестеге сәйкес жүргізіледі. Сауалнаманы қолмен іске қосуға болмайды.

Сауалнама аяқталғаннан кейін, домен құрылымы **Домен контроллерлері** бөлімінде көрсетіледі.

Егер сіз құрылғыларды жылжыту ережелерін конфигурациялап, қосқан болсаңыз, табылған жаңа құрылғылар автоматты түрде **Басқарылатын құрылғылар** тобына ауысады. Егер құрылғыларды жылжыту ережелері қосылмаған болса, табылған жаңа құрылғылар автоматты түрде **Тағайындалмаған құрылғылар** тобына ауысады.

Анықталған пайдаланушы есептік жазбаларын Kaspersky Security Center Web Console ішіндегі домен аутентификациясы үшін пайдалануға болады.

Домен контроллерін аутентификациялау және қосу

Доменді сұрау кезінде аутентификация және домен контроллеріне қосылу

Домен контроллерін сұрау кезінде Басқару сервері немесе тарату нүктесі домен контроллеріне бастапқы қосылымды орнату үшін қосылым протоколын анықтайды. Бұл протокол домен контроллерінің болашақтағы барлық қосылымдары үшін пайдаланылады. Домен контроллеріне бірінші рет қосылғанда, желілік агенттің жалаушаларын (`KLNAG_LDAP_TLS_REQCERT` және `KLNAG_LDAP_SSL_CACERT`) пайдаланып, қосылым опцияларын өзгертуге болады. Осы мақалада сипатталғандай, klscflag пәрменін пайдаланып, Желілік агент жалаушаларын конфигурациялауға болады.

Домен контроллеріне бастапқы қосылу келесідей іске асады:

1. Басқару сервері немесе тарату нүктесі LDAPS арқылы домен контроллеріне қосылуға әрекеттенуде.

   Әдепкі бойынша сертификатты тексеру қажет болмайды. Сертификатты мәжбүрлі түрде тексеру үшін `KLNAG_LDAP_TLS_REQCERT` жалаушасын 1 мәніне орнатыңыз.

   `KLNAG_LDAP_TLS_REQCERT` жалаушасының ықтимал мәндері:

   - `0` – сертификат сұралады, бірақ ол берілмесе немесе сертификатты тексеру сәтсіз аяқталса, TLS қосылымы әлі де сәтті жасалған деп саналады (әдепкі мән).
   - `1` – LDAP сервері сертификатын қатаң тексеру қажет.

Әдепкісінше KLNAG_LDAP_SSL_CACERT жалаушасы белгіленбесе, сертификаттар тізбегіне қол жеткізу үшін сертификаттау орталығының (CA) операциялық жүйеге тәуелді жолы қолданылады. Басқа жолды көрсету үшін KLNAG_LDAP_SSL_CACERT жалаушасын пайдаланыңыз.

2. LDAPS қосылымы сәтсіз болса, Басқару сервері немесе тарату нүктесі SASL (DIGEST-MD5) арқылы шифрланбаған TCP қосылымы арқылы домен контроллеріне қосылуға әрекет жасайды.

Басқару серверінде домен пайдаланушысын аутентификациялау кезінде аутентификация және домен контроллеріне қосылу

Домен пайдаланушысы Басқару серверіне аутентификация жасағанда, Басқару сервері домен контроллерімен байланыс орнату протоколын анықтайды.

FreeIPA және ALD Pro үшін LDAP және LDAPS хаттамалары тек домендік сауалнама үшін қолданылады. Kaspersky Security Center Linux жүйесі FreeIPA есептік жазбаларының LDAP(S) арқылы аутентификациясын қолдамайды. FreeIPA және ALD Pro пайдаланушыларына Web Console веб-консоліне кіруге мүмкіндік беру үшін IAM қызметі арқылы Kerberos аутентификациясын конфигурациялау керек.

Домен контроллеріне қосылу келесідей іске асады:

1. Басқару сервері домен контроллеріне LDAPS арқылы қосылуға әрекеттенеді.

   LDAP сервері сертификатын қатаң тексеру қажет.

   Әдепкісінше KLNAG_LDAP_SSL_CACERT жалаушасы белгіленбесе, сертификаттар тізбегіне қол жеткізу үшін сертификаттау орталығының (CA) операциялық жүйеге тәуелді жолы қолданылады. Басқа жолды көрсету үшін KLNAG_LDAP_SSL_CACERT жалаушасын пайдаланыңыз.

2. LDAPS қосылымы сәтсіз болса, домен контроллеріне қосылу қатесі орын алады және басқа қосылым протоколдары пайдаланылмайды.

Жалаушаларды конфигурациялау

Жалаушаларды конфигурациялау үшін klscflag утилитасын пайдалануға болады.

Пәрмен жолын іске қосыңыз және ағымдағы каталогты klscflag утилитасы бар каталогке өзгертіңіз. Басқару сервері құрылғысында klscflag утилитасы орнату директориясында орналасқан. Әдепкі бойынша жол - /opt/kaspersky/ksc64/sbin.

Мысалы, келесі пәрмен сертификатты мәжбүрлі түрде тексереді:

```
klscflag -fset -pv klnagent -n KLNAG_LDAP_TLS_REQCERT -t d -v 1
```

Samba домен контроллерлерін конфигурациялау

Kaspersky Security Center Linux тек Samba 4 жүйесінде жұмыс істейтін Linux домен контроллерлеріне қолдау көрсетеді.

Samba домен контроллері Microsoft Active Directory домен контроллері сияқты схема кеңейтімдеріне қолдау көрсетеді. Samba 4 схема кеңейтімін пайдаланып, Samba домен контроллерінің Microsoft Active Directory домен контроллерімен толық үйлесімділігін қосуға болады. Бұл қадам міндетті емес.

Samba домен контроллерінің Microsoft Active Directory домен контроллерімен толық үйлесімділігін қосу ұсынылады. Бұл Kaspersky Security Center Linux және Samba домен контроллері арасындағы дұрыс әрекеттестікті қамтамасыз етеді.

Samba домен контроллерінің Microsoft Active Directory домен контроллерімен толық үйлесімділігін қосу үшін:

1. RFC2307 схема кеңейтімін пайдалану үшін келесі пәрменді орындаңыз:

   ```
   samba-tool domain provision --use-rfc2307 --interactive
   ```

2. Samba домен контроллерінде схеманы жаңартуды қосыңыз. Ол үшін `/etc/samba/smb.conf` файлына келесі жолды қосыңыз:

   ```
   dsdb:schema update allowed = true
   ```

   Схеманы жаңарту қатемен аяқталса, master схемасы ретінде қызмет ететін домен контроллерін толық қалпына келтіру керек.

Samba домен контроллері ішіндегі барлық Linux негізіндегі хост үшін `/etc/samba/smb.conf` файлындағы `netbios name` мен `workgroup` параметрлерін көрсетіңіз. Әйтпесе сауалнама нәтижелері қайталанатын хосттарды қамтуы мүмкін.

Жабдықты түгендеу

Жабдықты түгендеу үшін қолданылатын жабдықтар тізімі (**Активтерді басқару** → **Жабдық**) екі тәсілмен толтырылады: автоматты түрде және қолмен. Әрбір желі сауалнамасынан кейін барлық анықталған құрылғы тізімге автоматты түрде қосылады; дегенмен желіде сауалнама өткізгіңіз келмесе, құрылғыларды қолмен қосуға болады. Тізімге маршрутизаторлар, принтерлер немесе құрылғы жабдықтары сияқты басқа құрылғыларды қолмен қосуға болады.

Құрылғының сипаттарында құрылғылар туралы толық ақпаратты көруге және өңдеуге болады.

Жабдықтар тізімінде келесі құрылғы түрлері болуы мүмкін:

- компьютерлер;
- ұялы құрылғылар;
- желілік құрылғылар;
- виртуалды құрылғылар;
- компьютер компоненттері;
- компьютерлік периферия;
- қосылатын құрылғылар;

- VoIP телефондары;
- желілік қоймалар.

Әкімші анықталған құрылғыларға *Корпоративтік кластың аппараттық жасақтамасы* белгісін беруі мүмкін. Бұл белгіні құрылғының сипаттарында қолмен тағайындауға немесе оны автоматты түрде тағайындау критерийлерін белгілеуге болады. Бұл жағдайда, *Корпоративтік кластың аппараттық жасақтамасы* белгісі құрылғының түрі бойынша белгіленеді.

Kaspersky Security Center жабдықты шығынға жазуға мүмкіндік береді. Ол үшін құрылғы сипаттарында **Шығынға жазылды** опциясын таңдаңыз. Мұндай құрылғы жабдықтар тізімінде көрсетілмейді.

Әкімші **Жабдық** қалтасындағы бағдарламаланатын логикалық контроллерлер (БЛК) тізімімен жұмыс істей алады. БЛК тізімдерімен жұмыс істеу туралы толық ақпарат *Kaspersky Industrial Cyber Security for Nodes пайдаланушы нұсқаулығында* келтірілген.

Жаңа құрылғылар туралы ақпаратты қосу

Желідегі жаңа құрылғылар туралы ақпаратты қосу үшін:

1. Бағдарламаның негізгі терезесінде **Активтерді басқару** → **Жабдық** бөліміне өтіңіз.
2. **Жаңа құрылғы** терезесін ашу үшін **Қосу** түймесін басыңыз.
3. **Жаңа құрылғы** терезесінде, **Құрылғы түрі** ашылмалы тізімінде қосқыңыз келетін құрылғы түрін таңдаңыз.
4. **ОК** түймесін басыңыз.

   Жалпы бөліміндегі құрылғы сипаттары терезесі ашылады.
5. **Жалпы** бөлімінде құрылғы туралы деректерді енгізу өрістерін толтырыңыз. **Жалпы** бөлімінде келесі параметрлер қолжетімді:
   - **Корпоративтік құрылғы**. Егер сіз құрылғыға *Корпоративтік* белгісін бергіңіз келсе, жалаушаны қойыңыз. Осы белгі бойынша құрылғыларды **Жабдық** қалтасынан іздеуге болады.
   - **Шығынға жазылды**. Егер сіз құрылғының **Жабдық** қалтасындағы құрылғылар тізімінде пайда болуын қаламасаңыз, жалаушаны қойыңыз.
6. **Қолдану** түймесін басыңыз.

Жаңа құрылғы **Жабдық** бетінің жұмыс аймағында көрсетіледі.

Кәсіпорын құрылғыларын анықтау критерийлерін конфигурациялау

Кәсіпорын құрылғыларын анықтау критерийлерін конфигурациялау үшін:

1. Бағдарламаның негізгі терезесінде **Активтерді басқару** → **Жабдық** бөліміне өтіңіз.
2. **Жабдық** бетінің жоғарғы жағында **Корпоративтік құрылғылар үшін ережені орнату** сілтемесін басыңыз.

   Корпоративтік құрылғылар үшін ережені орнату панелі шақырылады.

3. **Корпоративтік құрылғылар үшін ережені орнату** панелінде **Құрылғы үшін корпоративтік құрылғы атрибутын автоматты түрде орнату** опциясын қосыңыз. *Корпоративтік* атрибуты автоматты түрде тағайындалатын құрылғы түрлерін көрсетіңіз.

   Бұл параметр желі сауалнамасы арқылы қосылған құрылғыларға ғана әсер етеді. Қолмен қосылған құрылғылар үшін *Корпоративтік* параметрін қолмен орнатыңыз.

4. **ОК** түймесін басыңыз.

Корпоративтік құрылғыларды анықтау критерийлері конфигурацияланған.

Клиент құрылғыларында VDI динамикалық режимін пайдалану

Ұйымның желісінде уақытша виртуалды машиналарды қолдана отырып, виртуалды инфрақұрылымды орналастыруға болады. Kaspersky Security Center Linux бағдарламасы уақытша виртуалды машиналарды анықтайды және олар туралы деректерді Басқару сервері дерекқорына қосады. Пайдаланушы уақытша виртуалды машинамен жұмыс істеп болғаннан кейін, машина виртуалды инфрақұрылымнан алынып тасталады. Дегенмен, қашықтағы виртуалды машина туралы жазба Басқару серверінің дерекқорында сақталуы мүмкін. Сондай-ақ жоқ виртуалды машиналар Kaspersky Security Center Web Console ішінде көрсетілуі мүмкін.

Жоқ виртуалды машиналар туралы деректердің сақталуын болдырмау үшін Kaspersky Security Center Linux бағдарламасында Virtual Desktop Infrastructure (VDI) үшін динамикалық режимді қолдау іске асырылған. Әкімші VDI үшін динамикалық режимді қолдауды уақытша виртуалды машинада орнатылатын Желілік агенттің орнату пакетінің сипаттарында қоса алады.

Уақытша виртуалдық машинаны өшіру кезінде, Желілік агент Басқару серверіне өшіру туралы хабарлайды. Виртуалды машина сәтті өшірілген жағдайда, ол Басқару серверіне қосылған құрылғылар тізімінен алынып тасталады. Виртуалды машинаны өшіру дұрыс орындалмаса және Желілік агент Серверіне өшіру туралы хабарландыруды жібермесе, қайталайтын сценарий қолданылады. Бұл сценарийге сәйкес, виртуалды машина Сервермен синхрондаудың үш сәтсіз әрекетінен кейін Басқару серверіне қосылған құрылғылар тізімінен жойылады.

Желілік агенттің орнату пакетінің сипаттарында VDI динамикалық режимін қосу

VDI динамикалық режимін қосу үшін:

1. Бағдарламаның негізгі терезесінде **Бағдарламалық жасақтаманы басқару** → **Орнату пакеттері** бөліміне өтіңіз.

2. Желілік агенттің орнату пакетінің контекстік мәзірінде **Сипаттар** тармағын таңдаңыз.

   Сипаттар терезесі ашылады.

3. **Сипаттар** терезесінде **Кеңейтілген** бөлімін таңдаңыз.

4. **Кеңейтілген** бөлімінде **VDI үшін динамикалық режимді қосу** параметрін таңдаңыз.

Желілік агент орнатылған құрылғы VDI бөлігі болады.

VDI құрамына кіретін құрылғыларды басқару тобына жылжыту

VDI құрамына кіретін құрылғыларды басқару тобына жылжыту үшін:

1. **Активтерді басқару** → **Жылжыту ережелері** бөлімге өтіңіз.

2. **Қосу** түймесін басыңыз.

3. **Ереже шарттары** қойындысында **Виртуалды машиналар** қойындысын таңдаңыз.

4. **Виртуалды машина болып табылады** ережесі үшін **Иә** мәнін, ал **Virtual Desktop Infrastructure бөлігі** ережесі үшін **Иә мәнін орнатыңыз.**

5. **Сақтау** түймесін басыңыз.

Клиент құрылғыларын басқару

Kaspersky Security Center Linux клиент құрылғыларын басқаруға мүмкіндік береді:

- Басқарылатын құрылғылардың, соның ішінде кластерлер мен сервер массивтерінің параметрлері мен күйлерін қарау.
- Тарату нүктелерін конфигурациялау.
- Тапсырмаларды басқару.

Басқару топтары клиент құрылғыларын бір бірлік ретінде басқаруға болатын жинаққа біріктіру үшін пайдаланылуы мүмкін. Клиент құрылғысын тек бір басқару тобына қосуға болады. Құрылғылар **Ереже шарттары** негізделген топқа автоматты түрде тағайындалуы мүмкін:

- Құрылғыны жылжыту ережелерін жасау.
- Құрылғыны жылжыту ережелерін көшіру.
- Құрылғыны жылжыту ережелеріне арналған шарттар.

Шарт бойынша құрылғыларды сүзу үшін құрылғы таңдауларын пайдалануға болады. Сондай-ақ, құрылғы таңдауларын жасау, құрылғыларды іздеу және құрылғыларды басқару топтары арасында тарату үшін құрылғыларға тегтерді тағайындауға болады.

Басқарылатын құрылғының параметрлері

Басқарылатын құрылғының параметрлерін қарап шығу үшін:

1. Қолданбаның негізгі терезесінде **Активтерді басқару** → **Активтер (құрылғылар)** бөліміне өтіңіз.

   Басқарылатын құрылғылардың тізімі көрсетіледі.

2. Басқарылатын құрылғылар тізімінде қажетті құрылғының атауы бар сілтемеден өтіңіз.

Таңдалған құрылғы сипаттары терезесі ашылады.

Сипаттар терезесінің жоғарғы бөлігінде параметрлердің негізгі топтарын көрсететін келесі қойындылар көрсетіледі:

- **Жалпы**

  Бұл қойындыда келесі бөлімдер бар:

  - **Жалпы** бөлімі клиент құрылғысы туралы жалпы ақпаратты қамтиды. Ақпарат, клиент құрылғысын Басқару серверімен соңғы рет синхрондау барысында алынған деректер негізінде ұсынылады:

    - **Атауы**

      Өрісте басқару тобындағы клиент құрылғысының атауын қарап шығуға және өзгертуге болады.

- **Сипаттама**

  Өрісте клиент құрылғысының қосымша сипаттамасын енгізуге болады.

- **Құрылғының күйі**

  Құрылғыдағы антивирустық қорғаныс күйінің және желідегі құрылғы белсенділігінің әкімші белгілеген өлшемшарттары негізінде қалыптастырылатын клиент құрылғысының күйі.

- **Құрылғының иесі**

  Құрылғы иесінің аты. **Құрылғы иесін басқару** сілтемесін басу арқылы пайдаланушыны құрылғы иесі ретінде тағайындауға немесе жоюға болады.

- **Толық топ атауы**

  Құрамына клиент құрылғысы кіретін басқару тобы.

- **Антивирустық дерекқорларды соңғы рет жаңарту уақыты**

  Құрылғыдағы антивирустық дерекқорларды немесе бағдарламаларды соңғы рет жаңарту күні.

- **Басқару серверіне қосылған**

  Клиент құрылғысында орнатылған Желілік агентті Басқару серверіне соңғы рет қосу күні мен уақыты.

- **Байланысқа соңғы рет шығу уақыты**

  Құрылғы соңғы рет желіде көрінген күн мен уақыт.

- **Желілік агенттің нұсқасы**

  Орнатылған Желілік агенттің нұсқасы.

- **Жасалған күні**

  Құрылғының Kaspersky Security Center Linux-де жасалған күні.

- **Басқару серверімен байланысты үзбеу**

  Осы параметрі қосулы болса, басқарылатын құрылғы мен Басқару сервері арасында тұрақты қосылым сақталады. Осындай қосылымды қамтамасыз ететін push-серверлерді қолданбасаңыз, осы параметрді қолдана аласыз.

  Егер параметр өшірулі болса және push серверлері пайдаланылмаса, басқарылатын құрылғы деректерді синхрондау немесе ақпаратты жіберу үшін Басқару серверіне қосылады.

  Басқару серверімен байланысты үзбеу параметрі таңдалған құрылғылардың жалпы саны 300-ден аспауы тиіс.

  Бұл параметр басқарылатын құрылғыларда әдепкі бойынша өшіріледі. Бұл параметр Басқару сервері орнатылған құрылғыда әдепкі бойынша қосылады және оны өшіруге тырыссаңыз да қосулы қалады.

- **Сеанстар**

  Бұл бөлімде қазіргі уақытта құрылғыға кірген пайдаланушылар туралы ақпараты бар кесте берілген. Кестенің сәйкес бағандарында келесі деректер көрсетілген:

  - Пайдаланушы аты
  - SAM есептік жазбасының атауы

- Пайдаланушының негізгі аты
- Электрондық пошта мекенжайы

Домен пайдаланушыларының сеанстары туралы ақпаратты дұрыс көрсету үшін домен контроллері сұрауын пайдалану керек.

- **Желі** бөлімінде клиент құрылғысының желілік сипаттары туралы келесі ақпарат көрсетіледі:
  - **IP мекенжайы**

    Құрылғының IP мекенжайы.
  - **Windows домені**

    Құрылғыны қамтитын жұмыс тобы.
  - **DNS атауы**

    Клиент құрылғысының DNS домен атауы.
  - **NetBIOS атауы**

    Клиент құрылғысының NetBIOS атауы.
  - **IPv6 мекенжайы**
- **Жүйе** бөлімінде клиент құрылғысында орнатылған операциялық жүйе туралы ақпарат ұсынылған:
  - **ОЖ**
  - **Орталық процессор құрылымы**
  - **Құрылғы атауы**
  - **Виртуалды машинаның түрі**

    Виртуалды машинаның өндірушісі
  - **VDI бөлігі ретінде динамикалық виртуалды машина**

    Бұл жолда клиент құрылғысының VDI бөлігі ретінде динамикалық виртуалды машина екені көрсетілген.
- **Қорғаныс** бөлімінде клиент құрылғысында антивирустық қорғаныстың күйі туралы келесі ақпарат ұсынылған:
  - **Көзге көрінетін**

    Клиенттік құрылғының көріну күйі.
  - **Құрылғының күйі**

    Құрылғыдағы антивирустық қорғаныс күйінің және желідегі құрылғы белсенділігінің әкімші белгілеген өлшемшарттары негізінде қалыптастырылатын клиент құрылғысының күйі.

- **Күйдің сипаттамасы**

  Клиент құрылғысының қорғаныс күйі және Басқару серверіне қосылу.

- **Қорғаныс күйі**

  Клиент құрылғысынның тұрақты қорғанысының ағымдағы күйі.

  Құрылғыда күй өзгергеннен кейін, жаңа күй, клиент құрылғысы Басқару серверімен синхрондалғаннан кейін ғана құрылғының сипаттары терезесінде көрсетіледі.

- **Соңғы рет толық сканерлеу уақыты**

  Клиент құрылғысында зиянды БҚ соңғы іздеу күні мен уақыты.

- **Вирус анықталды**

  Қауіпсіздік бағдарламасын орнатқан сәттен бастап (құрылғыны бірінші рет тексеру) немесе қауіп есептегіші соңғы нөлденген сәттен бастап клиент құрылғысында анықталған қауіптердің жалпы саны.

- **Залалсыздандырудан өтпеген нысандар**

  Клиент құрылғысындағы кейін өңделетін файлдар саны.

  Өрісте ұялы құрылғылар үшін кейін өңделетін файлдар ескерілмейді.

- **Дискілерді шифрлау күйі**

  Құрылғының жергілікті дискілеріндегі файлдарды шифрлаудың ағымдағы күйі. Күйдің сипаттамасы Kaspersky Endpoint Security for Windows онлайн-анықтамасында келтірілген.

  Файлдарды тек Kaspersky Endpoint Security for Windows орнатылған басқарылатын құрылғыларда шифрлауға болады.

- **Бағдарлама анықтаған құрылғы күйі** бөлімінде клиент құрылғысында орнатылған басқарылатын бағдарлама анықтаған құрылғының күйі туралы ақпарат көрсетіледі. Құрылғының бұл күйі Kaspersky Security Center Linux анықтағаннан өзгеше болуы мүмкін.

- **Бағдарламалар**

  Бұл қойындыда клиенттік құрылғыда орнатылған барлық Kaspersky қолданбасының тізімі берілген. Бұл қойындыда таңдалған Kaspersky қолданбасын (желілік агенттен басқа) іске қосуға және тоқтатуға мүмкіндік беретін **Іске қосу** және **Тоқтату** түймелері бар. Әкімшілік серверімен байланыс сұрауларын алу үшін басқарылатын құрылғыларда 15000 UDP порты қолжетімді болса, бұл түймелерді пайдалануға болады. Басқарылатын құрылғы push хабарландырулары үшін қолжетімді болмаса, бірақ Басқару серверіне тұрақты қосылу режимі қосылған болса (**Жалпы Басқару серверімен байланысты үзбеу** параметрі қосылған), **Іске қосу** және **Тоқтату** түймелері белсенді болады. Әйтпесе, бағдарламаны іске қосу немесе тоқтату әрекеті кезінде қате туралы хабар пайда болады. Бағдарлама туралы жалпы ақпаратты, құрылғыда болған оқиғалар тізімін және бағдарлама параметрлерін көру үшін бағдарлама атауын басуға да болады.

- **Белсенді саясаттар мен профильдері**

  Осы қойындыда басқарылатын құрылғыға тағайындалған саясат тізімдері мен саясат профильдері көрсетіледі.

- **Тапсырмалар**

  Тапсырмалар қойыншасында сіз клиент құрылғысының тапсырмаларын басқара аласыз: қолданыстағы тапсырмалар тізімін қарау, жаңаларын жасау, тапсырмаларды жою, іске қосу және тоқтату, олардың параметрлерін өзгерту және орындалу нәтижелерін қарау. Тапсырмалар тізімі клиентті Басқару серверімен соңғы рет синхрондау барысында алынған деректер негізінде ұсынылады. Тапсырмалардың күйі туралы ақпаратты клиент құрылғысынан Басқару сервері сұрайды. Егер UDP порты 15000 Басқарылатын құрылғыларда Әкімшілік серверімен байланыс сұрауларын қабылдау үшін қол жетімді болса, тапсырма күйі көрсетіледі және тапсырмаларды басқару түймелері белсенді болады. Егер push-сервер басқарылатын құрылғымен байланыса алмаса, бірақ Басқару серверіне тұрақты қосылу режимі қосылған болса (**Басқару серверімен байланысты үзбеу** параметрі **Жалпы** бөлімінде қосылған), тапсырмалары бар әрекеттер қол жетімді.

  Байланыс болмаған жағдайда, күй көрсетілмейді.

- **Оқиғалар**

  Оқиғалар қойыншасында таңдалған клиент құрылғысы үшін Басқару серверінде тіркелген оқиғалар көрсетіледі.

  Құрылғылар оқиғаларын экспорттауға, көшіруге және жоюға болады.

- **Қауіпсіздік мәселелері**

  Қауіпсіздік мәселелері қойындысында клиенттік құрылғы үшін қауіпсіздік мәселелерін көруге, өңдеуге және жасауға болады. Қауіпсіздік мәселелері клиенттік құрылғыға орнатылған басқарылатын Kaspersky қолданбалары арқылы автоматты түрде жасалуы немесе әкімші қолмен жасауы мүмкін. Мысалы, кейбір пайдаланушылар зиянды бағдарламаны алынбалы жетектерден құрылғыларға жүйелі түрде жылжытса, әкімші қауіпсіздік мәселесін жасай алады. Әкімші қауіпсіздік мәселесі мәтінінде пайдаланушыға қарсы жасалуы керек жағдай мен ұсынылған әрекеттердің қысқаша сипаттамасын (мысалы, тәртіптік іс-әрекеттер) көрсете алады және пайдаланушыға не пайдаланушыларға сілтеме қоса алады.

  Қажетті әрекеттер орындалған қауіпсіздік мәселесі *өңделген* деп аталады. Өңделмеген қауіпсіздік мәселелерінің болуы құрылғының күйін *Критикалық* немесе *Ескерту* күйіне өзгерту шарты ретінде таңдалуы мүмкін.

  Бөлімде құрылғы үшін жасалған қауіпсіздік мәселелерінің тізімі берілген. Қауіпсіздік мәселелері маңыздылық деңгейі мен түріне қарай жіктеледі. Қауіпсіздік мәселесінің түрі қауіпсіздік мәселесін жасайтын Kaspersky қолданбасы арқылы анықталады. Өңделген қауіпсіздік мәселелерін **Өңделген** бағанына жалауша қою арқылы тізімде белгілеуге болады.

- **Тегтер**

  Тегтер қойыншасында клиент құрылғысын іздеуге негізделген кілт сөздер тізімін басқаруға болады: қолданыстағы тегтер тізімін қарау, тізімнен тегтер тағайындау, автоматты түрде тег қою ережелерін конфигурациялау, жаңа тегтер қосу және ескі тегтердің атын өзгерту, тегтерді жою.

- **Кеңейтілген**

  Бұл қойындыда келесі бөлімдер бар:

  - **Бағдарламалар тізімдемесі**. Осы бөлімде клиент құрылғысында орнатылған бағдарламалар мен оларға арналған жаңартулардың тізімдемесін көруге, сондай-ақ бағдарламалар тізімдемесінің көрсетілуін конфигурациялауға болады.

    Орнатылған бағдарламалар туралы ақпарат, клиент құрылғысында орнатылған Желілік агент қажетті ақпаратты Басқару серверіне берген жағдайда беріледі. Басқару серверіне ақпаратты беру параметрлерін **Қоймалар** бөліміндегі Желілік агент сипаттары немесе оның саясаты конфигурациялауға болады.

    Бағдарлама атауын басқан кезде бағдарлама туралы мәліметтері және сол бағдарлама үшін орнатылған жаңарту пакеттерінің тізімі бар терезе ашылады.

- **Орындалатын файлдар**. Осы бөлімде клиент құрылғысында табылған орындалатын файлдар көрсетіледі.

- **Тарату нүктелері**. Бұл бөлімде құрылғы өзара әрекеттесетін тарату нүктелерінің тізімі берілген.

  - **Файлға экспорттау**

    Файлға экспорттау түймесі арқылы сіз құрылғы өзара әрекеттесетін тарату нүктелерінің тізімін файлға сақтай аласыз. Әдепкі бойынша, бағдарлама құрылғылар тізімін CSV пішіміндегі файлға экспорттайды.

  - **Сипаттар**

    Сипаттар түймесі арқылы құрылғы өзара әрекеттесетін тарату нүктесінің параметрлерін көруге және конфигурациялауға болады.

- **Жабдық тізімдемесі**. Осы бөлімде клиент құрылғысында орнатылған жабдық туралы ақпаратты көруге болады.

  Желілік агент Windows жүйесімен жұмыс істейтін құрылғыға орнатылған болса, ол басқару серверіне құрылғының аппараттық жасақтамасы туралы келесі ақпаратты жібереді:

  - ЖЖҚ
  - Жаппай сақтау құрылғылары
  - Негізгі тақта
  - Процессор
  - Желілік адаптерлер
  - Мониторлар
  - Бейне адаптері
  - Дыбыстық карта

  Желілік агент Linux немесе macOS жүйесімен жұмыс істейтін құрылғыға орнатылған болса, ол басқару серверіне құрылғының аппараттық жасақтамасы туралы келесі ақпаратты жібереді (бұл ақпаратты операциялық жүйе қамтамасыз етсе):

  - Жалпы ЖЖҚ көлемі
  - Жаппай сақтау құрылғыларының жалпы көлемі
  - Негізгі тақта
  - Процессор
  - Желілік адаптерлер

- **Қолжетімді жаңартулар**. Бұл бөлімде құрылғыда орнатылмаған бағдарламалық жасақтама жаңартуларының тізімін көруге болады.

- **Бағдарламалық жасақтама осалдықтары**. Осы бөлімде клиент құрылғыларында орнатылған үшінші тарап бағдарламаларының осалдығы туралы ақпарат бар тізімді көруге болады.

Осалдықтарды файлға сақтау үшін, сақтағыңыз келетін осалдықтардың жанына жалаушалар қойып, **CSV файлына экспорттау** түймесін немесе **TXT файлына экспорттау** түймесін басыңыз.

Осы бөлім келесі параметрлерді қамтиды:

- **Тек түзетуге болатын осалдықтарды көрсету**

  Егер параметр қосулы болса, бөлімде патчпен жабуға болатын осалдықтар көрсетіледі.

  Параметр өшірулі болса, бөлімде патчпен жабуға болатын осалдықтар да, патч жоқ осалдықтар да көрсетіледі.

  Әдепкі бойынша, параметр қосулы.

- **Осалдықтың сипаттары**

  Бағдарламаларда таңдалған осалдықтың сипаттарын бөлек терезеде көру үшін тізімдегі бағдарламалардағы осалдықтың атын басыңыз. Сипаттар терезесінде келесі әрекеттерді орындауға болады:

  - Осы басқарылатын құрылғыдағы бағдарламалық жасақтамада (Kaspersky Security Center Web Console-де) осалдықты өткізіп жіберу.
  - Осалдық үшін ұсынылған түзетулер тізімін қарап шығу.
  - Осалдықты түзету үшін бағдарламалық жасақтама жаңартуларын қолмен көрсету (Kaspersky Security Center Web Console-де).
  - Осалдықтардың даналарын қарап шығу.
  - Осалдықты жабу үшін бар тапсырмалар тізімін қарап шығу және осалдықты жабу үшін тапсырмалар жасау.

- **Қашықтан диагностикалау**. Бұл бөлімде клиент құрылғыларын қашықтан диагностикалауға болады.

PostgreSQL, MariaDB немесе MySQL ДҚБЖ пайдалансаңыз, **Оқиғалар** қойындысы таңдалған клиент құрылғысы үшін оқиғалардың толық тізімін көрсетпеуі мүмкін. Бұл, ДҚБЖ оқиғалардың өте көп санын сақтаған кезде орын алады. Келесі әрекеттердің бірін орындау арқылы көрсетілетін оқиғалар санын көбейтуге болады:

- Керек емес оқиғаларды жою.
- Керек емес оқиғаларды сақтау мерзімін қысқарту.

Құрылғы үшін Басқару серверінде тіркелген оқиғалардың толық тізімін көру үшін Есептерді пайдаланыңыз.

Клиент құрылғысы мен Басқару серверінің арасындағы қосылымды қолмен тексеру. klnagchk утилитасы

Сіз klnagchk утилитасы арқылы қосылымды тексеріп, клиент құрылғысының Басқару серверіне қосылу параметрлері туралы толық ақпарат ала аласыз. klnagchk утилитасы Желілік агентті орнату қалтасында орналасқан.

Пәрмен жолынан іске қосылған кезде klnagchk утилитасы қолданылатын кілттерге байланысты келесі әрекеттерді орындайды:

- Құрылғыда орнатылған Желілік агентті Басқару серверіне қосу параметрлерінің мәндерін экранға шығарады немесе оқиғалар журналының файлына енгізеді.
- Желілік агенттің статистикасын (соңғы іске қосылған сәттен бастап) және утилитаның нәтижелерін оқиғалар журналының файлына жазады немесе ақпаратты экранға шығарады.
- Желілік агент пен Басқару сервері арасындағы байланысты орнатуға тырысады.

  Егер байланыс орнатылмаса, утилита Басқару сервері орнатылған құрылғының күйін тексеру үшін ICMP пакетін жібереді.

klnagchk утилитасын пайдалану арқылы клиент құрылғысы мен Басқару сервері арасындағы байланысты тексеру үшін,

Желілік агент орнатылған құрылғыда жергілікті әкімшілердің есептік жазбасы астындағы пәрмен желісінен klnagchk утилитасын іске қосыңыз.

Утилитаның пәрмен жолының синтаксисі:

```
klnagchk [-logfile <файл атауы>] [-sp] [-savecert <сертификат файлына апаратын жол>]
[-restart][-sendhb]
```

Кілттердің сипаттамалары:

- `-logfile <файл атауы>` – Желілік агентті Серверге қосу параметрлерінің мәндерін және утилитаның нәтижелерін журнал файлына жазып алады.

  Әдепкі бойынша, ақпарат стандартты шығару ағынында (stdout) сақталады. Егер кілт қолданылмаса, параметрлер, нәтижелер мен қате туралы хабарлар экранға шығады.
- `-sp` – прокси-сервердегі пайдаланушының түпнұсқалық растамасы үшін құпиясөзді көрсетеді.

  Басқару серверіне қосылу прокси-сервер арқылы жүзеге асырылса, кілт қолданылады.
- `-savecert <файл атауы>` – көрсетілген файлдағы Басқару серверіне қатынасудың түпнұсқалық растамасы үшін сертификатты сақтайды.
- `-restart` – утилита аяқталғаннан кейін Желілік агентті іске қосады.
- `-sendhb` – Желілік агентті Басқару серверімен синхрондауды іске қосады.

Іске қосылғаннан кейін, klnagchk утилитасы Желілік агент конфигурация файлдарына қатынасады және қосылым параметрлерін көрсетеді. Бұл параметрлер желілік агентті орнату кезінде және желілік агент саясаты параметрлерінде белгіленеді:

- `Current device` – Windows желісіндегі клиент құрылғысының атауы.
- `Network Agent version` – құрылғыда орнатылған Желілік агент нұсқасының нөмірі (патчтарымен).
- `Administration Server address` – Басқару серверінің мекенжайы.
- `Use SSL` – Басқару серверіне қосылу кезінде қорғалған қосылымның пайдаланылатынын көрсететін параметр.

Ықтимал мәндер:

- 0 – қорғалған арна пайдаланылмайды.
- 1 – қорғалған арна пайдаланылады.

- `Compress traffic` – клиент құрылғысы мен Басқару сервері арасындағы трафиктің қысылады ма екенін көрсететін параметр.
- `Numbers of the Administration Server SSL ports` – қорғалған арнаны пайдалану кезінде Басқару серверіне қосылуға рұқсат етілген порттардың нөмірлері.
- `Numbers of the Administration Server ports` – әдеттегі қосылымды пайдаланған кезде Басқару серверіне қосылуға рұқсат етілген порттар саны.
- `Use proxy server` – прокси-сервердің пайдаланылатынын көрсететін параметр.

  Ықтимал мәндер:

  - 0 – прокси-сервер пайдаланылмайды.
  - 1 – прокси-сервер қолданылуда.

- `Address` – қос нүктемен бөлінген прокси-сервердің мекенжайы мен порты. Бұл параметр прокси-серверді пайдалансаңыз ғана пайда болады.
- `User name` – прокси-серверге кіруге арналған пайдаланушы аты. Бұл параметр прокси-серверді пайдалансаңыз ғана пайда болады.
- `Password` – прокси-серверге кіруге арналған құпиясөз. Бұл параметр прокси-серверді пайдалансаңыз ғана пайда болады. Прокси-сервер құпиясөзін көрсету үшін пәрмендегі `sp` қосқышын пайдалану керек.
- `Administration Server certificate` – клиент құрылғысында Басқару сервер сертификаты бар-жоғын көрсететін параметр. Мысалы, Желілік агент Басқару серверіне ешқашан қосылмаған болса, сертификат болмауы мүмкін.

  Ықтимал мәндер:

  - `not installed` – клиент құрылғысында Басқару сервері сертификаты жоқ.
  - `available` – клиент құрылғысында Басқару сервері сертификаты бар.

- `Open UDP port` – Басқару серверінен синхрондау сұрауларын алу үшін Желілік агент UDP портын пайдаланады ма екенін көрсететін параметр.

  Ықтимал мәндер:

  - 0 – Басқару серверінен синхрондау сұрауларын алу үшін UDP порты жабық.
  - 1 – Басқару серверінен синхрондау сұрауларын қабылдау үшін UDP порты ашық.

- `Numbers of UDP ports` – Желілік агент пайдалана алатын UDP порттарының нөмірлері.
- `Location name` – құрылғының желідегі орны.
- `State of network location` – клиент құрылғысын бір Басқару серверінің қосылым профилінен екіншісіне ауыстыруға болады ма екенін көрсететін параметр.

Ықтимал мәндер:

- `Enabled` – байланыс профилін Басқару серверіне клиент құрылғысы үшін ауыстырып қосуға болады.
- `Disabled` – байланыс профилін Басқару серверіне клиент құрылғысы үшін ауыстырып қосу мүмкін емес.

- `Profile to use` – Басқару серверіне байланыс профилі.
- `Condition` – клиент құрылғысы қосылған желінің IP мекенжайы және ішкі желі маскасы.
- `Synchronization interval (min)` – стандартты синхрондау аралығы.
- `Connection timeout (in seconds)` – қосылымды күту уақыты.
- `Send / receive timeout (in seconds)` – оқу-жазу операциялары үшін қосылымды күту уақыты.
- `Device ID` – желідегі құрылғы идентификаторы. `Device ID` белгіленген Басқару сервері басқаратын клиент құрылғылары үшін бірегей болып табылады.
- `Locations of connection gateways` – қосылым шлюзі арқылы клиент құрылғысын Басқару серверіне қосуға арналған параметрлер.
- `Location of distribution points` – тарату нүктесінің көмегімен клиент құрылғысын Басқару серверіне қосуға арналған параметрлер.
- `Connection with server` – қосылым шлюзінің Басқару серверімен тұрақты байланысы бар-жоғын көрсететін параметр. Параметр клиент құрылғысы қосылу шлюзі рөлінде әрекет ететін жағдайда ғана көрсетіледі.

  Ықтимал мәндер:

  - `active` – қосылым шлюзінің Басқару серверімен тұрақты қосылымы бар.
  - `inactive` – қосылым шлюзінің Басқару серверімен тұрақты қосылымы жоқ.

- `Connection with server through connection gateway` – қосылу шлюзі арқылы Басқару серверіне қосылымның дұрыс орнатылғанын көрсететін параметр. Параметр клиент құрылғысы қосылу шлюзі рөлінде әрекет ететін жағдайда ғана көрсетіледі.

  Ықтимал мәндер:

  - `active` – қосылу шлюзі арқылы Басқару серверімен қосылым дұрыс орнатылды.
  - `inactive` – қосылу шлюзі арқылы Басқару серверімен қосылым дұрыс орнатылмаған.

Сондай-ақ, klnagchk утилитасының шығысында келесі жолақтардың бірі болуы мүмкін:

- `Administration Server is installed on this device` – klnagchk утилитасы Басқару сервері құрылғысында іске қосылған.
- `This device has been assigned a connection gateway but is not yet registered on Administration Server` – klnagchk утилитасы қосылым шлюзі режимінде желілік агент орнатылған құрылғыда іске қосылған. Конфигурацияланған қосылу шлюзі Басқару серверінен қосылымды күтеді, бірақ Басқару сервері құрылғыны басқарылатын құрылғылар арасында тізімдемейді. Басқару сервері қосылу шлюзіне қосылуды бастағанына көз жеткізуіңіз керек.

- `This device is a connection gateway` – klnagchk утилитасы қосылу шлюзі рөлін атқаратын құрылғыда іске қосылады.
- `Acts as a distribution point` – klnagchk утилитасы тарату нүктесі рөлін атқаратын құрылғыда іске қосылады.

klnagchk утилитасы Желілік агент қызметінің күйін тексереді. Қызмет іске қосылмаса, утилита тоқтайды. Егер қызмет іске қосылған болса, утилита келесі қосылымдар статистикасын көрсетеді:

- `Total number of synchronization requests` – клиент құрылғысын Басқару серверіне қосу әрекеттерінің саны.
- `The number of successful synchronization request` – клиент құрылғысын Басқару серверіне қосудың сәтті әрекеттерінің саны.
- `Total number of synchronizations` – клиент құрылғысы параметрлерін Басқару сервері параметрлерімен синхрондау әрекеттерінің саны.
- `The number of successful synchronizations` – клиент құрылғысының параметрлерін Басқару серверімен синхрондаудың сәтті әрекеттерінің саны.
- `Date/time of the last request for synchronization` – соңғы қосылымның күні мен уақыты.

Басқару сервері мен Желілік агент арасындағы қосылымды талданған кезде `Total number of synchronization requests` және `The number of successful synchronization request` пайдалану керек. Клиент құрылғысының параметрлері Басқару серверінің параметрлері өзгертілген жағдайда ғана (мысалы, жаңа тапсырмалар қосылғанда немесе саясат параметрлері өзгертілгенде) Басқару серверінің параметрлерімен синхрондалады. Әйтпесе, `Total number of synchronizations` және `The number of successful synchronizations` параметрлерінің мәндері өзгермейді.

Желілік агентті басқару серверіне қосуға қатысты мәселелерді шешу туралы қосымша ақпарат алу үшін Kaspersky Security Center жиі қойылатын сұрақтарын қараңыз.

Құрылғыны жылжыту ережелері

Құрылғыларды жылжыту ережелері көмегімен басқару топтарында құрылғыларды орналастыру процесін автоматтандыру ұсынылады. Жылжыту ережесі үш негізгі бөліктен тұрады: атауы, орындау шарттары (құрылғы атрибуттарының логикалық өрнегі) және мақсатты басқару тобы. Құрылғының атрибуттары ережені орындау шартына сай келсе, онда ереже құрылғыны мақсатты басқару тобына көшіреді.

Құрылғыны жылжыту ережелерінің басымдықтары бар. Басқару сервері құрылғының атрибуттарын әрбір ережені орындау шартына сай келу тұрғысынан, ережелер басымдығының азаюы тәртібінде тексереді. Құрылғының атрибуттары ережені орындау шартына сай келсе, онда құрылғы мақсатты топқа көшіріледі және бұл құрылғы үшін ережелерді өңдеу осымен тоқтайды. Егер құрылғының атрибуттары бірден бірнеше ережеге сай келсе, онда құрылғы үлкен басымдыққа ие ереженің мақсатты тобына көшіріледі (ережелер тізімінде жоғары тұр).

Құрылғыны жылжыту ережелері айқын емес түрде жасалуы мүмкін. Мысалы, қашықтан орнату тапсырмасының немесе пакетінің сипаттарында, Желілік агентті орнатқаннан кейін құрылғы кіруі тиісті басқару тобы көрсетілуі мүмкін. Сондай-ақ, жылжыту ережелерін Kaspersky Security Center Linux әкімшісі айқын түрде **Активтерді басқару** → **Жылжыту ережелері** бөлімінде жасай алады.

Жылжыту ережесі, әдепкі бойынша құрылғыларды басқару топтарында бір рет бастапқы орналастыруға арналған. Ереже бөлінбеген құрылғыларды бір рет қана жылжытады. Егер құрылғы бір рет осы ережемен көшірілген болса, тіпті құрылғыны тағайындалмаған құрылғылар тобына қолмен қайтарған жағдайда да, ереже оны қайтадан көшірмейді. Бұл, жылжыту ережелерін қолданудың ұсынылатын тәсілі.

Басқару топтарында әлдеқашан орналастырылған құрылғыларды жылжытуға болады. Бұл үшін ереже сипаттарында **Тек басқару тобында орналастырылмаған құрылғыларды жылжыту** жалаушасын алып тастаңыз.

Басқару топтарында әлдеқашан орналастырылған құрылғыларға қолданылатын жылжыту ережелерінің болуы, Басқару серверіне түсетін жүктемені едәуір арттырады.

Тек басқару тобында орналастырылмаған құрылғыларды жылжыту жалаушасы автоматты түрде жасалған жылжыту ережелерінің сипаттарында бұғатталған. Мұндай ережелер *Бағдарламаларды қашықтан орнату* тапсырмасын қосқанда немесе автономды орнату пакетін жасағанда құрылады.

Бір құрылғыда көп рет әрекет ете алатын жылжыту ережесін жасауға болады.

Бір құрылғы топтан топқа көп рет жылжыту, мысалы, құрылғыға арнайы саясатты қолдану, арнайы топтық тапсырманы іске қосу, белгілі бір тарату нүктесінен жаңарту мақсатында басқарылатын құрылғылармен жұмыс істеу тәсілдемесінен аулақ болу қатаң ұсынылады.

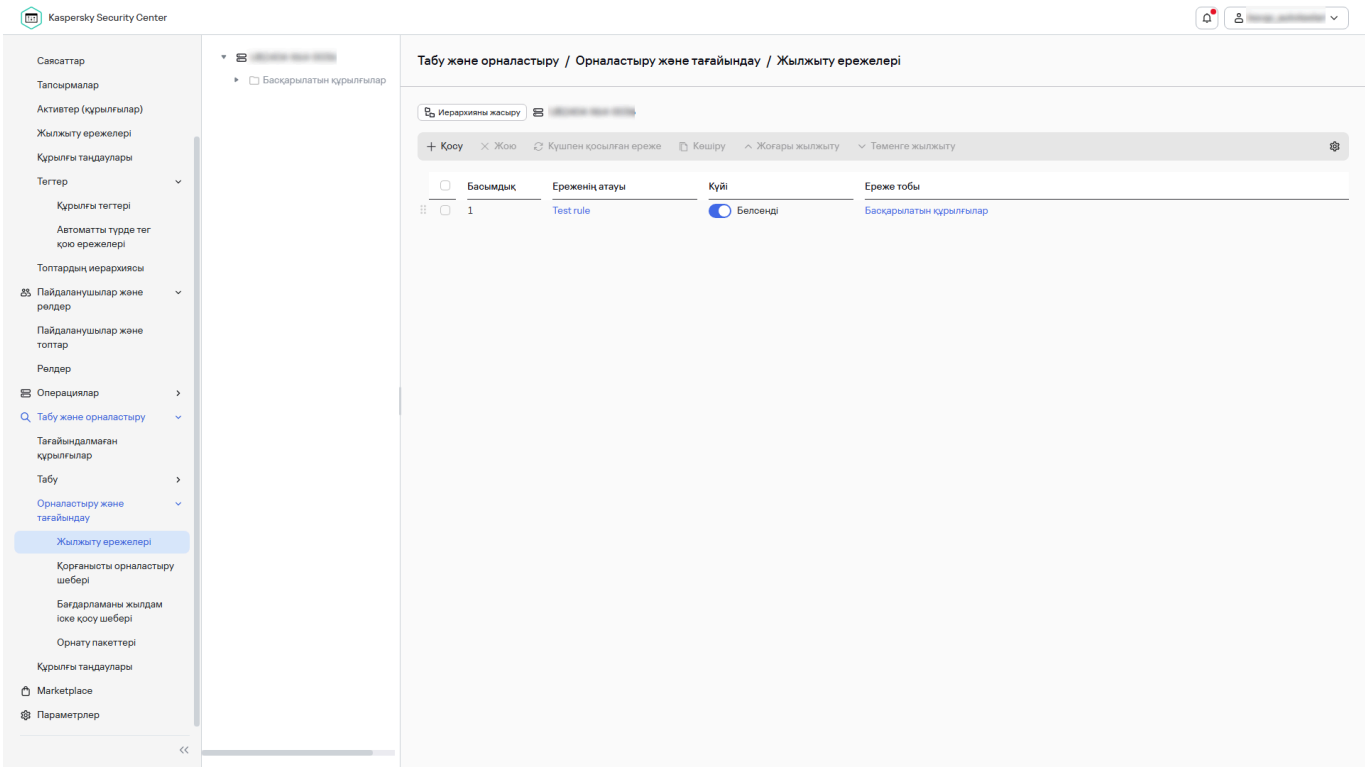
Мұндай сценарийлерге қолдау көрсетілмейді, өйткені олар Басқару серверіне және желілік трафикке жүктеу бойынша онша тиімсіз. Сондай-ақ, бұл сценарийлер Kaspersky Security Center Linux жұмыс моделіне қарама-қайшы келеді (әсіресе, қатынасу құқықтары, оқиғалар мен есептер саласында). Басқа шешім іздеу, мысалы, саясат профильдерін, құрылғыларды таңдауға арналған тапсырмаларды қолдану, әдістемеге сәйкес желілік агенттерді тағайындау керек.

Құрылғыны жылжыту ережелерін жасау

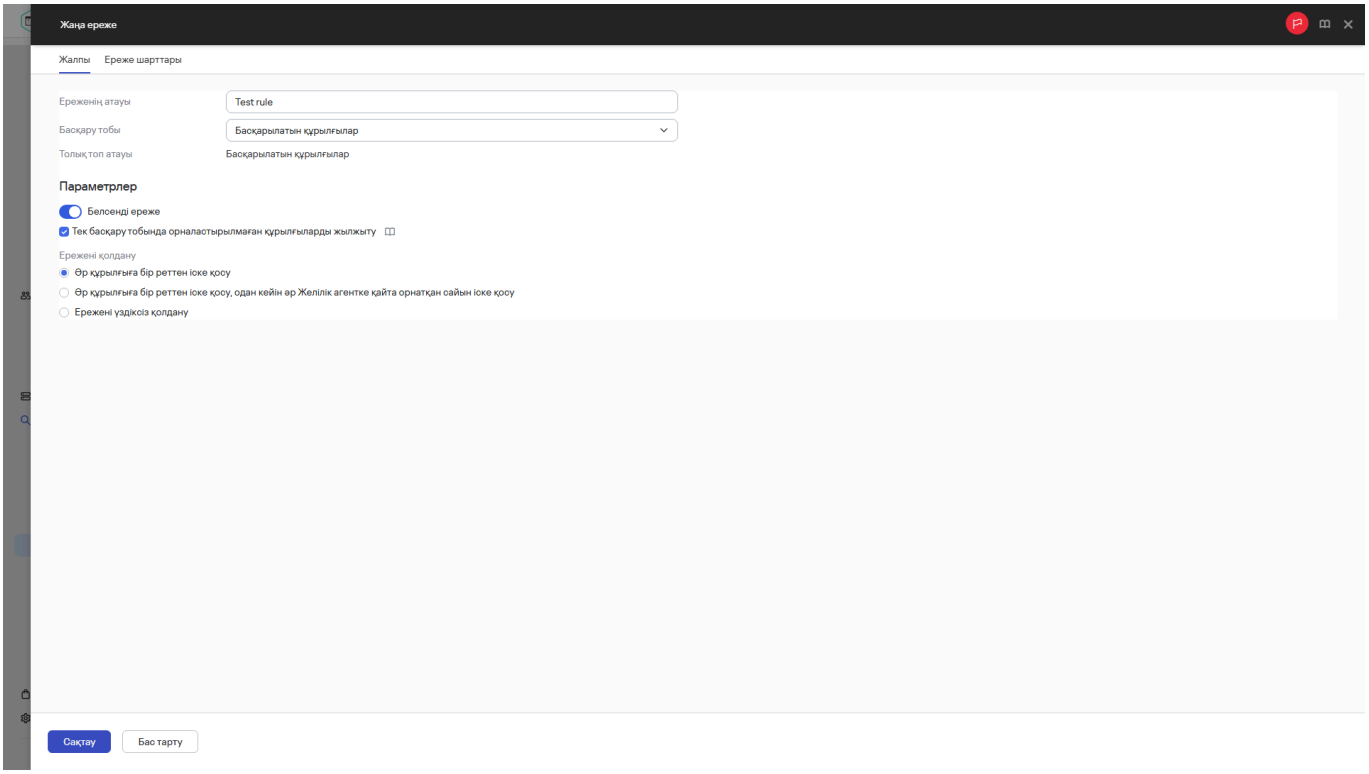
Құрылғыларды басқару топтары бойынша таратылатын құрылғыны жылжыту ережелерін конфигурациялауға болады.

Құрылғыны жылжыту ережесін жасау үшін:

1. Бағдарламаның негізгі терезесінде **Активтерді басқару → Жылжыту ережелері** бөліміне өтіңіз.



2. **Қосу** түймесін басыңыз. **Жаңа ереже** терезесі ашылады.



3. Ашылған терезеде, **Жалпы** қойыншасында келесі деректерді көрсетіңіз:

- **Ереженің атауы**

  Жаңа белсендіру ережесінің атын көрсетіңіз.

  Егер сіз ережені көшірсеңіз, жаңа ереже бастапқы ережемен бірдей атау алады, бірақ оған жақшаға индекс қосылады, мысалы: (1).

- **Басқару тобы**

  Құрылғылар автоматты түрде жылжытылатын басқару тобын таңдаңыз.

- **Ереже мәртебесі**

  Егер бұл параметр қосылса, ереже қосылады және сақталғаннан кейін бірден қолданыла бастайды.

  Егер бұл параметр өшірулі болса, ереже жасалады, бірақ ол қосылмайды. Бұл параметрді өшірмейінше, ереже жұмыс істемейді.

- **Басымдық**

  Сіз жылжытылатын ереженің басымдығын көрсете аласыз. Ең жоғары басымдық – 1. **Басымдық** мәні неғұрлым жоғары болса, ереженің басымдығы және оның тізімдегі орны соғұрлым төмен болады.

  Егер басымдық берілмесе, ережеге ең төменгі басымдық беріледі.

  Ережені көшірген кезде, ереженің көшірмесіне бастапқы ереженің басымдығы беріледі. Содан кейін, бастапқы ереженің басымдығы 1-ге артады.

- **Тек басқару тобында орналастырылмаған құрылғыларды жылжыту**

  Егер бұл параметр қосулы болса, тек тағайындалмаған құрылғылар таңдалған топқа көшіріледі.

  Егер бұл параметр өшірулі болса, басқа басқару топтарына жататын құрылғылар, сондай-ақ тағайындалмаған құрылғылар таңдалған топқа көшіріледі.

- **Ережені қолдану**

  Сіз келесі нұсқаның бірін таңдай аласыз:

  - **Әр құрылғыға бір реттен іске қосу**

    Ереже көрсетілген өлшемшарттарға сәйкес келетін әрбір құрылғы үшін бір рет қолданылады.

  - **Әр құрылғыға бір реттен іске қосу, одан кейін әр Желілік агентке қайта орнатқан сайын іске қосу**

    Ереже көрсетілген өлшемшарттарға сәйкес келетін әрбір құрылғы үшін бір рет қолданылады, содан кейін сол құрылғыларда Желілік агент қайта орнатылған кезде ғана қолданылады.

  - **Ережені үздіксіз қолдану**

    Ереже Басқару серверде автоматты түрде орнатылатын кестеге сәйкес қолданылады (әдетте бірнеше сағат сайын).

4. **Ереже шарттары** қойыншасында құрылғылар басқару тобына жылжытылатын кемінде бір өлшемшартті көрсетіңіз.

5. **Сақтау** түймесін басыңыз.

Жылжыту ережесі жасалады. Ол жылжыту ережелерінің тізімінде пайда болады.

Тізімдегі ереже неғұрлым жоғары болса, оның басымдығы да соғұрлым жоғары болады.

Басымдылықты өзгерту үшін:

1. Жылжыту ережелерінің құсбелгісін таңдаңыз.

2. Келесі әрекеттердің бірін орындаңыз:

   - **Басымдықты өзгерту** түймесін басып, жаңа басымдықты көрсетіңіз.

   - **Жоғары жылжыту** немесе **Төменге жылжыту** түймелерін басу арқылы ережені тізімде жоғары немесе төмен жылжытыңыз.

3. **Сақтау** түймесін басыңыз.

> **Ережені үздіксіз қолдану** параметрі таңдалса, жылжыту ережесі басымдыққа қарамастан қолданылады. Мұндай ережелер Басқару сервері автоматты түрде орнататын кестеге сәйкес қолданылады.

Егер құрылғының атрибуттары бірден бірнеше ережеге сай келсе, онда құрылғы үлкен басымдыққа ие ереженің мақсатты тобына көшіріледі (ережелер тізімінде жоғары тұр).

Құрылғыны жылжыту ережелерін көшіру

Құрылғыларды жылжыту ережелерін көшіруге болады, мысалы, әртүрлі мақсатты басқару топтары үшін бірнеше бірдей ереже керек болса.

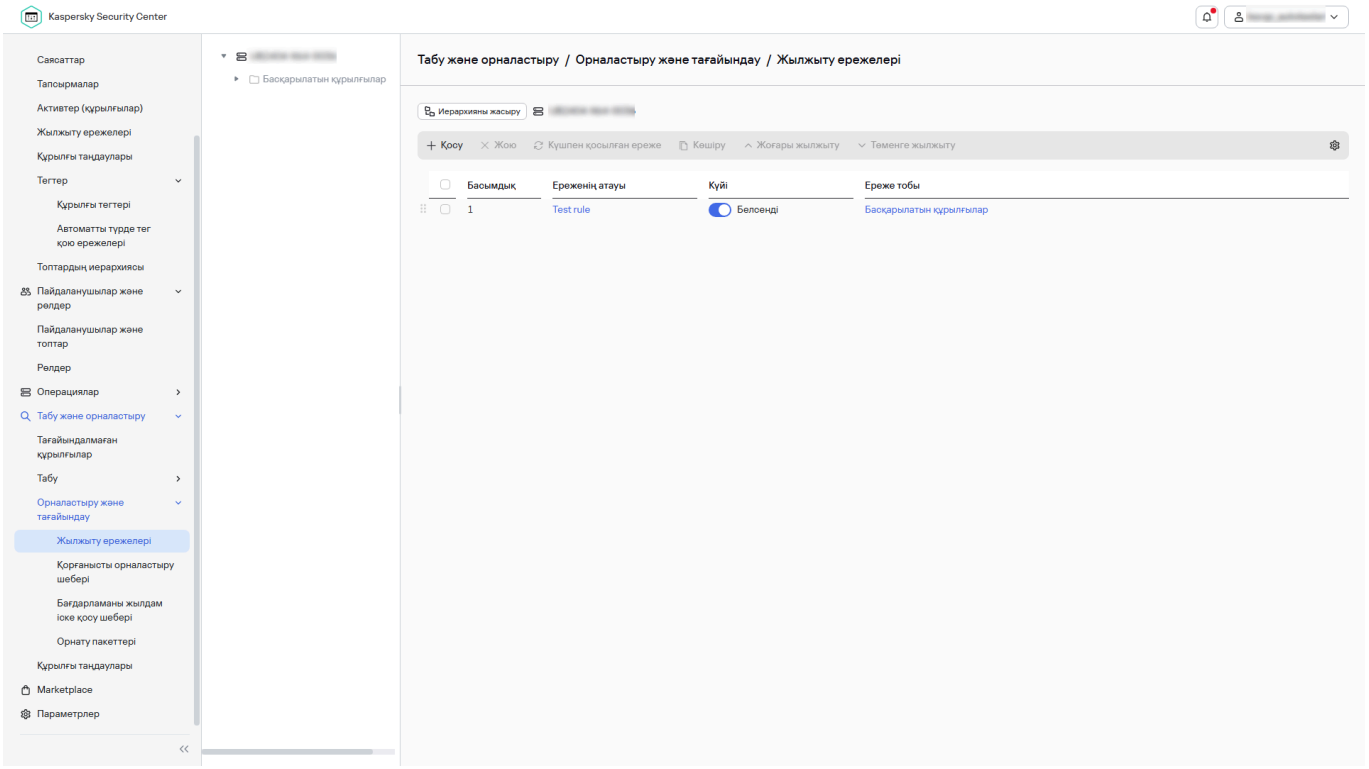
Құрылғыны жылжыту ережесін көшіру үшін:

1. Келесі әрекеттердің бірін орындаңыз:

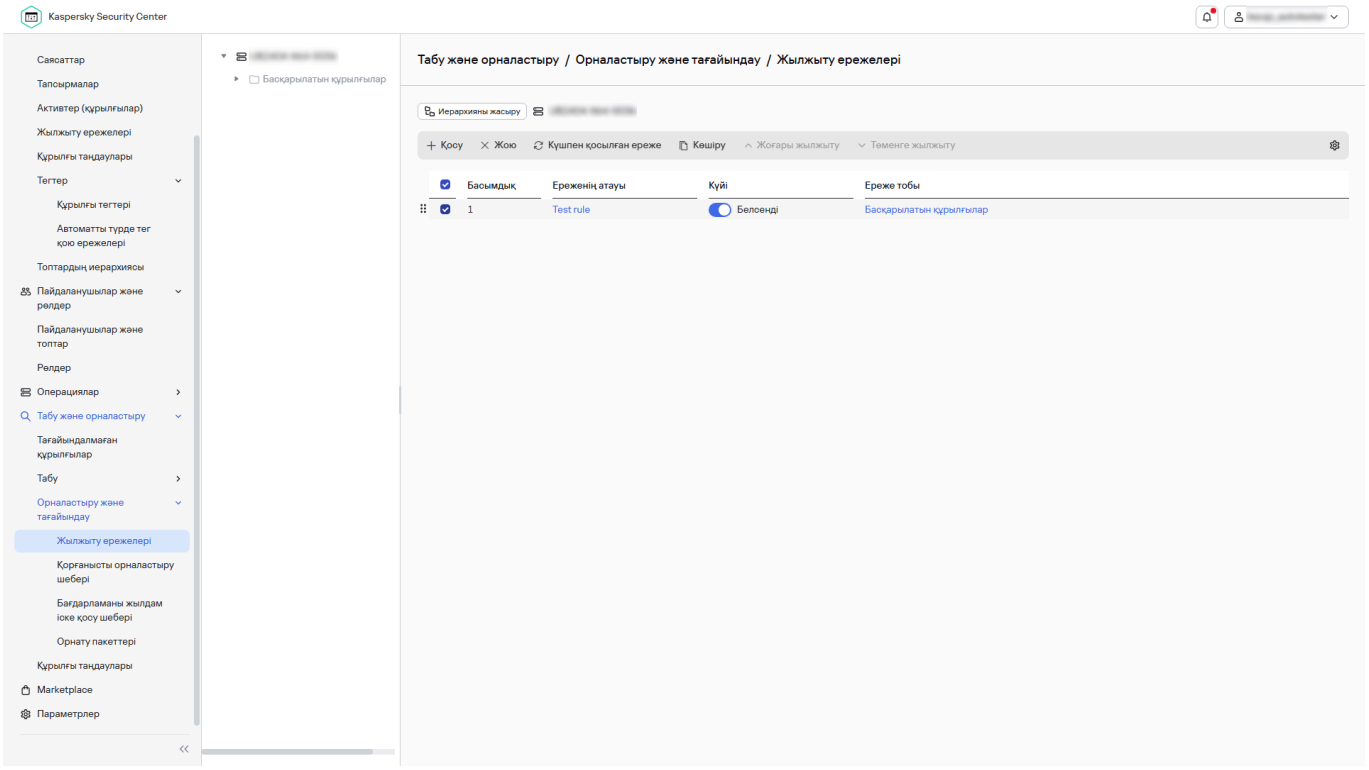
   - Бағдарламаның негізгі терезесінде **Активтерді басқару** → **Жылжыту ережелері** бөліміне өтіңіз.

   - Бағдарламаның негізгі терезесінде **Табу және орналастыру** → **Орналастыру және тағайындау** → **Жылжыту ережелері** бөліміне өтіңіз.

   Құрылғыларды жылжыту ережелерінің тізімі көрсетіледі.



2. Көшіре қажет ережеге қарама-қарсы жалауша қойыңыз.



3. **Көшіру** түймесін басыңыз.

4. Ашылған терезеде, қажет болса **Жалпы** қойыншасындағы деректерді өзгертіңіз немесе параметрлерді өзгертпей, тек ережені көшіре қажет болса, қолданыстағы мәндерді қалдырыңыз:

   - **Ереженің атауы**

     Жаңа белсендіру ережесінің атын көрсетіңіз.

     Егер сіз ережені көшірсеңіз, жаңа ереже бастапқы ережемен бірдей атау алады, бірақ оған жақшаға индекс қосылады, мысалы: (1).

- **Басқару тобы**

  Құрылғылар автоматты түрде жылжытылатын басқару тобын таңдаңыз.

- **Ереже мәртебесі**

  Егер бұл параметр қосылса, ереже қосылады және сақталғаннан кейін бірден қолданыла бастайды.

  Егер бұл параметр өшірулі болса, ереже жасалады, бірақ ол қосылмайды. Бұл параметрді өшірмейінше, ереже жұмыс істемейді.

- **Басымдық**

  Сіз жылжытылатын ереженің басымдығын көрсете аласыз. Ең жоғары басымдық – 1. **Басымдық** мәні неғұрлым жоғары болса, ереженің басымдығы және оның тізімдегі орны соғұрлым төмен болады.

  Егер басымдық берілмесе, ережеге ең төменгі басымдық беріледі.

  Ережені көшірген кезде, ереженің көшірмесіне бастапқы ереженің басымдығы беріледі. Содан кейін, бастапқы ереженің басымдығы 1-ге артады.

- **Тек басқару тобында орналастырылмаған құрылғыларды жылжыту**

  Егер бұл параметр қосулы болса, тек тағайындалмаған құрылғылар таңдалған топқа көшіріледі.

  Егер бұл параметр өшірулі болса, басқа басқару топтарына жататын құрылғылар, сондай-ақ тағайындалмаған құрылғылар таңдалған топқа көшіріледі.

- **Ережені қолдану**

  Сіз келесі нұсқаның бірін таңдай аласыз:

  - **Әр құрылғыға бір реттен іске қосу**

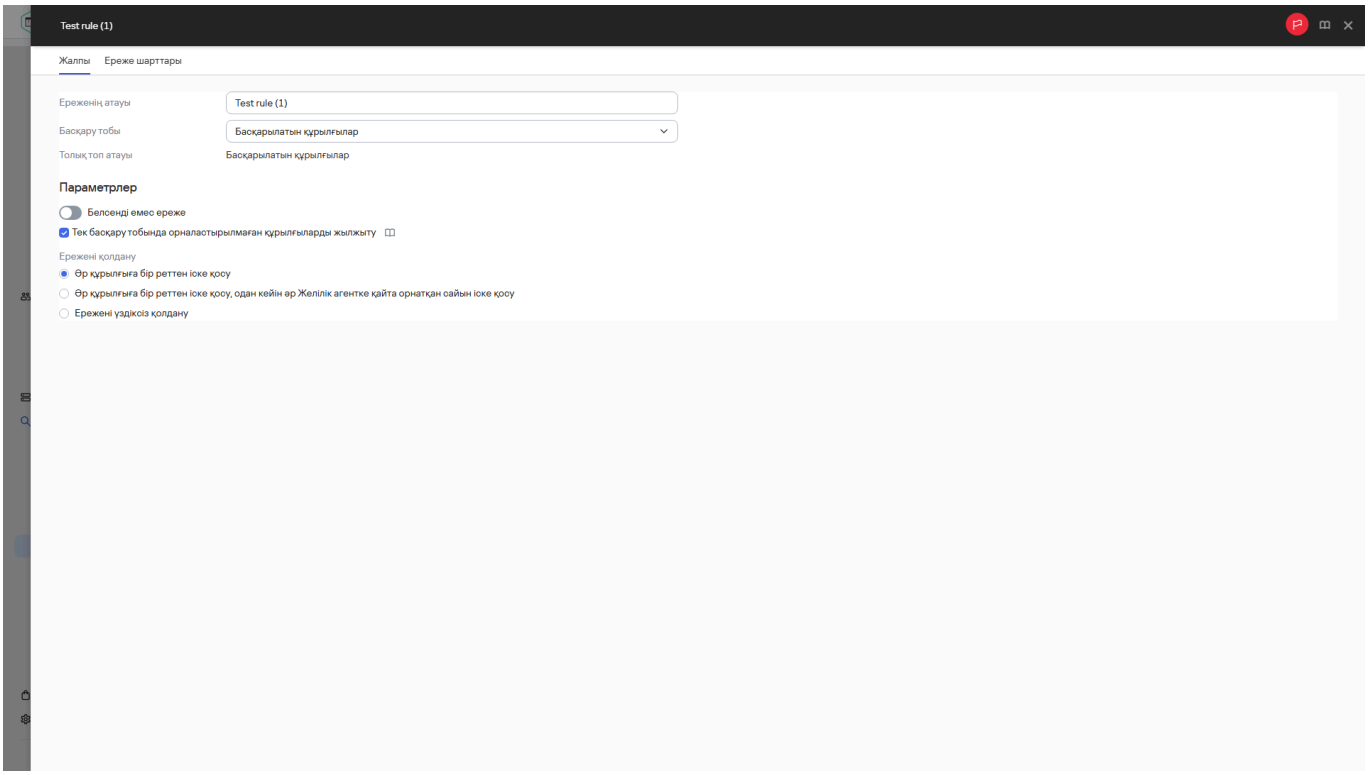
    Ереже көрсетілген өлшемшарттарға сәйкес келетін әрбір құрылғы үшін бір рет қолданылады.

  - **Әр құрылғыға бір реттен іске қосу, одан кейін әр Желілік агентке қайта орнатқан сайын іске қосу**

    Ереже көрсетілген өлшемшарттарға сәйкес келетін әрбір құрылғы үшін бір рет қолданылады, содан кейін сол құрылғыларда Желілік агент қайта орнатылған кезде ғана қолданылады.

  - **Ережені үздіксіз қолдану**

    Ереже Басқару серверде автоматты түрде орнатылатын кестеге сәйкес қолданылады (әдетте бірнеше сағат сайын).



5. **Ереже шарттары** қойыншасында автоматты түрде жылжыту қажет құрылғылар үшін өлшемшарттарды көрсетіңіз.

6. **Сақтау** түймесін басыңыз.

Жаңа жылжыту ережесі жасалады. Ол жылжыту ережелерінің тізімінде пайда болады.

Құрылғыны жылжыту ережелеріне арналған шарттар

Клиент құрылғыларын басқару топтарына жылжыту ережелерін жасау немесе көшіру кезінде, **Ереже шарттары** қойыншасында құрылғыларды жылжыту шарттарын жасайсыз. Қандай құрылғыларды жылжыту керектігін анықтау үшін келесі критерийлерді қолдануға болады:

- Клиент құрылғыларына берілген тегтер.
- Желі параметрлері. Мысалы, IP мекенжайлары бар құрылғыларды көрсетілген ауқымнан жылжытуға болады.
- Құрылғы иесі, оның рөлі және қауіпсіздік топтарына мүшелігі.
- Желілік агент немесе Басқару сервері сияқты клиент құрылғыларында орнатылған басқарылатын бағдарламалар.
- Клиент құрылғылары болып табылатын виртуалды машиналар.
- Домен контроллерінің ұйымдастырушылық бөлімшелері.
- Бұлттық сегменттер.

Төменде, сіз бұл ақпаратты құрылғыларды жылжыту ережесінде қалай көрсету керектігі туралы сипаттама таба аласыз.

Ережеде бірнеше шарттар көрсетілсе, AND логикалық операторы іске қосылады және барлық шарттар бір уақытта қолданылады. Егер сіз қандай да бір параметрлерді таңдамасаңыз немесе кейбір өрістерді бос қалдырсаңыз, мұндай шарттар қолданылмайды.

Тегтер қойыншасы

Бұл қойыншада бұған дейін клиент құрылғыларының сипаттамаларына қосылған кілт сөздер (тегтер) бойынша құрылғыларды іздеуді конфигурациялауға болады. Бұл үшін қажетті тегтерді таңдаңыз. Сонымен қатар, сіз келесі параметрлерді қосуға болады:

- **Көрсетілген тегтерсіз құрылғыларға қолдану**

  Сипаттамада таңдалған тегі бар бағдарламалар орнатылған барлық құрылғылар құрылғылар таңдауына қосылады. Егер бұл параметр өшірулі болса, құрылғыларды жылжыту ережесі барлық таңдалған тегтері бар құрылғыларға қолданылады.

  Әдепкі бойынша, параметр өшірулі.

- **Кем дегенде бір көрсетілген тег сәйкес келген жағдайда қолдану**

  Егер бұл параметр қосулы болса, құрылғыларды жылжыту ережесі таңдалған тегтердің кем дегенде біреуі бар клиент құрылғыларына қолданылады. Егер бұл параметр өшірулі болса, құрылғыларды жылжыту ережесі барлық таңдалған тегтері бар құрылғыларға қолданылады.

  Әдепкі бойынша, параметр өшірулі.

Желі қойыншасы

Бұл қойыншада құрылғыларды жылжыту ережесін ескеретін құрылғылардың желілік деректерін көрсетуге болады:

- **Windows желісіндегі құрылғының атауы**

  Windows желісіндегі құрылғы атауы (NetBIOS атауы) немесе IPv4 мекенжайы не IPv6 мекенжайы.

- **Windows домені**

  Құрылғыларды жылжыту ережесі көрсетілген Windows доменіне қосылған барлық құрылғыларға қолданылады.

- **Құрылғының DNS аты**

  Жылжытқыңыз келетін клиент құрылғысының доменінің DNS атауы. Желіңізде DNS сервері болса, осы өрісті толтырыңыз.

  > Kaspersky Security Center Linux үшін пайдаланып жатқан дерекқорда тіркелімді ескере отырып сұрыптау конфигурацияланған болса, құрылғының DNS атауын көрсеткенде тіркемді ескеріңіз. Әйтпесе, құрылғыны көшіру ережесі жұмыс істемейді.

- **DNS домені**

  Құрылғыларды жылжыту ережесі көрсетілген негізгі DNS суффиксіне қосылған барлық құрылғыларға қолданылады. Желіңізде DNS сервері болса, осы өрісті толтырыңыз.

- **IP ауқымы**

  Бұл параметр қосулы болса, енгізу өрістерінде сіз іздеген құрылғылар кіруі тиісті аралықтың бастапқы және соңғы IP мекенжайларын көрсетуге болады.

  Әдепкі бойынша, параметр өшірулі.

- **Басқару серверіне қосылуға арналған IP мекенжайы**

  Егер бұл параметр қосылса, клиент құрылғылары Басқару серверіне қосылатын IP мекенжайларын белгілеуге болады. Бұл үшін, барлық қажетті IP мекенжайларын қамтитын IP ауқымын көрсетіңіз.

  Әдепкі бойынша, параметр өшірулі.

- **Құрылғы "Домендер" тобының қосалқы тобында орналасқан**

  Егер бұл опция қосылған болса, "Домендер" тобының ішкі тобын таңдай аласыз. Тиісті құрылғылар таңдалған ішкі топта орналасуы керек.

  Әдепкі бойынша, параметр өшірулі.

- **Құрылғы мына IP ауқымында орналасқан**

  Бұл опция қосылса, **IP ауқымдары** бөлімінде бұдан алдын таңдалған IP ауқымын таңдай аласыз. Таңдалған IP ауқымында тиісті құрылғылар қамтылуы керек.

  Әдепкі бойынша, параметр өшірулі.

- **Байланыс профилі өзгертілді**

  Келесі мәндердің бірін таңдаңыз:

  - **Иә**. Құрылғыларды жылжыту ережесі тек қосылым профилі өзгертілген клиент құрылғыларына қатысты қолданылады.
  - **Жоқ**. Құрылғыларды жылжыту ережесі байланыс профилі өзгермеген клиенттік құрылғыларға ғана қолданылады.
  - **Мән таңдалмаған**. Шарт қолданылмайды.

- **Басқа Басқару серверімен басқарылады**

  Келесі мәндердің бірін таңдаңыз:

  - **Иә**. Құрылғыларды жылжыту ережесі тек басқа Басқару серверлері басқаратын клиент құрылғыларына қолданылады. Бұл Серверлер құрылғыларды жылжыту ережесін конфигурациялайтын Серверден ерекшеленеді.
  - **Жоқ**. Құрылғыларды жылжыту ережесі тек ағымдағы басқару сервері басқаратын клиенттік құрылғыларға қолданылады.
  - **Мән таңдалмаған**. Шарт қолданылмайды.

Құрылғының иесі қойындысы

Бұл қойындыда құрылғы иесіне, қауіпсіздік тобының мүшелігіне және рөлдерге негізделген құрылғы қозғалысы ережесін конфигурациялай аласыз:

- **Құрылғының иесі**

  Ішкі қауіпсіздік тобынан құрылғы иесінің пайдаланушы атын таңдаңыз. Осы бөлімде пайдаланушылар мен пайдаланушы рөлдері туралы көбірек біліңіз.

  > Құрылғы иесі ретінде біреуден артық пайдаланушы тіркеле алмайды.

- **Device owner's membership in Active Directory security group**

  Құрылғы иесі тиесілі сыртқы Active Directory қауіпсіздік тобын таңдаңыз.

  > Пайдаланушы, Active Directory қауіпсіздік тобының бөлігі немесе сол Active Directory қауіпсіздік тобының мүшесі болып табылатын топтың бөлігі болуы мүмкін.

- **Құрылғы иесінің рөлі**

  Құрылғы иесіне тағайындалған рөлді таңдаңыз. Пайдаланушы рөлдері туралы қосымша ақпарат алу үшін осы мақаланы қараңыз.

- **Құрылғы иесінің ішкі қауіпсіздік тобына мүшелігі**

  Құрылғының иесі тиесілі ішкі қауіпсіздік тобын таңдаңыз.

Бағдарламалар қойыншасы

Бұл қойыншада клиент құрылғыларында орнатылған басқарылатын бағдарламалар мен операциялық жүйелер негізінде құрылғыларды жылжыту ережесін конфигурациялауға болады:

- **Желілік агент орнатылған**

  Келесі мәндердің бірін таңдаңыз:

  - **Иә**. Құрылғыларды жылжыту ережесі тек Желілік агент орнатылған клиент құрылғыларына қолданылады.
  - **Жоқ**. Құрылғыларды жылжыту ережесі желілік агент орнатылмаған клиенттік құрылғыларға ғана қолданылады.
  - **Мән таңдалмаған**. Шарт қолданылмайды.

- **Бағдарламалар**

  Бұл құрылғыларға құрылғыларды жылжыту ережесі қолданылуы үшін клиент құрылғыларында қандай басқарылатын бағдарламалар орнатылуы керек екенін көрсетіңіз. Мысалы, **Kaspersky Security Center 16.3 Желілік агенті** немесе **Kaspersky Security Center 16.3 Басқару сервері** тармағын таңдаңыз.

Егер сіз басқарылатын бағдарламаны таңдамасаңыз, шарт қолданылмайды.

- **ОЖ нұсқасы**

  Операциялық жүйенің нұсқасына негізделген клиент құрылғыларын таңдауға болады. Ол үшін клиент құрылғыларында орнатылатын операциялық жүйелерді көрсетіңіз. Нәтижесінде, құрылғыларды жылжыту ережесі таңдалған операциялық жүйелері бар клиент құрылғыларына қолданылады.

  Бұл параметрі өшірулі болса, шарт қолданылмайды. Әдепкі бойынша, параметр өшірулі.

- **ОЖ архитектурасы**

  Сіз клиент құрылғыларын операциялық жүйенің бит өлшеміне қарай таңдай аласыз. **Операциялық жүйенің архитектурасы** өрісінде келесі мәндердің бірін таңдауға болады:

  - **Белгісіз**
  - **x86**
  - **AMD64**
  - **IA64**

  Клиент құрылғыларының операциялық жүйесінің архитектурасын тексеру үшін:

  1. Бағдарламаның негізгі терезесінде **Активтерді басқару** → **Активтер (құрылғылар)** бөліміне өтіңіз.
  2. Оң жақта **Бағандар параметрлері** түймесін (⚙) басыңыз.
  3. **ОЖ архитектурасы** параметрін таңдап, **Сақтау** түймесін басыңыз.

     Осыдан кейін әрбір басқарылатын құрылғы үшін операциялық жүйенің архитектурасы көрсетіледі.

- **ОЖ пакетінің менеджері**

  Сіз клиент құрылғыларын операциялық жүйенің пакет менеджеріне қарай таңдай аласыз. **ОЖ пакетінің менеджері** өрісінде келесі мәндердің бірін таңдауға болады:

  - rpm — Red Hat Enterprise Linux, CentOS, Fedora, SUSE, Oracle Linux операциялық жүйелерін іске қосатын құрылғылар үшін
  - apt (dpkg) — Debian, Ubuntu, Kali операциялық жүйелерін іске қосатын құрылғылар үшін
  - pkg — FreeBSD, OpenBSD операциялық жүйелерін іске қосатын құрылғылар үшін

  Клиент құрылғыларының операциялық жүйесінің пакет менеджерін тексеру үшін:

  1. Бағдарламаның негізгі терезесінде **Активтерді басқару** → **Активтер (құрылғылар)** бөліміне өтіңіз.
  2. Оң жақта **Бағандар параметрлері** түймесін (⚙) басыңыз.
  3. **ОЖ пакетінің менеджері** опциясын таңдап, **Сақтау** түймесін басыңыз.

     Операциялық жүйе пакет менеджері әрбір басқарылатын құрылғылар үшін көрсетіледі.

- **ОЖ жағарту бумасы нұсқасы**

  Бұл өрісте операциялық жүйенің пакет нұсқасын (*X.Y* форматында) көрсетуге болады, ол жылжыту ережесінің құрылғыға қалай қолданылатынын анықтайды. Әдепкі бойынша, нұсқаның мәндері белгіленбеген.

- **Пайдаланушы сертификаты**

  Келесі мәндердің бірін таңдаңыз:

  - **Орнатылған**. Құрылғыларды жылжыту ережесі тек ұялы құрылғы сертификаты бар ұялы құрылғыларға қолданылады.
  - **Орнатылмаған**. Құрылғыларды жылжыту ережесі тек ұялы құрылғы сертификаты жоқ ұялы құрылғыларға қатысты қолданылады.
  - **Мән таңдалмаған**. Шарт қолданылмайды.

- **ОЖ жинақ нөмірі**

  > Бұл параметр тек Windows операциялық жүйелері үшін қолданылады.

  Таңдалған операциялық жүйеде тең, анағұрлым ерте немесе анағұрлым кеш құрастыру нөмірі болуы керек пе екенін көрсетуге болады. Сондай-ақ, көрсетілген нөмірден басқа барлық құрастыру нөмірлері үшін құрылғыларды жылжыту ережелерін конфигурациялауға болады.

- **ОЖ шығарылымының нөмірі**

  > Бұл параметр тек Windows операциялық жүйелері үшін қолданылады.

  Таңдалған операциялық жүйеде тең, анағұрлым ерте немесе анағұрлым кеш жинақ нөмірі болуы керек пе екенін көрсетуге болады. Сондай-ақ, көрсетілген нөмірден басқа барлық жинақ нөмірлері үшін құрылғыларды жылжыту ережелерін конфигурациялауға болады.

Виртуалды машиналар қойыншасы

Бұл қойыншада, құрылғылардың виртуалды машиналар немесе виртуалды жұмыс үстелдері инфрақұрылымының (VDI) бөлігі екендігіне байланысты, бұл клиент құрылғыларын жылжыту ережелерінің параметрлерін конфигурациялауға болады:

- **Виртуалды машина болып табылады**

  Ашылмалы тізімде келесі мәндердің бірін таңдай аласыз:

  - **Қолданылмайды**. Шарт қолданылмайды.
  - **Жоқ**. Виртуалды машиналар емес құрылғыларды жылжыту.
  - **Иә**. Жылжытылатын құрылғылар виртуалды машиналар болуы керек.

- **Виртуалды машинаның түрі**

- **Virtual Desktop Infrastructure бөлігі**

  Ашылмалы тізімде келесі мәндердің бірін таңдай аласыз:

  - **Қолданылмайды**. Шарт қолданылмайды.
  - **Жоқ**. VDI бөлігі емес құрылғыларды жылжыту.
  - **Иә**. Жылжытылатын құрылғылар VDI бөлігі болуы керек.

Домен контроллері қойындысы

Бұл қойындыда доменнің ұйымдық бөлімшесінің құрамына кіретін құрылғыларды жылжыту қажет екенін көрсете аласыз. Сондай-ақ құрылғыларды көрсетілген домен бөлімшесінің барлық еншілес бөлімшелерінен жылжытуға болады:

- **Құрылғы келесі ұйымдық бөлімшеде қамтылған**

  Егер бұл параметр қосулы болса, құрылғыларды жылжыту ережесі параметрдегі тізімде көрсетілген домен контроллерінің ұйымдық бөлімшесіндегі құрылғыларға қолданылады.

  Әдепкі бойынша, параметр өшірулі.

- **Еншілес ұйымдық бөлімшелерін қосу**

  Бұл параметр қосулы болса, домен контроллерінің көрсетілген ұйымдық бірлігінің еншілес бөлімшелеріне кіретін құрылғылар таңдауға қосылады.

  Әдепкі бойынша, параметр өшірулі.

- **Құрылғыларды еншілес бөлімшелерден сәйкес ішкі топтарға жылжыту**
- **Жаңадан анықталған құрылғылардың контейнерлеріне қатысты ішкі топтарды жасау**
- **Доменде жоқ қосалқы топтарды жою**
- **Құрылғы келесі доменнің қауіпсіздік тобында қамтылған**

  Егер бұл параметр қосылса, құрылғыларды жылжыту ережесі параметрдегі тізімде доменнің қауіпсіздік тобындағы құрылғыларға қатысты қолданылады.

  Әдепкі бойынша, параметр өшірулі.

Бұлттық сегменттер қойыншасы

Бұл қойындыда бұлттық сегменттің құрамына кіретін құрылғыларды жылжыту қажет екенін көрсете аласыз. Сондай-ақ құрылғыларды көрсетілген домен бөлімшесінің барлық еншілес бөлімшелерінен жылжытуға болады:

- **Құрылғы бұлттық сегментте орналасқан**

  Бұл параметрді таңдағанда, құрылғыларды жылжыту ережесі бұлттық сегментке жататын клиент құрылғыларына қатысты қолданылады. Параметрдің астындағы тізімдегі ішкі желіге дейін қажетті бұлттық сегментті таңдауға болады.

Әдепкі бойынша, параметр өшірулі.

- **Қосалқы нысандарды қосу**

  Бұл параметр қосулы болса, іріктеуге көрсетілген бұлттық сегменттің барлық еншілес ұйымдық бірліктеріндегі құрылғылар кіреді.

  Әдепкі бойынша, параметр өшірулі.

- **Құрылғыларды кірістірілген нысандардан сәйкес қосалқы топтарға жылжыту**
- **Жаңадан анықталған құрылғылардың контейнерлеріне қатысты ішкі топтарды жасау**
- **Бұлттық сегменттерде сәйкестік жоқ ішкі топтарды жою**
- **Құрылғы API арқылы табылды**

  Ашылмалы тізімде келесі мәндердің бірін таңдай аласыз:

  - Мән таңдалмаған. Шарт қолданылмайды.
  - **Жоқ**. API арқылы табылмаған құрылғыларды жылжытыңыз.
  - **AWS**. AWS API арқылы анықталған құрылғыларды жылжыту.
  - **Azure**. Azure API арқылы анықталған құрылғыларды жылжыту.
  - **Google Cloud**. Google Cloud API арқылы анықталған құрылғыларды жылжыту.

  Осыдан кейін, таңдалған мәнге байланысты келесі өрістерді толтыруға болады:

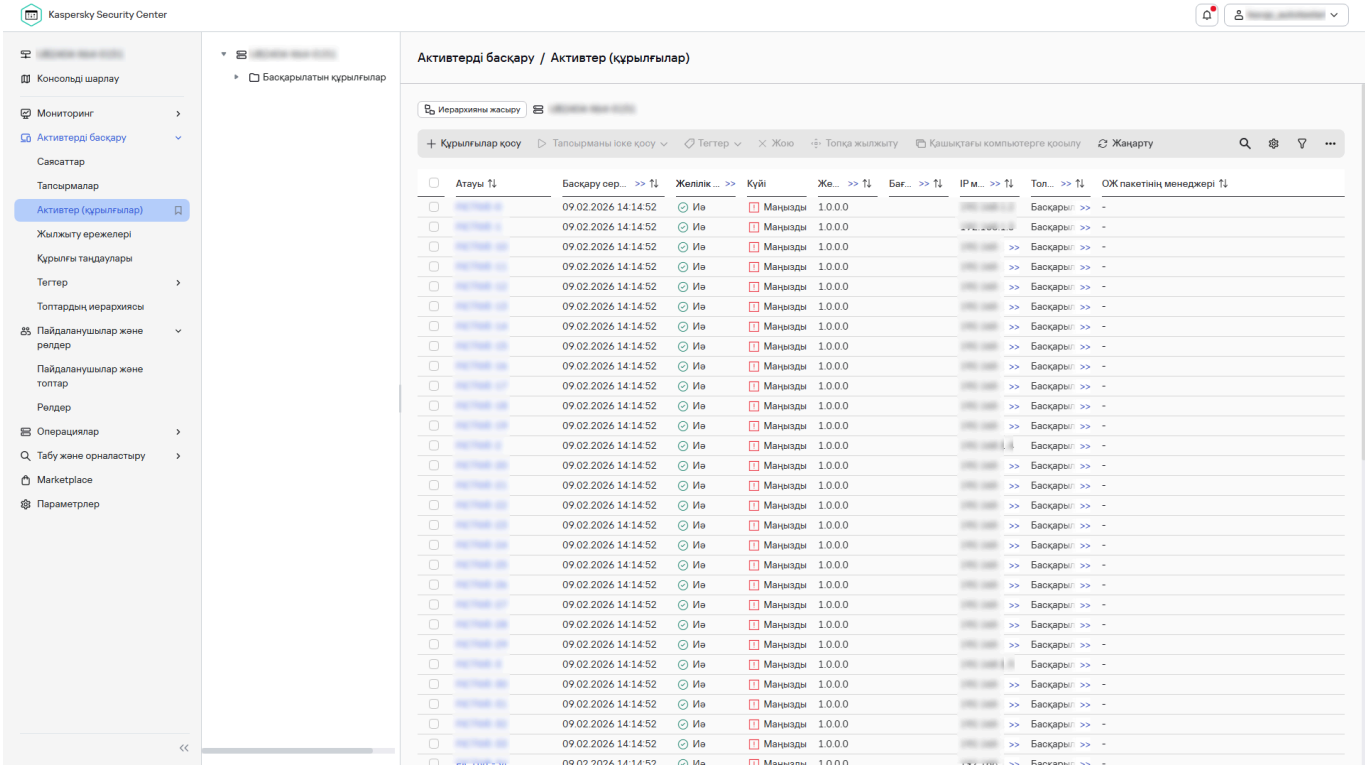
  - **Бұлтты құрылғының ішкі желісі**.
  - **Бұлтты құрылғының қолжетімділік аймағы**.
  - **Бұлтты құрылғыны орналастыру тобы**.

Басқару тобы құрамына құрылғыларды қолмен қосу

Құрылғыларды жылжыту ережелерін жасау арқылы немесе құрылғыларды бір басқару тобынан екіншісіне жылжыту арқылы немесе құрылғыларды таңдалған басқару тобына қосу арқылы құрылғыларды автоматты түрде басқару топтарына жылжытуға болады. Бұл бөлімде құрылғыларды басқару тобына қолмен қосу тәсілі сипатталған.

Таңдалған басқару тобына бір немесе бірнеше құрылғыны қолмен қосу үшін:

1. Бағдарламаның негізгі терезесінде **Активтерді басқару → Активтер (құрылғылар)** бөліміне өтіңіз.



Басқарылатын құрылғылар тізімі

2. Құрылғыларды қосқыңыз келетін басқару тобын таңдаңыз.

   - Түбірлік топ үшін:

     Бұл жағдайда келесі қадамға өтуге болады.

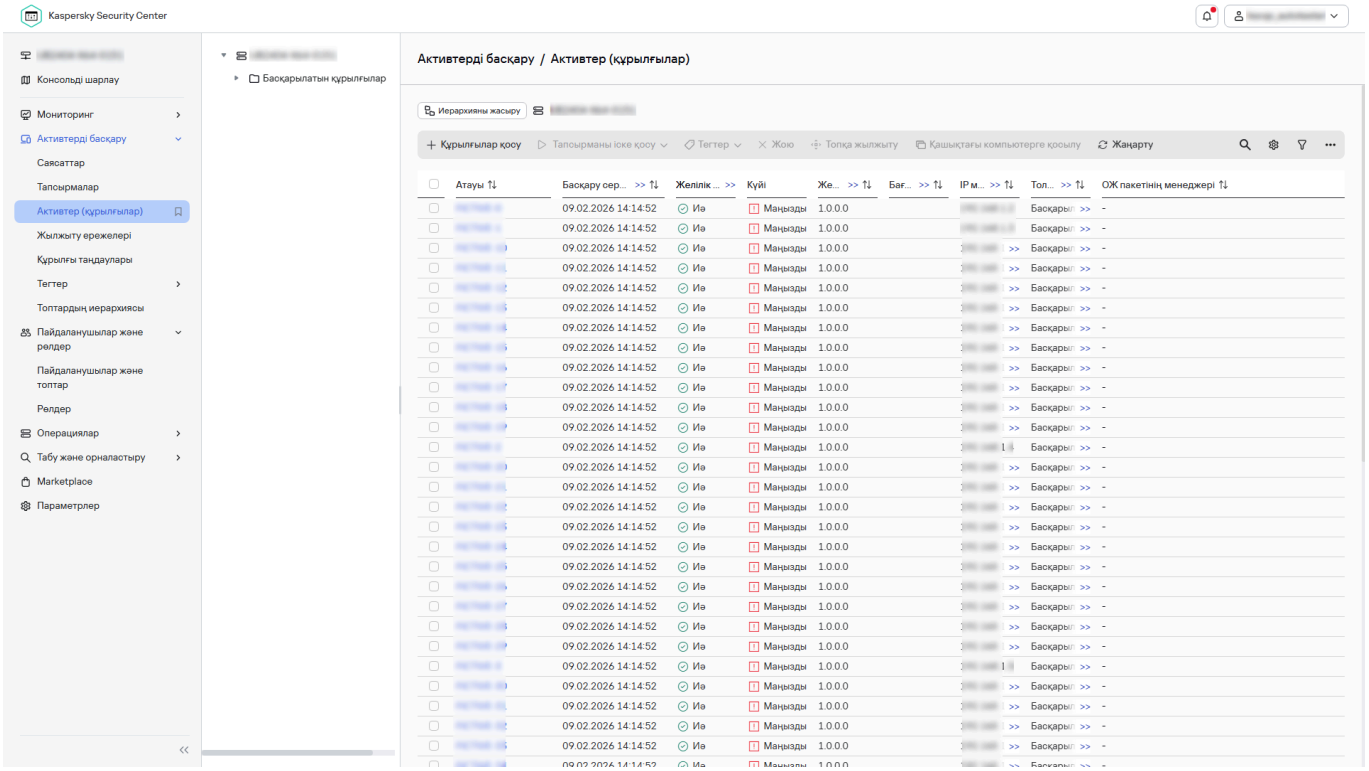
   - Ішкі топ үшін:

     a. Беттің жоғарғы жағындағы **Иерархияны көрсету** түймесін басыңыз.

     Түйме атауы **Иерархияны жасыру** деп өзгереді.

     b. Ашылған терезеде ішкі топтың атауын басыңыз.

Таңдалған топ жолы беттің жоғарғы жағында көрсетіледі. Қажет болса, топқа өту үшін басқару тобының атауы бар сілтемені басуға болады. Әдепкісінше жолдағы соңғы сілтеме белсенді емес. Сондай-ақ **Иерархияны жасыру** түймесін басу арқылы иерархия терезесін жабуға болады.



Басқару тобын таңдау

3. **Құрылғылар қосу** түймесін басыңыз.

   Нәтижесінде, құрылғыларды жылжыту шебері іске қосылады.

4. Басқару тобына қосқыңыз келетін құрылғылардың тізімін құрастырыңыз.

   Құрылғылар тізіміне құрылғыны қосқан кезде немесе құрылғыларды табу нәтижесінде Басқару сервері дерекқорына ақпарат қосылған құрылғыларды ғана қосуға болады.

   Тізімге құрылғыларды қалай қосқыңыз келетінін таңдаңыз:

   - **Құрылғылар қосу** түймесін басып, құрылғыларды келесі тәсілдердің бірімен көрсетіңіз:
     - Басқару сервері анықтаған құрылғылар тізімінен құрылғыларды таңдаңыз.
     - Құрылғылардың IP мекенжайларын немесе IP ауқымын көрсетіңіз.

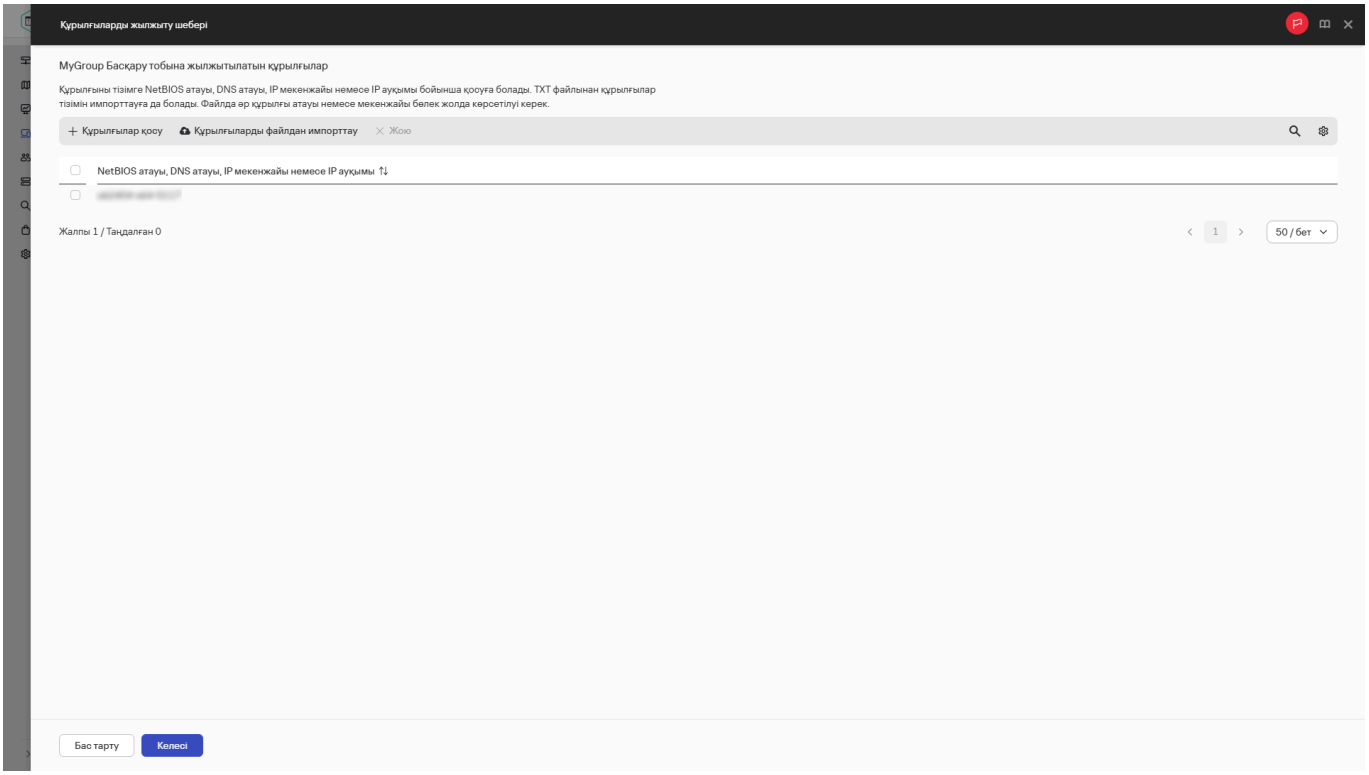
       IP ауқымында 1,048,576 IPS мекенжайынан артық болмауы керек.

     - Құрылғының DNS атауын көрсетіңіз.

       Құрылғы атауы бар өрісте бос орындар, бос жерлер, сондай-ақ тыйым салынған келесі таңбалар болмауы керек: , \ / * ' " ; : & ` ~ ! @ # $ ^ ( ) = + [ ] { } | < > %

- Құрылғыларды TXT пішіміндегі файлдан импорттау үшін **Құрылғыларды файлдан импорттау** түймесін басыңыз. Әрбір құрылғы мекенжайы (немесе құрылғы атауы) бөлек жолда орналасуы тиіс.

  Файлда бос орындар, бос жерлер, сондай-ақ тыйым салынған келесі таңбалар болмауы керек: , \ / * ' " ; : & ` ~ ! @ # $ ^ ( ) = + [ ] { } | < > %



Басқару тобына жылжыту үшін құрылғылар таңдау

5. Басқару тобына қосылатын құрылғылар тізімін қараңыз. Сіз құрылғыларды қосу немесе жою арқылы тізімді өңдей аласыз.

6. Тізімде қателердің жоқ екеніне көз жеткізгеннен кейін, **Келесі** түймесін басыңыз.

Шебер құрылғылар тізімін өңдеп, нәтижені көрсетеді. Шебер аяқталғаннан кейін, таңдалған құрылғылар басқару тобының құрамына енеді және олар үшін Басқару сервері берген атаулары бар құрылғылар тізімінде көрсетіледі.

Құрылғыларды немесе кластерлерді басқару тобының құрамына қолмен жылжыту

Құрылғыларды бір басқару тобынан екіншісіне немесе тағайындалмаған құрылғылар тобынан басқару тобына жылжытуға болады.

Сондай-ақ кластерлерді немесе серверлер массивтерін бір басқару топтан екіншісіне жылжытуға болады. Кластерді немесе серверлер массивін басқа топқа жылжытқанда, оның барлық түйіндері онымен бірге жылжытылады, өйткені кластер және оның кез келген түйіні әрқашан бір басқару топқа жатады. **Құрылғылар** қойындысында бір кластер түйінін таңдаған кезде **Топқа жылжыту** түймесі қолжетімсіз болады.

Таңдалған басқару топ құрамына бір немесе бірнеше құрылғыны немесе кластерді жылжыту үшін:

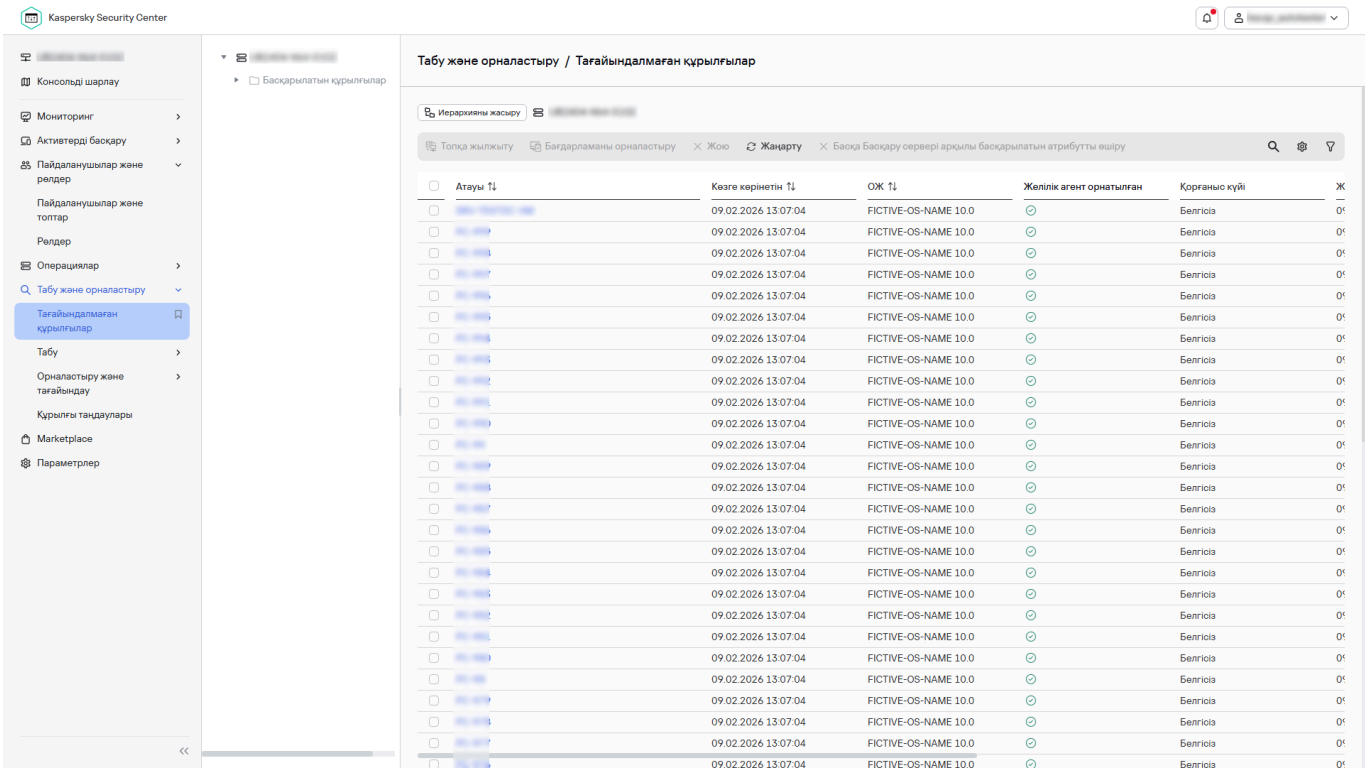
1. Құрылғыларды жылжытқыңыз келетін басқару тобын ашыңыз. Ол үшін келесі әрекеттердің бірін орындаңыз:

   - Басқару тобын ашу үшін негізгі мәзірде **Активтерді басқару → Активтер (құрылғылар)** тармағына өтіп, қажетті басқару тобын таңдаңыз.

     - Түбірлік топ үшін келесі қадамға өтуге болады.

     - Ішкі топ үшін беттің жоғарғы жағындағы **Иерархияны көрсету** түймесін басыңыз, содан кейін ашылатын терезеде қажетті басқару тобын таңдаңыз.

   - **Тағайындалмаған құрылғылар** тобын ашу үшін негізгі мәзірде **Активтерді басқару → Тағайындалмаған құрылғылар** бөліміне өтіңіз.



Тағайындалмаған құрылғылар тізімі

2. Басқару топта кластерлер немесе сервер массивтері болса, **Активтер (құрылғылар)** бөлімі екі қойындыға бөлінеді – **Құрылғылар** және **Кластерлер және серверлердің массивтері**. Жылжытқыңыз келетін нысанның қойындысын ашыңыз.

3. Басқа топқа жылжыту қажет құрылғылардың немесе кластерлердің жанындағы жалаушаларды белгілеңіз.

4. **Топқа жылжыту** түймесін басыңыз.

5. Басқару топтардың иерархиясында таңдалған құрылғыларды немесе кластерлерді жылжытқыңыз келетін Басқару топтың жанындағы жалаушаларды белгілеңіз.

6. **Жылжыту** түймесін басыңыз.

Таңдалған құрылғылар немесе кластерлер таңдалған басқару топқа жылжытылады.

Кластерлер мен серверлердің массивтері туралы

Kaspersky Security Center Linux кластерлік технологияны қолдайды. Желілік агент Басқару серверіне клиент құрылғысында орнатылған бағдарлама сервер массивінің бөлігі екені туралы ақпарат берсе, онда клиент құрылғысы кластер түйініне айналады.

Басқару топта серверлердің кластерлері немесе массивтері болса, **Активтер (құрылғылар)** бетінде екі қойынды көрсетіледі: біреуі жеке құрылғылар үшін, екіншісі серверлердің кластерлері мен массивтері үшін. Басқарылатын құрылғылар кластер түйіндері ретінде анықталғаннан кейін, кластер **Кластерлер және серверлердің массивтері** қойындысына бөлек нысан ретінде қосылады.

Кластер түйіндері немесе сервер массивтері басқа басқарылатын құрылғылармен бірге **Құрылғылар** қойындысында берілген. Түйіндердің сипаттарын жеке құрылғылар ретінде көруге және басқа операцияларды орындауға болады, бірақ кластер түйінін жою немесе оны кластерден бөлек басқа басқару тобына жылжыту мүмкін емес. Бүкіл кластерді ғана жоюға немесе жылжытуға болады.

Сервер кластерлерінде немесе массивтерінде келесі әрекеттерді орындауға болады:

- Сипаттарды көру.
- Кластерді немесе серверлер массивін басқа басқару топқа жылжыту.

  Кластерді немесе серверлер массивін басқа топқа жылжытқанда, оның барлық түйіндері онымен бірге жылжытылады, өйткені кластер және оның кез келген түйіні әрқашан бір басқару топқа жатады.

- Жою

  Серверлер кластері немесе массиві ұйымның желісінде бұдан былай болмаған кезде ғана серверлердің кластерін немесе массивін жойған дұрыс. Егер кластер әлі де желіңізде көрінсе және Желілік агент пен Kaspersky қолданбасы кластер түйіндерінде әлі орнатылған болса, Kaspersky Security Center Linux қашықтағы кластерді және оның түйіндерін басқарылатын құрылғылар тізіміне автоматты түрде қайтарады.

Кластерлердің немесе серверлердің массивтерінің сипаттары

Серверлер кластерінің немесе массивінің параметрлерін көру үшін:

1. Бағдарламаның негізгі терезесінде **Активтерді басқару** → **Активтер (құрылғылар)** → **Кластерлер және серверлердің массивтері** бөліміне өтіңіз.

   Сервер кластерлері мен массивтерінің тізімі көрсетіледі.

2. Сервердің қажетті кластерінің немесе массивінің атын басыңыз.

Таңдалған сервер кластерінің немесе массивінің сипаттар терезесі ашылады.

Жалпы

Жалпы бөлімінде серверлердің кластері немесе массиві туралы жалпы ақпарат көрсетіледі. Ақпарат, кластер түйіндерін Басқару сервермен соңғы рет синхрондау барысында алынған деректер негізінде ұсынылады:

- **Атауы**
- **Сипаттама**
- **Windows домені**

  Сервердің кластерін немесе массивін қамтитын Windows домені немесе жұмыс тобы.

- **NetBIOS атауы**

  Windows желісіндегі серверлер кластерінің немесе массивінің атауы.

- **DNS атауы**

  Сервер кластерінің немесе массивінің DNS домен атауы.

Тапсырмалар

Тапсырмалар қойындысында сервер кластерлеріне және массивтеріне тағайындалған тапсырмаларды басқаруға болады: бар тапсырмалар тізімін қарау, жаңаларын жасау, жою, тапсырмаларды бастау және тоқтату, тапсырма параметрлерін өзгерту және орындау нәтижелерін қарау. Берілген тапсырмалар кластер түйіндеріне орнатылған Kaspersky қауіпсіздік қолданбасына қатысты. Kaspersky Security Center Linux кластер түйіндерінен тапсырмалар тізімін және тапсырма күйі туралы ақпаратты алады. Байланыс болмаған жағдайда, күй көрсетілмейді.

Түйіндер

Бұл қойындыда серверлердің кластерінің немесе массивінің бөлігі болып табылатын түйіндер тізімі көрсетіледі. Құрылғы сипаттары терезесін көру үшін түйін атауын басуға болады.

Kaspersky қолданбасы

Сипаттар терезесінде кластер түйіндеріне орнатылған Kaspersky қауіпсіздік қолданбасына қатысты ақпарат пен параметрлері бар қосымша қойындылар да болуы мүмкін.

Тарату нүктелері мен қосылым шлюздерін конфигурациялау

Kaspersky Security Center Linux-тегі басқару топтарының құрылымы келесі функцияларды орындайды:

- Саясаттардың әрекет ету ауқымын белгілеу.

  Саясат профильдерінің көмегімен құрылғыларда параметрлердің сыртқы жиынтықтарын қолданудың баламалы тәсілі бар.

- Топтық тапсырмалардың әрекет ету ауқымын белгілеу.

  Басқару топтарының иерархиясына негізделмеген топтық тапсырмалардың әрекет ету ауқымын белгілеу тәсілдемесі бар: құрылғыларды таңдау және арнайы құрылғылар үшін тапсырмаларды қолдану.

- Құрылғыларға, виртуалды және қосалқы Басқару серверлеріне қатынасу құқықтарын белгілеу.

- Тарату нүктелерін тағайындау.

Басқару топтарының құрылымын құру кезінде тарату нүктелерін оңтайлы түрде тағайындау үшін ұйым желісінің топологиясын ескеру қажет. Тарату нүктелерінің оңтайлы таралуы арқасында ұйым желісіндегі желілік трафикті азайтуға мүмкіндік беріледі.

Ұйымның ұйымдық құрылымына және желілер топологиясына байланысты, басқару топтары құрылымының келесі типтік конфигурацияларын ажыратуға болады:

- Бір кеңсе
- Көптеген шағын оқшауланған кеңселер

Тарату нүктелері рөлін атқаратын құрылғылар рұқсатсыз қол жеткізудің кез келген түрінен, соның ішінде физикалық тұрғыдан қорғалуы тиіс.

Тарату нүктелері туралы

Желілік агенті орнатылған құрылғыларды тарату нүктесі ретінде пайдалануға болады. Бұл режимде Желілік агент Басқару серверден де, Kaspersky серверлерінен де алуға болатын жаңартуларды тарата алады. Соңғы жағдайда тарату нүктесі үшін жаңартуларды жүктеп алуды орнатыңыз.

Тарату нүктелерін ұйымның желісіне орналастыру келесі мақсаттарды көздейді:

- Басқару серверіне түсетін жүктемені азайту.
- Трафикті оңтайландыру.

- Басқару серверіне ұйым желісінің жетуі қиын бөліктеріндегі құрылғыларға қатынасу мүмкіндік беру. NAT артында орналасқан тарату нүктесінің болуы (Басқару серверіне қатысты) Басқару серверіне келесі әрекеттерді орындауға мүмкіндік береді:
  - IPv4 немесе IPv6 желілеріндегі UDP арқылы құрылғыларға хабарландырулар жіберу
  - IPv4 немесе IPv6 желісінде сауалнама өткізу
  - Бастапқы орналастыруды орындау
  - push-сервер ретінде қолдану

Тарату нүктесі басқару тобына тағайындалады. Бұл жағдайда, тарату нүктесінің әрекет ету ауқымы осы басқару тобындағы және оның барлық ішкі топтарындағы құрылғылар болады. Бұл ретте, тарату нүктесі болып табылатын құрылғы ол тағайындалған басқару тобында болуға міндетті емес.

Сіз тарату нүктесін қосылым шлюзі етіп жасай аласыз. Бұл жағдайда, тарату нүктесінің әрекет ету ауқымындағы құрылғылар Басқару серверіне тікелей емес, шлюз арқылы қосылады. Бұл режим, Басқару сервері мен басқарылатын құрылғылар арасында тікелей қосылым мүмкін болмайтын сценарийлерде пайдалы.

Linux басқаруымен жұмыс істейтін құрылғыны тарату нүктесі ретінде пайдалансаңыз, klnagent қызметі үшін файл дескрипторының шектеулерін ұлғайту ұсынылады, себебі тарату нүктесінің әрекет ету ауқымы көптеген құрылғыларды қамтыса, әдепкі бойынша ашылуы мүмкін файлдардың ең көп саны жетпей қалуы ықтимал.

Тарату нүктелерінің типтік конфигурациясы: бір кеңсе

"Бір кеңсе" типтік конфигурациясында барлық құрылғылар ұйымның желісінде орналаса отырып, бір-бірін "көреді". Ұйымның желісі тар арналармен байланысқан бірнеше бөлектенген бөліктен (желіден немесе желі сегменттерінен) құралуы мүмкін.

Басқару топтарының құрылымын құрудың келесі тәсілдері болуы мүмкін:

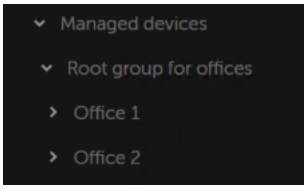
- Желі топологиясын ескере отырып, басқару тобының құрылымын құру. Басқару топтарының құрылымы желінің топологиясын нақты түрде көрсетуге міндетті емес. Желінің бөлектенген бөліктеріне қандай да бір басқару топтарының сай келуі жеткілікті. Тарату нүктелерін автоматты түрде тағайындауды қолдануға немесе тарату нүктелерін қолмен тағайындауға болады.

- Желінің топологиясын білдірмейтін басқару топтарының құрылымын құру. Бұл жағдайда, тарату нүктелерін автоматты түрде тағайындауды өшіру және желінің әрбір бөлектенген бөлігінде түбірлік басқару тобына, мысалы, **Басқарылатын құрылғылар** тобына бір немесе бірнеше құрылғыны тарату нүктелері ретінде тағайындау керек. Барлық тарату нүктелері бір деңгейде болады және бірдей "ұйым желісінің барлық құрылғылары" әрекет ету ауқымына ие болады. Желілік агенттердің әрқайсысы, бағыты ең қысқа болып саналатын тарату нүктесіне қосылатын болады. Тарату нүктесіне апаратын бағытты tracert утилитасының көмегімен анықтауға болады.

Тарату нүктелерінің типтік конфигурациясы: қашықтағы көптеген шағын кеңселер

Бұл типтік конфигурация, бәлкім, басты кеңсемен интернет арқылы байланысқан көптеген шағын қашықтағы кеңселерге сәйкес келеді. Қашықтағы кеңселердің әрқайсысы NAT артында орналасқан, яғни бір қашықтағы кеңседен екіншісіне қосылу мүмкін емес – кеңселер бір-бірінен оқшауланған.

Конфигурация басқару топтарының құрылымында міндетті түрде көрсетілуі керек: қашықтағы кеңселердің әрқайсысы үшін жеке басқару тобын құру керек (төмендегі суреттегі **1-кеңсе**, **2-кеңсе** топтары).



Қашықтағы кеңселер басқару топтарының құрылымында көрсетілген

Кеңсеге сай келетін әрбір басқару тобына бір немесе бірнеше тарату нүктесін тағайындау керек. Дискіде жеткілікті орны бар қашықтағы кеңсе құрылғыларын тарату нүктелері ретінде тағайындау керек. Мысалы, **1-кеңсе** тобында орналастырылған құрылғылар **1-кеңсе** басқару тобына тағайындалған тарату нүктелеріне жүгінетін болады.

Егер кейбір пайдаланушылар ноутбуктері бар кеңселер арасында физикалық түрде жылжытылатын болса, әр қашықтағы кеңседе жоғарыда аталған тарату нүктелеріне тағы екі және немесе одан да көп құрылғыны таңдап, оларды жоғарғы деңгейдегі басқару тобына тарату нүктелері ретінде тағайындау керек (жоғарыдағы суреттегі **Кеңселерге арналған түбірлік топ** тобы).

1-кеңсе басқару тобында болған, бірақ физикалық түрде **2-кеңсе** тобына сәйкес келетін кеңсеге көшірілген ноутбук. Жылжытқаннан кейін, ноутбуктағы Желілік агент **1-кеңсе** тобына тағайындалған тарату нүктелеріне жүгінуге тырысатын болады, бірақ бұл тарату нүктелері қолжетімді болмайды. Сонда Желілік агент **Кеңселерге арналған түбірлік топ** тобына тағайындалған тарату нүктелеріне жүгіне бастайды. Қашықтағы кеңселер бір-бірінен алшақ орналасқандықтан, **Кеңселерге арналған түбірлік топ** басқару тобына тағайындалған барлық тарату нүктелерінен **2-кеңсе** тобына тағайындалған тарату нүктелеріне жүгіну ғана сәтті болады. Яғни, ноутбук өзінің бастапқы кеңсесіне сәйкес келетін басқару тобында бола отырып, қазіргі уақытта физикалық түрде орналасқан кеңсенің тарату нүктесін қолдана беретін болады.

Тарату нүктелерінің саны мен конфигурациясын есептеу

Желіде клиент құрылғылары неғұрлым көп болса, тарату нүктелері да соғұрлым көп қажет болады. Тарату нүктелерін автоматты түрде тағайындауды өшірмеу ұсынылады. Тарату нүктелерін автоматты түрде тағайындау қосылған кезде, егер клиент құрылғыларының саны айтарлықтай көп болса, Басқару сервері тарату нүктелерін тағайындайды және олардың конфигурациясын анықтайды.

Арнайы бөлінген тарату нүктелерін пайдалану

Егер сіз тарату нүктелері ретінде белгілі бір құрылғыларды (мысалы, бұл үшін бөлінген серверлер) пайдалануды жоспарласаңыз, онда тарату нүктелерін автоматты түрде тағайындауды пайдаланбауға болады. Бұл жағдайда, тарату нүктелері ретінде тағайындағыңыз келетін құрылғыларда дискіде жеткілікті бос орын бар екеніне, олар үнемі өшірілмейтініне және "ұйқы режимі" өшірілгеніне көз жеткізіңіз.

Желілік құрылғылардың санына байланысты бір сегменті бар желідегі бірегей тағайындалған тарату нүктелерінің саны

Желі сегменттерінің әрқайсысындағы клиент құрылғыларының саны	Тарату нүктелерінің саны
300-нан кем	0 (тарату нүктелері керек емес)
300-нан артық	Қолайлы: (N/10 000 + 1), ұсынылады: (N/5000 + 2), мұндағы N желідегі құрылғылар саны

Желілік құрылғылардың санына байланысты бірнеше сегменті бар желідегі бірегей тағайындалған тарату нүктелерінің саны

Желі сегментіндегі клиент құрылғыларының саны	Тарату нүктелерінің саны
10-нан кем	0 (тарату нүктелері керек емес)
10–100	1
100-нан артық	Қолайлы: (N/10 000 + 1), ұсынылады: (N/5000 + 2), мұндағы N желідегі құрылғылар саны

Клиент құрылғыларын (жұмыс станцияларын) тарату нүктелері ретінде пайдалану

Егер сіз әдеттегі клиент құрылғысын (жұмыс станциясын) тарату нүктесі ретінде пайдалануды жоспарласаңыз, байланыс арналары мен Басқару серверіне шамадан тыс жүктемені болдырмау үшін төмендегі кестеде көрсетілгендей тарату нүктесін тағайындау ұсынылады:

Желілік құрылғылардың санына байланысты желінің бір сегментін қамтитын желідегі тарату нүктелерінің рөлін атқаратын жұмыс станцияларының саны

Желі сегменттерінің әрқайсысындағы клиент құрылғыларының саны	Тарату нүктелерінің саны
300-нан кем	0 (тарату нүктелері керек емес)
300-нан артық	(N/300 +1), мұндағы N – желідегі құрылғылардың саны; кемінде 3 тарату нүктесі

Желілік құрылғылардың санына байланысты желінің бірнеше сегментін қамтитын желідегі тарату нүктелерінің рөлін атқаратын жұмыс станцияларының саны

Желі сегментіндегі клиент құрылғыларының саны	Тарату нүктелерінің саны
10-нан кем	0 (тарату нүктелері керек емес)
10–30	1
31–300	2
300-нан артық	(N/300 +1), мұндағы N – желідегі құрылғылардың саны; кемінде 3 тарату нүктесі

Егер тарату нүктесі өшірілген болса немесе басқа себептерге байланысты қолжетімді болмаса, онда басқарылатын құрылғылар жаңартулар алу үшін осы тарату нүктесінің әрекет ету ауқымынан Басқару серверіне жүгіне алады.

Тарату нүктелерін автоматты түрде тағайындау

Тарату нүктелерін автоматты түрде тағайындау ұсынылады. Бұл жағдайда, Kaspersky Security Center Linux бағдарламасы тарату нүктелеріне қандай құрылғыларды тағайындау керектігін өзі таңдайды.

Microsoft Windows жүйесінде Arm жүйесінде жұмыс істейтін құрылғылар тарату нүктелері ретінде қызмет ете алмайды.

Тарату нүктелерін автоматты түрде тағайындау үшін:

1. Негізгі мәзірдегі басқару серверінің атауын басыңыз.

   Басқару серверінің сипаттары терезесі ашылады.

2. **Жалпы** қойыншасында **Тарату нүктелері** бөлімін таңдаңыз.

3. **Тарату нүктелерін автоматты түрде тағайындау** параметрін таңдаңыз.

   Егер тарату нүктелерінің құрылғыларын автоматты түрде тағайындау қосулы болса, тарату нүктелерінің параметрлерін қолмен конфигурациялау, сондай-ақ тарату нүктелерінің тізімін өзгерту мүмкін емес.

4. **Сақтау** түймесін басыңыз.

Нәтижесінде, Басқару сервері тарату нүктелерін автоматты түрде тағайындайды және олардың параметрлерін конфигурациялайды.

Тарату нүктелерін қолмен тағайындау

Kaspersky Security Center Linux құрылғыларды тарату нүктелеріне қолмен тағайындауға мүмкіндік береді.

Тарату нүктелерін автоматты түрде тағайындау ұсынылады. Бұл жағдайда, Kaspersky Security Center Linux бағдарламасы тарату нүктелеріне қандай құрылғыларды тағайындау керектігін өзі таңдайды. Алайда, егер сіз қандай да бір себептермен тарату нүктелерін автоматты түрде тағайындаудан бас тартқыңыз келсе (мысалы, арнайы бөлінген серверлерді пайдаланғыңыз келсе), Тарату нүктелерінің саны мен конфигурациясын алдын ала есептеу арқылы оларды қолмен тағайындауға болады.

Тарату нүктелері рөлін атқаратын құрылғылар рұқсатсыз қол жеткізудің кез келген түрінен, соның ішінде физикалық тұрғыдан қорғалуы тиіс.

Microsoft Windows жүйесінде Arm жүйесінде жұмыс істейтін құрылғылар тарату нүктелері ретінде қызмет ете алмайды.

Құрылғыны қолмен тарату нүктесі етіп тағайындау үшін:

1. Негізгі мәзірдегі басқару серверінің атауын басыңыз.

   Басқару серверінің сипаттары терезесі ашылады.

2. **Жалпы** қойыншасында **Тарату нүктелері** бөлімін таңдаңыз.

3. **Тарату нүктелерін қолмен тағайындау** параметрін таңдаңыз.

4. **Белгілеу** түймесін басыңыз.

5. Тарату нүктесі етіп жасағыңыз келетін құрылғыны таңдаңыз.

   Құрылғыны таңдау кезінде тарату нүктелерінің жұмысының ерекшеліктерін және тарату нүктесінің рөлін атқаратын құрылғыға қойылатын талаптарды ескеріңіз.

6. Таңдалған тарату нүктесінің әрекет ету ауқымына қосқыңыз келетін басқару тобын таңдаңыз.

7. **ОК** түймесін басыңыз.

   Қосылған тарату нүктесі **Тарату нүктелері** бөліміндегі тарату нүктелерінің тізімінде пайда болады

8. Оның сипаттары терезесін ашу үшін тізімдегі қосылған тарату нүктесін басыңыз.

9. Сипаттар терезесінде тарату нүктесінің параметрлерін конфигурациялаңыз:

   - **Жалпы** бөлімінде тарату нүктесінің клиент құрылғыларымен өзара әрекеттесу параметрлерін көрсетіңіз.

     - **SSL порты**

       SSL протоколын қолдана отырып, клиент құрылғыларының тарату нүктесіне қауіпсіз қосылу жүзеге асырылатын SSL портының нөмірі.

       Әдепкі бойынша порт нөмірі – 13000.

     - **Қосулы**

       Егер параметр қосулы болса, орнату пакеттерін топ шегіндегі клиент құрылғыларына автоматты түрде тарату үшін көп мекенжайлы IP таратылымы қолданылады.

       Көп мекенжайлы IP таратылымы бағдарламаларды орнату пакетінен клиент құрылғылары тобына орнатуға кететін уақытты азайтады, бірақ бағдарламаны бір клиент құрылғысына орнатқан кезде орнату уақытын арттырады.

     - **IP таратудың мекенжайы**

       Көп мекенжайлы таратылым орындалатын IP мекенжайы. IP мекенжайын 224.0.0.0 – 239.255.255.255 ауқымында белгілеуге болады

       Әдепкі бойынша Kaspersky Security Center Linux бағдарламасы белгіленген диапазонда бірегей көп мекенжайлы IP таратылымының мекенжайын тағайындайды.

     - **IP тарату портының нөмірі**

       Көп мекенжайлы таратылым портының нөмірі.

       Әдепкі бойынша порт нөмірі – 15001. Басқару сервері орнатылған құрылғы тарату нүктесі ретінде көрсетілсе, онда SSL протоколы арқылы қосылу үшін әдепкі бойынша 13001-порт қолданылады.

- **Қашықтағы құрылғылар үшін тарату нүктесінің мекенжайы**

  Қашықтағы құрылғылар тарату нүктесіне қосылатын желілік мекенжайы.

- **Қосулы**

  Жаңартулар келесі көздерден басқарылатын құрылғыларға қолданылады:

  - Бұл параметр қосулы болса, бұл тарату нүктесі болады.
  - Егер параметр өшірулі болса, басқа тарату нүктелері, Басқару сервері немесе Kaspersky жаңартулар серверлері.

  Егер сіз жаңартуларды тарату үшін тарату нүктелерін қолдансаңыз, трафикті үнемдей аласыз, себебі жүктеме санын азайтасыз. Сондай-ақ, Басқару серверіндегі жүктемені азайтуға және жүктемені тарату нүктелері арасында қайта бөлуге болады. Трафик пен жүктемені оңтайландыру үшін желідегі тарату нүктелерінің санын есептеп шығаруға болады.

  Егер сіз бұл параметрді өшірсеңіз, жаңарту жүктемелері мен Басқару серверіне түсетін жүктеме артуы мүмкін. Әдепкі бойынша, параметр қосулы.

- **Қосулы**

  Орнату пакеттері келесі көздерден басқарылатын құрылғыларға қолданылады:

  - Бұл параметр қосулы болса, бұл тарату нүктесі болады.
  - Егер параметр өшірулі болса, басқа тарату нүктелері, Басқару сервері немесе Kaspersky жаңартулар серверлері.

  Егер сіз орнату пакеттерін тарату үшін тарату нүктелерін қолдансаңыз, трафикті үнемдей аласыз, себебі жүктеме санын азайтасыз. Сондай-ақ, Басқару серверіндегі жүктемені азайтуға және жүктемені тарату нүктелері арасында қайта бөлуге болады. Трафик пен жүктемені оңтайландыру үшін желідегі тарату нүктелерінің санын есептеп шығаруға болады.

  Егер сіз бұл параметрді өшірсеңіз, орнату пакеттері жүктемелері мен Басқару серверіне түсетін жүктеме артуы мүмкін. Әдепкі бойынша, параметр қосулы.

- **Қосулы**

  Kaspersky Security Center Linux бағдарламасында тарату нүктесі мобильді протокол арқылы басқарылатын құрылғылар үшін және Желілік агент басқаратын құрылғылар үшін push сервері ретінде жұмыс істей алады. Мысалы, егер сіз KasperskyOS орнатылған құрылғыларды Басқару серверімен мәжбүрлеп синхрондауды қосқыңыз келсе, push сервері қосулы болуы керек. Push серверінде, push сервері қосылған тарату нүктесімен бірдей басқарылатын құрылғылар аймағы бар. Егер сізде бір басқару тобына тағайындалған бірнеше тарату нүктелері болса, олардың әрқайсысында ескерту серверін қосуға болады. Бұл жағдайда, Басқару сервері жүктемені тарату нүктелері арасында бөледі.

- **Push-серверінің порты**

  Push серверінің порт нөмірі. Сіз кез келген бос порттың нөмірін көрсете аласыз.

- **Әрекеттер аумағы** бөлімінде тарату нүктесі жаңартуларды тарататын басқару топтарын көрсетіңіз.

- **Жаңартулар көзі** бөлімінде тарату нүктесі үшін жаңарту көзін таңдауға болады:

  - **Жаңартулар көзі**

    Тарату нүктесі үшін жаңартулар көзін таңдаңыз:

    - Тарату нүктесі Басқару серверінен жаңартулар алып тұруы үшін, **Басқару серверінен шығарып алу** нұсқасын таңдаңыз.

    - Тарату нүктесіне тапсырма арқылы жаңартуларды алуға рұқсат беру үшін, **Жаңартуды жүктеп алу тапсырмасын пайдалану** тармағын таңдаңыз және *Жаңартуларды тарату нүктелерінің қоймаларына жүктеу* тапсырмасын көрсетіңіз:

      - Егер мұндай тапсырма құрылғы үшін бұрыннан бар болса, тізімнен тапсырманы таңдаңыз.

      - Егер құрылғы үшін мұндай тапсырма әлі болмаса, тапсырманы жасау үшін **Тапсырма жасау** сілтемесінен өтіңіз. Жаңа тапсырма жасау шебері іске қосылады. Содан кейін, шебердің нұсқауларын орындаңыз.

  - **diff файлдарды жүктеп алу**

    Бұл параметр айырмашылық файлдарын жүктеп алу функциясын қосады.

    Әдепкі бойынша, параметр қосулы.

- Егер тарату нүктелері интернетке қосылған кезде прокси-серверді пайдаланса, **Интернетке қосылу параметрлері** ішкі бөлімінде келесі параметрлерді көрсетуге болады:

  - **Прокси-серверді пайдалану**

    Егер бұл құсбелгі таңдалса, тарату нүктелерін Kaspersky жаңарту серверлеріне қосу үшін Интернет прокси-сервері пайдаланылады. Енгізу өрістерінде прокси-серверге қосылу параметрлерін баптауға болады.

    Әдепкі бойынша, жалауша алынып тасталған.

  - **Прокси серверінің мекенжайы**

    Прокси серверінің мекенжайы.

  - **Порт нөмірі**

    Қосылым орындалатын порт нөмірі.

  - **Жергілікті мекенжайларға арналған прокси-серверді айналып өту**

    Егер параметр қосулы болса, жергілікті желідегі құрылғыларға қосылған кезде прокси сервері пайдаланылмайды.

    Әдепкі бойынша, параметр өшірулі.

  - **Прокси-сервердегі аутентификация**

    Жалауша қойылған болса, енгізу өрістерінде прокси-сервердегі түпнұсқалық растама үшін есептік деректерді көрсетуге болады.

    Әдепкі бойынша, жалауша алынып тасталған.

  - **Пайдаланушы аты**

    Прокси-серверге қосылу орындалатын реттелетін есептік жазбасы.

- **Құпиясөз**

  Тапсырманы іске қосатын есептік жазбаның құпиясөзі.

- **KSN проксиі** бөлімінде бағдарламаны тарату нүктесі басқарылатын құрылғылардан KSN сұрауларын жіберу үшін пайдаланылатындай етіп орнатуға болады.

  - **Тарату нүктесі тарапынан KSN проксиін қосу**

    KSN прокси-сервері қызметі тарату нүктесі ретінде әрекет ететін құрылғыда орындалады. Бұл параметрді желі трафигін қайта тарату және оңтайландыру үшін пайдаланыңыз.

    Тарату нүктесі Kaspersky Security Network мәлімдемесінде көрсетілген KSN статистикасын Kaspersky ұйымына жібереді.

    Әдепкі бойынша, параметр өшірулі. Осы параметрді қосу, **Басқару серверін прокси-сервер ретінде пайдалану** және **Kaspersky Security Network бағдарламасын пайдалану шарттарын қабылдаймын** параметрлері Басқару серверінің сипаттары терезесінде қосылған жағдайда ғана күшіне енеді.

    Суық резерві бар істен шығуға төзімді кластер түйініне (белсенді / пассивті) тарату нүктесін тағайындауға және сол түйінде KSN прокси-серверін қосуға болады.

  - **KSN сұрауын Басқару серверіне қайта жіберу**

    Тарату нүктесі басқарылатын құрылғылардан KSN сұрауларын Басқару серверіне жібереді.

    Әдепкі бойынша, параметр қосулы.

  - **KSN бұлтына/KPSN бағдарламасына интернет арқылы тікелей кіру**

    Тарату нүктесі KSN-ге басқарылатын құрылғылардан KSN немесе KPSN бұлттық қызметіне сұраулар жібереді. Тарату нүктесінде жасалған KSN сұраулары да тікелей KSN Cloud немесе KPSN-ге жіберіледі.

  - **KPSN желісіне қосылған кезде прокси-сервер параметрлерін елемеу**

    Егер прокси-сервер параметрлері тарату нүктелерінің немесе Желілік агенттің сипаттарында конфигурацияланған болса, бірақ сіздің желіңіздің архитектурасы KPSN бағдарламасын тікелей пайдалануды талап етсе, осы жалаушаны қойыңыз. Әйтпесе, басқарылатын қолданбадан сұрау KPSN қолданбасына берілмейді.

    Бұл параметр **KSN бұлтына/KPSN бағдарламасына интернет арқылы тікелей кіру** параметрін таңдаған жағдайда қолжетімді болады.

  - **Порт**

    Басқарылатын құрылғылар KSN прокси-серверіне қосылу үшін қолдана алатын TCP портының нөмірі. Әдепкі бойынша 13111-порт орнатылған.

  - **UDP портын қолдану**

    Басқарылатын құрылғылардың KSN прокси серверіне UDP порты арқылы қосылуы үшін **UDP портын пайдалану** жалаушасын қойып, UDP порты нөмірін көрсетіңіз. Әдепкі бойынша, параметр қосулы.

  - **UDP порты**

    Басқарылатын құрылғылар KSN прокси-серверіне қосылу үшін қолдана алатын UDP портының нөмірі. Әдепкі бойынша, KSN прокси-серверіне қосылу 15111 UDP порты арқылы жүзеге асырылады.

- **HTTPS пайдалану**

  Басқарылатын құрылғылардың KSN прокси-серверіне HTTPS порты арқылы қосылуын қаласаңыз, **HTTPS пайдалану** параметрін қосыңыз және **HTTPS порты арқылы** өрісінде порт нөмірін көрсетіңіз. Әдепкі бойынша, KSN прокси-серверіне қосылу 17111 HTTPS порты арқылы жүзеге асырылады.

- **HTTPS порты**

  Басқарылатын құрылғылар KSN прокси-серверіне қосылу үшін қолдана алатын HTTPS портының нөмірі. Әдепкі бойынша, KSN прокси-серверіне қосылу 17111 HTTPS порты арқылы жүзеге асырылады.

- **Қосылым шлюзі** бөлімінде тарату нүктесін Желілік агент және Басқару сервері үлгілері үшін қосылым шлюзі ретінде конфигурациялауға болады:

  - **Қосылым шлюзі**

    Басқару сервері мен Желілік агенттер арасында тікелей байланыс желіңізді ұйымдастыруға байланысты орнатылмаса, тарату нүктесін Басқару сервері мен Желілік агенттер арасындағы қосылым шлюзі ретінде пайдалануға болады.

    Тарату нүктесінің Желілік агенттері мен Басқару сервері арасындағы қосылым шлюзі ретінде әрекет етуін қаласаңыз, бұл параметрді қосыңыз. Әдепкі бойынша, параметр өшірулі.

  - **Басқару серверінің тарабынан шлюзбен байланысты орнату (шлюз DMZ режимінде болса)**

    Басқару сервері демилитаризацияланған аймақтан (DMZ) тыс жерде болса, жергілікті желіде қашықтағы құрылғыларда орнатылған Желілік агенттер Басқару серверіне қосыла алмайды. Тарату нүктесін кері қосылымы бар қосылым шлюзі ретінде пайдалануға болады (Басқару сервері тарату нүктесімен байланысты орнатады).

    Басқару серверін демилитаризацияланған аймақтағы қосылым шлюзіне қосқыңыз келсе, осы параметрді қосыңыз.

  - **Kaspersky Security Center Web Console үшін жергілікті портты ашу**

    Демилитаризацияланған аймақта немесе интернетте орналасқан Web Console портын ашу үшін демилитаризацияланған аймақта қосылым шлюзі қажет болса, бұл параметрді қосыңыз. Web Console веб-консолін тарату нүктесіне қосу үшін пайдаланылатын порт нөмірін көрсетіңіз. Әдепкі бойынша 13299-порт орнатылған.

    Бұл параметр **Басқару серверінің тарабынан шлюзбен байланысты орнату (шлюз DMZ режимінде болса)** қолжетімді болады.

  Мобильді құрылғыларды Басқару серверіне қосылым шлюзі ретінде әрекет ететін тарату нүктесі арқылы қосқанда, келесі параметрлерді қосуға болады:

  - **Мобильді құрылғылар үшін портты ашу (тек Басқару серверінің SSL аутентификациясы)**

    Қосылым шлюзінің ұялы құрылғылар үшін портты ашуын қаласаңыз және ұялы құрылғылар тарату нүктесіне қосылу үшін пайдаланатын порт нөмірін көрсетсеңіз, бұл параметрді қосыңыз. Әдепкі бойынша 13292-порт орнатылған. Мобильді құрылғы Басқару сервері сертификатын тексереді. Байланыс орнатылған кезде, тек Басқару сервері түпнұсқалық растамасын орындайды.

- **Мобильді құрылғылар үшін портты ашу (екі жақты SSL аутентификация)**

  Қосылым шлюзінің Басқару сервері мен ұялы құрылғылардың екі жақты түпнұсқалық растамасы үшін пайдаланылатын портты ашуын қаласаңыз, осы параметрді қосыңыз. Мобильді құрылғы Басқару сервері сертификатын, ал Басқару сервері мобильді құрылғы сертификатын тексереді. Келесі параметрлерді белгілеңіз:

  - Ұялы құрылғылар тарату нүктесіне қосылу үшін пайдаланатын порт нөмірі. Әдепкі бойынша 13293-порт орнатылған.

  - Ұялы құрылғылар пайдаланатын қосылым шлюзі DNS домені атаулары. Домен атауларын үтірмен бөліңіз. Көрсетілген домен атаулары тарату нүктесі сертификатына қосылады. Ұялы құрылғылар пайдаланатын домен атаулары тарату нүктесі сертификатындағы жалпы атауға сәйкес келмесе, ұялы құрылғылар тарату нүктесіне қосылмайды.

    Әдепкі DNS домен атауы қосылым шлюзінің толық жарамды домен атауы болып табылады.

  Екі жағдайда да сертификаттар тек тарату нүктесінде TLS сеансын орнату кезінде тексеріледі. Сертификаттарды Басқару сервері тексеруге жібермейді. Мобильді құрылғымен TLS сеансын орнатқаннан кейін тарату нүктесі мобильді құрылғы мен Басқару сервері арасында синхрондау туннелін жасау үшін Басқару сервері сертификатын пайдаланады. Екі жақты SSL аутентификациясы үшін портты ашсаңыз, мобильді құрылғы сертификатын таратудың жалғыз жолы орнату бумасы арқылы жүзеге асады.

- Windows негізіндегі тарату нүктесі арқылы Windows желісінің сұрауын конфигурациялаңыз.

  - **Windows домендері**

    Сіз Windows домендеріне арналған құрылғыларды анықтауды қосып, оның кестесін белгілей аласыз.

- Тарату нүктесі көмегімен домен контроллері сауалнамасын орнатыңыз.

  - **Домен контроллерінің сауалнамасы**

    Домен контроллері үшін құрылғыларды табу мүмкіндігін қосуға болады.

    Сауалнама өрісінде ауыстырып-қосқыш түймесін **Қосулы** күйіне ауыстырғаннан кейін, сауалнамаға арналған домен контроллерлерін таңдауға және олар үшін сауалнама кестесін көрсетуге де болады.

    Linux операциялық жүйесі бар тарату нүктесін пайдалансаңыз, **Көрсетілген домендер сауалнамасын жүргізу** бөлімінде **Қосу** түймесін басып, домен контроллерінің мекенжайы мен пайдаланушының есептік жазба деректерін көрсетіңіз. Сауалнама жүргізілетін домен түрін көрсетуге де болады: Active Directory немесе Samba, FreeIPA, ALD Pro.

    Windows операциялық жүйесі бар тарату нүктесін пайдалансаңыз, келесі нұсқалардың бірін таңдауға болады:

    - **Ағымдағы домен сауалнамасын жүргізу**

    - **Бүкіл домендер тобының сауалнамасын жүргізу**

    - **Көрсетілген домендер сауалнамасын жүргізу**

- IP ауқымдарын сауалнамасын тарату нүктесі ретінде конфигурациялаңыз.

  - **IP ауқымдарының сауалнамасы.**

    IPv4 ауқымдары мен IPv6 желілері үшін құрылғыларды табу функциясын қосуға болады.

Ауқым сауалнамасын қосу параметрін қоссаңыз, сауалнама ауқымын қосып, сауалнама кестесін белгілеуге болады. IP ауқымдарын сауалнама ауқымдары тізіміне қоса аласыз.

IPv6 желілеріне сауалнама жүргізу үшін Zeroconf пайдалану параметрін қоссаңыз, тарату нүктесі нөлдік конфигурациясы бар желіні қолдана отырып, IPv6 желісіне сауалнама өткізеді (бұдан әрі *Zeroconf* деп те аталады). Бұл жағдайда, көрсетілген IP ауқымдары еленбейді, өйткені тарату нүктесі бүкіл желіге сауалнама өткізеді. **IPv6 желілеріне сауалнама жүргізу үшін Zeroconf пайдалану** параметрі, тарату нүктесі Linux басқаруымен жұмыс істеп тұрса қолжетімді. Zeroconf IPv6 сауалнамасын пайдалану үшін тарату нүктесінде avahi-browse утилитасын орнату қажет.

- **Кеңейтілген** бөлімінде тарату нүктесі таратылатын деректерді сақтау үшін пайдалануы керек қалтаны көрсетіңіз.

  - **Әдепкі бойынша қалтаны қолдану**

    Деректерді сақтау үшін осы нұсқаны таңдағанда, тарату нүктесінде Желілік агент орнатылған қалта қолданылады.

  - **Көрсетілген қалтаны пайдалану**

    Бұл нұсқаны таңдағанда, төмендегі өрісте қалта жолын көрсетуге болады. Қалта тарату нүктесінде де, қашықтан да, ұйым желісінің құрамына кіретін кез келген құрылғыда орналастырылуы мүмкін.

    Тарату нүктесінде Желілік агент іске қосылатын есептік жазба оқу және жазу үшін көрсетілген қалтаға қатынасу мүмкіндігіне ие болуы керек.

10. **OK** түймесін басыңыз.

Нәтижесінде, таңдалған құрылғылар тарату нүктелерінің рөлін атқарады.

Қосылым шлюзін тарату нүктесі ретінде демилитаризацияланған аймаққа қосу

Басқару сервері демилитаризацияланған аймақтан (DMZ) тыс болса, сыртқы құрылғыларда орнатылған Желілік агенттер онымен байланысу мүмкіндігін жоғалтады. Бұл жағдайда, сіз тарату нүктесін DMZ аймағындағы қосылым шлюзі ретінде пайдалана аласыз. Тарату нүктесі Басқару серверіне қосылымды жасау үшін порт ашады. Іске қосу кезінде Басқару сервері тарату нүктесіне қосылады және бүкіл жұмыс уақытында онымен байланысты үзбейді.

Егер сізге Басқару сервері мен басқарылатын құрылғыларыңыз арасында Желілік агент пен Басқару сервері арасындағы синхрондау кезеңінен тыс қосылым орнату қажет болса, push серверін қосып, тарату нүктесі жағында 13295 портын ашуыңыз керек.

Қосылым шлюзі ретінде арнайы тағайындалған құрылғыны пайдалануды ұсынамыз. Клиент құрылғыларының (ұялы құрылғыларды қоса алғанда) ең көп саны туралы ақпарат алу үшін өлшеу нұсқаулығын қараңыз.

Қосылым шлюзі Басқару серверімен байланыс орнатпайды, тек Басқару серверінен қосылымдарды күтеді. Бұл дегеніміз, демилитаризацияланған аймақта құрылғыға қосылым шлюзін орнатқаннан кейін, Басқару сервері басқарылатын құрылғылардың арасында құрылғыны тізімдемейді. Сол себепті, Басқару сервері қосылым шлюзіне қосылуды бастау үшін сізге арнайы процедура қажет болады.

Тарату нүктесі ретінде қосылым шлюзі бар құрылғыны қосу үшін:

1. Негізгі мәзірдегі басқару серверінің атауын басыңыз.

   Басқару серверінің сипаттары терезесі ашылады.

2. **Жалпы** қойыншасында **Тарату нүктелері** бөлімін таңдаңыз.

3. **Тарату нүктелерін қолмен тағайындау** параметрін таңдаңыз.

4. Құралдар тақтасындағы **Белгілеу** түймесін басыңыз.

5. Ашылған оң жақ тақтада келесі әрекеттердің бірін орындаңыз:

   a. **DMZ қосылу шлюзін мекенжайы бойынша пайдалану** опциясын таңдаңыз.

   b. **Қосылым шлюзінің мекенжайы** өрісінде құрылғының IP мекенжайын немесе DNS атауын көрсетіңіз.

   c. **Белгілеу** түймесін басыңыз.

   d. Тақта жабық, ал тарату нүктесі **Қосылу шлюзіне арналған уақытша жазба** көрсетіледі.

6. **Сақтау** түймесін басыңыз.

Басқару сервері көрсетілген мекенжай бойынша қосылым шлюзіне қосылуға тырысады. Бәрі сәтті өтсе, жазу атауы қосылым шлюзі құрылғысының атауына өзгереді. Бұған бес минутқа дейін уақыт кетеді.

Егер сіз **Қосылу шлюзіне арналған уақытша жазба** атауын басу арқылы тарату нүктесінің қасиеттерін ашсаңыз, барлық опциялар сұр түске боялады. Сіз тек тарату нүктесінің атауын көрсететін Жалпы қойындысын көре аласыз. Әдепкі бойынша порт нөмірі – 13000. Сіз тарату нүктесін тек Басқару сервері оған қосылғаннан кейін конфигурациялай аласыз. Қосылым шлюзінің уақытша жазбасы аталған жазбаға айналғанда, қосылым шлюзі Тағайындалмаған құрылғылар тобында да пайда болады.

Бұрын конфигурацияланған желіге қосылым шлюзін қосу үшін:

1. Желілік агентті қосылым шлюзі режимінде орнатыңыз.

2. Жаңадан қосылған қосылым шлюзіне қосқыңыз келетін құрылғыларда Желілік агентті қайта орнатыңыз.

Басқару тобы үшін тарату нүктелерінің тізімін өзгерту

Сіз белгілі бір басқару тобына тағайындалған тарату нүктелерінің тізімін көре аласыз және тарату нүктелерін қосу немесе жою арқылы тізімді өзгерте аласыз.

Басқару тобы үшін тарату нүктелерінің тізімін қарау және өзгерту үшін:

1. Бағдарламаның негізгі терезесінде **Активтерді басқару** → **Активтер (құрылғылар)** бөліміне өтіңіз.

2. Беттің жоғарғы жағындағы **Иерархияны көрсету** түймесін басу арқылы тағайындалған тарату нүктелерін көргіңіз келетін басқару тобын таңдаңыз, содан кейін ашылатын терезеде қажетті топтың атауын басыңыз.

   Ол үшін **Тарату нүктелері** мәзір тармағын пайдаланыңыз.

   Таңдалған топ жолы беттің жоғарғы жағында көрсетіледі. Қажет болса, бұл жолда топқа өту үшін басқару тобының атауы бар сілтемені басуға болады. Әдепкісінше жолдағы соңғы сілтеме белсенді емес.

3. Бағдарламаның негізгі терезесінде **Активтерді басқару** → **Тарату нүктелері** бөліміне өтіңіз.

4. Басқару тобына тарату нүктелерін қосу үшін **Белгілеу** түймені басыңыз.

5. Тағайындалған тарату нүктелерін жою үшін тізімнен құрылғыларды таңдап, **Белгілеуден бас тарту** түймені басыңыз.

Өзгерістерге байланысты, тарату нүктелері тізімге қосылады немесе қолданыстағы тарату нүктелері тізімнен жойылады.

Push серверін қосу

Kaspersky Security Center Linux бағдарламасында тарату нүктесі мобильді протокол арқылы басқарылатын құрылғылар үшін және Желілік агент басқаратын құрылғылар үшін push сервері ретінде жұмыс істей алады. Мысалы, егер сіз KasperskyOS орнатылған құрылғыларды Басқару серверімен мәжбүрлеп синхрондауды қосқыңыз келсе, push сервері қосулы болуы керек. Push серверінде, push сервері қосылған тарату нүктесімен бірдей басқарылатын құрылғылар аймағы бар. Егер сізде бір басқару тобына тағайындалған бірнеше тарату нүктелері болса, олардың әрқайсысында ескерту серверін қосуға болады. Бұл жағдайда, Басқару сервері жүктемені тарату нүктелері арасында бөледі.

Басқарылатын құрылғы мен Басқару сервері арасындағы тұрақты байланысты қамтамасыз ету үшін тарату нүктелерін push серверлері ретінде пайдаланғыңыз келуі мүмкін. Тұрақты байланыс жергілікті тапсырмаларды іске қосу және тоқтату, басқарылатын бағдарламаның статистикасын алу немесе туннель жасау сияқты кейбір операциялар үшін қажет. Тарату нүктесін push серверінің сервері ретінде қолдансаңыз, сізге басқарылатын құрылғыларда **Басқару серверімен байланысты үзбеу** параметрін қолдану немесе Желілік агенттің UDP портына пакеттерді жіберу қажет емес.

Push сервері бір мезгілдегі 50 000 қосылымға дейінгі жүктемені қолдайды.

Тарату нүктесінде push серверін қосу үшін:

1. Негізгі мәзірдегі басқару серверінің атауын басыңыз.

   Басқару серверінің сипаттары терезесі ашылады.

2. **Жалпы** қойыншасында **Тарату нүктелері** бөлімін таңдаңыз.

3. Push серверін қосқыңыз келетін тарату нүктесінің атауын басыңыз.

   Тарату нүктесі сипаттары терезесі ашылады.

4. **Жалпы** бөлімінде **Қосулы** параметрін қосыңыз.

5. **Push-серверінің порты** өрісінде порт нөмірін көрсетіңіз. Сіз кез келген бос порттың нөмірін көрсете аласыз.

6. **Қашықтағы құрылғының мекенжайы** өрісінде тарату нүктесінің IP мекенжайын немесе атауын көрсетіңіз.

7. **OK** түймесін басыңыз.

Push сервері таңдалған тарату нүктесінде қосылған.

klnagent қызметі үшін файл дескрипторларының шектеуін арттыру

Егер Linux басқаруымен жұмыс істейтін тарату нүктесінің тарату аймағы көптеген құрылғыларды қамтыса, ашық файлдар санына (файл дескрипторлары) әдепкі түрде қойылатын шектеу жеткіліксіз болуы мүмкін. Бұған жол бермеу үшін klnagent қызметі үшін файл дескрипторының шектеуін арттыруға болады.

klnagent қызметі үшін файл дескрипторының шектеуін арттыру үшін

1. Тарату нүктесі ретінде әрекет ететін Linux негізіндегі құрылғыда келесі пәрменді орындаңыз:

   ```
   systemctl edit klnagent64.service
   ```

2. `[Service]` бөлімінің `LimitNOFILE` параметрінде файл дескрипторларының қатаң және жұмсақ шектерін көрсетіңіз:

   `LimitNOFILE=<жұмсақ ресурс шегі>:<қатты ресурс шегі>`

   Мысалы, `LimitNOFILE=32768:131072`. Файл дескрипторының жұмсақ шектеулері қатаң шектеуден аз немесе оған тең болуы керек екенін ескеріңіз.

3. Параметрлердің дұрыстығына көз жеткізу үшін келесі пәрменді іске қосыңыз:

   ```
   systemd-analyze verify klnagent64.service
   ```

   Параметрлер қате көрсетілген болса, бұл пәрмен келесі қателердің бірін тудыруы мүмкін:

   - `/lib/systemd/system/klnagent64.service:11: Failed to parse resource value, ignoring: 32768:13107`

     Егер бұл қате орын алса, демек, `LimitNOFILE` жолындағы таңбалар дұрыс көрсетілмеген. Енгізілген жолды тексеру және түзету қажет.

   - `/lib/systemd/system/klnagent64.service:11: Soft resource limit chosen higher than hard limit, ignoring: 32768:13107`

     Бұл қате орын алса, сіз енгізген файл дескрипторларын жұмсақ шектеу қатаң шектеуден асып кетеді. Енгізілген жолды тексеріп, файл дескрипторының жұмсақ шектеуі қатаң шектеуден аз немесе оған тең екеніне көз жеткізу керек.

4. systemd процесін қайта бастау үшін келесі пәрменді іске қосыңыз:

   ```
   systemctl daemon-reload
   ```

5. Желілік агент қызметін қайта іске қосу үшін келесі пәрменді орындаңыз:

   ```
   systemctl restart klnagent
   ```

6. Көрсетілген параметрлердің дұрыс қолданылғанына көз жеткізу үшін келесі пәрменді орындаңыз:

   `less /proc/<nagent процесінің идентификаторы>/limits`

   мұндағы `<nagent процесінің идентификаторы>` параметрі — желілік агент процесінің идентификаторы. Сәйкестендіргішті алу үшін келесі пәрменді орындауыңызға болады:

   ```
   ps -ax | grep klnagent
   ```

Linux операциялық жүйесімен жұмыс істейтін тарату нүктесі үшін ашылатын файлдар саны ұлғайтылды.

Құрылғы күйлері туралы

Kaspersky Security Center Linux бағдарламасы әрбір басқарылатын құрылғыға күй тағайындайды. Нақты күйі, пайдаланушы анықтаған шарттардың орындалғанына байланысты. Кейбір шарттар үшін Kaspersky Security Center Linux құрылғысына күй тағайындау кезінде құрылғының желіде көрінуін ескереді (төмендегі кестені қараңыз). Мысалы, басқарылатын құрылғыға *Критикалық* күйі берілген болса, *Дерекқорлар ескірген* шарты орындалғандықтан, құрылғы үшін көзге көрінетін болғандықтан, құрылғыға *ОК* күйі беріледі. Егер Kaspersky Security Center Linux құрылғыны екі сағат ішінде желіден таппаса, құрылғының көрінуі *Офлайн* мәніне ие болады.

Келесі күйлер бар:

- *Критикалық* немесе *Критикалық/Көзге көрінетін*.
- *Ескерту* немесе *Ескерту/Көзге көрінетін*.
- *ОК* немесе *ОК/Көзге көрінетін*.

Төмендегі кестеде құрылғыға *Критикалық* немесе *Ескерту* күйін және олардың мүмкін мәндерін тағайындау үшін әдепкі бойынша шарттар келтірілген.

Құрылғыға күйлер белгілеу шарттары

Шарт	Шарттың сипаттамасы	Қолжетімді мәндері
Қауіпсіздік бағдарламасы орнатылмаған	Желілік агент құрылғыға орнатылған, бірақ қауіпсіздік бағдарламасы орнатылмаған.	• Қосқыш қосулы. • Қосқыш өшірулі.
Тым көп вирус анықталды	Вирустарды іздеу тапсырмаларының, мысалы, Зиянды БҚ іздеу тапсырмаларының жұмысы нәтижесінде, құрылғыда вирустар табылды және анықталған вирустардың саны көрсетілген мәннен асып түседі.	0-ден артық.
Нақты уақыт режимінде қорғау деңгейі әкімші орнатқан деңгейден өзгеше	Құрылғы желіде көрінеді, бірақ құрылғы күйіне арналған шартта нақты уақыт режимінде қорғау деңгейі әкімші орнатқан деңгейден өзгеше.	• Тоқтатылды. • Кідіртілді. • Орындалуда.
Зиянды БҚ іздеуі ұзақ уақыт орындалмады	Құрылғы желіде көрінеді және құрылғыда қауіпсіздік бағдарламасы орнатылған, бірақ *Зиянды БҚ іздеу* тапсырмасы да, жергілікті тексеру тапсырмасы да көрсетілген уақыттан артық орындалмады. Шарт тек жеті күн бұрын немесе одан бұрын Басқару сервері дерекқорына қосылған құрылғыларға қолданылады.	1-күннен артық.
Дерекқорлар ескірген	Құрылғы желіде көрінеді және құрылғыда қауіпсіздік бағдарламасы орнатылған, бірақ антивирустық дерекқорлар бұл құрылғыда көрсетілген уақыттан артық жаңартылмаған. Шарт тек бір күн бұрын немесе одан бұрын Басқару сервері дерекқорына қосылған құрылғыларға қолданылады.	1-күннен артық.
Қосылмағанына көп болды	Желілік агент құрылғыға орнатылған, бірақ құрылғы Басқару серверіне көрсетілген уақыттан артық қосылмаған, себебі құрылғы өшірулі.	1-күннен артық.
Белсенді қауіптер анықталды	**Белсенді қауіптер** қалтасындағы өңделмеген нысандар саны көрсетілген мәннен асып түседі.	0 данадан артық.

Шарт	Шарттың сипаттамасы	Қолжетімді мәндері
Қайта бастаудан кейінгі қажетті уақыт	Құрылғы желіде көрінеді, бірақ қолданба көрсетілген уақыт аралығынан ұзағырақ уақыт бойы қайта іске қосуды талап етті.	0 минуттан көбірек.
Қайта бастау себебі	Құрылғы желіде көрінеді, бірақ қолданба таңдалған себептердің біріне байланысты құрылғыны қайта іске қосуды талап етеді.	• Белгісіз себеп • Бағдарлама қайта іске қосуға дейін жұмыс істемейді • Жаңартуды аяқтау үшін қайта іске қосу қажет; бағдарлама жұмыс істеуде • Жаңартуды қолдану үшін қайта іске қосу қажет • Сканерлеуді немесе залалсыздандыруды аяқтау үшін қайта жүктеу керек • Қашықтан орнатуды/жоюды аяқтау үшін қайта іске қосу қажет • Дискідегі деректерді шифрлауды аяқтау
Үйлесімсіз бағдарламалар орнатылды	Құрылғы желіде көрінеді, бірақ Желілік агент орындаған бағдарламалық жасақтаманы түгендеу кезінде, құрылғыда үйлесімсіз бағдарламалардың орнатылғаны анықталды.	• Қосқыш өшірулі. • Қосқыш қосулы.
Бағдарламалық жасақтама осалдықтары анықталды	Құрылғы желіде көрінеді және оған Желілік агент орнатылған, бірақ *Осалдықтарды және қажетті жаңартуларды іздеу* тапсырмасын орындау нәтижесінде құрылғыда критикалық деңгейі белгіленген бағдарламаларда осалдықтар анықталды.	• Критикалық. • Жоғары. • Орташа. • Осалдықты жабу мүмкін емес болса, елемеу. • Жаңарту орнатуға белгіленген болса, елемеу.
Лицензия мерзімі өтті	Құрылғы желіде көрінеді, бірақ лицензияның жарамдылық мерзімі өтіп кеткен.	• Қосқыш өшірулі. • Қосқыш қосулы.
Лицензияның қолданылу мерзімі жақында аяқталады	Құрылғы желіде көрінеді, бірақ лицензиялық жарамдылық мерзімі көрсетілген күндер санынан аз уақыттан кейін өтіп кетеді.	0 күннен көп.

Шарт	Шарттың сипаттамасы	Қолжетімді мәндері
Windows Update жаңартуларын іздеу ұзақ уақыт бойы орындалмады	Құрылғы желіде көрінеді, бірақ *Windows Update жаңартуларын синхрондау* тапсырмасы көрсетілген уақыт аралығында орындалмаған.	1-күннен артық.
Жарамсыз шифрлау күйі	Желілік агент құрылғыға орнатылған, бірақ құрылғыны шифрлау нәтижесі көрсетілген мәнге тең.	• Пайдаланушының бас тартуына байланысты саясатқа сәйкес келмейді (тек сыртқы құрылғылар үшін). • Қатеге байланысты саясатқа сай емес. • Саясат қолданылуда – қайта іске қосу қажет. • Шифрлау саясаты белгіленбеген. • Қолдау көрсетілмейді. • Саясат қолданылуда.
Мобильді құрылғы параметрлері саясатқа жауап бермейді	Ұялы құрылғының параметрлері сәйкестік ережелерін тексеру кезінде Kaspersky Endpoint Security for Android саясатында белгіленген параметрлерден ерекшеленеді.	• Қосқыш өшірулі. • Қосқыш қосулы.
Өңделмеген қауіпсіздік мәселелері табылды	Құрылғыда өңделмеген қауіпсіздік мәселелері бар. Қауіпсіздік мәселелері клиенттік құрылғыға орнатылған басқарылатын Kaspersky қолданбалары арқылы автоматты түрде жасалуы немесе әкімші қолмен жасауы мүмкін.	• Қосқыш өшірулі. • Қосқыш қосулы.
Бағдарлама анықтаған құрылғы күйі	Құрылғының күйін басқарылатын бағдарлама анықтайды. Басқарылатын құрылғылар Kaspersky Security Center Linux параметрлеріне қарамастан басқарылатын қолданбалармен анықталған күйге ие болуы мүмкін. Бұл күй Kaspersky Security Center Linux анықтаған күйлердің бірін қайтарғаннан кейін, Басқару сервер басқарылатын құрылғыға басқарылатын құрылғы қайтарған және Басқару сервер тағайындағандардың ең маңызды күйін тағайындайды. Басқарылатын қолданбалар анықтаған күйлердің басқарылатын қолданбалар арқылы берілген сипаттамалары бар. Сипаттамаларды басқарылатын құрылғылар тізімінде, **Күйдің сипаттамасы** бағанында көре аласыз.	• Қосқыш өшірулі. • Қосқыш қосулы.
Құрылғыда бос орын жоқ	Құрылғының бос диск кеңістігі көрсетілген мәннен аз немесе құрылғы Басқару серверімен синхрондала алмайды. Құрылғы Басқару серверімен сәтті синхрондалғанда және құрылғының бос диск кеңістігі көрсетілген мәннен көп немесе тең болса, *Критикалық* немесе *Ескерту* күйлері *ОК* күйіне өзгереді.	0 МБ-тан көбірек.
Құрылғы басқарылмайтын күйге айналды	Құрылғылар табылған кезде құрылғы желіде көрінетін болып анықталады, бірақ Басқару серверімен синхрондаудың үштен артық сәтсіз әрекеті орындалды.	• Қосқыш өшірулі. • Қосқыш қосулы.
Қорғаныс өшірілген	Құрылғы көзге көрінеді, бірақ құрылғыдағы қауіпсіздік бағдарламасы көрсетілген уақыттан артық өшірулі. Бұл жағдайда қауіпсіздік бағдарламасының күйі *Тоқтатылған* немесе *Ақау* болып табылады және келесілерден ерекшеленеді: *Іске қосылуда*, *Орындалуда*, немесе *Кідіртілді*.	0 минуттан көбірек.
Қауіпсіздік бағдарламасы іске қосылмаған	Құрылғы көзге көрінеді және қауіпсіздік бағдарламасы құрылғыда орнатылған, бірақ іске қосылмаған.	• Қосқыш өшірулі. • Қосқыш қосулы.

Kaspersky Security Center Linux бағдарламасы белгіленген шарттарды орындау кезінде басқару тобындағы құрылғы күйін автоматты түрде ауыстырып қосуды конфигурациялауға мүмкіндік береді. Белгіленген шарттарды орындау кезінде, клиент құрылғысына келесі күйлердің бірі беріледі: *Критикалық* немесе *Ескерту*. Белгіленген шарттарды орындамаған жағдайда, клиент құрылғысына *ОК* күйі беріледі.

Бір шарттың әртүрлі мәндеріне әртүрлі күйлер сәйкес келуі мүмкін. Мысалы, әдепкі бойынша **3 күннен артық** мәні бар **Дерекқорлар ескірген** шартын ұстанған кезде клиент құрылғысына *Ескерту* күйі, ал **7 күннен артық** мәні бар шартты ұстанған кезде клиент құрылғысына *Критикалық* күйі беріледі.

Kaspersky Security Center Linux бағдарламасын алдыңғы нұсқасынан жаңартып жатсаңыз, *Критикалық* немесе *Ескерту* күйін тағайындау үшін **Дерекқорлар ескірген** шартының мәні өзгермейді.

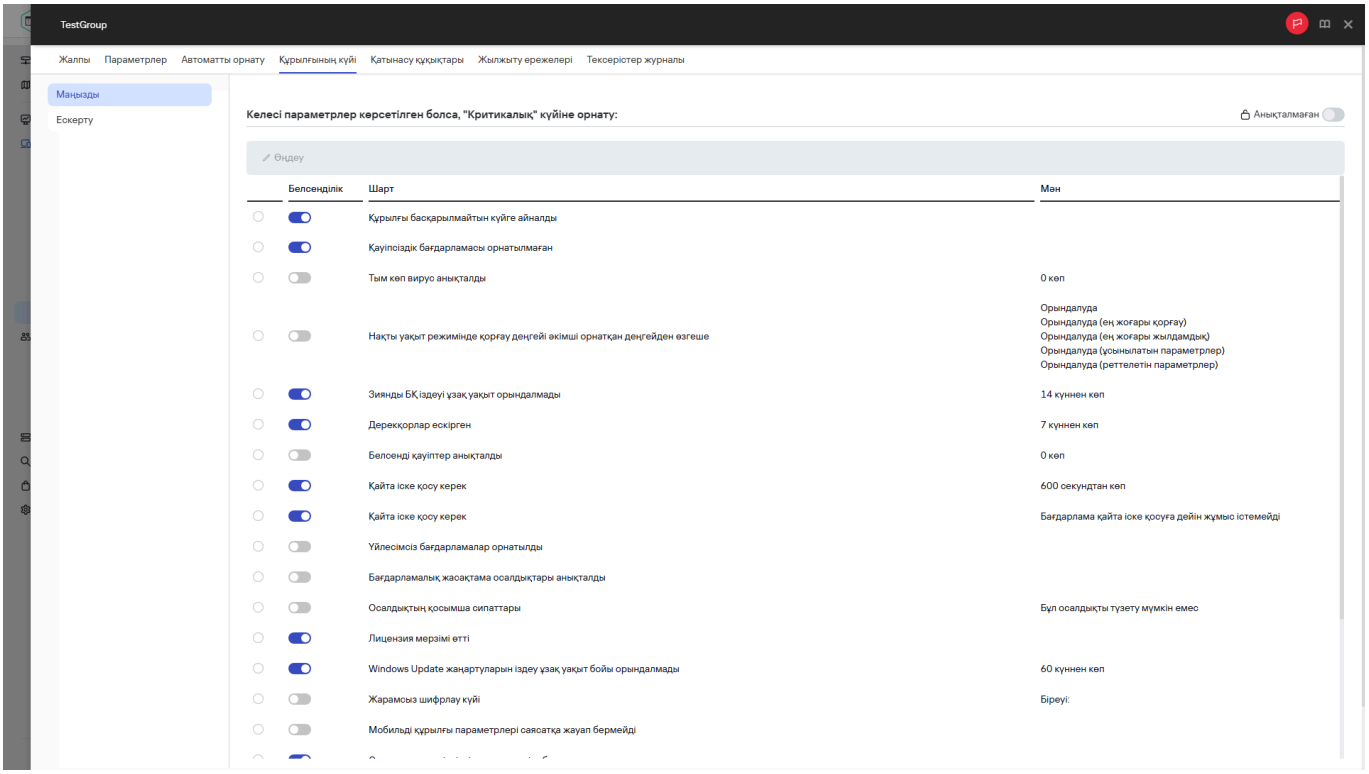
Құрылғылардың күйлерін ауыстыруды конфигурациялау

Құрылғыға *Критикалық* немесе *Ескерту* күйлерін тағайындау шарттарын өзгерте аласыз.

Құрылғының күйін Критикалық деп өзгерту үшін:

1. Бағдарламаның негізгі терезесінде **Активтерді басқару** → **Топтардың иерархиясы** бөліміне өтіңіз.
2. Келесі жолдардың бірімен құрылғы күйлерін өзгерткіңіз келетін басқару тобының сипаттарына өтіңіз:
   - Басқару тобының атауын басыңыз.
   - Беттің жоғарғы жағындағы **Иерархияны көрсету** түймесін басыңыз. Ашылатын навигация панелінде тінтуір курсорын қажетті топ атауының үстіне апарып, параметрлер белгішесін (⚙) басыңыз.

   Басқару тобының сипаттары терезесі ашылады.
3. Сипаттар терезесінен **Құрылғының күйі** қойындысын таңдаңыз.
4. **Маңызды** бөлімін таңдаңыз.
5. **Келесі параметрлер көрсетілген болса, "Критикалық" күйіне орнату** блогында құрылғыны *Критикалық* күйіне ауыстырып қосу үшін шартты қосыңыз.



Алайда, сіз ата-ана саясатында бұғатталмаған параметрлерді өзгерте аласыз.

6. Тізімдегі шарттың жанына қосқышты орнатыңыз.
7. Тізімнің жоғарғы сол жақ бұрышындағы **Өңдеу** түймесін басыңыз.
8. Таңдалған шарт үшін өзіңізге қажетті мәнді белгілеңіз.

   Мәндерді барлық шарттар үшін бірдей орнату мүмкін емес.
9. **OK** түймесін басыңыз.
10. Өзгерістерін сақтау үшін **Сақтау** түймесін басыңыз.

Белгіленген шарттарды орындамаған жағдайда, басқарылатын құрылғыға *Критикалық* күйі тағайындалады.

Құрылғының күйін Ескерту деп өзгерту үшін:

1. Бағдарламаның негізгі терезесінде **Активтерді басқару** → **Топтардың иерархиясы** бөліміне өтіңіз.
2. Ашылған топтар тізімінде құрылғылардың күйлерін ауыстырып қосуды өзгерткіңіз келетін топтың атауы бар сілтемеден өтіңіз.
3. Пайда болған сипаттар терезесінде **Құрылғының күйі** қойыншасын таңдаңыз.
4. **Ескерту** бөлімін таңдаңыз.
5. **Келесі параметрлер көрсетілген болса, "Ескерту" күйіне орнату** блогында құрылғыны *Ескерту* күйіне ауыстырып қосу үшін шартты қосыңыз.

   Алайда, сіз ата-ана саясатында бұғаталмаған параметрлерді өзгерте аласыз.
6. Тізімдегі шарттың жанына қосқышты орнатыңыз.
7. Тізімнің жоғарғы сол жақ бұрышындағы **Өңдеу** түймесін басыңыз.
8. Таңдалған шарт үшін өзіңізге қажетті мәнді белгілеңіз.

   Мәндерді барлық шарттар үшін бірдей орнату мүмкін емес.
9. **OK** түймесін басыңыз.
10. Өзгерістерін сақтау үшін **Сақтау** түймесін басыңыз.

Белгіленген шарттарды орындамаған жағдайда, басқарылатын құрылғыға *Ескерту* күйі тағайындалады.

Құрылғыны таңдаулары

Құрылғыны таңдалары – бұл белгіленген шарттарға сәйкес құрылғыларды сүзгілеуге арналған құрал. Бірнеше құрылғыны басқару үшін құрылғы таңдауларын пайдалануға болады: мысалы, тек таңдалған құрылғылар туралы есептерді көру немесе осы құрылғылардың барлығын басқа басқару тобына жылжыту.

Kaspersky Security Center Linux бағдарламасы *құрылғының алдын ала анықталған таңдауларының* кең ауқымын ұсынады (мысалы, **Маңызды күйі бар құрылғылар**, **Қорғаныс өшірілген**, **Белсенді қауіптер анықталды**). Алдын ала анықталған таңдауды жоюға болмайды. Сондай-ақ қосымша *пайдаланушы анықтайтын таңдауларды* жасауға және конфигурациялауға болады.

Пайдаланушының таңдауларында іздеу аймағын белгілеуге және барлық құрылғыларды, басқарылатын құрылғыларды немесе тағайындалмаған құрылғыларды таңдауға болады. Іздеу параметрлері шарттарда белгіленеді. Құрылғы таңдауларында әртүрлі іздеу параметрлері бар бірнеше шарттар жасауға болады. Мысалы, сіз екі шарт жасай аласыз және әрқайсысында әртүрлі IP ауқымдарын белгілей аласыз. Егер бірнеше шарттар белгіленген болса, құрылғы таңдауларына кез келген шартты қанағаттандыратын құрылғылар енеді. Керісінше, бір шартта іздеу параметрлері бір-біріне қабаттасады. Егер таңдау шартында IP ауқымы және орнатылған бағдарламаның атауы белгіленген болса, онда құрылғы таңдауларына бір уақытта көрсетілген бағдарлама орнатылған және олардың IP мекенжайлары көрсетілген ауқымға кіретін құрылғылар ғана кіреді.

Құрылғы таңдауларынан құрылғылар тізімін қарау

Kaspersky Security Center Linux құрылғы таңдауынан құрылғылар тізімін көруге мүмкіндік береді.

Құрылғы таңдауынан құрылғылар тізімін көру үшін:

1. Бағдарламаның негізгі терезесінде **Активтерді басқару** → **Құрылғы таңдаулары** немесе **Табу және орналастыру** → **Құрылғы таңдаулары** бөліміне өтіңіз.
2. Таңдаулар тізімінде құрылғыны таңдаудың атауын басыңыз.

   Бетте құрылғы таңдауына енгізілген құрылғылар туралы ақпараты бар кесте көрсетілген.
3. Құрылғылар кестесінің деректерін келесідей топтастыруға және сүзуге болады:
   - Параметрлер белгішесін (⚙) басыңыз және кестеде көрсетілетін бағандарды таңдаңыз.
   - (▽) сүзу белгішесін нұқыңыз, ашылған мәзірде сүзу критерийін көрсетіңіз және қолданыңыз.

     Сүзілген құрылғылар кестесі көрсетіледі.

Құрылғы таңдауында бір немесе бірнеше құрылғыны таңдап, осы құрылғыларға қолданылатын тапсырманы жасау үшін **Жаңа тапсырма**.

Таңдалған құрылғыларды құрылғы таңдауынан басқа басқару тобына жылжыту үшін **Топқа жылжыту** түймесін басыңыз және мақсатты басқару тобын таңдаңыз.

Құрылғы таңдауларын жасау

Құрылғы таңдауларын жасау үшін:

1. Бағдарламаның негізгі терезесінде **Активтерді басқару** → **Құрылғы таңдаулары** бөліміне өтіңіз.

   Құрылғылар таңдауы тізімі бар бет көрсетіледі.
2. **Қосу** түймесін басыңыз.

   Құрылғыны таңдау параметрлері терезесі ашылады.
3. Жаңа таңдау атауын енгізіңіз.

4. Құрылғы таңдауларына қосылатын құрылғыларды қамтитын топты көрсетіңіз:

   - **Кез келген құрылғыларды іздеу** – **Басқарылатын құрылғылар** немесе **Тағайындалмаған құрылғылар** топтарында таңдау шарттарына сәйкес келетін құрылғыларды іздеу.
   - **Басқарылатын құрылғыларды іздеу** – **Басқарылатын құрылғылар** тобында таңдау шарттарына сәйкес келетін құрылғыларды іздеу.
   - **Тағайындалмаған құрылғыларды іздеу** – **Тағайындалмаған құрылғылар** тобында таңдау шарттарына сәйкес келетін құрылғыларды іздеу.

   Қосалқы Басқару серверлерінде таңдау критерийлеріне сәйкес келетін құрылғыларды іздеуді қосу үшін **Қосалқы Басқару серверлерінен алынған деректерді қамту** жалаушасын қоя аласыз.

5. **Қосу** түймесін басыңыз.
6. Ашылған терезеде, құрылғыларды осы таңдауға қосу үшін орындалуы тиісті шарттарды көрсетіңіз және **OK** түймесін басыңыз.
7. **Сақтау** түймесін басыңыз.

Құрылғы таңдаулары жасалып, құрылғы таңдаулары тізіміне қосылған.

Құрылғы таңдауларын конфигурациялау

Құрылғы таңдаулары параметрлерін конфигурациялау үшін:

1. Бағдарламаның негізгі терезесінде **Активтерді басқару → Құрылғы таңдаулары** бөліміне өтіңіз.

   Құрылғылар таңдауы тізімі бар бет көрсетіледі.

2. Тиісті пайдаланушы құрылғылар таңдауын таңдап, **Сипаттар** түймесін басыңыз.

   Құрылғыны таңдау параметрлері терезесі ашылады.

3. **Жалпы** қойыншасында **Жаңа шарт** сілтемесінен өтіңіз.
4. Құрылғы осы таңдауға қосылуы үшін орындалуы керек шарттарды көрсетіңіз.
5. **Сақтау** түймесін басыңыз.

Параметрлер қолданылған және сақталған.

Төменде құрылғыларды таңдауға жатқызу шарттарының параметрлері сипатталған. Шарттар логикалық "немесе" бойынша біріктіріледі: ұсынылған шарттардың кем дегенде біреуін қанағаттандыратын құрылғылар таңдауға түседі.

Жалпы

Жалпы бөлімінде таңдау шартының атауын өзгертуге және осы шартты кері қайтару қажет пе екенін көрсетуге болады:

Таңдау шартын кері қайтару

Әдепкі бойынша, параметр өшірулі.

Бұл опцияны қоссаңыз, берілген таңдау шарты инверсияланады. Шартқа сәйкес келмейтін барлық құрылғылар таңдауға кіреді.

Келесі мысалда инверсия жұмысының логикасы көрсетілген:

- **Шарт**: құрылғыда Linux түріндегі операциялық жүйе және 00.0.000 құрастыру нөмірі бар.
- **Инверсияланған жағдай**: құрылғыда келесінің баламасы болатын NOT (Linux түрі және 00.0.000 құрастыру нөмірі) бар операциялық жүйе бар.

  NOT түріндегі Linux НЕМЕСЕ NOT 00.0.000 құрастыру нөмірі бар операциялық жүйе бар.

Осылайша таңдауға, мысалы, Windows түріндегі және 00.0.000 құрастыру нөмірі бар немесе Linux түріндегі және 00.0.000-ден басқа жинақ нөмірі бар құрылғылар кіреді.

Желі инфрақұрылымы

Желі бөлімінде құрылғыларды олардың желілік деректері негізінде таңдауға қосу өлшемшарттарын конфигурациялауға болады:

- **Құрылғы атауы**

  Windows желісіндегі құрылғы атауы (NetBIOS атауы) немесе IPv4 мекенжайы не IPv6 мекенжайы.

- **Домен**

  Көрсетілген жұмыс тобына кіретін барлық құрылғылар көрсетіледі.

- **Басқару тобы**

  Көрсетілген басқару тобына кіретін құрылғылар көрсетіледі.

- **Сипаттама**

  Құрылғы сипаттары терезесінде қамтылған мәтін: **Жалпы** бөлімінің **Сипаттама** өрісінде.

  Сипаттама мәтінінде келесі таңбаларды қолдануға болады:

  - Бір сөздің ішінде:
    - *****. 0 немесе одан да көп таңбадан ұзын кез келген жолды алмастырады.

      Мысалы:

      Сервер, **Серверлік** сөздерін сипаттау үшін **Сервер*** жолын қолдануға болады.

    - **?.** Кез келген бір таңбаны ауыстырады.

      Мысалы:

      SUSE Linux корпоративтік сервері 12 немесе **SUSE Linux корпоративтік сервері 15** сияқты сөз тіркестерін сипаттау үшін **SUSE Linux Enterprise Server 1 деп тересіз бе?**.

      Жұлдызша (*****) немесе сұрақ белгісі (**?**) мәтін сипаттамасында бірінші таңба ретінде қолданылуы мүмкін емес.

- Бірнеше сөздерді байланыстыру үшін:

  - Бос орын. Сипаттамаларында аталған сөздердің кез келгені бар барлық құрылғыларды көрсетеді.

  Мысалы:

  Қосалқы немесе **Виртуалдық** сөзін қамтитын сөйлемшені сипаттау үшін **Қосалқы Виртуалды** жолын қолдануға болады.

  - **+**. Сөздің алдында жазған кезде, мәтінде сөздің міндетті түрде болуын білдіреді.

  Мысалы:

  Қосалқы сөзін де, **Виртуалды** сөзін де қамтитын сөйлемшені сипаттау үшін **+Қосалқы+Виртуалды** жолын қолдануға болады.

  - **-**. Сөздің алдында жазған кезде, мәтінде сөздің міндетті түрде болмауын білдіреді.

  Мысалы:

  Қосалқы сөзі болуы, бірақ **Виртуалды** сөзі болмауы тиісті сөйлемшені сипаттау үшін **+Қосалқы-Виртуалды** жолын қолдануға болады.

  - **"<мәтін үзіндісі>"**. Тырнақшаға алынған мәтін үзіндісі мәтінде толығымен болуы керек.

  Мысалы:

  Қосалқы Сервер сөзтіркесін қамтитын сөйлемшені сипаттау үшін, **"Қосалқы Сервер"** жолын қолдануға болады.

- **IP ауқымы**

  Бұл параметр қосулы болса, енгізу өрістерінде сіз іздеген құрылғылар кіруі тиісті аралықтың бастапқы және соңғы IP мекенжайларын көрсетуге болады.

  Әдепкі бойынша, параметр өшірулі.

- **Басқа Басқару серверімен басқарылады**

  Келесі мәндердің бірін таңдаңыз:

  - **Иә**. Құрылғыларды жылжыту ережесі тек басқа Басқару серверлері басқаратын клиент құрылғыларына қолданылады. Бұл Серверлер құрылғыларды жылжыту ережесін конфигурациялайтын Серверден ерекшеленеді.

  - **Жоқ**. Құрылғыларды жылжыту ережесі тек ағымдағы басқару сервері басқаратын клиенттік құрылғыларға қолданылады.

  - **Мән таңдалмаған**. Шарт қолданылмайды.

Домен контроллері бөлімінде құрылғыларды домен мүшелігін таңдауға қосу өлшемшарттарын орнатуға болады:

- **Доменнің ұйымдық бөлімшесіндегі құрылғы**

  Егер бұл параметр қосулы болса, енгізу өрісінде көрсетілген домен бөлімшесіндегі құрылғылар таңдауға қосылады.

  Әдепкі бойынша, параметр өшірулі.

- **Құрылғы доменнің қауіпсіздік тобының мүшесі болып табылады**

  Егер бұл параметр қосулы болса, енгізу өрісінде көрсетілген доменнің қауіпсіздік тобындағы құрылғылар таңдауға қосылады.

  Әдепкі бойынша, параметр өшірулі.

Желілік белсенділік бөлімінде құрылғыларды олардың желілік белсенділігі негізінде таңдауға қосу өлшемшарттарын конфигурациялауға болады:

- **Тарату нүктесі ретінде әрекет етеді**

  Ашылмалы тізімде, іздеу кезінде құрылғыларды таңдау құрамына қосу өлшемшартын таңдауға болады:

  - **Иә**. Таңдауға тарату нүктелері болып табылатын құрылғылар қосылады.
  - **Жоқ**. Тарату нүктелері ретінде әрекет ететін құрылғылар таңдауға кірмейді.
  - **Мән таңдалмаған**. Өлшемшарт қолданылмайды.

- **Басқару серверімен байланысты үзбеу**

  Ашылмалы тізімде, іздеу кезінде құрылғыларды таңдау құрамына қосу өлшемшартын таңдауға болады:

  - **Қосулы**. Таңдау **Басқару серверімен байланысты үзбеу** жалаушасы қойылған құрылғыларды қамтиды.
  - **Өшірулі**. Таңдау **Басқару серверімен байланысты үзбеу** жалаушасы алынған құрылғыларды қамтиды.
  - **Мән таңдалмаған**. Өлшемшарт қолданылмайды.

- **Байланыс профилі ауыстырылды**

  Ашылмалы тізімде, іздеу кезінде құрылғыларды таңдау құрамына қосу өлшемшартын таңдауға болады:

  - **Иә**. Таңдауға қосылым профилін ауыстырып қосу нәтижесінде Басқару серверіне қосылған құрылғылар кіреді.
  - **Жоқ**. Таңдауға қосылым профилін ауыстыру нәтижесінде басқару серверіне қосылған құрылғылар кірмейді.
  - **Мән таңдалмаған**. Өлшемшарт қолданылмайды.

- **Басқару серверіне соңғы қосылу уақыты**

  Осы жалаушаны пайдаланып, Басқару серверіне соңғы қосылу уақыты бойынша құрылғыларды іздеу өлшемшартын белгілей аласыз.

  Егер жалауша қойылса, енгізу өрістерінде, клиент құрылғысында орнатылған Желілік агенттің Басқару серверіне соңғы қосылуы орындалған аралықтың мәндерін (күні мен уақыты) көрсетуге болады. Таңдауға белгіленген аралыққа сәйкес келетін құрылғылар қосылады.

  Егер жалауша алынып тасталса, онда өлшемшарт қолданылмайды.

  Әдепкі бойынша, жалауша алынып тасталған.

- **Жаңа құрылғылар желі сауалнамасымен анықталды**

  Соңғы бірнеше күнде желіде сауалнама өткізу кезінде табылған жаңа құрылғыларды іздеу.

  Егер бұл параметр қосулы болса, онда **Анықтау кезеңі (тәу)** өрісінде көрсетілген күндер санында құрылғыларды анықтау процесінде табылған жаңа құрылғылар ғана таңдауға қосылады.

Егер бұл параметр өшірулі болса, онда құрылғыны анықтау процесінде табылған барлық құрылғылар таңдауға қосылады.

Әдепкі бойынша, параметр өшірулі.

- **Құрылғы көрінеді**

  Ашылмалы тізімде, іздеу кезінде құрылғыларды таңдау құрамына қосу өлшемшартын таңдауға болады:

  - **Иә**. Бағдарлама қазіргі уақытта желіде көрінетін құрылғыларды таңдауға қосады.
  - **Жоқ**. Қолданба қазіргі уақытта желіде көрінбейтін құрылғыларды таңдауға қосады.
  - **Мән таңдалмаған**. Өлшемшарт қолданылмайды.

Құрылғы күйлері

Басқарылатын құрылғы күйі бөлімінде, басқарылатын бағдарламадан құрылғы күйінің сипаттамасы бойынша таңдауға құрылғыларды қосу өлшемшарттарын конфигурациялауға болады:

- **Құрылғының күйі**

  Құрылғы күйлерінің бірін таңдауға болатын ашылмалы тізім: *OK*, *Маңызды* немесе *Ескерту*.

- **Нақты уақыт режимінде қорғаныс күйі**

  Нақты уақыт режимінде қорғау тапсырмасы күйінің мәнін таңдауға болатын ашылмалы тізім. Нақты уақыт режимінде қорғау күйі көрсетілген құрылғылар таңдауға қосылады.

- **Құрылғы күйінің сипаттамасы**

  Бұл өрісте орындалса, құрылғыға келесі күйлердің бірін тағайындайтын шарттардың жанындағы құсбелгі ұяшықтарын таңдай аласыз: *OK, Маңызды* немесе *Ескерту*.

Басқарылатын бағдарламалардың құрамдастарының күйі бөлімінде, басқарылатын бағдарламалардың құрамдастарының күйлері бойынша құрылғыларды таңдауға қосу өлшемшарттарын конфигурациялауға болады:

- **Деректердің жайылып кетуіне жол бермеу күйі**

  Деректердің жайылып кетуінен қорғау құрамдасының күйі бойынша құрылғыларды іздеу (*Белгісіз, Тоқтатылды, Іске қосылды, Кідіртілді, Орындалуда, Сәтсіз аяқталды*).

- **Бірлескен жұмыс серверлерінің қорғаныс күйі**

  Бірлескен жұмыс серверлері үшін қорғау күйі бойынша құрылғыларды іздеу (*Белгісіз*, *Тоқтатылды*, *Іске қосылды, Кідіртілді*, *Орындалуда*, *Сәтсіз аяқталды*).

- **Пошталық серверлердің антивирустық қорғаныс күйі**

  Пошта серверінің қорғау күйі бойынша құрылғыларды іздеу (*Белгісіз, Тоқтатылды, Іске қосылды, Кідіртілді, Орындалуда, Сәтсіз аяқталды*).

- **Endpoint Sensor күйі**

  Құрылғыларды Endpoint Sensor құрамдасының күйі бойынша іздеу (*Белгісіз, Тоқтатылды, Іске қосылды, Кідіртілді, Орындалуда, Сәтсіз аяқталды*).

Басқарылатын бағдарламалардағы күйге әсер ететін мәселелер бөлімінде, басқарылатын бағдарлама анықтаған ықтимал мәселелер тізіміне сәйкес құрылғыларды таңдауға қосу өлшемшарттарын конфигурациялауға болады. Егер сіз таңдаған құрылғыда кем дегенде бір мәселе болса, құрылғы таңдауға қосылады. Бірнеше бағдарлама үшін көрсетілген мәселені таңдағанда, сізде барлық тізімдерде осы мәселені автоматты түрде таңдау мүмкіндігі болады.

Сіз басқарылатын бағдарламалар күйлерінің сипаттамасы үшін жалаушаларды қоя аласыз, оларды алған кезде құрылғылар таңдауға қосылады. Бірнеше бағдарлама үшін көрсетілген күйді таңдағанда, сізде барлық тізімдерде осы күйді автоматты түрде таңдау мүмкіндігі болады.

Жүйе мәліметтері

ОЖ бөлімінде, орнатылған операциялық жүйенің негізінде құрылғыларды таңдауға қосу өлшемшарттарын конфигурациялауға болады.

- **Платформа түрі**

  Егер жалауша қойылса, тізімнен операциялық жүйелерді таңдауға болады. Көрсетілген операциялық жүйелер орнатылған құрылғылар іздеу нәтижелеріне қосылады.

- **ОЖ жағарту бумасы нұсқасы**

  Бұл өрісте операциялық жүйенің пакет нұсқасын (*X.Y* форматында) көрсетуге болады, ол жылжыту ережесінің құрылғыға қалай қолданылатынын анықтайды. Әдепкі бойынша, нұсқаның мәндері белгіленбеген.

- **ОЖ архитектурасы**

  Ашылмалы тізімде операциялық жүйенің биттік өлшемін таңдауға болады, оның болуы бойынша құрылғыға құрылғыны жылжыту ережесі қолданылады (**Белгісіз**, **x86**, **AMD64** немесе **IA64**). Әдепкі бойынша, тізімде бірде-бір нұсқа таңдалмаған, операциялық жүйенің биттік өлшемі белгіленбеген.

- **ОЖ жинақ нөмірі**

  > Бұл параметр тек Windows операциялық жүйелері үшін қолданылады.

  Операциялық жүйенің құрастыру нөмірі. Таңдалған операциялық жүйеде тең, анағұрлым ерте немесе анағұрлым кеш құрастыру нөмірі болуы керек пе екенін көрсетуге болады. Сондай-ақ, көрсетілгеннен басқа барлық құрастыру нөмірлерін іздеуді конфигурациялауға болады.

- **ОЖ шығарылымының нөмірі**

  > Бұл параметр тек Windows операциялық жүйелері үшін қолданылады.

  Операциялық жүйе шығарылымының идентификаторы. Таңдалған операциялық жүйеде тең, анағұрлым ерте немесе анағұрлым кеш шығарылым идентификаторы болуы керек пе екенін көрсетуге болады. Сондай-ақ, көрсетілгеннен басқа барлық шығарылым идентификаторы нөмірлерін іздеуді конфигурациялауға болады.

Виртуалды машиналар бөлімінде, бұл құрылғылардың виртуалды машиналар немесе Virtual Desktop Infrastructure бөлігі екендігіне байланысты құрылғыларды таңдауға қосу өлшемшарттарын конфигурациялауға болады:

- **Виртуалды машина болып табылады**

  Ашылмалы тізімнен келесі элементтерді таңдауға болады:

  - **Анықталмаған**.
  - **Жоқ**. Виртуалды машиналар емес құрылғыларды табу.
  - **Иә**. Ізделетін құрылғылар виртуалды машиналар болуы керек.

- **Виртуалды машинаның түрі**

  Ашылмалы тізімнен виртуалды машина өндірушісін таңдауға болады.

  Бұл ашылмалы тізім **Виртуалды машина болып табылады** ашылмалы тізімінде **Иә** немесе **Маңызды емес** мәні таңдалған болса қолжетімді.

- **Virtual Desktop Infrastructure бөлігі**

  Ашылмалы тізімнен келесі элементтерді таңдауға болады:

  - **Анықталмаған**.
  - **Жоқ**. Virtual Desktop Infrastructure-дың бөлігі болып табылмайтын құрылғыларды табу.
  - **Иә**. Ізделетін құрылғылар Virtual Desktop Infrastructure (VDI) бөлігі болуы тиіс.

Жабдық тізімдемесі бөлімінде құрылғыларды оларға орнатылған жабдық бойынша таңдауға қосу өлшемшарттарын конфигурациялауға болады:

> lshw утилитасы, жабдық туралы ақпарат алғыңыз келетін Linux құрылғыларында орнатылғанын тексеріңіз. Виртуалды машиналардан алынған жабдық туралы мәлімет пайдаланылатын гипервизорға байланысты толық болмауы мүмкін

- **Құрылғы**

  Ашылмалы тізімнен жабдық түрін таңдауға болады. Мұндай жабдықтары бар барлық құрылғылар іздеу нәтижесіне қосылған.

  Өрісте толық мәтінді іздеуге қолдау көрсетіледі.

- **Өндіруші**

  Ашылмалы тізімнен жабдық өндірушісінің атауын таңдауға болады. Мұндай жабдықтары бар барлық құрылғылар іздеу нәтижесіне қосылған.

  Өрісте толық мәтінді іздеуге қолдау көрсетіледі.

- **Құрылғы атауы**

  Көрсетілген атауы бар құрылғы таңдауға қосылады.

- **Сипаттама**

  Құрылғының немесе жабдықтың сипаттамасы. Өрісте көрсетілген сипаттамасы бар құрылғылар таңдау құрамына енгізіледі.

Құрылғының сипаттамасын құрылғының сипаттары терезесінде еркін түрде енгізуге болады. Өрісте толық мәтінді іздеуге қолдау көрсетіледі.

- **Құрылғы өндірушісі**

  Құрылғы өндірушісінің атауы. Өрісте көрсетілген өндіруші жасаған құрылғылар таңдау құрамына енгізіледі.

  Өндірушінің атауын құрылғының сипаттары терезесінде енгізуге болады.

- **Сериялық нөмір**

  Өрісте көрсетілген сериялық нөмірі бар жабдық таңдауға қосылады.

- **Қойма нөмірі**

  Өрісте көрсетілген қойма нөмірі бар жабдық таңдауға қосылады.

- **Пайдаланушы**

  Өрісте көрсетілген пайдаланушының аппараттық жасақтамасы таңдауға қосылады.

- **Орналасуы**

  Құрылғының немесе жабдықтың орналасқан жері (мысалы, кеңседе немесе филиалда). Өрісте көрсетілген жерде орналасқан компьютерлер немесе басқа құрылғылар таңдау құрамына кіреді.

  Жабдықтың орналасуын жабдықтың сипаттары терезесінде еркін түрде енгізуге болады.

- **Орталық процессор тактілік жиілігі, МГц түрінде, келесіден бастап**

  Процессордың ең төменгі тактілік жиілігі. Енгізу өрістерінде (қоса алғанда) көрсетілген жиіліктер ауқымына сәйкес келетін орталық процессорлары бар құрылғылар таңдау құрамына енгізіледі.

- **Орталық процессор тактілік жиілігі, МГц түрінде, осыған дейін**

  Процессордың ең жоғарғы тактілік жиілігі. Енгізу өрістерінде (қоса алғанда) көрсетілген жиіліктер ауқымына сәйкес келетін орталық процессорлары бар құрылғылар таңдау құрамына енгізіледі.

- **Виртуалды орталық процессор ядроларының саны, басы**

  CPU виртуалды өзектерінің ең аз саны. Енгізу өрістерінде (қоса алғанда) көрсетілген виртуалды өзектер санының ауқымына келетін орталық процессорлары бар құрылғылар таңдау құрамына енгізіледі.

- **Виртуалды орталық процессор ядроларының саны, соңы**

  CPU виртуалды өзектерінің ең көп саны. Енгізу өрістерінде (қоса алғанда) көрсетілген виртуалды өзектер санының ауқымына келетін орталық процессорлары бар құрылғылар таңдау құрамына енгізіледі.

- **Қатты дискінің көлемі, ГБ түрінде, келесіден бастап**

  Құрылғының қатты дискісінің ең аз көлемі. Енгізу өрістеріндегі (қоса алғанда) мәндер ауқымына сәйкес келетін қатты дискілері бар құрылғылар таңдау құрамына енгізіледі.

- **Қатты дискінің көлемі, ГБ түрінде, келесіге дейін**

  Құрылғының қатты дискісінің ең көп көлемі. Енгізу өрістеріндегі (қоса алғанда) мәндер ауқымына сәйкес келетін қатты дискілері бар құрылғылар таңдау құрамына енгізіледі.

- **ЖЖҚ өлшемі, МБ түрінде, келесіден бастап**

  Құрылғы ЖЖҚ-сының минималды өлшемі. Енгізу өрістерінде (қоса алғанда) көрсетілген өлшем ауқымына сәйкес келетін ЖЖҚ-сы бар құрылғылар таңдауға қосылады.

- **ЖЖҚ өлшемі, МБ түрінде, келесіге дейін**

  Құрылғы ЖЖҚ-сының максималды өлшемі. Енгізу өрістерінде (қоса алғанда) көрсетілген өлшем ауқымына сәйкес келетін ЖЖҚ-сы бар құрылғылар таңдауға қосылады.

Үшінші тарап бағдарламалық жасақтамасы туралы мәліметтер

Бағдарламалар тізімдемесі бөлімінде қандай бағдарламалар орнатылғанына байланысты құрылғыларды таңдауға қосу өлшемшарттарын конфигурациялауға болады:

- **Бағдарлама атауы**

  Бағдарламаны таңдауға болатын ашылмалы тізім. Көрсетілген бағдарлама орнатылған құрылғылар таңдауға қосылады.

- **Бағдарламаның нұсқасы**

  Таңдалған бағдарламаның нұсқасын көрсететін енгізу өрісі.

- **Өндіруші**

  Құрылғыда орнатылған бағдарламаның өндірушісін таңдауға болатын ашылмалы тізім.

- **Бағдарлама күйі**

  Бағдарлама күйін таңдауға болатын ашылмалы тізім (*Орнатылған*, *Орнатылмаған*). Таңдалған күйге байланысты, аталған бағдарлама орнатылған немесе орнатылмаған құрылғылар таңдауға қосылады.

- **Жаңарту бойынша іздеу**

  Егер бұл параметр қосулы болса, іздеу сіз іздеген құрылғыларда орнатылған бағдарламаларды жаңарту деректері бойынша орындалады. Жалауша қойылғаннан кейін, **Бағдарлама атауы**, **Бағдарламаның нұсқасы** және **Бағдарлама күйі** өрістерінің орнына сәйкесінше **Жаңартудың атауы**, **Жаңартудың нұсқасы** және **Күйі** өрістері көрсетіледі.

  Әдепкі бойынша, параметр өшірулі.

- **Үйлесімсіз қауіпсіздік бағдарламасының аты**

  Үшінші тарап қауіпсіздік бағдарламаларын таңдауға болатын ашылмалы тізім. Іздеу кезінде, таңдалған бағдарлама орнатылған құрылғылар таңдауға қосылады.

- **Бағдарлама тегі**

  Ашылмалы тізімнен бағдарлама тегін таңдауға болады. Сипаттамада таңдалған тегі бар бағдарламалар орнатылған барлық құрылғылар құрылғылар таңдауына қосылады.

- **Көрсетілген тегтерсіз құрылғыларға қолдану**

  Параметр қосулы болса, онда таңдауға, сипаттамасында таңдалған тегтері жоқ құрылғылар қосылады.

  Бұл параметр өшірулі болса, өлшемшарт қолданылмайды.

Әдепкі бойынша, параметр өшірулі.

Осалдықтар мен жаңартулар бөлімінде, құрылғыларды Windows Update жаңарту көздері бойынша таңдауға қосу өлшемшарттарын конфигурациялауға болады:

WUA Басқару серверіне ауысты

Ашылмалы тізімнен келесі іздеу нұсқаларының бірін таңдауға болады:

- **Иә**. Егер бұл нұсқа таңдалса, іздеу нәтижелеріне Windows Update жаңартуларын Басқару серверінен алатын құрылғылар кіреді.
- **Жоқ**. Бұл нұсқа таңдалса, нәтижелер жаңартуларды Windows Update арқылы басқа дереккөздерден алатын құрылғыларды қамтиды.

Kaspersky бағдарламалары туралы мәліметтер

Kaspersky бағдарламалары бөлімінде құрылғыларды таңдалған басқарылатын бағдарламаның негізінде таңдауға қосу өлшемшарттарын конфигурациялауға болады:

- **Бағдарлама атауы**

  Ашылмалы тізімде, Kaspersky бағдарламасының атауы бойынша іздеу кезінде құрылғыларды таңдау құрамына қосу өлшемшартын таңдауға болады.

  Тізімде, әкімшінің жұмыс станциясында басқару плагиндері орнатылған бағдарламалардың атаулары ғана берілген.

  Егер бағдарлама таңдалмаса, онда өлшемшарт қолданылмайды.

- **Бағдарламаның нұсқасы**

  Енгізу өрісінде Kaspersky бағдарламасы нұсқасының нөмірі бойынша іздеу кезінде құрылғыларды таңдау құрамына қосу өлшемшартын көрсетуге болады.

  Егер нұсқа нөмірі көрсетілмесе, онда өлшемшарт қолданылмайды.

- **Маңызды жаңартудың атауы**

  Енгізу өрісінде бағдарлама үшін белгіленген жаңарту пакетінің атауы немесе нөмірі бойынша іздеу кезінде құрылғыларды таңдау құрамына қосу өлшемшартын көрсетуге болады.

  Егер өріс толтырылмаса, онда өлшемшарт қолданылмайды.

- **Бағдарлама күйі**

  Бағдарлама күйін таңдауға болатын ашылмалы тізім (*Орнатылған*, *Орнатылмаған*). Таңдалған күйге байланысты, аталған бағдарлама орнатылған немесе орнатылмаған құрылғылар таңдауға қосылады.

- **Модульдердің соңғы жаңарту мерзімін таңдау**

  Бұл параметрдің көмегімен құрылғыларда орнатылған бағдарлама модульдерінің соңғы рет жаңартылған уақыты бойынша құрылғыларды іздеу өлшемшартын белгілеуге болады.

  Егер жалауша қойылса, енгізу өрістерінде құрылғыларда орнатылған бағдарлама модульдерінің соңғы жаңартылуы орындалған аралық мәндерін (күні мен уақыты) көрсетуге болады.

  Егер жалауша алынып тасталса, онда өлшемшарт қолданылмайды.

  Әдепкі бойынша, жалауша алынып тасталған.

- **Құрылғы Басқару сервері арқылы басқарылады**

  Ашылмалы тізімде Kaspersky Security Center Linux басқаратын құрылғыны таңдау құрамына қосуға болады:

  - **Иә**. Бағдарлама Kaspersky Security Center Linux басқаратын құрылғыларды таңдауды қамтиды.
  - **Жоқ**. Қолданба Kaspersky Security Center Linux арқылы басқарылмайтын құрылғыларды таңдауға қосады.
  - **Мән таңдалмаған**. Өлшемшарт қолданылмайды.

- **Қауіпсіздік бағдарламасы орнатылған**

  Ашылмалы тізімде қауіпсіздік бағдарламасы орнатылған құрылғыны таңдау құрамына қосуға болады:

  - **Иә**. Бағдарлама, қауіпсіздік бағдарламасы орнатылған құрылғыларды таңдауға қосады.
  - **Жоқ**. Қолданба қауіпсіздік қолданбасы орнатылмаған барлық құрылғыны таңдауға қосады.
  - **Мән таңдалмаған**. Өлшемшарт қолданылмайды.

Антивирустық қорғаныс бөлімінде құрылғыларды қорғаныс күйі бойынша таңдауға қосу өлшемшарттарын конфигурациялауға болады:

- **Дерекқорлардың шығарылған күні**

  Осы параметр таңдалса, клиент құрылғыларын іздеу антивирустық дерекқордың шығарылу күні бойынша орындалады. Енгізу өрістерінде іздеу жүргізілетін уақыт аралығын белгілеуге болады.

  Әдепкі бойынша, параметр өшірулі.

- **Дерекқорлардағы жазбалар саны**

  Егер бұл параметр қосылса, клиент құрылғыларын іздеу дерекқордағы жазбалар саны бойынша жүзеге асырылады. Енгізу өрістерінде антивирустық дерекқордың жазбалары санының төменгі және жоғарғы мәндерін орнатуға болады.

  Әдепкі бойынша, параметр өшірулі.

- **Вирустарға соңғы рет тексеру уақыты**

  Егер бұл параметр қосулы болса, клиент құрылғыларын іздеу соңғы рет зиянды БҚ іздеу уақыты бойынша жүзеге асырылады. Енгізу өрістерінде зиянды БҚ іздеу соңғы рет жүргізілген аралықты көрсетуге болады.

  Әдепкі бойынша, параметр өшірулі.

- **Қауіптер анықталды**

  Егер бұл параметр қосулы болса, клиент құрылғыларын іздеу табылған вирустар санына сәйкес жүзеге асырылады. Енгізу өрістерінде табылған вирустар санының төменгі және жоғарғы мәндерін орнатуға болады.

  Әдепкі бойынша, параметр өшірулі.

Шифрлау бөлікшесінде таңдалған шифрлау алгоритмі негізінде таңдауға құрылғыларды қосу критерийлерін конфигурациялауға болады:

Шифрлау алгоритмі

Advanced Encryption Standard (AES) симметриялық блоктық шифрлау алгоритмі стандарты. Ашылмалы тізімнен шифрлау кілтінің өлшемін таңдай аласыз (56 Бит, 128 Бит, 192 Бит немесе 256 Бит).

Қолжетімді мәндер: *AES56*, *AES128*, *AES192*, және *AES256*.

Бағдарлама компоненттер бөлікшесі Kaspersky Security Center Web Console веб-консолінде сәйкес басқару плагиндері орнатылған қолданба құрамдастарының тізімін қамтиды.

Бағдарлама компоненттер қойыншасында, таңдалған бағдарламаға қатысты құрамдастар нұсқаларының нөмірлеріне сәйкес құрылғыларды іріктеуге қосу өлшемшартын белгілеуге болады:

- **Күйі**

  Басқарылатын бағдарлама Басқару серверіне жіберген құрамдастың күйіне сәйкес құрылғыларды іздеу. Келесі күйлердің бірін таңдауға болады: *Құрылғыдан деректер жоқ*, *Тоқтатылды*, *Кідіртілді*, *Іске қосулы*, *Орындалуда*, *Сәтсіз аяқталды*, *Орнатылмаған*, *Лицензия қолдау көрсетпейді*. Егер басқарылатын құрылғыда орнатылған бағдарламаның таңдалған құрамдасы көрсетілген күйге ие болса, құрылғы құрылғыны таңдауға кіреді.

  Бағдарламалар жіберген күйлер:

  - *Тоқтатылды* – құрамдас өшірілген және қазіргі уақытта жұмыс істемейді.
  - *Кідіртілді* – құрамдас, мысалы, пайдаланушы басқарылатын бағдарламада қорғанысты кідірткеннен кейін кідіртіледі.
  - *Іске қосылды* – құрамдас қазіргі уақытта инициализация процесінде.
  - *Орындалуда* – құрамдас қосулы және дұрыс жұмыс істейді.
  - *Сәтсіз аяқталды* – құрамдастың операциясын орындау кезінде қате пайда болды.
  - *Орнатылмаған* – пайдаланушы бағдарламаны іріктеп орнату кезінде орнату құрамдасын таңдамады.
  - *Лицензия қолдау көрсетпейді* - Лицензия таңдалған құрамдасқа қолданылмайды.

  Басқа күйлерден айырмашылығы, *Құрылғыдан деректер жоқ* күйін басқарылатын бағдарлама жібермейді. Бұл параметр, бағдарламаларда таңдалған құрамдас күйі туралы ақпарат жоқ екенін көрсетеді. Мысалы, бұл жағдай, таңдалған құрамдас құрылғыда орнатылған бағдарламалардың ешқайсысына тиесілі болмаса немесе құрылғы өшірулі болса, орын алуы мүмкін.

- **Нұсқа**

  Тізімде таңдалған құрамдас нұсқасының нөміріне сәйкес құрылғыларды іздеу. Сіз `3.4.1.0` сияқты нұсқа нөмірін енгізе аласыз, содан кейін таңдалған құрамдастың тең, анағұрлым ерте немесе анағұрлым кейінгі нұсқасы болуы керек пе екенін көрсете аласыз. Сондай-ақ, іздеуді көрсетілген нұсқадан басқа құрамдастың барлық нұсқалары бойынша конфигурациялауға болады.

Тегтер

Тегтер бөлімінде бұған дейін басқарылатын құрылғылардың сипаттамаларына қосылған кілт сөздер (тегтер) бойынша құрылғыларды таңдауға қосу өлшемшарттарын конфигурациялауға болады:

Кем дегенде бір көрсетілген тег сәйкес келген жағдайда қолдану

Егер бұл параметр қосулы болса, іздеу нәтижелерінде сипаттамасында таңдалған тегтердің кемінде біреуі бар құрылғылар көрсетіледі.

Егер бұл параметр өшірулі болса, іздеу нәтижелерінде тек сипаттамаларында барлық таңдалған тегтері бар құрылғылар көрсетіледі.

Әдепкі бойынша, параметр өшірулі.

Критерийге тегтерді қосу үшін **Қосу** түймесін басыңыз және **Тег** енгізу өрісін басу арқылы тегтерді таңдаңыз. Құрылғы таңдауында таңдалған тегтері бар құрылғыларды қосу немесе алып тастау керектігін көрсетіңіз.

- **Бұл тег бар барлық құрылғылар**

  Егер бұл нұсқа таңдалса, іздеу нәтижелерінде сипаттамасында таңдалған тегі бар құрылғылар көрсетіледі. Құрылғыларды іздеу үшін 0 немесе одан да ұзын таңбалардан тұратын кез келген жолды ауыстыратын * таңбасын пайдалануға болады.

  Әдепкі бойынша, осы нұсқа таңдалған.

- **Бұл тег жоқ барлық құрылғылар**

  Егер бұл нұсқа таңдалса, іздеу нәтижелерінде сипаттамасында таңдалған тегі жоқ құрылғылар көрсетіледі. Құрылғыларды іздеу үшін 0 немесе одан да ұзын таңбалардан тұратын кез келген жолды ауыстыратын * таңбасын пайдалануға болады.

Пайдаланушылар

Пайдаланушылар бөлімінде құрылғыларды операциялық жүйеге кірген пайдаланушылардың есептік жазбалары бойынша таңдауға қосу өлшемшарттарын конфигурациялауға болады.

- **Жүйеге соңғы кірген пайдаланушы**

  Бұл параметр қосылса, критерийді конфигурациялаған пайдаланушы есептік жазбасын таңдауға болады. Іздеу нәтижелеріне, жүйеге соңғы рет кіруді таңдалған пайдаланушы орындаған құрылғылар кіреді.

- **Жүйеге кемінде бір рет кірген пайдаланушы**

  Егер бұл параметр қосылса, **Шолу** түймесін басқан кезде пайдаланушы есептік жазбасын көрсетуге болады. Іздеу нәтижелеріне, аталған пайдаланушы жүйеге кемінде бір рет кірген құрылғылар кіреді.

Құрылғының иесі

Құрылғының иесі бөлімінде тіркелген құрылғы иелеріне, олардың рөлдеріне және қауіпсіздік топтарындағы мүшелігіне сәйкес таңдауға құрылғыларды қосу критерийлерін конфигурациялауға болады:

- **Құрылғының иесі**

  Ішкі қауіпсіздік тобынан құрылғы иесінің пайдаланушы атын таңдаңыз. Осы бөлімде пайдаланушылар мен пайдаланушы рөлдері туралы көбірек біліңіз.

  > Құрылғы иесі ретінде біреуден артық пайдаланушы тіркеле алмайды.

- **Device owner's membership in Active Directory security group**

  Құрылғы иесі тиесілі сыртқы Active Directory қауіпсіздік тобын таңдаңыз.

  Пайдаланушы, Active Directory қауіпсіздік тобының бөлігі немесе сол Active Directory қауіпсіздік тобының мүшесі болып табылатын топтың бөлігі болуы мүмкін.

- **Құрылғы иесінің рөлі**

  Құрылғы иесіне тағайындалған рөлді таңдаңыз. Пайдаланушы рөлдері туралы қосымша ақпарат алу үшін осы мақаланы қараңыз.

- **Құрылғы иесінің ішкі қауіпсіздік тобына мүшелігі**

  Құрылғының иесі тиесілі ішкі қауіпсіздік тобын таңдаңыз.

Құрылғы таңдауларынан құрылғылар тізімін экспорттау

Kaspersky Security Center Linux жүйесі бұл құрылғылар туралы ақпаратты құрылғы таңдауынан сақтауға және CSV немесе TXT файлына экспорттауға мүмкіндік береді.

Құрылғы таңдауынан құрылғылар тізімін экспорттау үшін:

1. Құрылғы таңдауынан құрылғылары бар кестені ашыңыз.
2. Экспорттағыңыз келетін құрылғыларды таңдау үшін келесі әдістердің бірін пайдаланыңыз:
   - Нақты бір құрылғыларды таңдау үшін олардың жанындағы жалаушаларды белгілеңіз.
   - Ағымдағы кесте бетіндегі барлық құрылғыларды таңдау үшін құрылғы кестесінің тақырыбында жалаушаны белгілеп, **Ағымдағы бетте барлығын таңдау** жалаушасын белгілеңіз.
   - Кестеден барлық құрылғыларды таңдау үшін құрылғы кестесінің тақырыбында жалаушаны белгілеп, **Барлығын таңдау** опциясын таңдаңыз.
3. **CSV файлына экспорттау** немесе **TXT файлына экспорттау** түймесін басыңыз. Кестеге енгізілген таңдалған құрылғылар туралы барлық ақпарат экспортталады.

Құрылғы кестесін сүзген болсаңыз, тек көрсетілген бағандардың сүзілген деректері экспортталатынын ескеріңіз.

Таңдаудағы басқару топтарынан құрылғыларды жою

Құрылғы үлгісімен жұмыс істегенде, құрылғыларды жою қажет басқару топтарымен жұмыс істеуге өтпей-ақ, құрылғыларды басқару топтарынан тікелей таңдаудың өзінде жоюға болады.

Басқару топтарынан құрылғыларды жою үшін:

1. Бағдарламаның негізгі терезесінде **Активтерді басқару → Құрылғы таңдаулары** немесе **Табу және орналастыру → Құрылғы таңдаулары** бөліміне өтіңіз.

2. Таңдаулар тізімінде құрылғыны таңдаудың атауын басыңыз.

   Бетте құрылғы таңдауына енгізілген құрылғылар туралы ақпараты бар кесте көрсетілген.

3. Жойғыңыз келетін құрылғыларды таңдап, **Жою** түймесін басыңыз.

   Нәтижесінде, таңдалған құрылғылар өздері кіретін басқару топтарынан жойылады.

Құрылғы тегтері

Kaspersky Security Center Linux құрылғыларға *тегтерді* тағайындауға мүмкіндік береді. Тег дегеніміз – құрылғыларды топтау, сипаттау немесе іздеу үшін пайдалануға болатын жолақ мәні. Құрылғыларға тағайындалған тегтер, құрылғылар іріктемесін жасау, құрылғыларды іздеу және құрылғыларды басқару топтары бойынша бөлу кезінде пайдаланылуы мүмкін.

Тегтерді құрылғыларға қолмен немесе автоматты түрде тағайындауға болады. Бөлек құрылғыны белгілегіңіз келсе, тегті қолмен тағайындауға болады. Автоматты түрде тегті тағайындауды Kaspersky Security Center Linux келесі тәсілдердің бірімен орындайды:

- Көрсетілген тег тағайындау ережелеріне сәйкес.
- Көрсетілген қолданбаға сәйкес.

Бір тегті тағайындау үшін тегтерді тағайындаудың әртүрлі тәсілдерін қолдану ұсынылады. Мысалы, тег ереже арқылы тағайындалса, ол тегті құрылғыларға қолмен тағайындау ұсынылмайды.

Тегтерді ережелер тағайындаса, тегтер құрылғыларға көрсетілген ережелерді сақтау арқылы автоматты түрде тағайындалады. Әрбір тегке бөлек ереже сай келеді. Ережелер құрылғының желілік сипаттарына, операциялық жүйеге, құрылғыда орнатылған бағдарламаларға және құрылғының басқа да сипаттарына қатысты қолданылуы мүмкін. Мысалы, CentOS операциялық жүйесінің басқаруымен жұмыс істейтін құрылғыларға `[CentOS]` тегін тағайындайтын ережені конфигурациялауыңызға болады. Содан соң, CentOS операциялық жүйесінің басқаруымен жұмыс істейтін барлық құрылғыларды таңдау және оларға тапсырма тағайындау үшін, осы тегті құрылғы таңдауларын жасау кезінде қолдануға болады.

Әрбір тэгке бір ғана автоматты тэг енгізу ережесін қосуға болады. Бір тэг үшін жаңа ереже жасасаңыз, алдыңғысы ауыстырылады.

Тег келесі жағдайларда құрылғыдан автоматты түрде жойылады:

- Құрылғы тегті белгілеу ережелерінің шарттарын қанағаттандыруды тоқтатады.
- Тегті белгілеу ережесі өшірулі немесе қосулы.

Әрбір Басқару серверіне арналған тегтер мен ережелер тізімдері барлық Басқару серверлері, соның ішінде негізгі Басқару сервері және қосалқы виртуалды Басқару серверлері үшін тәуелсіз болып саналады. Ереже тек өзі жасалған Басқару серверінің басқаруымен жұмыс істейтін құрылғыларға ғана қолданылады.

Құрылғы тегтерін жасау

Құрылғының тегін жасау үшін:

1. Бағдарламаның негізгі терезесінде **Активтерді басқару** → **Тегтер** → **Құрылғы тегтері** бөліміне өтіңіз.
2. **Қосу** түймесін басыңыз.
   Тег жасау терезесі көрсетіледі.
3. **Тег** өрісінде тег атауын енгізіңіз.
4. Өзгерістерін сақтау үшін **Сақтау** түймесін басыңыз.

Жаңа жасалған тег құрылғы тегтерінің тізімінде пайда болады.

Құрылғы тегтерін өзгерту

Құрылғының тегін қайта атау үшін:

1. Бағдарламаның негізгі терезесінде **Активтерді басқару** → **Тегтер** → **Құрылғы тегтері** бөліміне өтіңіз.
2. Қайта атау қажет болған тегті бөлектеңіз.
   Тегтің сипаттары терезесі ашылады.
3. **Тег** өрісінде тегтің атауын өзгертіңіз.
4. Өзгерістерін сақтау үшін **Сақтау** түймесін басыңыз.

Жаңартылған тег құрылғы тегтері тізімінде пайда болады.

Құрылғы тегтерін жою

Қолмен тағайындалған тегтерді ғана жоюға болады.

Қолмен тағайындалған құрылғының тегін жою үшін:

1. Бағдарламаның негізгі терезесінде **Активтерді басқару** → **Тегтер** → **Құрылғы тегтері** бөліміне өтіңіз.
   Тегтер тізімі көрсетіледі.
2. Жойғыңыз келетін құрылғы тегтерін таңдаңыз.

3. **Жою** түймесін басыңыз.

4. Пайда болған терезеде **Иә** түймесін басыңыз.

Құрылғының таңдалған тегі жойылды. Жойылған тег, ол тағайындалған барлық құрылғылардан автоматты түрде алынып тасталады.

Құрылғыға автоматты түрде тағайындалған тегті жойған кезде, ереже жойылмайды және құрылғы ереже шарттарына бірінші рет сай болған кезде тег жаңа құрылғыға тағайындалады. Ереже шарттарында көрсетілген тегті автоматты түрде тағайындау ережесін жойсаңыз, ол тағайындалған барлық құрылғылардан жойылады, бірақ тегтер тізімінен жойылмайды. Қажет болса, тізімнен тегті қолмен жоюға болады.

Егер бұл тег құрылғыға бағдарлама немесе Желілік агент арқылы тағайындалса, жойылған тег құрылғыдан автоматты түрде жойылмайды. Бұл тегтерді басқару үшін klscflag утилитасын пайдаланыңыз.

Тег тағайындалған құрылғыларды қарап шығу

Тегтері тағайындалған құрылғыларды қарап шығу үшін:

1. Бағдарламаның негізгі терезесінде **Активтерді басқару** → **Тегтер** → **Құрылғы тегтері** бөліміне өтіңіз.

2. Тағайындалған құрылғылар тізімін қарағыңыз келетін құрылғы үшін тег атауының жанындағы **Құрылғыларды көру** сілтемесінен өтіңіз.

   Сіз **Активтер (құрылғылар)** сілтемесін басқан тег бойынша сүзілген құрылғылары бар негізгі мәзірдің **Құрылғыларды көру** бөліміне қайта бағытталасыз.

3. Құрылғы тегтерінің тізіміне оралу үшін браузердегі **Артқа** түймесін басыңыз.

Тағайындалған тегі бар құрылғыларды көргеннен кейін, сіз жаңа тег жасап, тағайындай аласыз немесе бар тегті басқа құрылғыларға тағайындай аласыз. Бұл жағдайда, сүзгіні тег бойынша алып тастауға, құрылғыларды таңдауға және тегті тағайындауға тура келеді.

Құрылғыға тағайындалған тегтерді қарап шығу

Құрылғыға тағайындалған тегтерді қарап шығу үшін:

1. Бағдарламаның негізгі терезесінде **Активтерді басқару** → **Активтер (құрылғылар)** бөліміне өтіңіз.

2. Тегтерін қарап шығу қажет құрылғыны таңдаңыз.

3. Ашылған құрылғы сипаттары терезесінде **Тегтер** қойыншасын таңдаңыз.

Таңдалған құрылғыға тағайындалған тегтер тізімі көрсетіледі. **Тег белгіленді** бағанында тегтің қалай тағайындалғанын көруге болады.

Құралдар тақтасында келесі әрекеттерді орындауға болады:

- Құрылғыға басқа тэгті тағайындау.
- Бұрыннан тағайындалған тэгті өшіру.
- Басқару серверінде бар барлық құрылғы тэгтерін көру.

Тағайындалған тэгтерді құрылғыдан жергілікті түрде көру мүмкін емес.

Құрылғыға тегтерді қолмен тағайындау

Құрылғыға тегті қолмен тағайындау үшін:

1. Тег тағайындағыңыз келетін құрылғыға тағайындалған тегтерді қарап шығыңыз.
2. **Қосу** түймесін басыңыз.
3. Ашылған терезеде келесі әрекеттердің бірін орындаңыз:
   - Жаңа тегті жасау және қосу үшін **Жаңа тегті жасау** тармағын таңдап, тег атауын көрсетіңіз.
   - Қолданыстағы тегті таңдау үшін, **Бар тегті тағайындау** тармағын таңдап, ашылмалы тізімнен қажетті тегті таңдаңыз.
4. Өзгерістерді қолдану үшін **OK** түймесін басыңыз.
5. Өзгерістерін сақтау үшін **Сақтау** түймесін басыңыз.

Таңдалған тег құрылғыға тағайындалады.

Тағайындалған тегті құрылғыдан жою

Құрылғыдан тағайындалған тегті алып тастау үшін:

1. Бағдарламаның негізгі терезесінде **Активтерді басқару** → **Активтер (құрылғылар)** бөліміне өтіңіз.
2. Тегтерін қарап шығу қажет құрылғыны таңдаңыз.
3. Ашылған құрылғы сипаттары терезесінде **Тегтер** қойыншасын таңдаңыз.
4. Алып тастау қажет тегке қарама қарсы жалауша қойыңыз.

5. Тізімнің жоғарғы жағындағы **Тегті белгілеуден бас тарту** түймесін басыңыз.

6. Пайда болған терезеде **OK** түймесін басыңыз.

Тег құрылғыдан алып тасталады.

Құрылғыдан алынған тег жойылмайды. Қажет болса, оны қолмен жоюға болады.

Бағдарламалар немесе Желілік агент арқылы құрылғыға тағайындалған тегтерді қолмен жою мүмкін емес. Бұл тегтерді басқару үшін klscflag утилитасын пайдаланыңыз.

Құрылғыларға автоматты түрде тег қою ережелерін қарап шығу

Құрылғыларға автоматты түрде тег қою ережелерін қарап шығу үшін,

Келесі әрекеттердің бірін орындаңыз:

- Бағдарламаның негізгі терезесінде **Активтерді басқару** → **Тегтер** → **Автоматты түрде тег қою ережелері** бөліміне өтіңіз.
- Бағдарламаның негізгі терезесінде **Активтерді басқару** → **Тегтер** → **Құрылғы тегтері**, содан соң **Автоматты түрде тег қою ережелерін орнату** сілтемесінен өтіңіз.
- Құрылғыға тағайындалған тегтерді қараңыз, сосын **Автоматты түрде тег қою ережелерін орнату** түймесін басыңыз.

Құрылғыларға автоматты түрде тег қою ережелері тізімі көрсетіледі.

Құрылғыларға автоматты түрде тег қою ережелерін өзгерту

Құрылғыларға автоматты түрде тег қою ережелерін өзгерту үшін:

1. Құрылғыларға автоматты түрде тег қою ережелерін қарап шығыңыз.
2. Өзгерту қажет ережені таңдаңыз.

   Ереже параметрлері бар терезе ашылады.
3. Ереженің негізгі параметрлерін өзгертіңіз:

   a. **Ереженің атауы** өрісінде ереженің атауын өзгертіңіз.

   Атауы 256 таңбадан аспауы керек.

b. Келесі әрекеттердің бірін орындаңыз:

- Қосқышты **Ереже қосулы** күйіне қойып, ережені қосыңыз.
- Қосқышты **Ереже өшірулі** күйіне қойып, ережені өшіріңіз.

4. Келесі әрекеттердің бірін орындаңыз:

- Жаңа шартты қосқыңыз келсе, **Қосу** түймесін басыңыз және ашылған терезеде жаңа шарттың параметрлерін көрсетіңіз.
- Егер сіз қолданыстағы шартты өзгерткіңіз келсе, өзгертуді қажет ететін шартты бөлектеңіз және оның параметрлерін өзгертіңіз.
- Егер сіз шартты жойғыңыз келсе, жойылатын шарт атауының жанына жалаушаны қойып, **Жою** түймесін басыңыз.

5. Шарт параметрлері терезесінде **ОК** түймесін басыңыз.

6. Өзгерістерін сақтау үшін **Сақтау** түймесін басыңыз.

Өзгертілген ереже тізімде көрсетіледі.

Құрылғыларға автоматты түрде тег қою ережелерін жасау

Құрылғыларға автоматты түрде тег қою ережелерін жасау үшін:

1. Құрылғыларға автоматты түрде тег қою ережелерін қарап шығыңыз.

2. **Қосу** түймесін басыңыз.

   Жаңа ереже параметрлері бар терезе ашылады.

3. Ереженің негізгі параметрлерін көрсетіңіз:

   a. **Ереженің атауы** өрісінде ереженің атауын енгізіңіз.

   Атауы 256 таңбадан аспауы керек.

   b. Келесі әрекеттердің бірін орындаңыз:

   - Қосқышты **Ереже қосулы** күйіне қойып, ережені қосыңыз.
   - Қосқышты **Ереже өшірулі** күйіне қойып, ережені өшіріңіз.

   c. **Тег** өрісінде құрылғы тегінің жаңа атауын көрсетіңіз немесе тізімнен қолданыстағы құрылғы тегін таңдаңыз.

   Атауы 256 таңбадан аспауы керек.

4. Шартты таңдау өрісінде, жаңа шартты қосу үшін **Қосу** түймесін басыңыз.

   Жаңа шарт параметрлері бар терезе ашылады.

5. Шарттың атауын көрсетіңіз.

   Атауы 256 таңбадан аспауы керек. Шарттың атауы бір ереже шеңберінде бірегей болуы керек.

6. Ереженің іске қосылуын келесі шарттар бойынша конфигурациялаңыз. Бірнеше шарт таңдауға болады.

   - **Желі** – құрылғының желілік сипаттары (мысалы, құрылғының DNS атауы немесе құрылғының IP ішкі желісіне жатуы).

     Kaspersky Security Center Linux үшін пайдаланып жатқан дерекқорда тіркелімді ескере отырып сұрыптау конфигурацияланған болса, құрылғының DNS атауын көрсеткенде тіркемді ескеріңіз. Әйтпесе, автоматты түрде тег қою ережелері жұмыс істемейді.

   - **Бағдарламалар**— құрылғыда Желілік агенттің болуы, операциялық жүйенің түрі, нұсқасы және архитектурасы.

   - **Виртуалды машиналар** – құрылғының виртуалды машиналардың белгілі бір түріне тиесілі болуы.

   - **Бағдарламалар тізімдемесі** – құрылғыда әртүрлі өндірушілердің бағдарламаларының болуы.

7. Өзгерістерін сақтау үшін **OK** түймесін басыңыз.

   Қажет болса, бір ереже үшін бірнеше шарт белгілеуге болады. Бұл жағдайда, құрылғылар үшін шарттардың кемінде біреуі орындалса, тег оларға тағайындалады.

8. Өзгерістерін сақтау үшін **Сақтау** түймесін басыңыз.

Жасалған ереже, таңдалған Басқару сервері басқаратын құрылғыларда орындалады. Құрылғы параметрлері ереженің шарттарына сәйкес келсе, бұл құрылғыға тег тағайындалады.

Алдағыда, ереже келесі жағдайларда қолданылады:

- Сервердің жүктелуіне байланысты, автоматты түрде, үнемі.
- Ережені өзгерткеннен кейін.
- Ережені қолмен орындағаннан кейін.
- Басқару сервері ереже шарттарына сәйкес келетін өзгерістерді құрылғы параметрлерінде немесе осы құрылғыны қамтитын топ параметрлерінде анықтағаннан кейін.

Сіз бірнеше тег тағайындау ережесін жасай аласыз. Бірнеше тег тағайындау ережесін жасаған болсаңыз және осы ережелердің шарттары бір уақытты орындалып жатса, бір құрылғыға бірнеше тег тағайындалуы мүмкін. Барлық тағайындалған тегтер тізімін құрылғының сипаттарында қарап шыға аласыз.

Құрылғыларға автоматты түрде тег қою ережелерін орындау

Ереже орындалған кезде, осы ереженің сипаттарында көрсетілген тег ереженің сипаттарында көрсетілген шарттарға сәйкес келетін құрылғыға тағайындалады. Тек белсенді ережелерді орындауға болады.

Құрылғыларға автоматты түрде тег қою ережелерін орындау үшін:

1. Құрылғыларға автоматты түрде тег қою ережелерін қарап шығыңыз.
2. Орындалатын белсенді ережелерге қарама-қарсы жалаушаларды қойыңыз.
3. **Іске қосу ережесі** түймесін басыңыз.

Таңдалған ережелер орындалады.

Құрылғылардан автоматты түрде тег қою ережелерін жою

Құрылғыларға автоматты түрде тег қою ережелерін жою үшін:

1. Құрылғыларға автоматты түрде тег қою ережелерін қарап шығыңыз.
2. Жойғыңыз келетін ережеге қарама-қарсы жалаушаны қойыңыз.
3. **Жою** түймесін басыңыз.
4. Пайда болған терезеде **OK** түймесін басыңыз.

Таңдалған ереже жойылады. Осы ереженің сипаттарында көрсетілген тег тағайындалған барлық құрылғылардан алынады.

Құрылғыдан алынған тег жойылмайды. Қажет болса, оны қолмен жоюға болады.

klscflag утилитасы арқылы құрылғылар тегтерін басқару

Құрылғыға тэгтер жинағын тағайындау үшін тэгтерді тағайындағыңыз келетін клиент құрылғысында klscflag утилитасын іске қосу керек.

Klscflag утилитасы құрылғыға тағайындалған бар тэгтерді қайта жазады. Бұл пәрмендегі қажетті тэгтер жинағын көрсету арқылы тэгтерді қосуға немесе өшіруге болатынын білдіреді. Утилитада жеке тэгтерді қосу немесе өшіру үшін бөлек пәрмендер жоқ. Оның орнына сіз тэгтердің бүкіл жинағын өзгертесіз.

klscflag сияқты пәрмендердегі тэг атауларын көрсеткен кезде, барлығын бас әріппен алу сияқты бірдей әріп әдісін пайдаланған жөн. Барлығын бас әріппен қолдану арқылы ДҚБЖ конфигурациясына байланысты тек әрпі өзгеше тэгтерге қатысты ықтимал мәселелерге жол бермеуге көмектеседі.

Құрылғыға klscflag утилитасы көмегімен бір не бірнеше тэгті тағайындау үшін:

1. Түбірлік артықшылықтары бар есептік жазбада пәрмен сұрауын іске қосып, ағымдағы каталогті klscflag утилитасы бар каталогке ауыстырыңыз. klscflag утилитасы желілік агент орнатылған каталогте орналасқан. Әдепкі орнату каталогі — /opt/kaspersky/klnagent64/sbin/.

2. Келесі пәрмендердің бірін енгізіңіз:

   - Тэгтер жинағын тағайындау үшін:

     ```
     /opt/kaspersky/klnagent64/sbin/klscflag -ssvset -pv 1103/1.0.0.0 -s
     KLNAG_SECTION_TAGS_INFO -n KLCONN_HOST_TAGS -sv "[\"ТЕГ АТАУЫ 1\",\"ТЕГ АТАУЫ
     2\",\"ТЕГ АТАУЫ 3\"]" -svt ARRAY_T -ss "|ss_type = \"SS_PRODINFO\";"
     ```

     мұндағы `[\"ТЕГ АТАУЫ 1\",\"ТЕГ АТАУЫ 2\",\"ТЕГ АТАУЫ 3\]` — құрылғыға тағайындағыңыз келетін тэгтер тізімі.

     Шаршы жақшаларды бос қалдырсаңыз, құрылғыдан барлық тэгтер жойылады:

     ```
     /opt/kaspersky/klnagent64/sbin/klscflag -ssvset -pv 1103/1.0.0.0 -s
     KLNAG_SECTION_TAGS_INFO -n KLCONN_HOST_TAGS -sv "[]" -svt ARRAY_T -ss "|ss_type =
     \"SS_PRODINFO\";"
     ```

   - Бар тэгтер жинағына жаңа тэг тағайындау үшін:

     ```
     /opt/kaspersky/klnagent64/sbin/klscflag -ssvset -pv 1103/1.0.0.0 -s
     KLNAG_SECTION_TAGS_INFO -n KLCONN_HOST_TAGS -sv "[\"ЖАҢА ТЕГ АТАУЫ\",\"ТЕГ АТАУЫ
     1\",\"ТЕГ АТАУЫ 2\",\"ТЕГ АТАУЫ 3\"]" -svt ARRAY_T -ss "|ss_type =
     \"SS_PRODINFO\";"
     ```

     мұндағы `ЖАҢА ТЕГ АТАУЫ` is the name of the tag that you want to assign to your device and `ТЕГ АТАУЫ 1`, `ТЕГ АТАУЫ 2`, `ТЕГ АТАУЫ 3` — құрылғыға бұрыннан тағайындалған тэгтердің атаулары.

   - Құрылғыға бұрыннан тағайындалған басқа тэгтерді жоймай, белгілі бір тэгті жою үшін пәрменді тэгтердің жаңартылған жинағымен іске қосыңыз.

     Мысалы, ағымдағы тегтеріңіз `ТЕГ АТАУЫ 1`, `ТЕГ АТАУЫ 2`, `ТЕГ АТАУЫ 3` болса және `ТЕГ АТАУЫ 2` тэгін өшіргіңіз келсе, келесі пәрменді орындаңыз:

     ```
     /opt/kaspersky/klnagent64/sbin/klscflag -ssvset -pv 1103/1.0.0.0 -s
     KLNAG_SECTION_TAGS_INFO -n KLCONN_HOST_TAGS -sv "[\"ТЕГ АТАУЫ 1\",\"ТЕГ АТАУЫ 3\"]"
     -svt ARRAY_T -ss "|ss_type = \"SS_PRODINFO\";"
     ```

3. Желілік агент қызметін қайта іске қосу үшін келесі пәрменді орындаңыз:

   ```
   systemctl restart klnagent
   ```

   Klscflag утилитасы құрылғыға көрсетілген тэгтерді тағайындайды.

4. klscflag утилитасы берілген тэгтерді сәтті тағайындағанына көз жеткізу үшін құрылғыға тағайындалған тэгтерді көріңіз.

Сондай-ақ, құрылғылардың тегтерін қолмен тағайындауға болады.

Деректерді шифрлау және қорғау

Деректерді шифрлау портативті құрылғы немесе қатты диск ұрланған/жоғалған жағдайда ақпараттың абайсызда ағып кету қаупін азайтады. Сондай-ақ, деректерді шифрлау рұқсатсыз пайдаланушылар мен бағдарламалардың деректерге қол жеткізуіне жол бермейді.

Желіңізде Kaspersky Endpoint Security for Windows бағдарламасы орнатылған Windows операциялық жүйесі бар басқарылатын құрылғылар болса, деректерді шифрлау функциясын пайдалана аласыз. Бұл жағдайда Windows операциялық жүйесімен басқарылатын құрылғыларда шифрлаудың келесі түрлерін басқаруға болады:

- BitLocker дискісін шифрлау;
- Kaspersky дискісін шифрлау.

VDI жүйесінде шифрлауды қосуға кеңес бермейміз.

Kaspersky Endpoint Security for Windows құрамдастарының көмегімен, мысалы, шифрлауды қосуға немесе өшіруге, шифрланған қатты дискілердің тізімін көруге, шифрлау туралы есептерді құруға және көруге болады.

Шифрлауды конфигурациялау үшін Kaspersky Security Center Linux-те Kaspersky Endpoint Security for Windows саясатын конфигурациялаңыз. Kaspersky Endpoint Security for Windows бағдарламасы белсенді саясатқа сәйкес шифрлауды және шифрсыздауды орындайды. Ережелерді конфигурациялау бойынша толығырақ нұсқаулар және шифрлау ерекшеліктерінің сипаттамасы Kaspersky Endpoint Security for Windows онлайн-анықтамасында келтірілген.

Басқару серверінің иерархияларына арналған шифрлауды басқару әзірше Web Console-де қолжетімді емес. Шифрланған құрылғыларды басқару үшін негізгі басқару серверін пайдаланыңыз.

Пайдаланушы интерфейсінің параметрлері арқылы шифрлауды басқаруға қатысты кейбір интерфейс элементтерін көрсетуге немесе жасыруға болады.

Шифрланған қатты дискілер тізімін қарау

Kaspersky Security Center Linux бағдарламасында сіз шифрланған қатты дискілер туралы және дискілер деңгейінде шифрланған құрылғылар туралы ақпаратты қарай аласыз. Дискіде ақпарат шифрсызданғаннан кейін, диск тізімнен автоматты түрде алынып тасталады.

Шифрланған қатты дискілер тізімін қарау үшін,

Бағдарламаның негізгі терезесінде **Операциялар → Деректерді шифрлау және қорғау → Шифрланған құрылғы** бөліміне өтіңіз.

Бөлім мәзірде болмаса, демек, ол жасырылған. Пайдаланушы интерфейсі конфигурацияларында бөлімді көрсету үшін **Деректерді шифрлау және қорғау опциясын көрсету** параметрін қосыңыз.

Шифрланған қатты дискілер тізімін CSV немесе TXT пішіміндегі файлдарға экспорттауға болады. Бұл үшін **CSV файлына экспорттау** немесе **TXT файлына экспорттау** түймесін басыңыз.

Шифрлау оқиғалары тізімін қарау

Kaspersky Endpoint Security for Windows құрылғыларындағы деректерді шифрлау немесе шифрсыздау тапсырмаларын орындау барысында Kaspersky Security Center Linux бағдарламасына келесі типтегі оқиғалар туралы ақпарат жібереді:

- дискідегі орынның жетіспеушілігіне байланысты файлды шифрлау немесе шифрсыздау немесе шифрланған мұрағат жасау мүмкін емес;
- лицензиямен байланысты мәселелерге байланысты файлды шифрлау немесе шифрсыздау немесе шифрланған мұрағат жасау мүмкін емес;
- қатынасу құқықтарының болмауына байланысты файлды шифрлау немесе шифрсыздау немесе шифрланған мұрағат жасау мүмкін емес;
- бағдарламаға шифрланған файлға қатынасуға тыйым салынған;
- Белгісіз қателер.

Құрылғыларда деректерді шифрлау кезінде туындаған оқиғалар тізімін қарап шығу үшін:

бағдарламаның негізгі терезесінде **Операциялар → Деректерді шифрлау және қорғау → Шифрлау оқиғалары** бөліміне өтіңіз.

Бөлім мәзірде болмаса, демек, ол жасырылған. Пайдаланушы интерфейсі конфигурацияларында бөлімді көрсету үшін **Деректерді шифрлау және қорғау опциясын көрсету** параметрін қосыңыз.

Шифрланған қатты дискілер тізімін CSV немесе TXT пішіміндегі файлдарға экспорттауға болады. Бұл үшін **CSV файлына экспорттау** немесе **TXT файлына экспорттау** түймесін басыңыз.

Сондай-ақ, әрбір басқарылатын құрылғы үшін шифрлау оқиғалары тізімін қарап шығуға да болады.

Басқарылатын құрылғының шифрлау оқиғаларын қарап шығу үшін:

1. Бағдарламаның негізгі терезесінде **Активтерді басқару → Активтер (құрылғылар)** бөліміне өтіңіз.
2. Басқарылатын құрылғының атын басыңыз.
3. **Жалпы** қойындысында **Қорғаныс** бөліміне өтіңіз.
4. **Деректерді шифрлау қателерін қарап шығу** сілтемесінен өтіңіз.

Шифрлау туралы есептерді қалыптастыру және қарау

Сіз келесі есептерді құрастыра аласыз:

- Басқарылатын құрылғыларды шифрлаудың күйі туралы есеп. Бұл есепте түрлі басқарылатын құрылғылардың деректерін шифрлау туралы мәлімет көрсетілген. Мысалы, есепте конфигурацияланған шифрлау ережелері бар саясат қолданылатын құрылғылардың саны көрсетілген. Сондай-ақ, мысалы, қанша құрылғыны қайта іске қосу керектігін білуге болады. Сондай-ақ, есепте әрбір құрылғы үшін шифрлау технологиясы мен алгоритмі туралы ақпарат қамтылған.

- Жаппай сақтау құрылғыларының шифрлау күйлері туралы есеп беру. Бұл есеп, басқарылатын құрылғыларды шифрлау күйі туралы есепке ұқсас ақпаратты қамтиды, бірақ деректерді тек жаппай сақтау құрылғыларына және алынбалы жетектерге ғана ұсынады.

- Шифрланған құрылғыға қатынасу құқықтары туралы есеп. Бұл есеп шифрланған қатты дискіге қандай пайдаланушы есептік жазбалары кіретінін көрсетеді.

- Файлдарды шифрлау қателері туралы есеп. Есепте құрылғылардағы деректерді шифрлау немесе шифрсыздау тапсырмаларын орындау кезінде пайда болған қателер туралы ақпарат бар.

- Шифрланған файлдарға қатынасты бұғаттау туралы есеп. Есепте бағдарламалардың шифрланған файлдарға қатынасуын бұғаттау туралы ақпарат бар. Бұл есеп, авторизацияланбаған пайдаланушы немесе бағдарлама шифрланған файлдарға немесе қатты дискілерге қатынас алуға әрекеттеніп жатса, пайдалы болады.

Сіз **Мониторинг** → **Есептер** бөлімінде кез келген есептемені іске қоса аласыз. Сондай-ақ **Операциялар** → **Деректерді шифрлау және қорғау** бөлімінде келесі шифрлау есептерін жасауға болады:

- Жаппай сақтау құрылғыларының шифрлау күйлері туралы есеп беру
- Шифрланған құрылғыға қатынасу құқықтары туралы есеп
- Файлдарды шифрлау қателері туралы есеп

***Деректерді шифрлау және қорғау** бөлімінде шифрлау есептемесін іске қосу үшін:*

1. Интерфейс параметрлерінде **Деректерді шифрлау және қорғау опциясын көрсету** параметрі қосулы екеніне көз жеткізіңіз.
2. Саясат сипаттары терезесінде **Оқиғаларды конфигурациялау** қойыншасына өтіңіз.
3. **Маңызды** бөлімінде **Оқиғаны қосу** түймесін басып, *Файлдарды шифрлау/шифрын шешу ережелерін қолдану қатесі* оқиғасының жанындағы құсбелгіні қойыңыз.
4. **ОК** түймесін басыңыз.
5. Бағдарламаның негізгі терезесінде **Операциялар** → **Деректерді шифрлау және қорғау** бөліміне өтіңіз.

6. Келесі бөлімдердің бірін ашыңыз:

   - **Шифрланған құрылғы** – жаппай сақтау құрылғыларын шифрлау күйі туралы есепті немесе шифрланған құрылғыға қатынасу құқықтары туралы есепті іске қосады.

   - **Шифрлау оқиғалары** – файлдарды шифрлау қателері туралы есепті іске қосады.

7. Іске қосу қажет есептің атауын таңдаңыз.

Есепті іске қосу процесі басталады.

Шифрланған қатты дискіге автономды режимде қатынасу мүмкіндігін ұсыну

Пайдаланушы шифрланған құрылғыға қатынасуды сұрай алады, мысалы, егер Kaspersky Endpoint Security бағдарламасы басқарылатын құрылғыға орнатылмаған болса. Сұрауды алғаннан кейін сіз қатынасу кілті файлын жасап, оны пайдаланушыға жібере аласыз. Барлық пайдалану жағдайы және толық нұсқаулар Kaspersky Endpoint Security онлайн-анықтамасында келтірілген.

Kaspersky Endpoint Security for Windows жүйесінде шифрланған құрылғыға офлайн режимде кіру мүмкіндігін беру үшін:

1. Пайдаланушыдан қатынасты сұрау файлын алыңыз (FDERTC кеңейтімі бар файл). Kaspersky Endpoint Security for Windows бағдарламасында файлды жасау үшін Kaspersky Endpoint Security for Windows онлайн-анықтамасындағы нұсқауларды орындаңыз.

2. Бағдарламаның негізгі терезесінде **Операциялар → Деректерді шифрлау және қорғау → Шифрланған құрылғы** бөліміне өтіңіз.

   Шифрланған қатты дискілер тізімі көрсетіледі.

3. Пайдаланушы қатынас сұраған дискіні таңдаңыз.

4. **Құрылғыға офлайн режимде қатынасуға рұқсат беру** түймесін басыңыз.

5. Ашылған терезеде Kaspersky Endpoint Security for Windows плагинін таңдаңыз.

6. Kaspersky Endpoint Security for Windows бағдарламасына арналған онлайн анықтамадағы нұсқауларды орындаңыз (бөлімнің соңындағы Kaspersky Security Center Web Console арналған нұсқауларды қараңыз).

Содан соң, пайдаланушы алынған файлды шифрланған қатты дискіге қатынасу үшін және дискіде сақталатын деректерді оқу үшін пайдалана алады.

Басқару серверлері арасында шифрлау кілттерін беру

Егер басқарылатын құрылғыда деректерді шифрлау функциясы қосылса, шифрлау кілті Басқару серверінде сақталады. Шифрлау кілті шифрланған деректерге қол жеткізу және шифрлау саясатын басқару үшін қолданылады.

Шифрлау кілті келесі жағдайларда басқа Басқару серверіне берілуі керек:

- Құрылғыны басқа басқару серверіне тағайындау үшін басқарылатын құрылғыда желілік агентті қайта конфигурациялау. Егер бұл құрылғыда шифрланған деректер болса, шифрлау кілті мақсатты Басқару серверіне берілуі керек. Әйтпесе, деректерді шифрсыздау мүмкін болмайды.

- S1 басқару сервері басқаратын D1 құрылғысына қосылған алынбалы дискіні шифрлау, содан кейін бұл алынбалы дискіні S2 басқару сервері басқаратын D2 құрылғысына қосу. Алынбалы дискідегі деректерге қол жеткізу үшін шифрлау кілті S1 Басқару серверінен S2 Басқару серверіне берілуі керек.

- Файлды S1 басқару сервері басқаратын D1 құрылғысында шифрлау, содан кейін S2 басқару сервері басқаратын D2 құрылғысында файлға кіру мүмкіндігін алуға әрекеттену. Файлға қол жеткізу үшін шифрлау кілті S1 Басқару серверінен S2 Басқару серверіне берілуі керек.

Шифрлау кілттерін келесі тәсілдермен беруге болады:

- Автоматты түрде, шифрлау кілті берілуі тиісті екі Басқару серверінің сипаттарында **Шифрлау кілттерін алу үшін Басқару серверлерінің иерархиясын пайдалану** параметрін қосу арқылы. Егер бұл параметр Басқару серверлерінің бірі үшін өшірулі болса, шифрлау кілттерін автоматты түрде беру мүмкін емес.

  Басқару сервері сипаттарында **Шифрлау кілттерін алу үшін Басқару серверлерінің иерархиясын пайдалану** параметрін қосқанда, Басқару сервері шифрлау кілттерін негізгі Басқару серверіне (егер бар болса) жоғарыдағы иерархияның бір деңгейіне жібереді.

  Шифрланған деректерге қатынасуға тырысқанда, Басқару сервері алдымен өз қоймасынан шифрлау кілтін іздейді. Егер **Шифрлау кілттерін алу үшін Басқару серверлерінің иерархиясын пайдалану** параметрі қосулы болса және қажетті шифрлау кілті қоймада болмаса, Басқару сервері қажетті шифрлау кілтін алу үшін негізгі Басқару серверіне (егер бар болса) қосымша сұрау жібереді. Сұрау иерархияның ең жоғарғы деңгейіндегі Серверге дейін барлық негізгі Басқару серверлеріне жіберіледі.

- Шифрлау кілттері бар файлды экспорттау және импорттау арқылы, бір Басқару серверінен екіншісіне қолмен.

  Шифрлау кілттерін экспорттау және импорттау – бұл шифрлау кілттерін басқару функционалына кіретін әрекеттер. Осы әрекеттерді орындау мақсатында Kaspersky Security Center пайдаланушылары үшін функцияға кіру құқығын келесідей конфигурациялаңыз:

  - Шифрлау кілттерін қосалқы басқару серверінен экспорттайтын пайдаланушы үшін шифрлау кілтін басқару функциясына **Оқу** құқығын беру.

  - Қажетті Басқару серверіне шифрлау кілттерін импорттайтын пайдаланушы үшін Шифрлау кілтін басқару функциясына **Жазу** құқығын беру.

Иерархиядағы Басқару серверлері арасында шифрлау кілттерін автоматты түрде беруді қосу үшін:

1. Қажетті басқару серверінің сипаттарына өтіңіз:

   a. Негізгі мәзірден бөлім таңдаңыз (**Marketplace**, **Консольді шарлау** және **Параметрлер** бөлімдерінен басқа), содан кейін беттің жоғарғы жағындағы **Иерархияны көрсету** түймесін басыңыз.

   b. Ашылатын навигация панелінде тінтуір курсорын қажетті басқару серверінің үстіне апарып, параметрлер белгішесін (⚙) басыңыз.

   Сонымен қатар басқару серверінің атауын басуға болады, содан кейін негізгі мәзірде атауы көрсетілген кезде, сервер сипаттары терезесін ашу үшін оны негізгі мәзірде басыңыз.

2. Ашылатын сипаттар терезесінен **Шифрлау алгоритмі** бөлімін таңдаңыз.

3. **Шифрлау кілттерін алу үшін Басқару серверлерінің иерархиясын пайдалану** параметрін қосыңыз.

4. Өзгерістерді қолдану үшін **ОК** түймесін басыңыз.

Шифрлау кілттері келесі синхрондау кезінде (жүрек соғу жиілігі пакеті) негізгі Басқару серверіне (егер бар болса) жіберіледі. Бұл Басқару сервері, сұрау бойынша қосалқы Басқару серверіне өз қоймасынан шифрлау кілтін де ұсынады.

Басқару серверлері арасында шифрлау кілттерін қолмен беру үшін:

1. Шифрлау кілттерін экспорттағыңыз келетін басқару серверінің сипаттарына өтіңіз:

   a. Негізгі мәзірден бөлім таңдаңыз (**Marketplace**, **Консольді шарлау** және **Параметрлер** бөлімдерінен басқа), содан кейін беттің жоғарғы жағындағы **Иерархияны көрсету** түймесін басыңыз.

   b. Ашылатын навигация панелінде тінтуір курсорын қажетті басқару серверінің үстіне апарып, параметрлер белгішесін (⚙) басыңыз.

   Сонымен қатар басқару серверінің атауын басуға болады, содан кейін негізгі мәзірде атауы көрсетілген кезде, сервер сипаттары терезесін ашу үшін оны негізгі мәзірде басыңыз.

2. Ашылатын сипаттар терезесінен **Шифрлау алгоритмі** бөлімін таңдаңыз.

3. **Басқару серверінен шифрлау кілттерін экспорттау** түймесін басыңыз.

   Серверден шифрлау кілттерін экспорттайтын пайдаланушыға Шифрлау кілтін басқару функциясына **Оқу** құқығы берілгеніне көз жеткізіңіз.

4. **Шифрлау кілттерін экспорттау** терезесінде:

   - **Шолу** түймесін басыңыз, содан соң файлды қайда сақтау керектігін көрсетіңіз.
   - Файлды рұқсатсыз қатынасудан қорғау үшін құпиясөзді енгізіңіз.

   Құпиясөзді еске сақтаңыз. Жоғалған құпиясөзді қалпына келтіру мүмкін емес. Егер құпиясөз жоғалса, экспорттау процедурасын қайталау қажет. Сондықтан, құпиясөзді жазып алып, жақын жерде ұстаңыз.

5. Файлды басқа Басқару серверіне жіберіңіз, мысалы, ортақ қатынасы бар қалта немесе алынбалы жетек арқылы.

6. Шифрлау кілттерін импорттау қажет басқару серверінің сипаттарына өтіңіз.

7. Сипаттар терезесінен **Шифрлау алгоритмі** бөлімін таңдаңыз.

8. **Басқару серверіне шифрлау кілттерін импорттау** түймесін басыңыз.

   Серверге шифрлау кілттерін импорттайтын пайдаланушыға шифрлау кілтін басқару функциясына **Жазу** құқығы берілгеніне көз жеткізіңіз.

9. **Шифрлау кілттерін импорттау** терезесінде:

   - **Шолу** түймесін басып, шифрлау кілттерін қамтитын файлды таңдаңыз.
   - Құпиясөзді көрсетіңіз.

10. **OK** түймесін басыңыз.

    Шифрлау кілттері мақсатты Басқару серверіне жіберіледі.

Клиент құрылғылары үшін Басқару серверін ауыстыру

Нақты клиенттік құрылғылар үшін Басқару серверін басқасына өзгертуге болады. Ол үшін *Басқару серверін ауыстыру* тапсырмасын пайдаланыңыз.

Клиент құрылғылары жұмыс істейтін Басқару серверін басқа Сервермен ауыстыру үшін:

1. Құрылғыларды басқаратын Басқару серверіне қосылыңыз.
2. Басқару серверіне техникалық қызмет көрсету тапсырмасын жасаңыз.

   Жаңа тапсырма жасау шебері іске қосылады. Содан кейін, шебердің нұсқауларын орындаңыз. **Жаңа тапсырма** тапсырмасын жасау шебері терезесінде **Kaspersky Security Center 16.3** бағдарламасын және **Басқару серверін ауыстыру** тапсырма түрін таңдаңыз. Содан кейін Басқару серверін өзгерткіңіз келетін құрылғыларды көрсетіңіз:

   - **Басқару тобына тапсырманы белгілеу**

     Тапсырма бұрын жасалған басқару тобына кіретін құрылғыларға тағайындалады. Бар топтардың бірін көрсетуге немесе жаңа топ құруға болады.

     Мысалы, хабар белгілі бір басқару тобындағы құрылғыларға арналған болса, пайдаланушыларға хабар жіберу тапсырмасын іске қосу үшін осы параметрді пайдалануға болады.

     Тапсырма Басқару тобына тағайындалса, **Қауіпсіздік** қойындысы тапсырма сипаттары терезесінде көрсетілмейді, себебі топтық тапсырмалар олар тиесілі болып саналатын қауіпсіздік топтарының параметрлеріне бағынады.

   - **Құрылғының мекенжайларын қолмен белгілеу немесе тізімнен импорттау**

     Сіз DNS атауларын, IP мекенжайларын, сондай-ақ тапсырманы тағайындауды қажет ететін құрылғылардың IP мекенжайы ауқымдарын белгілей аласыз.

     Бұл параметрді белгіленген ішкі желі үшін тапсырманы орындау үшін пайдалануға болады. Мысалы, сіз бухгалтерлердің құрылғыларына белгілі бір бағдарламаны орната аласыз немесе вирус жұқтыруы мүмкін ішкі желідегі құрылғыларды тексере аласыз.

   - **Құрылғы таңдауына тапсырманы белгілеу**

     Тапсырма құрылғы таңдауларына кіретін құрылғыларға тағайындалады. Қолданыстағы таңдаулардың бірін көрсетуге болады.

Мысалы, операциялық жүйенің белгілі бір нұсқасы бар құрылғыларда тапсырманы іске қосу үшін осы параметрді пайдалануға болады.

3. Жасалған тапсырманы іске қосыңыз.

Тапсырма аяқталғаннан кейін, ол жасалған клиент құрылғылары тапсырма параметрлерінде көрсетілген басқару серверінің басқаруына өтеді.

Басқару сервері шифрлауды және деректерді қорғауды басқаруды қолдаса, онда *Басқару серверін ауыстыру* тапсырмасын жасау кезінде ескерту көрсетіледі. Ескертуде басқа Сервер басқаратын құрылғыларды ауыстырғаннан кейін құрылғыларда шифрланған деректер болған кезде пайдаланушыларға бұрын жұмыс істеген шифрланған деректерге ғана қатынасу мүмкіндігі берілетіні туралы ақпарат бар. Басқа жағдайларда, шифрланған деректерге қатынас берілмейді. Шифрланған деректерге қатынасу ұсынылмайтын скрипттерің толық сипаттамасы Kaspersky Endpoint Security for Windows анықтамасында берілген.

Басқару серверлері арасындағы қақтығыстардан аулақ болу

Егер желіде бірнеше Басқару сервері болса, олар бірдей клиент құрылғыларын көре алады. Бұл, мысалы, басқару серверінің басқа басқару сервері орнатқан қолданбаны орнатуына және басқа қайшылықтарға әкелуі мүмкін. Қолданбаның басқа басқару сервері басқаратын құрылғыға орнатылуына жол бермеу үшін **Тек осы Басқару сервері арқылы басқарылатын құрылғыларда орнату** тапсырма сипаттарындағы *Бағдарламаны қашықтан орнату* опциясын қосу керек.

Тек осы Басқару сервері арқылы басқарылатын құрылғыларда орнату опциясын қоссаңыз, содан кейін *Бағдарламаны қашықтан орнату* тапсырмасын іске қоссаңыз, құрылғылардың басқа басқару сервері арқылы басқарылатынын анықтау үшін тексеру орындалады. Басқа басқару сервері басқаратын құрылғылар үшін **Басқа Басқару серверімен басқарылады** төлсипаты `true` мәніне орнатылады. *Бағдарламаны қашықтан орнату* тапсырмасы бұл құрылғыларға қолданылмайды.

Басқа Басқару серверімен басқарылады төлсипат мәндері басқарылатын құрылғылар тізіміндегі және тағайындалмаған құрылғылар тізіміндегі **Басқа Басқару серверімен басқарылады** бағанында көрсетіледі.

Басқа Басқару серверімен басқарылады сипаты келесі операцияларға арналған өлшемшарт ретінде де қолданылуы мүмкін:

- Басқарылатын құрылғыларды көрсету
- Құрылғыны таңдаулары
- Құрылғыны жылжыту ережелері
- Автоматты түрде тег қою ережелері

Басқа Басқару серверімен басқарылады атрибутын қалпына келтіру үшін:

1. Kaspersky Security Center Web Console негізгі мәзірінде **Активтерді басқару → Тағайындалмаған құрылғылар** тармағына өтіңіз.

2. Қажетті құрылғыны таңдап, **Басқа Басқару сервері арқылы басқарылатын атрибутты өшіру** түймесін басыңыз.

Басқа Басқару серверімен басқарылады төлсипаты қалпына келтірілді.

Басқа Басқару серверіне қосылу шлюздері арқылы Басқару серверіне қосылған құрылғыларды жылжыту

Басқа басқару серверіне қосылу шлюздері арқылы басқару серверіне қосылған басқа құрылғыларды жылжыту. Мысалы, басқару серверінің басқа нұсқасын орнату қажет болғанда және артық уақыт алатындықтан, құрылғыларға желілік агентті қайта орнатқыңыз келмесе, осы әрекет қажет болуы мүмкін.

Нұсқауларда сипатталған пәрмендер әкімші құқықтары бар тіркелгі бойынша клиент құрылғыларда орындалуы керек.

Қосылым шлюзі арқылы қосылған құрылғыны басқа Басқару серверге жылжыту үшін:

1. Жаңа басқару серверіне ауысу үшін klmover утилитасын `-address <сервер мекенжайы>` параметрімен іске қосыңыз.

2. `klnagchk -nagwait -tl 4` пәрменді орындаңыз.

3. Жаңа қосылым шлюзін орнату үшін келесі пәрмендерді орындаңыз:

   - `klscflag -ssvset -pv klnagent -s FileTransfer -n ft_gateway_mode -sv false -svt BOOL_T -ss "|ss_type = \"SS_SETTINGS\";"`

   - `klscflag -ssvset -pv klnagent -s FileTransfer -n ft_gateway_loc -sv "<gateway_ip_or_name>" -svt STRING_T -ss "|ss_type = \"SS_SETTINGS\";"`

     Бұл жердегі `<gateway ip or name>` — интернеттен қолжетімді қосылым шлюзінің мекенжайы.

   - `klscflag -ssvset -pv klnagent -s FileTransfer -n ft_gateway_ssl_port -sv 13000 -svt INT_T -ss "|ss_type = \"SS_SETTINGS\";"`

     `13000` – қосылым шлюзі тыңдайтын TCP портының нөмірі.

4. Network AgentЖелілік агент қызметін іске қосу үшін `klnagchk -restart -tl 4` пәрменді орындаңыз.

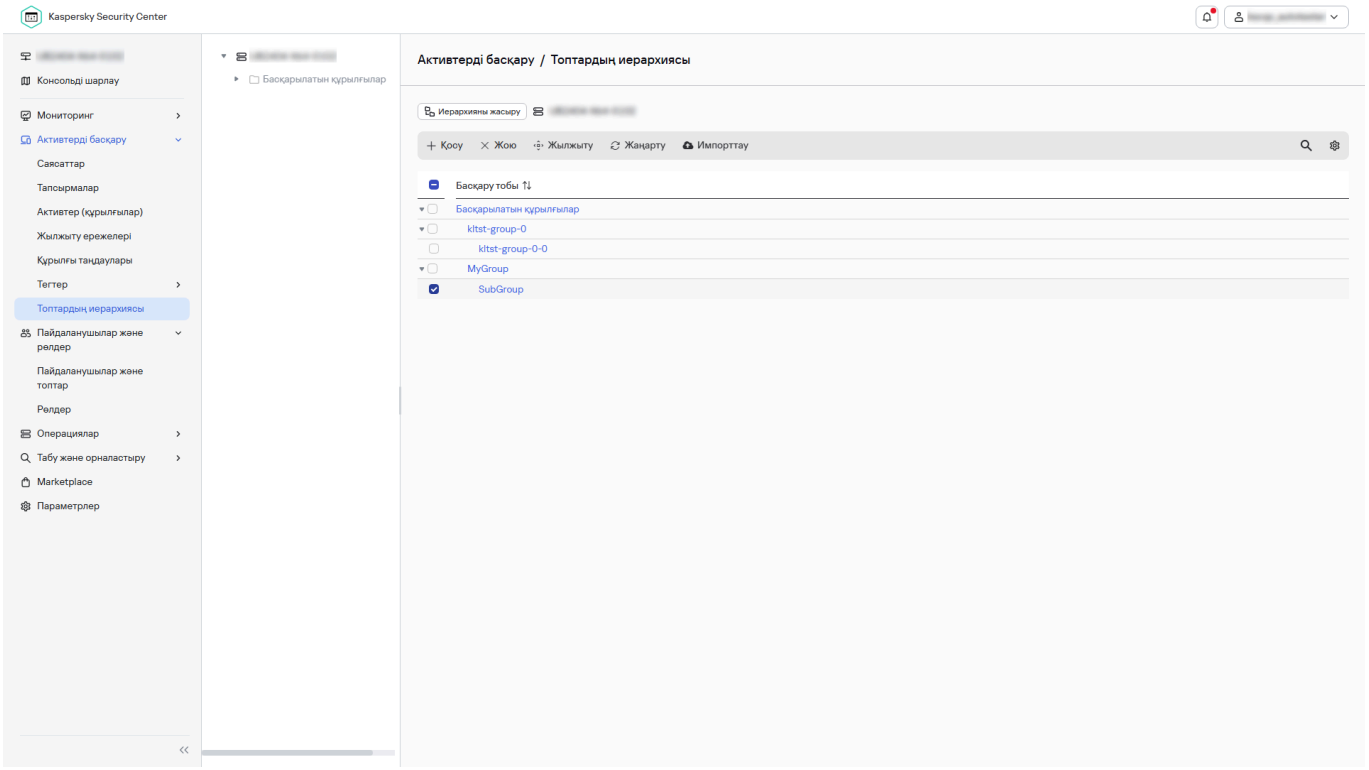
Құрылғы жаңа и серверіне жылжытылады және жаңа қосылым шлюзі арқылы қосылады.

Құрылғы белсенді емес кезде әрекеттерді қарау және конфигурациялау

Егер басқару тобының клиент құрылғылары белсенді болмаса, сіз бұл туралы хабарландыру ала аласыз. Сондай-ақ, мұндай құрылғыларды автоматты түрде жоюға болады.

Басқару тобында құрылғылар белсенді болмаған кезде әрекеттерді көру немесе конфигурациялау үшін:

1. Бағдарламаның негізгі терезесінде **Активтерді басқару** → **Топтардың иерархиясы** бөліміне өтіңіз.
2. Келесі жолдардың бірімен қажетті басқару тобының сипаттарына өтіңіз:
   - Басқару тобының атауын басыңыз.
   - Беттің жоғарғы жағындағы **Иерархияны көрсету** түймесін басыңыз. Ашылатын навигация панелінде тінтуір курсорын қажетті топ атауының үстіне апарып, параметрлер белгішесін (⚙) басыңыз.



Басқару топтары иерархиясы

Басқару тобының сипаттары терезесі ашылады.

3. Сипаттар терезесінде **Параметрлер** қойыншасына өтіңіз.
4. **Иелену** бөлімінде келесі параметрлерді қосыңыз немесе өшіріңіз:
   - **Тектік топтан иелену**

     Егер жалауша қойылса, осы бөлімдегі параметрлер клиент құрылғысы кіретін тектік топтан иеленетін болады. Егер жалауша қойылса, **Құрылғының желідегі белсенділігі** параметрлер блогындағы параметрлерді өзгерту мүмкін емес.

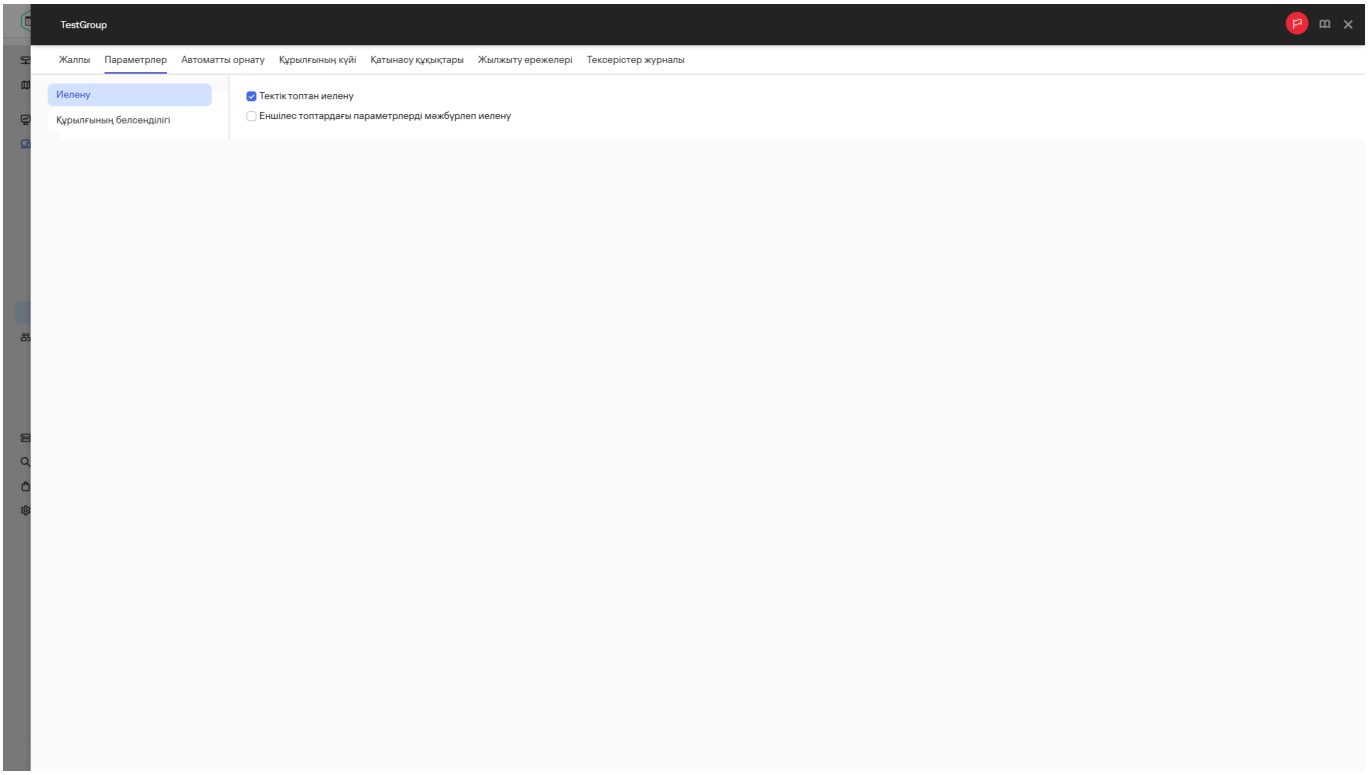
Бұл параметр тектік басқару тобы бар басқару тобы үшін ғана қолжетімді.

Әдепкі бойынша, параметр қосулы.

- **Еншілес топтардағы параметрлерді мәжбүрлеп иелену**

  Параметрлер мәндері еншілес топтарға бөлінеді, бірақ еншілес топтардың сипаттарында бұл параметрлер өзгертулер үшін қолжетімді емес.

  Әдепкі бойынша, параметр өшірулі.



Басқару тобының сипаттары

5. **Құрылғының белсенділігі** бөлімінде келесі параметрлерді қосыңыз немесе өшіріңіз:

   - **Құрылғы мынанша (тәулік) астам белсенді емес болса, әкімшіге хабарлау**

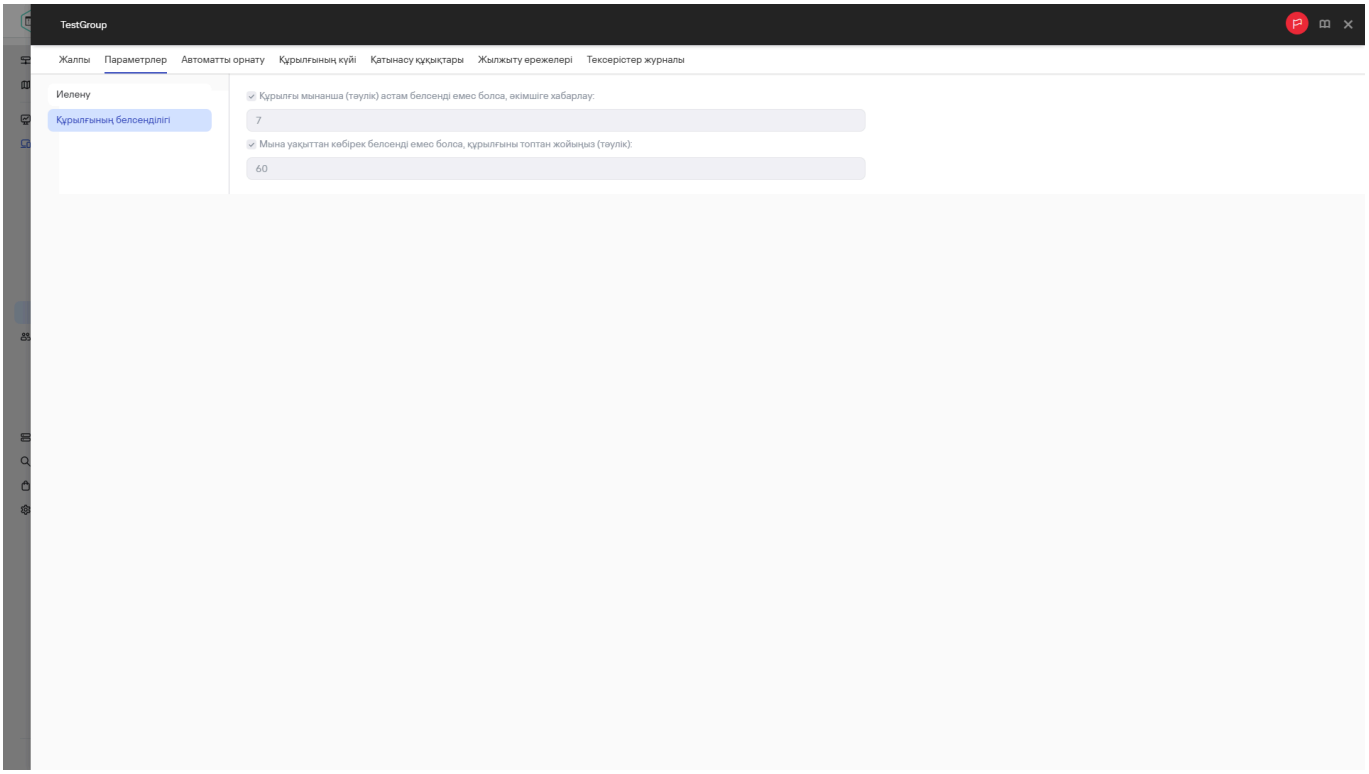
     Егер бұл параметр қосулы болса, әкімші құрылғылардың белсенді еместігі туралы хабарландыру алады. Енгізу өрісінде сіз **Құрылғы желіде ұзақ уақыт бойы белсенді емес болып қалды** оқиғасын қалыптастыратын уақыт аралығын орната аласыз. Әдепкі бойынша белгіленген уақыт аралығы – 7 күн.

     Әдепкі бойынша, параметр қосулы.

   - **Мына уақыттан көбірек белсенді емес болса, құрылғыны топтан жойыңыз (тәулік)**

     Егер бұл параметр қосулы болса, құрылғы басқару тобынан автоматты түрде жойылатын уақыт аралығын көрсетуге болады. Әдепкі бойынша белгіленген уақыт аралығы – 60 күн.

Әдепкі бойынша, параметр қосулы.



Басқару тобының сипаттары

6. **Сақтау** түймесін басыңыз.

Сіздің өзгертулеріңіз сақталды және қолданылды.

Құрылғылардың пайдаланушыларына хабар жіберу

Құрылғылардың пайдаланушыларына хабар жіберу үшін:

1. Бағдарламаның негізгі терезесінде **Тапсырмалар** бөліміне өтіңіз.
2. **Қосу** түймесін басыңыз.

   Жаңа тапсырма жасау шебері іске қосылады.
3. **Тапсырма түрі** ашылмалы тізімінде **Пайдаланушыға хабар жіберу** опциясын таңдаңыз.
4. Басқару топты, тапсырма қолданылатын құрылғылар немесе құрылғы таңдауын көрсету үшін параметр таңдаңыз.
5. Жасалған тапсырманы іске қосыңыз.

Тапсырма аяқталғаннан кейін, жасалған хабар таңдалған құрылғылардың пайдаланушыларына жіберілетін болады. **Пайдаланушыға хабар жіберу** тек Windows операциялық жүйесінің басқаруындағы құрылғылар үшін қолжетімді.

Клиент құрылғыларын қашықтан қосу, өшіру және қайта іске қосу

Kaspersky Security Center Linux бағдарламасы клиент құрылғыларын қашықтан басқаруға, қосуға, өшіруге және қайта іске қосуға мүмкіндік береді.

Клиент құрылғыларын қашықтан басқару үшін:

1. Бағдарламаның негізгі терезесінде **Тапсырмалар** бөліміне өтіңіз.
2. **Қосу** түймесін басыңыз.

   Жаңа тапсырма жасау шебері іске қосылады.
3. **Тапсырма түрі** ашылмалы тізімінен **Құрылғыларды басқару** опциясын таңдаңыз.
4. Басқару топты, тапсырма қолданылатын құрылғылар немесе құрылғы таңдауын көрсету үшін параметр таңдаңыз.
5. Пәрменді (қосу, өшіру немесе қайта жүктеу) таңдаңыз.
6. Қажет болса, өшіру және қайта іске қосу пәрмендері үшін келесі параметрлерді конфигурациялаңыз:
   - Пайдаланушыдағы сұрауға арналған хабарды және сұрауды қайталау мерзімін, сондай-ақ құрылғыны қайта іске қосуды немесе өшіруді қайта бастауды көрсету үшін **Пайдаланушыдан растауды сұрау** қосқышын қосыңыз.
   - **Бұғатталған сеанстарда бағдарламаларды келесі уақыттан кейін мәжбүрлеп жабу (мин)** құсбелгісін қойып, уақытты көрсетіңіз.

   Бұл параметрлер тек Windows клиенттік құрылғыларына қолданылады. Linux операциялық жүйесі бар құрылғылар тапсырма аяқталғаннан кейін бірден қайта іске қосылады немесе өшеді.
7. Жасалған тапсырманы іске қосыңыз.

Тапсырма аяқталғаннан кейін, пәрмен (қосу, өшіру немесе қайта іске қосу) таңдалған құрылғыларда орындалатын болады.

Басқарылатын құрылғыларға қашықтан қатынасу

Kaspersky Security Center Linux басқарылатын құрылғыларға қашықтан қосылуға мүмкіндік береді. Әкімші құрылғыда орнатылған желілік агент арқылы басқарылатын құрылғыға қашықтан қол жеткізе алады. Желілік агентті пайдаланып клиент құрылғысына қашықтан қосылу, клиент құрылғысының TCP және UDP порттары қатынасу үшін жабық болған жағдайда да мүмкін болады. Құрылғымен байланыс орнатқаннан кейін әкімші осы құрылғыда сақталған ақпаратқа толық рұқсат алады және оған орнатылған қолданбаларды басқара алады.

Қашықтағы қосылымды орнату әдістері Kaspersky Security Center Web Console бар құрылғыда қай платформа қолданылатынына байланысты. Kaspersky Security Center Web Console-ді басқару сервері құрылғысынан басқа құрылғыға, Windows немесе Linux негізіндегі құрылғыға орнатуға болады.

Linux құрылғысында орнатылған Kaspersky Security Center Web Console-ден келесі қосылымдарды орнатуға болады:

- Linux негізіндегі басқарылатын құрылғыға келесі әдіспен:
  - Қашықтағы компьютер қосылымы (RDP)
  - Virtual Network Computing (VNC)
- Windows негізіндегі басқарылатын құрылғыға келесі әдіспен:
  - Қашықтағы компьютер қосылымы (RDP)
  - Virtual Network Computing (VNC)

Windows құрылғысында орнатылған Kaspersky Security Center Web Console-ден келесі қосылымдарды орнатуға болады:

- Linux негізіндегі басқарылатын құрылғыға келесі әдіспен:
  - Қашықтағы компьютер қосылымы (RDP)
  - Virtual Network Computing (VNC)
- Windows негізіндегі басқарылатын құрылғыға келесі әдіспен:
  - Қашықтағы компьютер қосылымы (RDP)
  - Windows жұмыс үстелін бірлесіп пайдалану (WDS)

Microsoft Windows on Arm жұмыс істейтін құрылғыдан Kaspersky Security Center Web Console веб-консоліне кірген кезде басқарылатын құрылғыларға қашықтан қосылу қолдау көрсетілмейді.

Құрылғыға қашықтан қосылу үшін сізде мыналар болуы керек:

- klsctunnel утилитасы

  Kaspersky утилитасы басқарылатын құрылғылар мен басқару сервері арасындағы қосылымды туннельмен жіберу үшін пайдаланылады.

  Kaspersky Security Center Linux жүйесі TCP қосылымдарын Kaspersky Security Center Web Console-ден басқару сервері арқылы, содан кейін желілік агент арқылы басқарылатын құрылғыдағы көрсетілген портқа туннельмен жіберуге мүмкіндік береді. Туннельмен жіберу басқарылатын құрылғыдағы TCP портына Kaspersky Security Center Web Console орнатылған құрылғыдағы клиент қолданбасын қосуға арналған (Kaspersky Security Center Web Console мен мақсатты құрылғы арасында тікелей қосылу мүмкін болмаса).

Қашықтағы клиент құрылғысы мен Басқару сервері арасындағы байланысты туннельдеу, құрылғыда Басқару серверіне қосылуға арналған порт қолжетімді болмаған кезде қажет. Құрылғыдағы порт келесі жағдайларда қолжетімді болмауы мүмкін:

- Қашықтағы құрылғы NAT механизмі қолданылатын жергілікті желіге қосылған.
- Қашықтағы құрылғы Басқару серверінің жергілікті желісіне кіреді, бірақ оның порты желілік экранмен жабылған.

Қашықтағы қосылым Kaspersky Security Center Web Console арқылы немесе қолмен орнатылған кезде, утилитаны Kaspersky веб-сайтынан жүктеп алуға болады.

klsctunnel утилитасы Басқару сервері құрылғысында орнатылған және қашықтағы қосылымдардың барлық түрлері (RDP, VNC, WDS) үшін пайдаланылады.

- RDP немесе VNC клиенті

  RDP немесе VNC клиенті басқару сервері құрылғысына орнатылады. Бұл клиент klsctunnel утилитасы қамтамасыз ететін жергілікті қосылым үшін мекенжай мен портты пайдалану арқылы басқарылатын құрылғыға қашықтан қол жеткізуге мүмкіндік береді.

  Пайдаланушының ағымдағы қашықтағы компьютер сеансына RDP қосылымы пайдаланушыға хабарламай орнатылады. Әкімші сеансқа қосылғаннан кейін, құрылғы пайдаланушысы хабарландырусыз сеанстан ажыратылады.

- Windows компьютерлік бөлісу қызметі (тек Windows негізіндегі басқарылатын құрылғылар үшін)

  Бұл мүмкіндік осы сеанстағы пайдаланушыны ажыратпай-ақ клиент құрылғысындағы сеансқа қосылуға мүмкіндік береді. Бұл жағдайда, құрылғыдағы әкімші мен сеанс пайдаланушысы жұмыс үстеліне ортақ қол жеткізе алады.

  Қолданыстағы қашықтағы жұмыс үстелі сеансына қосылған кезде, құрылғыдағы осы сеанстың пайдаланушысы әкімшіден қосылуға сұрау алады. Құрылғыдағы қашықтан әрекет ету және оның нәтижелері туралы ақпарат Kaspersky Security Center Linux жасаған есептерде сақталмайды.

  Әкімші қашықтағы клиент құрылғысында әрекеттер аудитін конфигурациялай алады. Аудит кезінде қолданба әкімші ашқан және/немесе өзгерткен клиент құрылғысындағы файлдар туралы ақпаратты сақтайды.

Kaspersky Security Center Web Console бар Linux негізіндегі құрылғыдан Linux негізіндегі басқарылатын құрылғыға қашықтан қол жеткізу

Алдын ала талаптар

Бастамас бұрын, келесі әрекеттерді орындағаныңызға көз жеткізіңіз:

- Linux жұмыс істейтін басқарылатын құрылғыда желілік агенттің 15.3 немесе одан кейінгі нұсқасы орнатылған.
- RDP сервері Linux жүйесінде жұмыс істейтін басқарылатын құрылғыға орнатылады (басқарылатын құрылғыға қашықтағы компьютер қосылымы арқылы қосылсаңыз).

- VNC сервері Linux жүйесінде жұмыс істейтін басқарылатын құрылғыға орнатылады (басқарылатын құрылғыға Virtual Network Computing арқылы қосылсаңыз).

- RDP қосылымдарын туннельмен жіберуге арналған порт ашылады (Басқару серверінің сипаттары терезесінің **Қосылу порттары** бөлімінде **RDP қосылымдарын туннельмен жіберуге арналған ашық порт** опциясы қосылған).

- Әкімшіде RDP қосылымдарын орнату үшін **RDP сеанстарын бастау** құқығы бар (басқарылатын құрылғыға қашықтағы компьютер қосылымын пайдалану арқылы қосылсаңыз).

- Әкімшіде VNC үшін қосылымды туннельмен жіберу қосылымын орнатуға арналған **Туннельдеуді бастау** құқығы бар (басқарылатын құрылғыға Virtual Network Computing көмегімен қосылсаңыз).

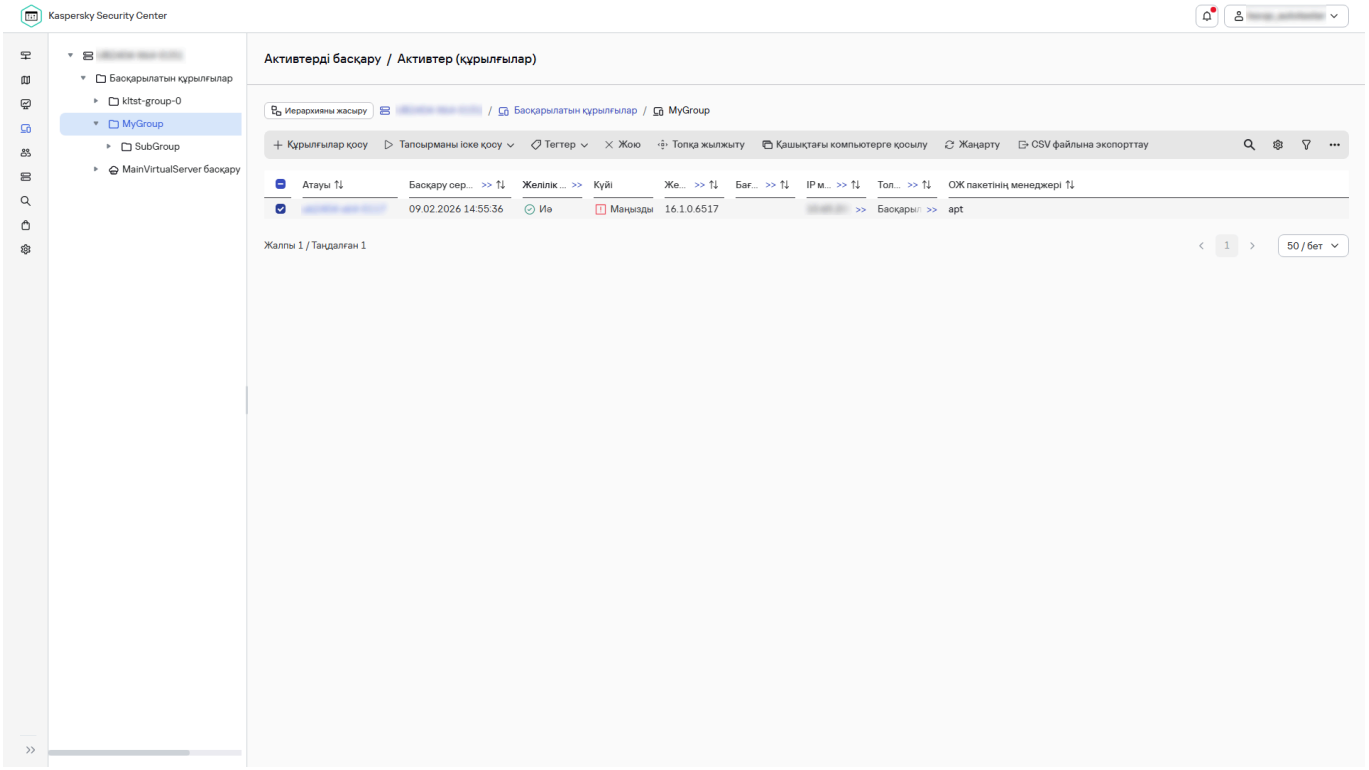
Linux негізіндегі құрылғыда ашылған Kaspersky Security Center Web Console арқылы RDP немесе VNC көмегімен Linux негізіндегі басқарылатын құрылғыға қосылу үшін:

1. Негізгі мәзірде **Активтерді басқару → Активтер (құрылғылар)** бөліміне өтіңіз немесе құрылғы таңдауын ашыңыз.

2. Қашықтан қосылатын басқарылатын құрылғының жанындағы құсбелгіні қойып, **Қашықтағы компьютерге қосылу** түймесін басыңыз.

   Қашықтағы компьютерге қосылу терезесі ашылады.

   Бірнеше құрылғыны, мобильді құрылғыны немесе macOS жүйесі бар құрылғыны таңдасаңыз, **Қашықтағы компьютерге қосылу** түймесі өшіріледі.



Басқарылатын құрылғылар тізімі

3. **Жүктеп алу** түймесін басу арқылы klsctunnel утилитасын жүктеп алыңыз, содан кейін оны іске қосыңыз.

Утилитаны жүктеп алған кезде, келесілерді ескеріңіз:

- klsctunnel утилитасының жаңартылған нұсқасын алу үшін басқару серверінің Kaspersky жаңарту серверлеріне қол жеткізе алатынын тексеріңіз.

  Тапсырмаларды басқару серверінің репозиторийіне жүктеп алу тапсырмасын іске қосып, жаңартулар көзі ретінде Kaspersky жаңарту серверлерін таңдай аласыз. Тапсырма сәтті аяқталса, басқару сервері Kaspersky жаңарту серверлеріне қол жеткізе алады.

- Утилита файлы жүктеп алу үшін қолжетімсіз болса, қате туралы хабар көрсетіледі. Бұл жағдайда утилитаны қолмен жүктеп алып, /var/opt/kaspersky/klnagent_srv directory жолындағы басқару серверінің құрылғысына қойыңыз.

4. **Қашықтағы компьютерге қосылу** терезесінде қосылым портын көрсетіңіз. Әдепкі бойынша порт нөмірі – 3389.

5. **Блоб жасау** түймесін басу арқылы кодталған қосылым параметрлері бар мәтіннің blob нысанын жасаңыз, содан кейін мәтінді klsctunnel утилитасындағы сәйкес өріске көшіріп, қойыңыз.

   Blob басқару сервері мен басқарылатын құрылғы арасында қосылым орнату үшін қажетті параметрлерді қамтиды. Blob үш минут жарамды. Оның мерзімі өтіп кетсе, жаңа blob жасаңыз.

6. Klsctunnel утилитасында прокси-серверді пайдалансаңыз, прокси-сервердің қосылым параметрлерін көрсетіңіз.

   klsctunnel утилитасы қашықтан қол жеткізу клиентінің жергілікті қосылымына арналған мекенжай мен портты көрсетеді.

   Утилита әкімшіге туннель қосылымын жабуға мүмкіндік береді. Туннель қосылымы жабылса, қашықтағы компьютерге арналған ағымдағы қосылым тоқтатылады.

7. Қашықтан қол жеткізу клиентін (RDP немесе VNC) іске қосыңыз және klsctunnel утилитасы қамтамасыз ететін мекенжай мен портты пайдалану арқылы оны басқарылатын құрылғыға қосыңыз.

Басқарылатын құрылғыға қосылым орнатылды және компьютер қашықтан қол жеткізу клиентінің терезесінде қолжетімді.

Kaspersky Security Center Web Console бар Linux негізіндегі құрылғыдан Windows негізіндегі басқарылатын құрылғыға қашықтан қол жеткізу

Қашықтағы компьютер қосылымы (RDP)

Алдын ала талаптар

Бастамас бұрын, келесі әрекеттерді орындағаныңызға көз жеткізіңіз:

- Басқарылатын құрылғының операциялық жүйе параметрлерінде қашықтан қосылуға рұқсат етіледі.

- Windows жүйесімен жұмыс істейтін басқарылатын құрылғыда желілік агенттің 13.0 немесе одан кейінгі нұсқасы орнатылған.

- Әкімшіде RDP қосылымдарын орнатуға арналған **RDP сеанстарын бастау** құқығы бар.
- RDP қосылымдарын туннельмен жіберуге арналған порт ашылады (Басқару серверінің сипаттары терезесінің **Қосылу порттары** бөлімінде **RDP қосылымдарын туннельмен жіберуге арналған ашық порт** опциясы қосылған).

Linux негізіндегі құрылғыда ашылған Kaspersky Security Center Web Console арқылы RDP көмегімен Windows негізіндегі басқарылатын құрылғыға қосылу үшін:

1. Негізгі мәзірде **Активтерді басқару → Активтер (құрылғылар)** бөліміне өтіңіз немесе құрылғы таңдауын ашыңыз.
2. Қашықтан қосылатын басқарылатын құрылғының жанындағы құсбелгіні қойып, **Қашықтағы компьютерге қосылу** түймесін басыңыз.

   Қашықтағы компьютерге қосылу терезесі ашылады.

   Бірнеше құрылғыны, мобильді құрылғыны немесе macOS жүйесі бар құрылғыны таңдасаңыз, **Қашықтағы компьютерге қосылу** түймесі өшіріледі.
3. **Қашықтағы компьютерге қосылу** терезесінде **RDP** қосылым түрін таңдаңыз.
4. Басқарылатын құрылғының операциялық жүйе параметрлерінде қашықтағы қосылымға рұқсат етілмесе, **Параметрлерді өзгерту** түймесін басу арқылы орталықтан қашықтан қосылуға рұқсат беріңіз.

   Параметрлер дұрыс қолданылса, хабарландыру көрсетіледі. Сондай-ақ басқарылатын құрылғыда **Параметрлер → Жүйе → Қашықтағы компьютер** бөлімінде **Қашықтағы компьютерді қосу** опциясы қосылады.

   Басқарылатын құрылғының операциялық жүйе параметрлерінде қашықтағы қосылымға рұқсат етілсе, **Параметрлерді өзгерту** түймесі көрсетілмейді.
5. **Жүктеп алу** түймесін басу арқылы klsctunnel утилитасын жүктеп алыңыз, содан кейін оны іске қосыңыз.

   Утилитаны жүктеп алған кезде, келесілерді ескеріңіз:

   - klsctunnel утилитасының жаңартылған нұсқасын алу үшін басқару серверінің Kaspersky жаңарту серверлеріне қол жеткізе алатынын тексеріңіз.

     Тапсырмаларды басқару серверінің репозиторийіне жүктеп алу тапсырмасын іске қосып, жаңартулар көзі ретінде Kaspersky жаңарту серверлерін таңдай аласыз. Тапсырма сәтті аяқталса, басқару сервері Kaspersky жаңарту серверлеріне қол жеткізе алады.
   - Утилита файлы жүктеп алу үшін қолжетімсіз болса, қате туралы хабар көрсетіледі. Бұл жағдайда утилитаны қолмен жүктеп алып, /var/opt/kaspersky/klnagent_srv directory жолындағы басқару серверінің құрылғысына қойыңыз.
6. **Блоб жасау** түймесін басу арқылы кодталған қосылым параметрлері бар мәтіннің blob нысанын жасаңыз, содан кейін мәтінді klsctunnel утилитасындағы сәйкес өріске көшіріп, қойыңыз.

   Blob басқару сервері мен басқарылатын құрылғы арасында қосылым орнату үшін қажетті параметрлерді қамтиды. Blob үш минут жарамды. Оның мерзімі өтіп кетсе, жаңа blob жасаңыз.
7. Klsctunnel утилитасында прокси-серверді пайдалансаңыз, прокси-сервердің қосылым параметрлерін көрсетіңіз.

   klsctunnel утилитасы қашықтағы құрылғыға қосылымның мекенжайы мен портын көрсетеді.

Утилита әкімшіге туннель қосылымын жабуға мүмкіндік береді. Туннель қосылымы жабылса, қашықтағы компьютерге арналған ағымдағы қосылым тоқтатылады.

8. RDP клиентін іске қосыңыз және оны klsctunnel утилитасы қамтамасыз ететін мекенжай мен портты пайдалану арқылы басқарылатын құрылғыға қосыңыз.

Басқарылатын құрылғыға қосылым орнатылды және компьютер RDP клиент терезесінде қолжетімді.

Пайдаланушының қашықтағы жұмыс үстелінің қолданыстағы сеансына қосылу, пайдаланушыны хабарландырусыз жүзеге асырылады. Әкімші сеансқа қосылғаннан кейін, құрылғы пайдаланушысы хабарландырусыз сеанстан ажыратылады.

Virtual Network Computing жүйесі (VNC)

Алдын ала талаптар

Бастамас бұрын, келесі әрекеттерді орындағаныңызға көз жеткізіңіз:

- Windows жүйесімен жұмыс істейтін басқарылатын құрылғыда желілік агенттің 13.0 немесе одан кейінгі нұсқасы орнатылған.
- Windows іске қосылған басқарылатын құрылғыға VNC сервері орнатылады.
- Әкімшіде VNC үшін туннель қосылымын орнатуға арналған **Туннельдеуді бастау** құқығы бар.
- RDP қосылымдарын туннельмен жіберуге арналған порт ашылады (Басқару серверінің сипаттары терезесінің **Қосылу порттары** бөлімінде **RDP қосылымдарын туннельмен жіберуге арналған ашық порт** опциясы қосылған).

Linux негізіндегі құрылғыда ашылған Kaspersky Security Center Web Console арқылы VNC көмегімен Windows негізіндегі басқарылатын құрылғыға қосылу үшін:

1. Негізгі мәзірде **Активтерді басқару** → **Активтер (құрылғылар)** бөліміне өтіңіз немесе құрылғы таңдауын ашыңыз.
2. Қашықтан қосылатын басқарылатын құрылғының жанындағы құсбелгіні қойып, **Қашықтағы компьютерге қосылу** түймесін басыңыз.

   Қашықтағы компьютерге қосылу терезесі ашылады.

   Бірнеше құрылғыны, мобильді құрылғыны немесе macOS жүйесі бар құрылғыны таңдасаңыз, **Қашықтағы компьютерге қосылу** түймесі өшіріледі.
3. **Қашықтағы компьютерге қосылу** терезесінде **VNC** қосылым түрін таңдаңыз.
4. **Жүктеп алу** түймесін басу арқылы klsctunnel утилитасын жүктеп алыңыз, содан кейін оны іске қосыңыз.

   Утилита файлы жүктеп алу үшін қолжетімсіз болса, қате туралы хабар көрсетіледі. Бұл жағдайда утилитаны қолмен жүктеп алыңыз.
5. **Қашықтағы компьютерге қосылу** терезесінде VNC қосылым портын көрсетіңіз. Әдепкі бойынша порт нөмірі – 5900.

6. **Блоб жасау** түймесін басу арқылы кодталған қосылым параметрлері бар мәтіннің blob нысанын жасаңыз, содан кейін мәтінді klsctunnel утилитасындағы сәйкес өріске көшіріп, қойыңыз.

   Blob басқару сервері мен басқарылатын құрылғы арасында қосылым орнату үшін қажетті параметрлерді қамтиды. Blob үш минут жарамды. Оның мерзімі өтіп кетсе, жаңа blob жасаңыз.

7. Klsctunnel утилитасында прокси-серверді пайдалансаңыз, прокси-сервердің қосылым параметрлерін көрсетіңіз.

   klsctunnel утилитасы VNC клиентінің жергілікті қосылымына арналған мекенжай мен портты көрсетеді.

   Утилита қашықтағы пайдаланушыға туннель қосылымын жабуға мүмкіндік береді. Туннель қосылымы жабылса, қашықтағы компьютерге арналған ағымдағы қосылым тоқтатылады.

8. VNC клиентін іске қосыңыз және оны klsctunnel утилитасы қамтамасыз ететін мекенжай мен портты пайдалану арқылы басқарылатын құрылғыға қосыңыз.

Басқарылатын құрылғыға қосылым орнатылды және жұмыс үстелі VNC клиентінің терезесінде қолжетімді.

Kaspersky Security Center Web Console бар Windows негізіндегі құрылғыдан Linux негізіндегі басқарылатын құрылғыға қашықтан қол жеткізу

Қашықтағы компьютер қосылымы (RDP)

Алдын ала талаптар

Бастамас бұрын, келесі әрекеттерді орындағаныңызға көз жеткізіңіз:

- Linux іске қосылған басқарылатын құрылғыға RDP сервері орнатылады.
- Linux жұмыс істейтін басқарылатын құрылғыда желілік агенттің 15.3 немесе одан кейінгі нұсқасы орнатылған.
- Әкімшіде RDP қосылымдарын орнатуға арналған **RDP сеанстарын бастау** құқығы бар.
- RDP қосылымдарын туннельмен жіберуге арналған порт ашылады (Басқару серверінің сипаттары терезесінің **Қосылу порттары** бөлімінде **RDP қосылымдарын туннельмен жіберуге арналған ашық порт** опциясы қосылған).

Windows негізіндегі құрылғыда ашылған Kaspersky Security Center Web Console арқылы RDP көмегімен Linux негізіндегі басқарылатын құрылғыға қосылу үшін:

1. Негізгі мәзірде **Активтерді басқару** → **Активтер (құрылғылар)** бөліміне өтіңіз немесе құрылғы таңдауын ашыңыз.
2. Қашықтан қосылатын басқарылатын құрылғының жанындағы құсбелгіні қойып, **Қашықтағы компьютерге қосылу** түймесін басыңыз.

   Қашықтағы компьютерге қосылу терезесі ашылады.

   Бірнеше құрылғыны, мобильді құрылғыны немесе macOS жүйесі бар құрылғыны таңдасаңыз, **Қашықтағы компьютерге қосылу** түймесі өшіріледі.

3. **Қашықтағы компьютерге қосылу** терезесінде **RDP** қосылым түрін таңдаңыз.

4. **Жүктеп алу** түймесін басу арқылы klsctunnel утилитасын жүктеп алыңыз, содан кейін оны іске қосыңыз.

   Утилитаны жүктеп алған кезде, келесілерді ескеріңіз:

   - klsctunnel утилитасының жаңартылған нұсқасын алу үшін басқару серверінің Kaspersky жаңарту серверлеріне қол жеткізе алатынын тексеріңіз.

     Тапсырмаларды басқару серверінің репозиторийіне жүктеп алу тапсырмасын іске қосып, жаңартулар көзі ретінде Kaspersky жаңарту серверлерін таңдай аласыз. Тапсырма сәтті аяқталса, басқару сервері Kaspersky жаңарту серверлеріне қол жеткізе алады.

   - Утилита файлы жүктеп алу үшін қолжетімсіз болса, қате туралы хабар көрсетіледі. Бұл жағдайда утилитаны қолмен жүктеп алып, /var/opt/kaspersky/klnagent_srv directory жолындағы басқару серверінің құрылғысына қойыңыз.

5. **Блоб жасау** түймесін басу арқылы кодталған қосылым параметрлері бар мәтіннің blob нысанын жасаңыз, содан кейін мәтінді klsctunnel утилитасындағы сәйкес өріске көшіріп, қойыңыз.

   Blob басқару сервері мен басқарылатын құрылғы арасында қосылым орнату үшін қажетті параметрлерді қамтиды. Blob үш минут жарамды. Оның мерзімі өтіп кетсе, жаңа blob жасаңыз.

6. Klsctunnel утилитасында прокси-серверді пайдалансаңыз, прокси-сервердің қосылым параметрлерін көрсетіңіз.

   Мұны істеу үшін **Прокси-серверді пайдалану** құсбелгісін қойып, қосылым параметрлерін көрсетіңіз.

7. **Портты ашу** түймесін басыңыз.

   Қашықтағы жұмыс үстеліне қосылу жүйесіне кіру терезесі ашылады.

8. Қазіргі уақытта Kaspersky Security Center Web Console-ге кірген есептік жазбаның кіру деректерін көрсетіңіз, содан кейін басқарылатын құрылғыға қосылыңыз.

   klsctunnel утилитасы қашықтағы құрылғыға қосылымның мекенжайы мен портын көрсетеді.

   Утилита әкімшіге туннель қосылымын жабуға мүмкіндік береді. Туннель қосылымы жабылса, қашықтағы компьютерге арналған ағымдағы қосылым тоқтатылады.

Клиент құрылғысына қосылғаннан кейін, клиент құрылғысының жұмыс үстелі Microsoft Windows қашықтан қосылу терезесінде қолжетімді.

Пайдаланушының қашықтағы жұмыс үстелінің қолданыстағы сеансына қосылу, пайдаланушыны хабарландырусыз жүзеге асырылады. Әкімші сеансқа қосылғаннан кейін, құрылғы пайдаланушысы хабарландырусыз сеанстан ажыратылады.

Virtual Network Computing жүйесі (VNC)

Алдын ала талаптар

Бастамас бұрын, келесі әрекеттерді орындағаныңызға көз жеткізіңіз:

- Linux жұмыс істейтін басқарылатын құрылғыда желілік агенттің 15.3 немесе одан кейінгі нұсқасы орнатылған.

- Linux іске қосылған басқарылатын құрылғыға VNC сервері орнатылады.

- Әкімшіде VNC үшін туннель қосылымын орнатуға арналған **Туннельдеуді бастау** құқығы бар.
- RDP қосылымдарын туннельмен жіберуге арналған порт ашылады (Басқару серверінің сипаттары терезесінің **Қосылу порттары** бөлімінде **RDP қосылымдарын туннельмен жіберуге арналған ашық порт** опциясы қосылған).

Windows негізіндегі құрылғыда ашылған Kaspersky Security Center Web Console арқылы VNC көмегімен Linux негізіндегі басқарылатын құрылғыға қосылу үшін:

1. Негізгі мәзірде **Активтерді басқару → Активтер (құрылғылар)** бөліміне өтіңіз немесе құрылғы таңдауын ашыңыз.
2. Қашықтан қосылатын басқарылатын құрылғының жанындағы құсбелгіні қойып, **Қашықтағы компьютерге қосылу** түймесін басыңыз.

   Қашықтағы компьютерге қосылу терезесі ашылады.

   Бірнеше құрылғыны, мобильді құрылғыны немесе macOS жүйесі бар құрылғыны таңдасаңыз, **Қашықтағы компьютерге қосылу** түймесі өшіріледі.
3. **Қашықтағы компьютерге қосылу** терезесінде **VNC** қосылым түрін таңдаңыз.
4. **Жүктеп алу** түймесін басу арқылы klsctunnel утилитасын жүктеп алыңыз, содан кейін оны іске қосыңыз.

   Утилита файлы жүктеп алу үшін қолжетімсіз болса, қате туралы хабар көрсетіледі. Бұл жағдайда утилитаны қолмен жүктеп алыңыз.
5. **Қашықтағы компьютерге қосылу** терезесінде VNC қосылым портын көрсетіңіз. Әдепкі бойынша порт нөмірі – 5900.
6. **Блоб жасау** түймесін басу арқылы кодталған қосылым параметрлері бар мәтіннің blob нысанын жасаңыз, содан кейін мәтінді klsctunnel утилитасындағы сәйкес өріске көшіріп, қойыңыз.

   Blob басқару сервері мен басқарылатын құрылғы арасында қосылым орнату үшін қажетті параметрлерді қамтиды. Blob үш минут жарамды. Оның мерзімі өтіп кетсе, жаңа blob жасаңыз.
7. Klsctunnel утилитасында прокси-серверді пайдалансаңыз, прокси-сервердің қосылым параметрлерін көрсетіңіз.

   Мұны істеу үшін **Прокси-серверді пайдалану** құсбелгісін қойып, қосылым параметрлерін көрсетіңіз.
8. **Портты ашу** түймесін басыңыз.

   klsctunnel утилитасы VNC клиентінің жергілікті қосылымына арналған мекенжай мен портты көрсетеді.

   Утилита қашықтағы пайдаланушыға туннель қосылымын жабуға мүмкіндік береді. Туннель қосылымы жабылса, қашықтағы компьютерге арналған ағымдағы қосылым тоқтатылады.
9. VNC клиентін іске қосыңыз және оны klsctunnel утилитасы қамтамасыз ететін мекенжай мен портты пайдалану арқылы басқарылатын құрылғыға қосыңыз.

Басқарылатын құрылғыға қосылым орнатылды және жұмыс үстелі VNC клиентінің терезесінде қолжетімді.

Kaspersky Security Center Web Console бар Windows негізіндегі құрылғыдан Windows негізіндегі басқарылатын құрылғыға қашықтан қол жеткізу

Қашықтағы компьютер қосылымы (RDP)

Алдын ала талаптар

Бастамас бұрын, келесі әрекеттерді орындағаныңызға көз жеткізіңіз:

- Windows жүйесімен жұмыс істейтін басқарылатын құрылғыда желілік агенттің 13.0 немесе одан кейінгі нұсқасы орнатылған.
- Әкімшіде RDP қосылымдарын орнатуға арналған **RDP сеанстарын бастау** құқығы бар.
- RDP қосылымдарын туннельмен жіберуге арналған порт ашылады (Басқару серверінің сипаттары терезесінің **Қосылу порттары** бөлімінде **RDP қосылымдарын туннельмен жіберуге арналған ашық порт** опциясы қосылған).
- Басқарылатын құрылғының операциялық жүйе параметрлерінде қашықтан қосылуға рұқсат етіледі.

Windows негізіндегі құрылғыда ашылған Kaspersky Security Center Web Console арқылы RDP көмегімен Windows негізіндегі басқарылатын құрылғыға қосылу үшін:

1. Негізгі мәзірде **Активтерді басқару** → **Активтер (құрылғылар)** бөліміне өтіңіз немесе құрылғы таңдауын ашыңыз.
2. Қашықтан қосылатын басқарылатын құрылғының жанындағы құсбелгіні қойып, **Қашықтағы компьютерге қосылу** түймесін басыңыз.

   Қашықтағы компьютерге қосылу терезесі ашылады.

   Бірнеше құрылғыны, мобильді құрылғыны немесе macOS жүйесі бар құрылғыны таңдасаңыз, **Қашықтағы компьютерге қосылу** түймесі өшіріледі.
3. **Қашықтағы компьютерге қосылу** терезесінде **Қашықтағы компьютер қосылымы** қосылым түрін таңдаңыз.
4. Басқарылатын құрылғының операциялық жүйе параметрлерінде қашықтағы қосылымға рұқсат етілмесе, **Параметрлерді өзгерту** түймесін басу арқылы орталықтан қашықтағы қосылымға рұқсат беріңіз.

   Параметрлер дұрыс қолданылса, хабарландыру көрсетіледі. Сондай-ақ басқарылатын құрылғыда **Параметрлер** → **Жүйе** → **Қашықтағы компьютер** бөлімінде **Қашықтағы компьютерді қосу** опциясы қосылады.

   Басқарылатын құрылғының операциялық жүйе параметрлерінде қашықтағы қосылымға рұқсат етілсе, **Параметрлерді өзгерту** түймесі көрсетілмейді.
5. **Жүктеп алу** түймесін басу арқылы klsctunnel утилитасын жүктеп алыңыз, содан кейін оны іске қосыңыз.

Утилитаны жүктеп алған кезде, келесілерді ескеріңіз:

- klsctunnel утилитасының жаңартылған нұсқасын алу үшін басқару серверінің Kaspersky жаңарту серверлеріне қол жеткізе алатынын тексеріңіз.

  Тапсырмаларды басқару серверінің репозиторийіне жүктеп алу тапсырмасын іске қосып, жаңартулар көзі ретінде Kaspersky жаңарту серверлерін таңдай аласыз. Тапсырма сәтті аяқталса, басқару сервері Kaspersky жаңарту серверлеріне қол жеткізе алады.

- Утилита файлы жүктеп алу үшін қолжетімсіз болса, қате туралы хабар көрсетіледі. Бұл жағдайда утилитаны қолмен жүктеп алып, /var/opt/kaspersky/klnagent_srv directory жолындағы басқару серверінің құрылғысына қойыңыз.

6. **Блоб жасау** түймесін басу арқылы кодталған қосылым параметрлері бар мәтіннің blob нысанын жасаңыз, содан кейін мәтінді klsctunnel утилитасындағы сәйкес өріске көшіріп, қойыңыз.

   Blob басқару сервері мен басқарылатын құрылғы арасында қосылым орнату үшін қажетті параметрлерді қамтиды. Blob үш минут жарамды. Оның мерзімі өтіп кетсе, жаңа blob жасаңыз.

7. Klsctunnel утилитасында прокси-серверді пайдалансаңыз, прокси-сервердің қосылым параметрлерін көрсетіңіз.

   Мұны істеу үшін **Прокси-серверді пайдалану** құсбелгісін қойып, қосылым параметрлерін көрсетіңіз.

8. **Портты ашу** түймесін басыңыз.

   Қашықтағы жұмыс үстеліне қосылу жүйесіне кіру терезесі ашылады.

9. Қазіргі уақытта Kaspersky Security Center Web Console-ге кірген есептік жазбаның кіру деректерін көрсетіңіз, содан кейін басқарылатын құрылғыға қосылыңыз.

   klsctunnel утилитасы қашықтағы құрылғыға қосылымның мекенжайы мен портын көрсетеді.

   Утилита әкімшіге туннель қосылымын жабуға мүмкіндік береді. Туннель қосылымы жабылса, қашықтағы компьютерге арналған ағымдағы қосылым тоқтатылады.

Клиент құрылғысына қосылғаннан кейін, клиент құрылғысының жұмыс үстелі Microsoft Windows қашықтан қосылу терезесінде қолжетімді.

Пайдаланушының қашықтағы жұмыс үстелінің қолданыстағы сеансына қосылу, пайдаланушыны хабарландырусыз жүзеге асырылады. Әкімші сеансқа қосылғаннан кейін, құрылғы пайдаланушысы хабарландырусыз сеанстан ажыратылады.

Windows жұмыс үстелін бірлесіп пайдалану (WDS)

Алдын ала талаптар

Бастамас бұрын, келесі әрекеттерді орындағаныңызға көз жеткізіңіз:

- Windows жүйесімен жұмыс істейтін басқарылатын құрылғыда желілік агенттің 13.0 немесе одан кейінгі нұсқасы орнатылған.
- Әкімшіде WDS қосылымын орнатуға арналған **Бұрыннан бар RDP сеанстарына қосылу** құқығы бар.
- Осалдық пен патчтарды басқаруға арналған лицензия қолжетімді.

- Әкімшінің жұмыс станциясында Microsoft Windows Vista операциялық жүйесі немесе одан кейінгі нұсқасы орнатылған. Басқару сервері орнатылған құрылғының операциялық жүйесінің түрі Windows компьютерлік бөлісу қызметі арқылы қосылуға шектеу емес.

  Windows компьютерлік бөлісу қызметі мүмкіндігінің Windows басылымында қамтылғанын тексеру және Windows тізілімінде CLSID\{32BE5ED2-5C86-480F-A914-0FF8885A1B3F} кілтінің бар екеніне көз жеткізу.

- Клиент құрылғысында Microsoft Windows Vista операциялық жүйесі немесе одан кейінгі нұсқасы орнатылған.

Windows негізіндегі құрылғыда ашылған Kaspersky Security Center Web Console арқылы VNC көмегімен Windows негізіндегі басқарылатын құрылғыға қосылу үшін:

1. Негізгі мәзірде **Активтерді басқару → Активтер (құрылғылар)** бөліміне өтіңіз немесе құрылғы таңдауын ашыңыз.

2. Қашықтан қосылатын басқарылатын құрылғының жанындағы құсбелгіні қойып, **Қашықтағы компьютерге қосылу** түймесін басыңыз.

   Қашықтағы компьютерге қосылу терезесі ашылады.

   Бірнеше құрылғыны, мобильді құрылғыны немесе macOS жүйесі бар құрылғыны таңдасаңыз, **Қашықтағы компьютерге қосылу** түймесі өшіріледі.

3. **Қашықтағы компьютерге қосылу** терезесінде **Windows компьютерлік бөлісу қызметін пайдалану** қосылым түрін таңдаңыз.

   Осалдықтар мен патчтарды басқару лицензиясы қолжетімді болмаса, қате туралы хабар көрсетіледі.

4. **Жүктеп алу** түймесін басу арқылы klsctunnel утилитасын жүктеп алыңыз, содан кейін оны іске қосыңыз.

   Утилита файлы жүктеп алу үшін қолжетімсіз болса, қате туралы хабар көрсетіледі. Бұл жағдайда утилитаны қолмен жүктеп алыңыз.

5. Таңдалған құрылғыда белсенді қолжетімді пайдаланушы сеанстарының тізімінде қосылғыңыз келетін сеансты таңдаңыз.

   Қашықтағы пайдаланушы қосылымға рұқсат беруі керек. Қашықтағы пайдаланушы қосылудан бас тартса немесе қашықтағы пайдаланушы күту уақытында қосылуға рұқсат бермесе, қате туралы хабар көрсетіледі.

6. **Блоб жасау** түймесін басу арқылы кодталған қосылым параметрлері бар мәтіннің blob нысанын жасаңыз, содан кейін мәтінді klsctunnel утилитасындағы сәйкес өріске көшіріп, қойыңыз.

   Blob басқару сервері мен басқарылатын құрылғы арасында қосылым орнату үшін қажетті параметрлерді қамтиды. Blob үш минут жарамды. Оның мерзімі өтіп кетсе, жаңа blob жасаңыз.

7. Klsctunnel утилитасында прокси-серверді пайдалансаңыз, прокси-сервердің қосылым параметрлерін көрсетіңіз.

   Мұны істеу үшін **Прокси-серверді пайдалану** құсбелгісін қойып, қосылым параметрлерін көрсетіңіз.

8. **Портты ашу** түймесін басыңыз.

   klsctunnel утилитасы VNC клиентінің жергілікті қосылымына арналған мекенжай мен портты көрсетеді.

   Утилита қашықтағы пайдаланушыға туннель қосылымын жабуға мүмкіндік береді. Туннель қосылымы жабылса, қашықтағы компьютерге арналған ағымдағы қосылым тоқтатылады.

Жұмыс үстеліне ортақ қатынасу жаңа терезеде іске қосылады. Құрылғымен өзара әрекеттескіңіз келсе, терезенің жоғарғы сол жақ бұрышындағы мәзір () белгішесін басып, **Интерактивті режим** тармағын таңдаңыз.

Ұялы құрылғыларды басқару үшін

Kaspersky Security Center арқылы мобильдік құрылғылар қорғанысын басқару мобильдік құрылғыларды басқару компоненті арқылы жүзеге асырылады. Қорғаныс қолданбасын іске қосу үшін әрбір мобильдік құрылғыда лицензия кілтін қосу керек. Егер сіз ұйым қызметкерлеріне тиесілі ұялы құрылғыларды басқаруды жоспарласаңыз, Ұялы құрылғыларды басқаруды қосыңыз және конфигурациялаңыз.

Мобильдік құрылғыларды басқару арқылы қызметкерлердің Android және iOS құрылғыларын басқаруға болады. Қорғаныс Android жүйесіне арналған Kaspersky Endpoint Security қолданбасы мен мобильдік құрылғыларға орнатылған iOS құрылғыларын басқару жүйесі арқылы қамтамасыз етіледі. Бұл мобильдік қолданба мобильдік құрылғыларды веб-қауіптерден, вирустардан және қауіп төндіретін басқа қолданбалардан қорғайды. Kaspersky Security Center Web Console арқылы орталықтандырылған басқару үшін Kaspersky Security Center Web Console бағдарламасы орнатылған құрылғыға келесі басқару веб-плагиндерін орнату қажет:

- Kaspersky Mobile Devices Protection and Management плагині.

  Kaspersky Mobile Devices Protection and Management плагині Android және iOS құрылғыларын Kaspersky Security Center Web Console веб-консолінде басқаруға мүмкіндік береді.

- iOS MDM серверінің параметрлері плагині.

  iOS MDM сервері параметрлерінің плагині iOS құрылғыларын басқару серверіне қосу және iOS құрылғыларын басқару үшін пайдаланылатын iOS MDM серверінің параметрлерін реттеуге мүмкіндік береді.

Қорғанысты орналастыру және мобильдік құрылғыларды басқару туралы ақпаратты Kaspersky Security for Mobile анықтамасынан және Kaspersky Secure Mobility Management

https://support.kaspersky.com/secure-mobility-management/9.0/216448
анықтамасынан қараңыз.

Firebase Cloud Messaging қолдану

Android құрылғыларына пәрмендерді уақтылы жеткізу үшін Kaspersky Security Center Linux push хабарландыру механизмін пайдаланады. Push хабарландырулары Android құрылғылары мен басқару сервері арасында Firebase Cloud Messaging (бұдан әрі FCM) арқылы алмасады. Kaspersky Security Center Web Console веб-консолінде Android құрылғыларын қызметке қосу үшін Firebase Cloud Messaging параметрлерін көрсетуге болады.

Firebase Cloud Messaging параметрлерін алу үшін Google есептік жазбаңыз болуы керек.

FCM қолдануды қосу үшін:

1. Kaspersky Security Center Web Console негізгі терезесінде **Активтерді басқару** → **Mobile** → **Devices** тармағын таңдаңыз.

2. Үш нүктелі (⋮) мәзірді ашып, **Forced Android device synchronization** опциясын таңдаңыз.

3. **Firebase project number** өрісінде FCM жіберушінің идентификаторын енгізіңіз.

4. **Private key** өрісінде жеке кілт файлын таңдаңыз.

   Басқару серверімен келесіде синхрондау үшін Android құрылғылары Firebase Cloud Messaging қызметіне қосылады.

Басқа Firebase жобасына ауысқанда, FCM жұмысы 10 минуттан кейін жалғасады.

FCM сервисі келесі мекенжайлар ауқымында жұмыс істейді:

- Android құрылғылары тарапынан 443 (HTTPS), 5228 (HTTPS), 5229 (HTTPS), 5230 (HTTPS) порттарына келесі мекенжайлардан кіру мүмкіндігі қажет:
  - google.com
  - fcm.googleapis.com
  - oauth2.googleapis.com
  - android.apis.google.com
  - немесе "Google ASN 15169" тізіміндегі барлық IP мекенжайларына
- Басқару сервері тарапынан 443-портқа (HTTPS) келесі мекенжайлардан қатынасу қажет:
  - fcm.googleapis.com
  - немесе "Google ASN 15169" тізіміндегі барлық IP мекенжайларына

Прокси сервер параметрлері Kaspersky Security Center Web Console сипаттарында көрсетілсе, онда бұл параметрлер FCM-мен әрекеттесу үшін пайдаланылады.

FCM орнату: Sender ID мен жабық кілт файлын алу

FCM конфигурациялау үшін:

1. Google порталында тіркелу.
2. Firebase консоліне өтіңіз.
3. Келесі әрекеттердің бірін орындаңыз:
   - Жобаны жасау үшін **Жоба жасау** түймесін басып, экрандағы нұсқауларды орындаңыз.
   - Бар жобаны ашыңыз.
4. Тегершік белгішесін басып, **Жоба параметрлері** тармағын таңдаңыз.

   Жоба параметрлері терезесі ашылады.
5. **Cloud Messaging** қойындысын таңдаңыз.

6. **Firebase Cloud Messaging API (V1)** бөліміндегі **Sender ID** өрісінен Sender ID көшіріп алыңыз.

7. **Қызметтің есептік жазбалары** қойындысын таңдап, **Жаңа жеке кілтті жасау** түймесін басыңыз.

8. Ашылған терезеде жеке кілт файлын жасау және жүктеп салу үшін **Кілтті жасау** түймесін басыңыз.

Firebase Cloud Messaging конфигурацияланған.

Жалпыға ортақ кілттер инфрақұрылымымен біріктіру

Сертификаттарды шығару әрекетін Microsoft Certification Authority (CA) бағдарламасымен жалпыға ортақ кілт инфрақұрылымы (PKI) арқылы интеграциялауға болады. PKI интеграциясы басқару серверінің домен пайдаланушыларына сертификаттар беруді жеңілдетуге арналған. Біріктіру нәтижесінде, сертификаттарды шығару автоматты түрде жүзеге асырылады.

Сертификаттар шығару үшін PKI интеграциясын реттеу туралы толық ақпаратты Kaspersky Secure Mobility Management анықтамасынан қараңыз.

Көрсетілген параметрлермен PKI интеграциясын орындауға және PKI-ны белгілі бір сертификат түрлері үшін сертификат көзі ретінде тағайындауға болады. PKI интеграциясы параметрлері барлық сертификат түрі үшін жеке әдепкі үлгіні орнатуға мүмкіндік береді.

Сертификаттар шығару үшін PKI интеграциясын пайдалану ерекшеліктері:

- PKI интеграциясы әдепкі бойынша өшірілген. PKI қосу және оның параметрлерін реттеу туралы толық ақпаратты Kaspersky Secure Mobility Management анықтамасынан қараңыз.

- Сертификатты шығару әрекеті желілік агент Windows арқылы жүзеге асады, ол басқару сервері мен Microsoft CA арасындағы интеграцияны іске қосады. Желілік агент орнатылған бірнеше құрылғы болуы мүмкін болғандықтан, Microsoft CA бағдарламасына қосылатын құрылғыны **Issuance rules** ережелерінде көрсетуге болады. Бұл құрылғыда PKI интеграциясы орындалатын есептік жазбаның сертификаттар қоймасында орнатылған Enrollment Agent (EA) сертификаты болуы керек. Сертификатты CA доменінің әкімшісі береді.

- PKI интеграциясы орындалатын есептік жазбаның домен пайдаланушысы болуы және *қызмет ретінде кіру* құқығы болуы керек.

- Kaspersky Security Center Linux бір уақытта тек бір PKI (Microsoft CA) интеграциясымен жұмыс істей алады.

Басқару топтарын басқару

Бұл бөлімде басқару топтарымен жұмыс істеу туралы ақпарат бар.

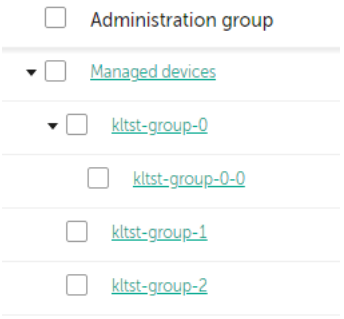
Басқару топтарымен келесі әрекеттерді орындауға болады:

- басқару тобының құрамына иерархияның кез келген деңгейлеріндегі салынған топтардың ерікті санын қосу;
- құрылғының басқару топтарының құрамына қосу;
- жеке құрылғыларды және тұтас топтарды басқа топтарға жылжыту арқылы басқару топтарының иерархиясын өзгерту;
- басқару топтарының құрамынан салынған топтар мен құрылғыларды жою;
- басқару топтарына қосалқы және виртуалды Басқару серверлерін қосу;
- құрылғыларды бір Сервердің басқару топтары құрамынан басқа Сервердің басқа топтарына тасымалдау;
- Kaspersky қандай бағдарламалары топ құрамына қосылатын құрылғыларға автоматты түрде орнатылатынын анықтаңыз.

Басқарғыңыз келетін басқару топтарына (немесе осы топтар тиесілі басқару серверіне) арналған **Басқару топтарын басқару** аймағында **Өзгерту** рұқсаты болса ғана, бұл әрекеттерді орындай аласыз.

Басқару топтарын жасау

Kaspersky Security Center орнатылғаннан кейін бірден басқару топтарының иерархиясында бір ғана Басқару тобы бар – **Басқарылатын құрылғылар**. Басқару топтарының иерархиясын құру кезінде **Басқарылатын құрылғылар** қалтасына құрылғылар мен виртуалды машиналарды қосып, салынған топтарды қосуға болады (төмендегі суретті қараңыз).

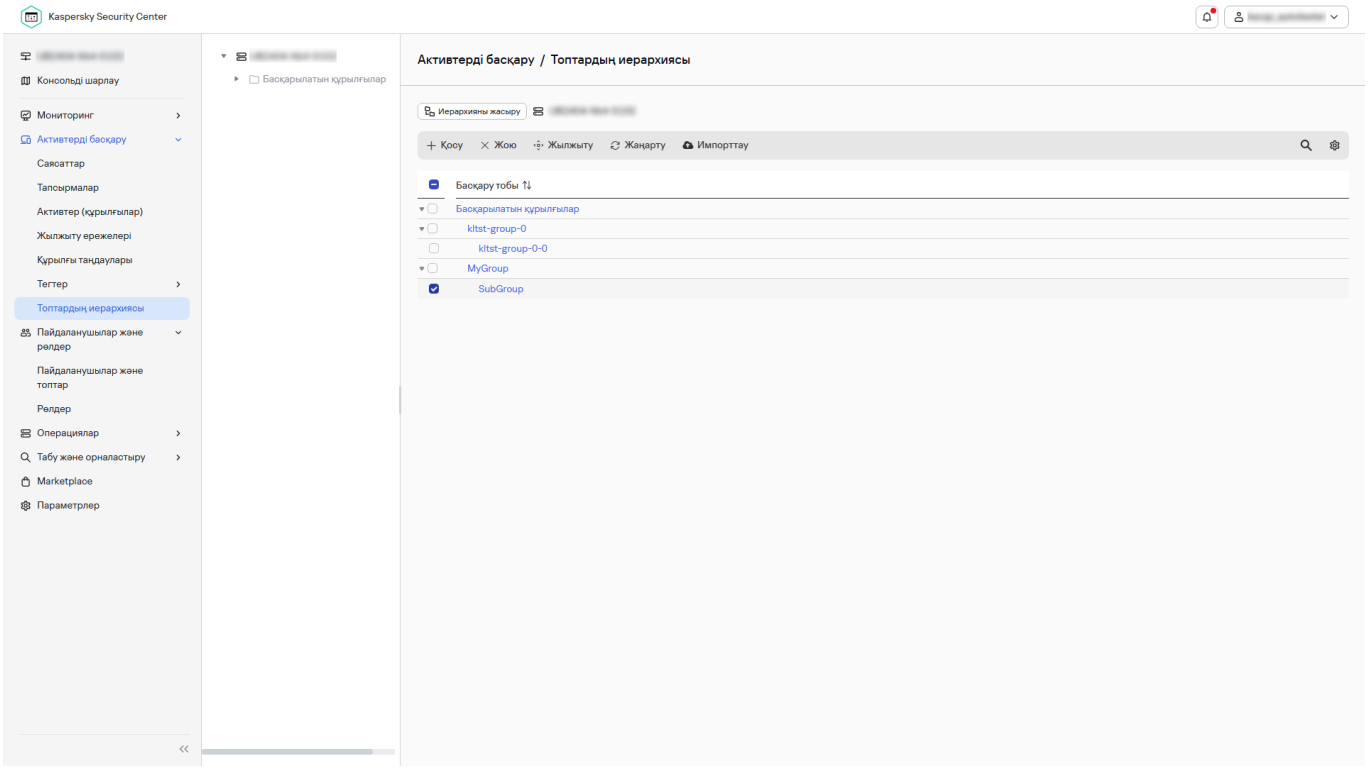


Басқару топтарының иерархиясын қарау

Басқару тобын жасау үшін:

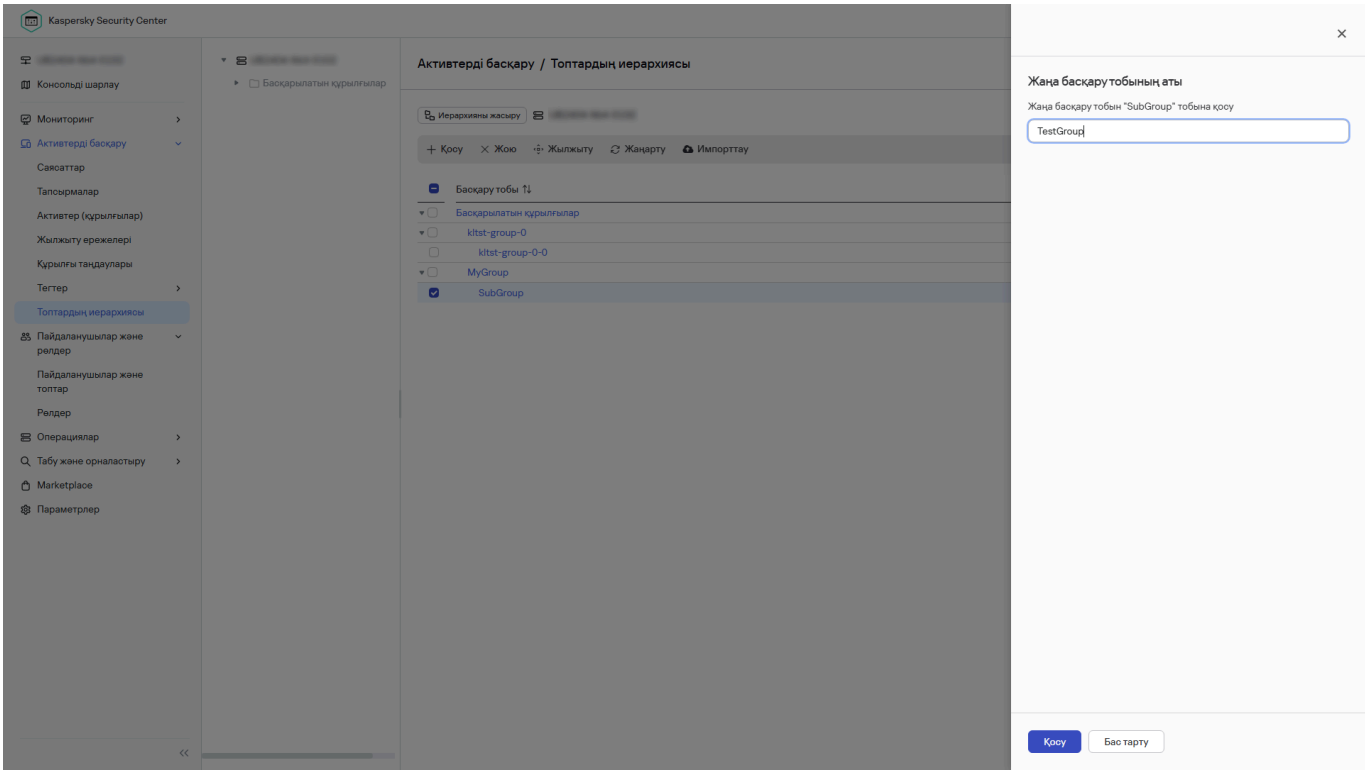
1. Бағдарламаның негізгі терезесінде **Активтерді басқару → Топтардың иерархиясы** бөліміне өтіңіз.

2. Басқару тобының құрылымында жаңа басқару тобы кіруі тиісті топқа сәйкес келетін салынған қалтаны таңдаңыз.



3. **Қосу** түймесін басыңыз.

4. Ашылған **Жаңа басқару тобының аты** терезесінде топтың атауын енгізіп, **Қосу** түймесін басыңыз.



Нәтижесінде, басқару топтарының иерархиясында атауы көрсетілген жаңа басқару тобы пайда болады.

Басқару топтарының құрылымын құру үшін:

1. Бағдарламаның негізгі терезесінде **Активтерді басқару** → **Топтардың иерархиясы** бөліміне өтіңіз.
2. **Импорттау** түймесін басыңыз.

Нәтижесінде, басқару топтарының құрылымын жасау шебері іске қосылады. Содан кейін, шебердің нұсқауларын орындаңыз.

Бағдарламаларды басқару тобының құрылғыларына автоматты түрде орнату

Басқару тобында Kaspersky қолданбасын клиент құрылғыларына автоматты түрде қашықтан орнату үшін қолданылатын орнату пакеттерін көрсетуге болады.

Қолданбаларды басқару тобының құрылғыларына автоматты түрде орнатуды конфигурациялау үшін:

1. Негізгі мәзірдегі **Активтерді басқару** → **Топтардың иерархиясы** бөліміне өтіңіз.
2. Келесі жолдардың бірімен қажетті басқару тобының сипаттарына өтіңіз:
   - Басқару тобының атауын басыңыз.
   - Беттің жоғарғы жағындағы **Иерархияны көрсету** түймесін басыңыз. Ашылатын навигация панелінде тінтуір курсорын қажетті топ атауының үстіне апарып, параметрлер белгішесін (⚙) басыңыз.

   Басқару тобының сипаттары терезесі ашылады.
3. Сипаттар терезесіндегі **Автоматты орнату** қойындысына өтіңіз.
4. Құрылғыларда орнатылатын қолданбалардың орнату пакеттерін таңдап, таңдауыңызды **Сақтау** түймесін басыңыз.

   Нұсқалары ғана басқаша бірдей қолданбаның бірнеше орнату пакетін таңдасаңыз, соңғы нұсқадағы орнату пакеті сақталады.

Орнату пакеттерін таңдағаннан кейін, әрбір қолданба үшін басқару тобындағы құрылғылардағы қолданбаларды орнатуға арналған топ тапсырмалары жасалады. Бұл тапсырмалар клиент құрылғыларында басқару тобына қосылғаннан кейін бірден іске қосылады.

Басқару топтарын жылжыту

Салынған басқару топтарын топтар иерархиясының ішінде жылжытуға болады.

Басқару тобы барлық салынған топтармен, қосалқы Басқару серверлерімен, құрылғылармен, топтық саясаттармен және тапсырмалармен бірге жылжытылады. Оған басқару топтарының иерархиясындағы жаңа жайғасымына сәйкес келетін барлық параметрлер қолданылады.

Топ атауы иерархияның бір деңгейінде бірегей болуы керек. Сіз басқару тобын жылжытып жатқан қалтада ұқсас атауы бар топ бұрыннан болса, жылжытпас бұрын топтың атауын өзгерту керек. Жылжытылатын топтың атауын алдын ала өзгертпеген болсаңыз, жылжыту кезінде оның атауына автоматты түрде түр **(<реттік нөмір>)** жалғауы, мысалы: **(1)**, **(2)** қосылады.

Басқарылатын құрылғылар тобының атын өзгерту және жылжыту мүмкін емес.

Басқару тобын басқару топтары иерархиясының басқа деңгейіне жылжыту үшін:

1. Негізгі мәзірде **Активтерді басқару** → **Топтардың иерархиясы** тармағына өтіп, жылжытқыңыз келетін басқару тобының жанындағы құсбелгіні таңдаңыз.

2. Құралдар тақтасындағы **Жылжыту** түймесін басыңыз.

3. Ашылған терезеде басқару тобын қайда жылжытқыңыз келетінін таңдап, **Жылжыту** түймесін басыңыз.

Терезе жабылады және басқару тобы топтар иерархиясының басқа деңгейіне жылжытылады.

Басқару топтарын жою

Қосалқы басқару серверлерін, салынған топтарды, клиент құрылғыларын, топ тапсырмаларын немесе сол топ үшін жасалған саясаттарды қамтитын басқару тобын жойсаңыз, оларды барлығы да жойылады.

Басқару тобын жоймас бұрын, оның құрамынан қосалқы Басқару серверінен, салынған топтарды және клиент құрылғыларын жою қажет.

Басқару тобын жою үшін:

1. Негізгі мәзірде **Активтерді басқару** → **Топтардың иерархиясы** тармағына өтіп, жойғыңыз келетін басқару тобының жанындағы құсбелгіні таңдаңыз.

2. Құралдар тақтасындағы **Жою** түймесін басыңыз.

Басқару тобы жойылды.

Kaspersky бағдарламалық жасақтамасын орналастыру

Бұл бөлімде Kaspersky Security Center Web Console көмегімен ұйымыңыздағы клиент құрылғыларында Kaspersky бағдарламаларын қалай орналастыру керектігі сипатталған.

Сценарий: Kaspersky бағдарламалық жасақтамасын орналастыру

Бұл сценарийде Kaspersky Security Center Web Console көмегімен Kaspersky бағдарламалық жасақтамасын орналастыру рәсімі сипатталған. Бағдарламаны жылдам іске қосу шеберін және қорғанысты орналастыру шеберін қолдануға немесе барлық қажетті қадамдарды қолмен орындауға болады.

Келесі бағдарламалар Kaspersky Security Center Web Console көмегімен орналастыру үшін қолжетімді:

- Kaspersky Endpoint Security for Linux
- Kaspersky Endpoint Security for Windows

Кезеңдер

Kaspersky бағдарламалық жасақтамасын орналастыру келесі кезеңдерден тұрады:

1. **Бағдарламаларды басқару веб-плагинін жүктеу**

   Бұл кезеңді бағдарламаны жылдам іске қосу шебері өңдейді. Шеберді іске қоспауды таңдасаңыз, плагиндерді қолмен жүктеп алыңыз.

2. **Орнату пакеттерін жүктеу және жасау**

   Бұл кезеңді бағдарламаны жылдам іске қосу шебері өңдейді.

   Бағдарламаны жылдам іске қосу шебері орнату пакетін басқару веб-плагинімен бірге жүктеуге мүмкіндік береді. Шеберді іске қосу кезінде осы параметрді таңдамасаңыз немесе шеберді іске қоспасаңыз, орнату пакетін қолмен жүктеу керек.

   Kaspersky қолданбаларын Kaspersky Security Center Linux көмегімен кейбір құрылғыларда, мысалы, қашықтағы қызметкерлердің құрылғыларында орната алмасаңыз, қолданбалар үшін жеке орнату пакеттерін жасай аласыз. Kaspersky бағдарламаларын орнату үшін автономды пакеттерді қолдансаңыз, қашықтан орнату тапсырмасын жасау және іске қосу, сондай-ақ Kaspersky Endpoint Security for Windows үшін тапсырмаларды жасау және конфигурациялау қажет емес.

   Сондай-ақ, Kaspersky сайтынан Желілік агенттің және қауіпсіздік бағдарламаларының дистрибутивтерін жүктеп алуға болады. Егер қандай да бір себептермен бағдарламаларды қашықтан орнату мүмкін болмаса, бағдарламаларды жергілікті орнату үшін жүктелген дистрибутивтерді пайдалануға болады.

3. **Қашықтан орнату тапсырмасын жасау, конфигурациялау және іске қосу**

   Бұл қадам қорғанысты орналастыру шеберіне кіреді. Қорғанысты орналастыру шеберін іске қоспаған болсаңыз, осы тапсырманы қолмен жасау және конфигурациялау керек.

Әртүрлі басқару топтары немесе құрылғылар таңдауы үшін бірнеше қашықтан орнату тапсырмасын қолмен жасауға болады. Осы тапсырмаларда бір бағдарламаның әртүрлі нұсқаларын орналастыруға болады.

Желідегі барлық құрылғылардың анықталғанына көз жеткізіңіз, содан кейін қашықтан орнату тапсырмасын (немесе тапсырмаларын) іске қосыңыз.

SUSE Linux Enterprise Server 15 операциялық жүйесі бар құрылғыларға Желілік агентті орнатқыңыз келсе, алдымен Желілік агентті орнату үшін insserv-compat пакетін орнатыңыз.

Желілік агентті RED OS 7.3.4 не одан кейінгі нұсқадағы немесе MSVSPHERE 9.2 не одан кейінгі нұсқадағы операциялық жүйені қолданатын құрылғыларға орнатқыңыз келсе, желілік агенттің дұрыс жұмыс істеуіне арналған libxcrypt-compat пакетін орнатыңыз.

4. **Тапсырмаларды құру және конфигурациялау**

   Kaspersky Endpoint Security *Жаңарту* тапсырмасы конфигурациялануы керек.

   Бұл қадам бағдарламаны жылдам іске қосу шеберіне кіреді: тапсырма әдепкі бойынша параметрлермен автоматты түрде жасалады және конфигурацияланады. Бағдарламаны жылдам іске қосу шеберін іске қоспаған болсаңыз, осы тапсырманы қолмен жасау және конфигурациялау керек. Бағдарламаны жылдам іске қосу шеберін іске қосқан болсаңыз, онда тапсырманы іске қосу кестесі сіздің талаптарыңызға сай келетініне көз жеткізіңіз. (Әдепкі бойынша, тапсырманы іске қосу уақыты үшін **Қолмен** мәні белгіленген, бірақ сізге осы мәнді өзгерту қажет болуы мүмкін).

5. **Саясаттар жасау**

   Kaspersky Endpoint Security саясатын қолмен немесе бастапқы конфигурациялау шеберін пайдаланып жасаңыз. Саясаттың әдепкі параметрлерін пайдалануға болады; сонымен қатар саясаттың әдепкі параметрлерін қажеттіліктеріңізге сәйкес кез келген уақытта өзгертуге болады.

6. **Нәтижелерді тексеру**

   Орналастырудың сәтті орындалғанына көз жеткізіңіз: әрбір бағдарлама үшін саясаттар мен тапсырмалар жасалған және осы бағдарламалар басқарылатын құрылғыларға орнатылған.

Нәтижелер

Сценарийдің аяқталуы арқасында:

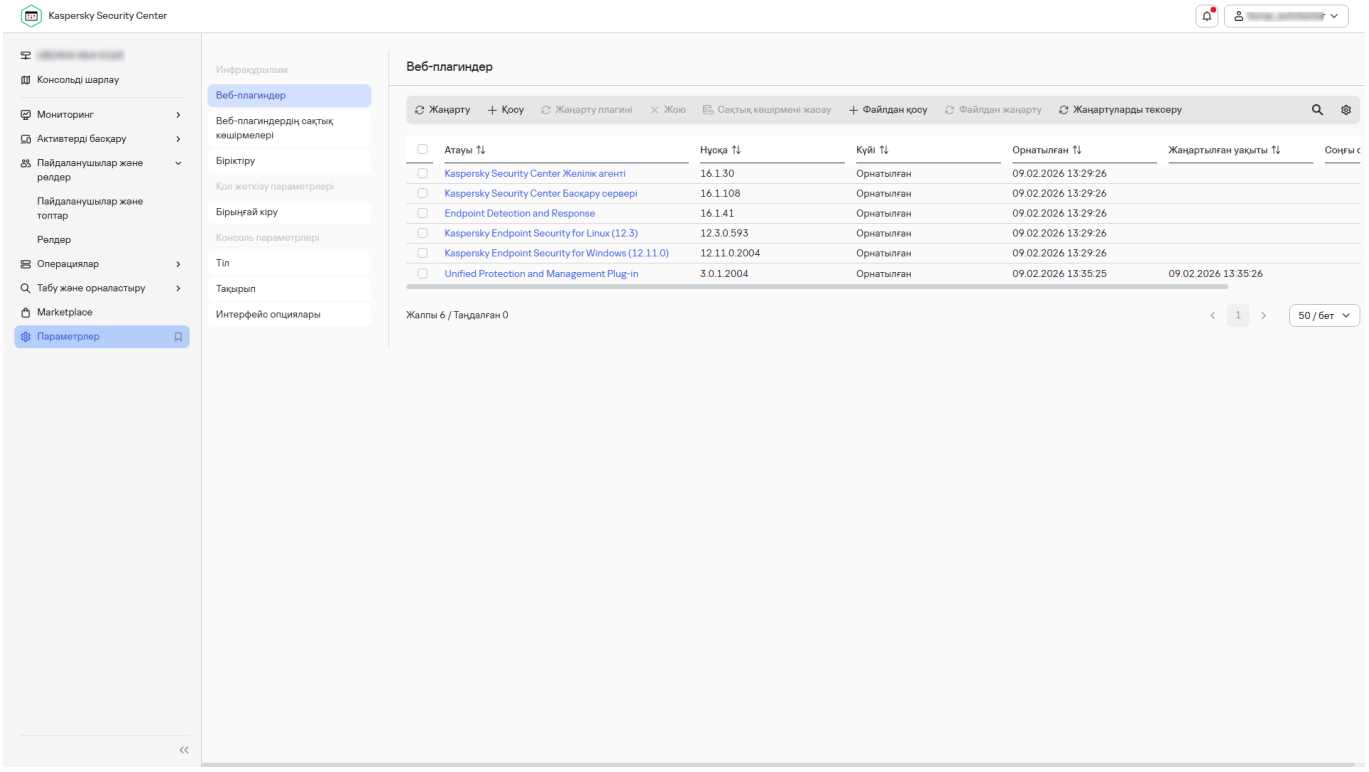
- Таңдалған тапсырмалар үшін барлық қажетті саясаттар мен тапсырмалар жасалады.
- Тапсырмаларды іске қосу кестесі өз талаптарыңызға сай конфигурацияланады.
- Таңдалған клиент құрылғыларында таңдалған бағдарламалар орналастырылған немесе орналастырылуға жоспарланған.

Kaspersky бағдарламаларын басқаруға арналған плагинін қосу

Kaspersky Endpoint Security for Linux немесе Kaspersky Endpoint Security for Windows сияқты Kaspersky бағдарламасын орналастыру үшін сол бағдарлама үшін басқарудың веб-плагинін жүктеп алуыңыз керек.

Kaspersky бағдарламаларының веб-плагиндерін жүктеу үшін:

1. Қолданбаның негізгі терезесінде **Параметрлер** → **Веб-плагиндер** бөліміне өтіңіз.



Орнатылған веб-плагиндердің тізімі

2. Пайда болған терезеде **Қосу** түймесін басыңыз.

   Қолжетімді басқару плагиндері тізімі көрсетіледі.

3. Қолжетімді плагиндер тізімінде жүктеу қажет болған плагин атауын таңдаңыз (мысалы, Kaspersky Endpoint Security for Linux).

   Плагин сипаттамасы бар бет көрсетіледі.

4. Плагин сипаттамасы бетінде **Плагинді орнату** түймесін басыңыз.

5. Орнату аяқталғаннан кейін, **OK** түймесін басыңыз.

Басқару плагині әдепкі бойынша конфигурацияда жүктеледі және басқару плагиндерінің тізімінде пайда болады.

Плагиндерді қосуға және жүктелген плагиндерді файлдан жаңартуға болады. Сіз басқару веб-плагиндерін Kaspersky Техникалық қолдау қызметі веб-сайтынан жүктеп ала аласыз.

Файлдағы басқару веб-плагинін жүктеп алу немесе жаңарту үшін:

1. Қолданбаның негізгі терезесінде **Параметрлер** → **Веб-плагиндер** бөліміне өтіңіз.
2. Плагин файлын мен файл жазуын көрсетіңіз:
   - Файлдағы плагинді жүктеу үшін **Файлдан қосу** түймесін басыңыз.
   - Файлдағы плагин үшін жаңартуды жүктеу мақсатымен **Файлдан жаңарту** түймесін басыңыз.
3. Файл мен файл жазуын көрсетіңіз.
4. Көрсетілген файлдарды жүктеңіз.

Басқару веб-плагині файлдан жүктеледі және басқару веб-плагиндерінің тізімінде пайда болады.

Орнату пакеттері

Орнату пакеті — Kaspersky қолданбасын қашықтан орнату үшін жасалған файлдар жиынтығы. Орнату пакеті бағдарламаны орнатуға және бірден орнатқаннан кейін оның жұмысқа қабілетін қамтамасыз етуге қажетті параметрлер жиынтығын қамтиды. Параметрлердің мәндері әдепкі бойынша бағдарлама параметрлерінің мәндеріне сәйкес келеді. Орнату пакеті қолданбаның жеткізу жиынтығына кіретін KPD және KUD кеңейтімдері бар файлдар көмегімен жасалады.

Орнату пакеттері келесі тәсілдермен жасалады:

- көрсетілген дистрибутивтерден, олардың құрамына кіретін *сипаттауыштар* негізінде автоматты түрде (орнату және нәтижені талдау ережелерін және басқа ақпаратты қамтитын kud кеңейтімі бар файлдар);
- стандартты немесе қолдау көрсетілетін қолданбалар үшін ZIP, CAB, TAR немесе TAR.GZ мұрағат файлынан.

Жасалған орнату пакеттері ішкі қалталары мен файлдары салынған қалталар болып саналады. Бастапқы дистрибутивтен басқа, орнату пакеті өңделетін параметрлерді (инсталлятордың өзінің параметрлерін және орнатуды аяқтау үшін операциялық жүйені қайта іске қосу қажеттілігі сияқты жағдайларды өңдеу ережелерін қоса), сондай-ақ шағын көмекші модульдерді қамтиды.

Нақты қолдау көрсетілетін қолданба үшін ерекше орнату параметрлерінің мәндерін орнату пакетін жасаған кезде Kaspersky Security Center Web Console консолінің пайдаланушы интерфейсінде белгілеуге болады. Kaspersky Security Center Linux құралдарымен қолданбаларды қашықтан орнату жағдайында орнату пакеттері қолданбаның инсталляторын іске қосқан кезде оған әкімші белгілеген барлық параметрлер қолжетімді болатындай етіп құрылғыларға жеткізіледі. Kaspersky қолданбаларын орнатудың бөтен құралдарын қолданған кезде барлық орнату пакетінің, яғни дистрибутив пен оның параметрлерінің құрылғыдағы қолжетімділігін қамтамасыз ету жеткілікті. Орнату пакеттері Kaspersky Security Center Linux ортақ қатынасы бар қалтаның сәйкес ішкі қалтасында жасалады және сақталады.

Орнату пакеттерінің параметрлерінде артықшылықты есептік жазбалардың деректерін көрсетпеңіз.

Microsoft Windows топтық саясаттары тетігінің көмегімен орналастыруға қолдау көрсетілмейді.

Kaspersky Security Center Linux орнатылғаннан кейін, бірден орнатуға дайын бірнеше орнату пакеттері, соның ішінде Microsoft Windows платформасына арналған Желілік агент пакеттері мен қауіпсіздік қолданбалары автоматты түрде жасалады.

Қолданбаға арналған лицензия үшін лицензиялық кілтті орнату пакетінің сипаттарында белгілеуге болатынына қарамастан, оқуға арналған орнату пакеттерінің орасан зор қолжетімділігі себебінен бұл лицензияларды тарату тәсілін қолданбаған жөн. Автоматты түрде таратылған лицензиялық кілттерді немесе лицензиялық кілттерді орнату тапсырмаларын қолданған жөн.

Kaspersky бағдарламаларына арналған орнату пакеттерін жүктеп алу және жасау

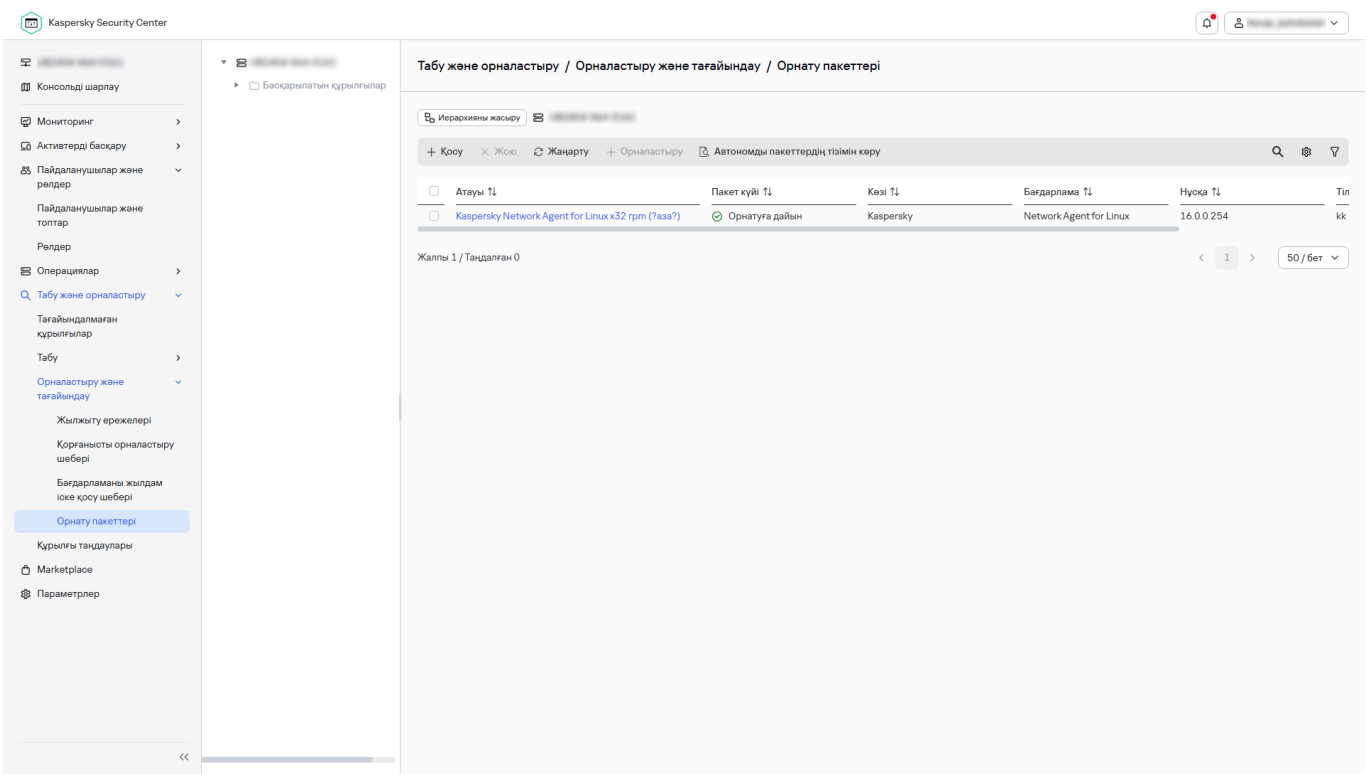
Басқару сервері интернетке қатынаса алса, сіз Kaspersky веб-серверлерінен Kaspersky бағдарламаларының орнату пакеттерін жасай аласыз.

Kaspersky бағдарламаларына арналған орнату пакеттерін жүктеп алу және жасау үшін:

1. Бағдарламаның негізгі терезесінде **Бағдарламалық жасақтаманы басқару** → **Орнату пакеттері** бөліміне өтіңіз.

   Сондай-ақ, Kaspersky бағдарламаларына арналған жаңа пакеттер туралы ақпаратты экрандағы хабарландырулар тізімінен көруге болады. Жаңа пакет туралы хабарландырулар болса, хабарландырудың жанындағы сілтеме бойынша қолжетімді орнату пакеттерінің тізіміне өтуге болады.

   Басқару серверінде қолжетімді орнату пакеттерінің тізімі көрсетіледі.

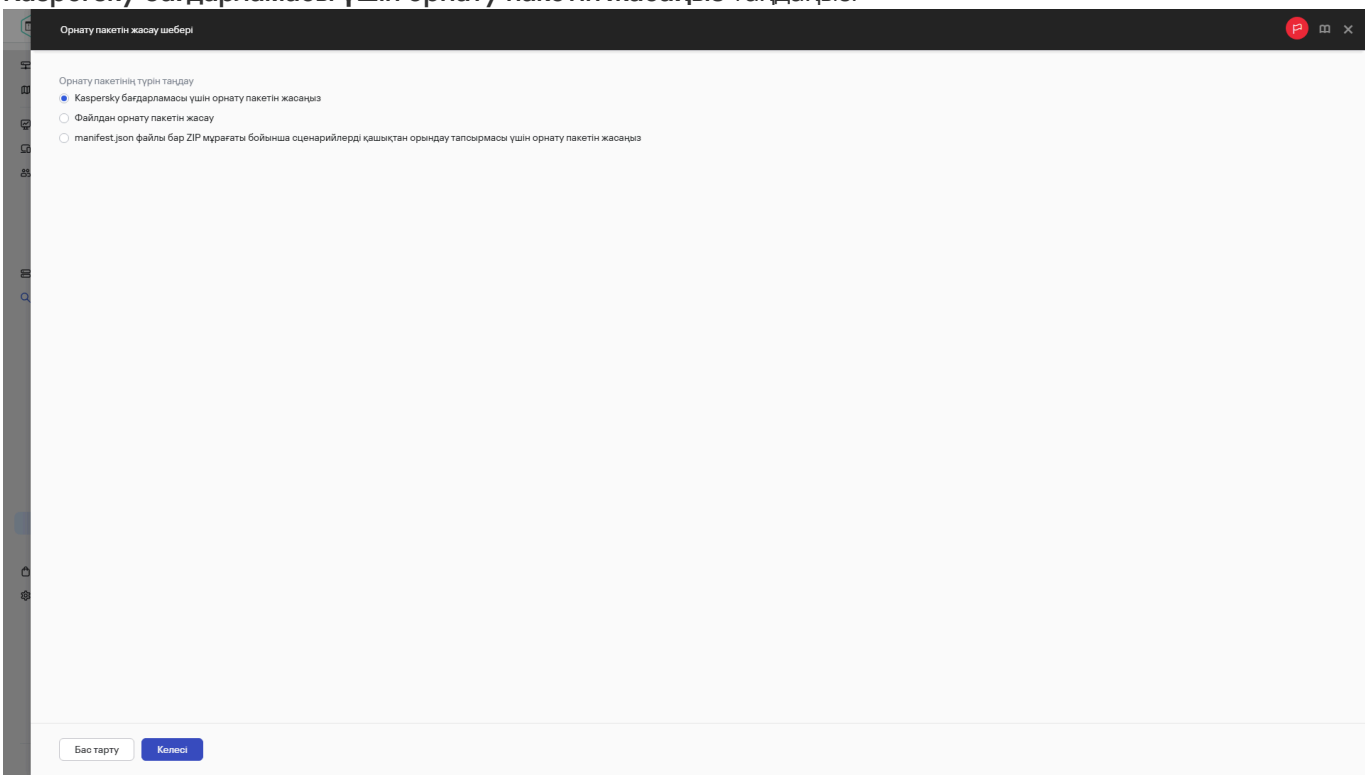


Орнату пакеттерінің тізімі

2. **Қосу** түймесін басыңыз.

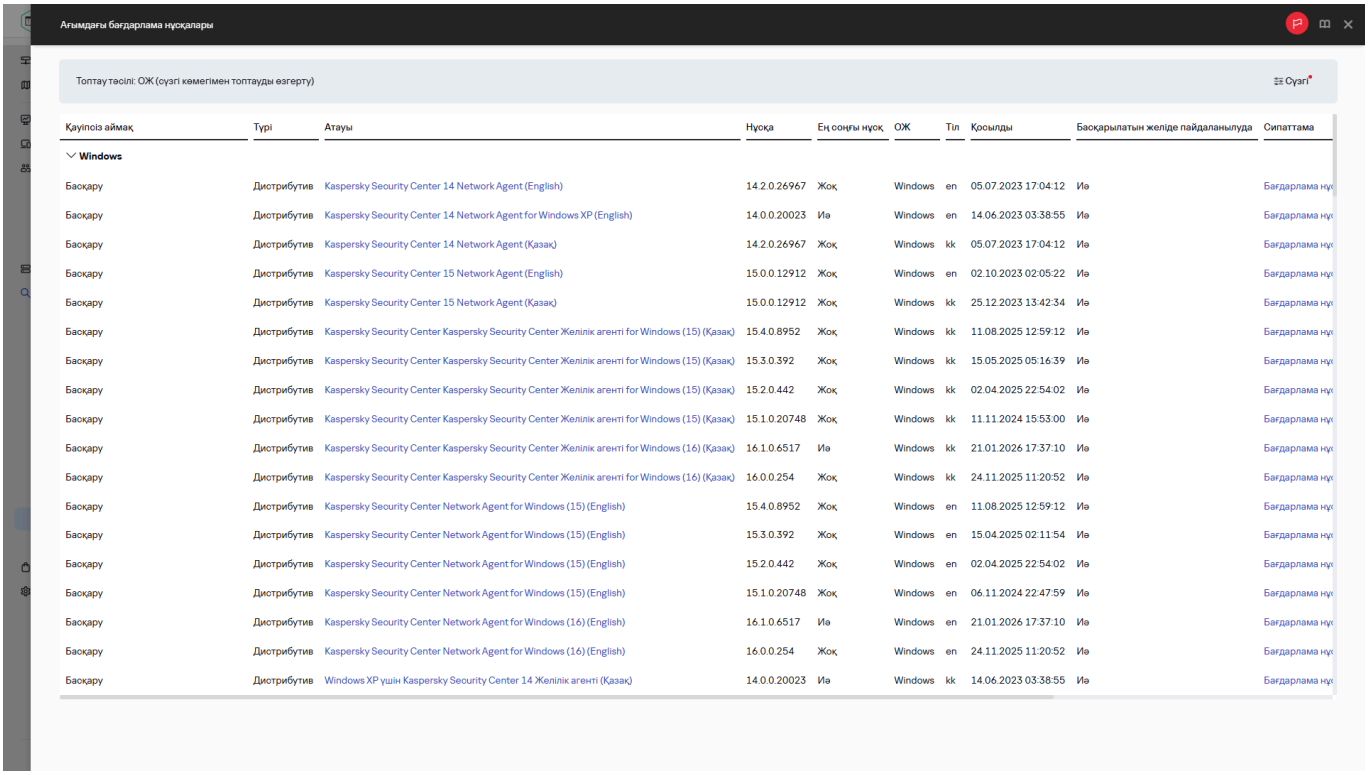
   Орнату пакетін жасау шебері іске қосылады. Шебердің жұмысын жалғастыру үшін **Келесі** түймесін басыңыз.

3. **Kaspersky бағдарламасы үшін орнату пакетін жасаңыз** таңдаңыз.



Орнату пакеті түрін таңдау

Kaspersky веб-серверлерінде қолжетімді орнату пакеттерінің тізімі көрсетіледі. Тізімде тек Kaspersky Security Center Linux бағдарламасының ағымдағы нұсқасымен үйлесімді бағдарламалардың орнату пакеттері бар. Әдепкі бойынша, тізімде тек ағылшын тіліндегі және интерфейс тіліне сәйкес келетін тілдегі қолданбалар көрсетіледі. Басқа тілдерді көрсету үшін **Сүзгі** түймесін басып, сүзгі параметрлерін конфигурациялаңыз.

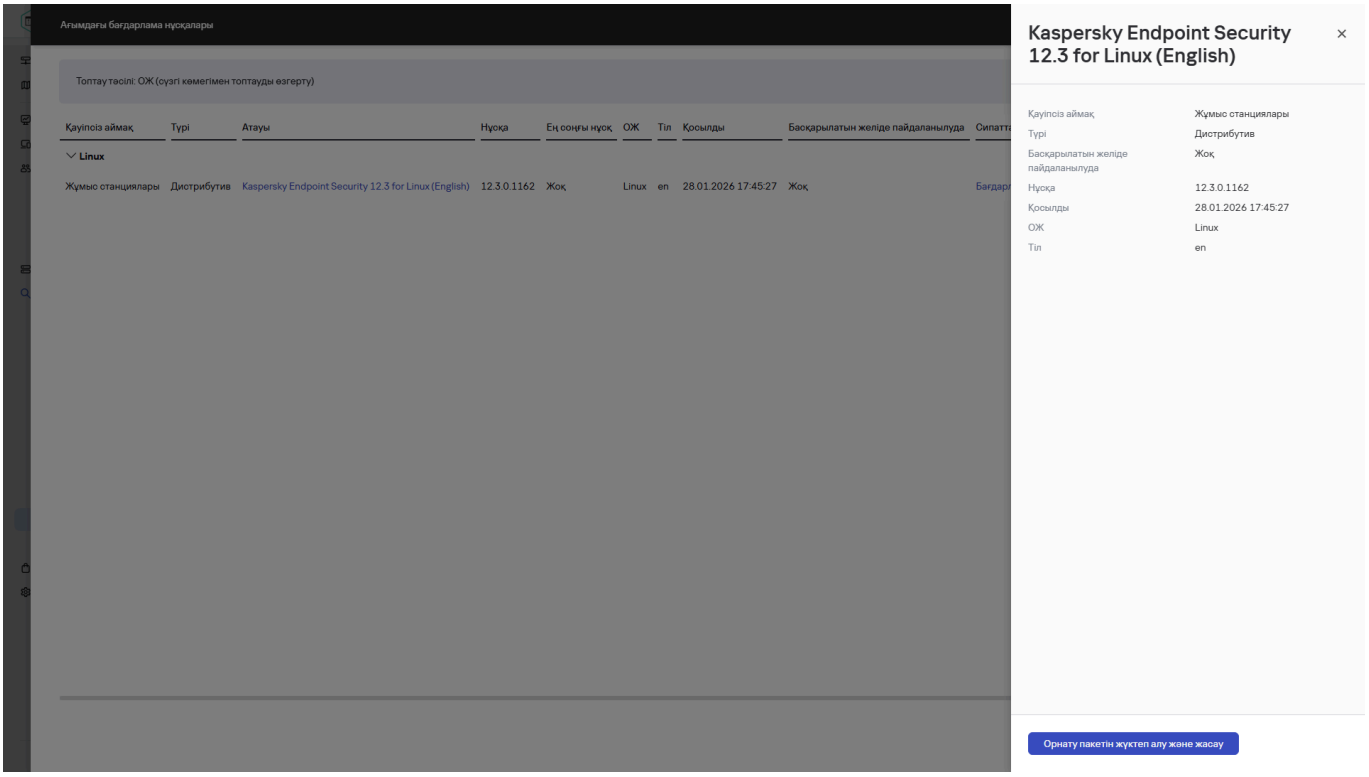


Қолжетімді орнату пакеттерінің тізімі

4. Қажетті орнату пакетін, мысалы, Kaspersky Endpoint Security for Linux таңдаңыз.

   Орнату пакеті туралы ақпараты бар терезе ашылады.

Қолданыстағы заңдар мен ережелерге сәйкес келсе, сенімді шифрлауды іске асыратын криптографиялық құралдарды қамтитын орнату пакетін жүктеп, пайдалана аласыз. Ұйымыңыздың қажеттіліктері үшін жарамды Kaspersky Endpoint Security for Windows орнату пакетін жүктеп алу үшін ұйымыңыздың клиент құрылғылары орналасқан елдің заңнамасын қараңыз.



Орнату пакетін жүктеп алу

5. Ақпаратпен танысып, **Орнату пакетін жүктеп алу және жасау** түймесін басыңыз.

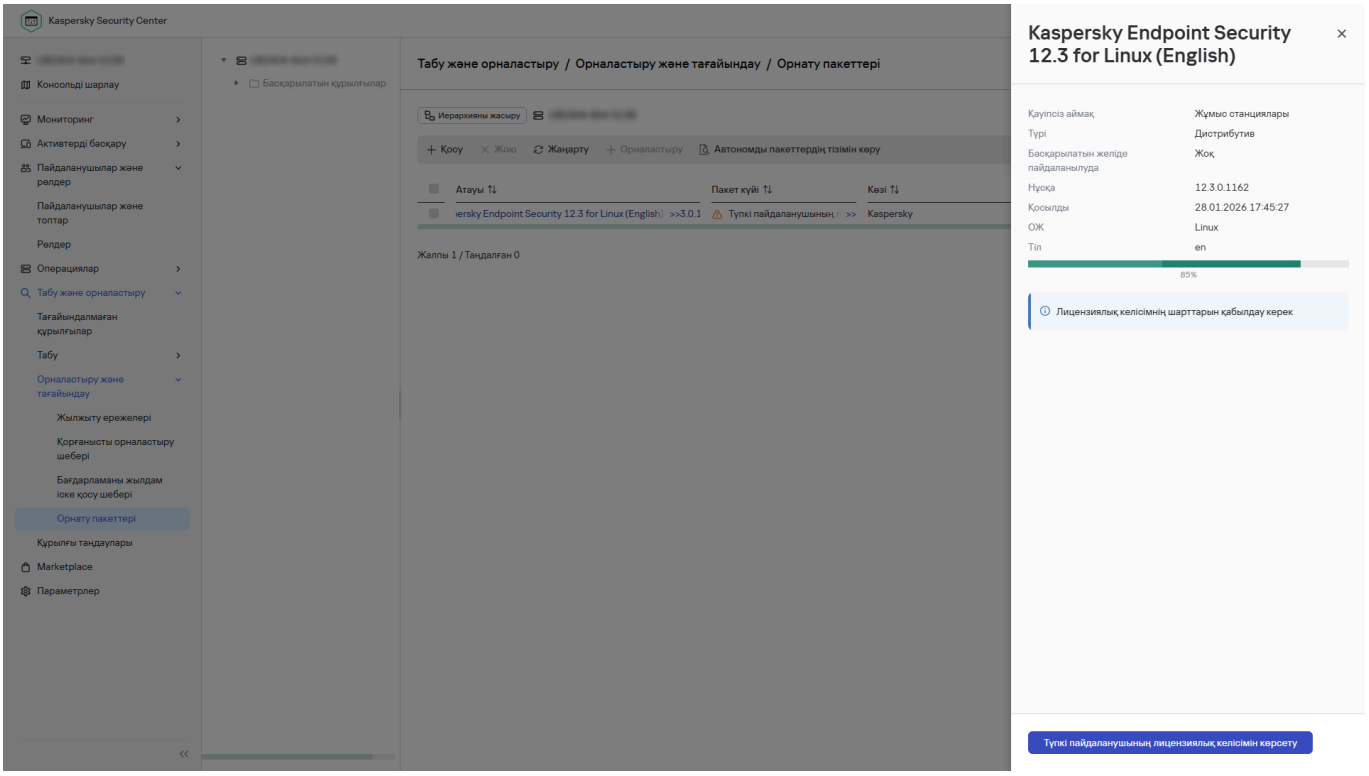
   Дистрибутив пакетін орнату пакетіне түрлендіру мүмкін болмаса, **Орнату пакетін жүктеп алу және жасау** түймесінің орнына **Дистрибутивті жүктеп алу** түймесі көрсетіледі.

Кейбір Kaspersky бағдарламаларын жүктеу алдында немесе кезінде **Түпкі пайдаланушының лицензиялық келісімін көрсету** түймесі көрсетіледі Осы түйме көрсетілсе:

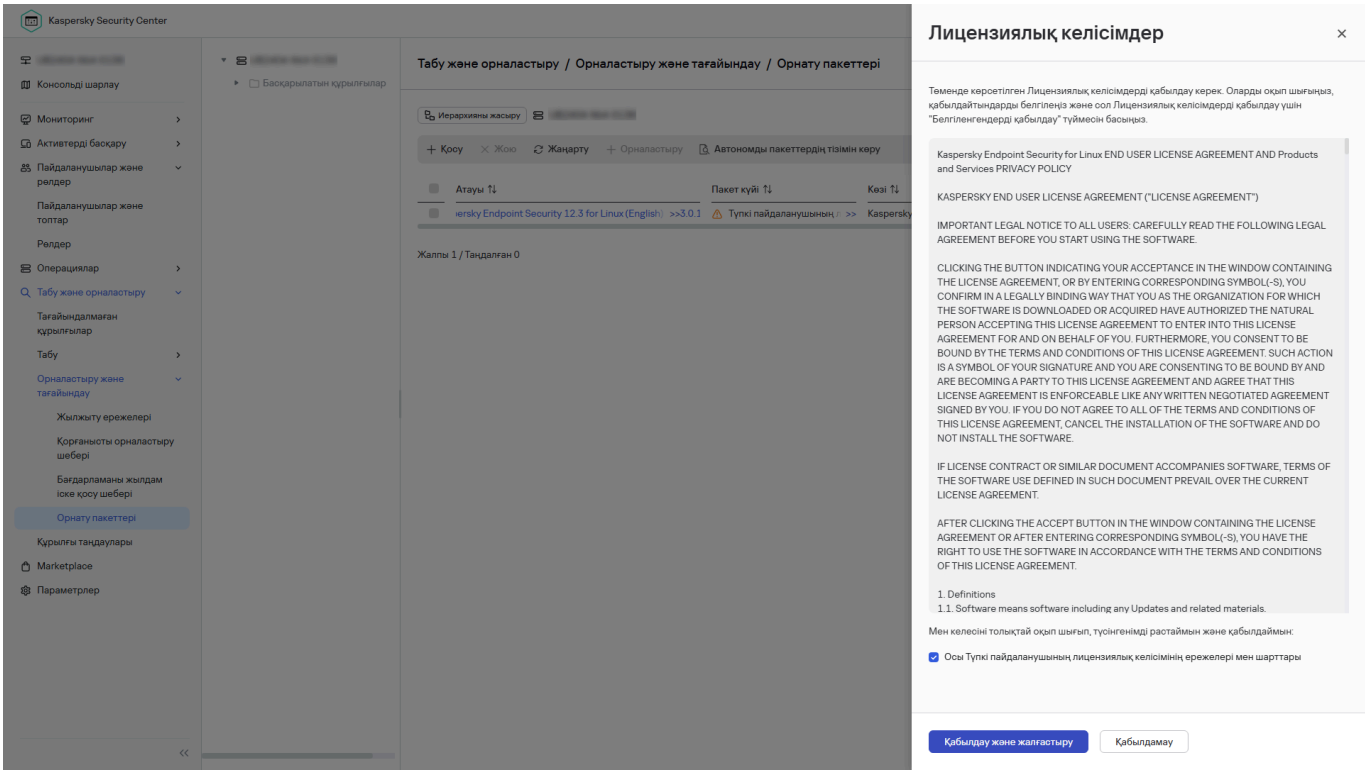
a. Лицензиялық келісімін (EULA) оқу үшін **Түпкі пайдаланушының лицензиялық келісімін көрсету** түймесін басыңыз.

b. Экранда пайда болған Лицензиялық келісімді оқып, **Қабылдау** түймесін басыңыз.

   Лицензиялық келісімді қабылдағаннан кейін, жүктеу жалғасады. **Қабылдамау** түймесін бассаңыз, жүктеу тоқтатылады.



Орнату пакетін жүктеп алу



EULA қабылдау

Шебердің терезесін жабуға болады. Бұл жағдайда жүктеп алу процесі фондық режимде жалғасады. Орнату пакетін жүктеп алу күйін бақылауға, сондай-ақ **Пакет күйі** бағанында күйлерге сүзгі қолдануға және сұрыптауға болады.

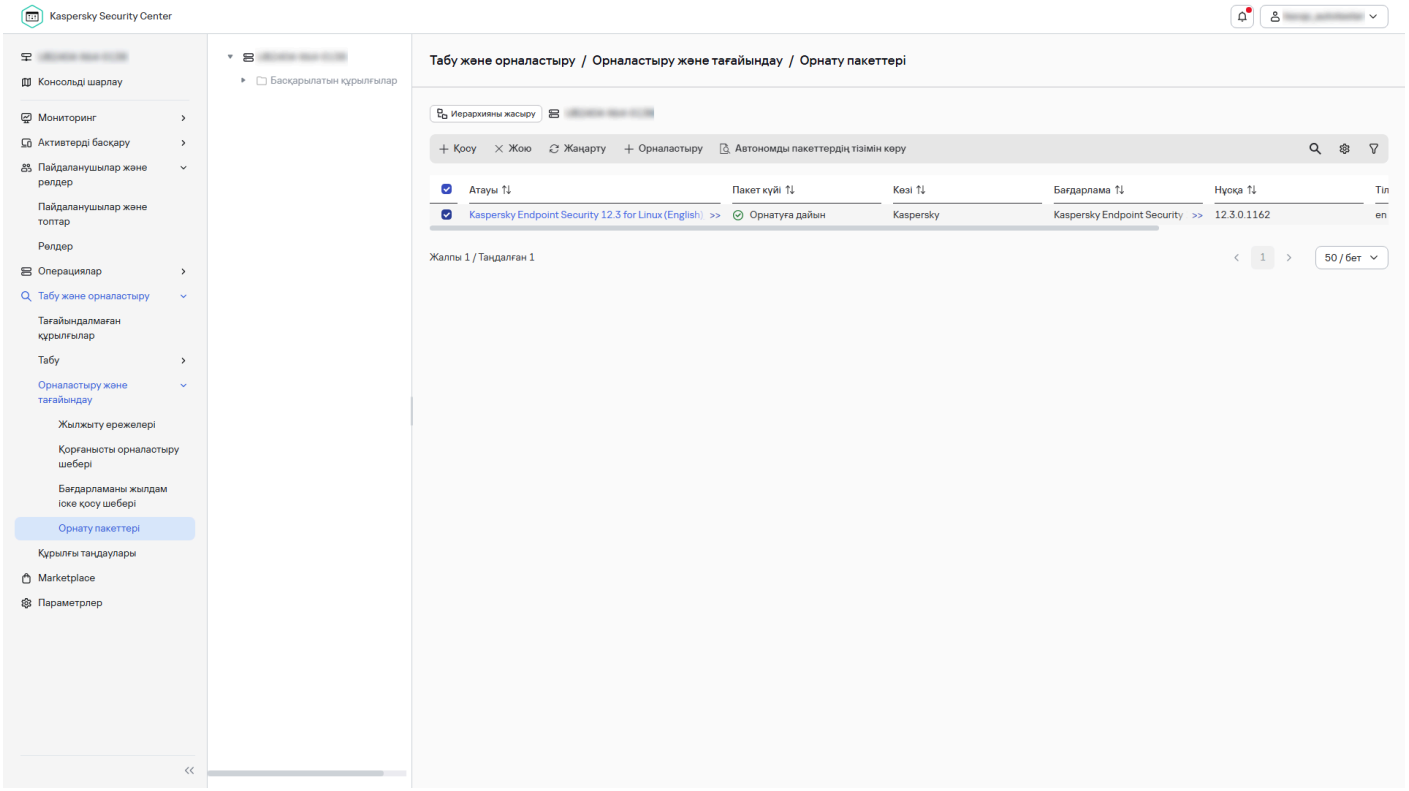
Жүктеп алу процесі тоқтап, жүктеп алу күйі **Түпкі пайдаланушының лицензиялық келісімін қабылдау** күйіне ауысса, орнату пакетінің атауын басып, 5.a және 5.b қадамдарын орындаңыз.

Әдепкісінше **Орындалып жатыр** және **Түпкі пайдаланушының лицензиялық келісімін қабылдау** күйлеріндегі орнату пакеттері тізімнің басына қойылады.

Таңдалған дистрибутивтегі деректердің өлшемі ағымдағы шекті мәннен асып кетсе, қате туралы хабарлама көрсетіледі. Сіз шекті мәнді өзгерте аласыз және орнату пакетін құруды жалғастыра аласыз.

6. Жүктеу аяқталғаннан кейін, **Жабу** түймесін басыңыз.

Таңдалған орнату пакеті, Packages қалтасына салынған Басқару серверінің ортақ қатынас бар қалтасына жүктеледі. Жүктелгеннен кейін, орнату пакеті орнату пакеттерінің тізімінде көрсетіледі.



Орнату пакеттерінің тізімі

Файлдан орнату пакетін жасау

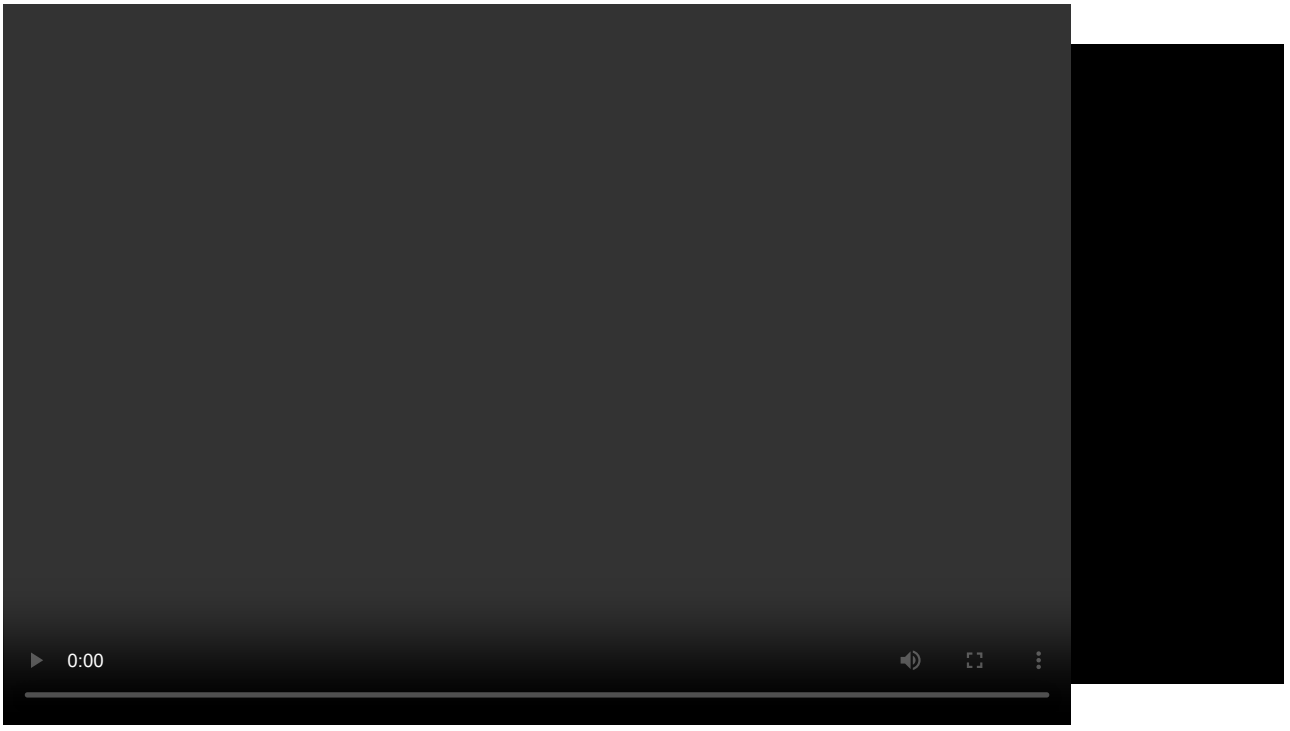
Сіз конфигурацияланған орнату пакеттерін пайдалана аласыз:

- клиент құрылғыларына кез келген бағдарламаны (мысалы, мәтіндік редактор) орнатыңыз, мысалы, тапсырма арқылы;
- жеке орнату пакетін жасау.

Пайдаланушы орнату пакеті – бұл файлдар жиынтығы бар қалта. Таңдаулы орнату пакетін жасау көзі – *мұрағаттық файл* болып табылады. Мұрағаттық файлда пайдаланушы орнату пакетіне қосылуы керек файл немесе файлдар бар.

Пайдаланушы орнату пакетін жасау кезінде, сіз пәрмен жолының параметрлерін көрсете аласыз, мысалы, бағдарламаны тыныш режимде орнату үшін.

Windows үшін таңдаулы орнату пакетін қалай жасау және орналастыру керектігін білу үшін бейнені көріңіз. Windows және Linux құрылғыларына арналған осы оқулықтың мәтіндік нұсқасы төменде қолжетімді.

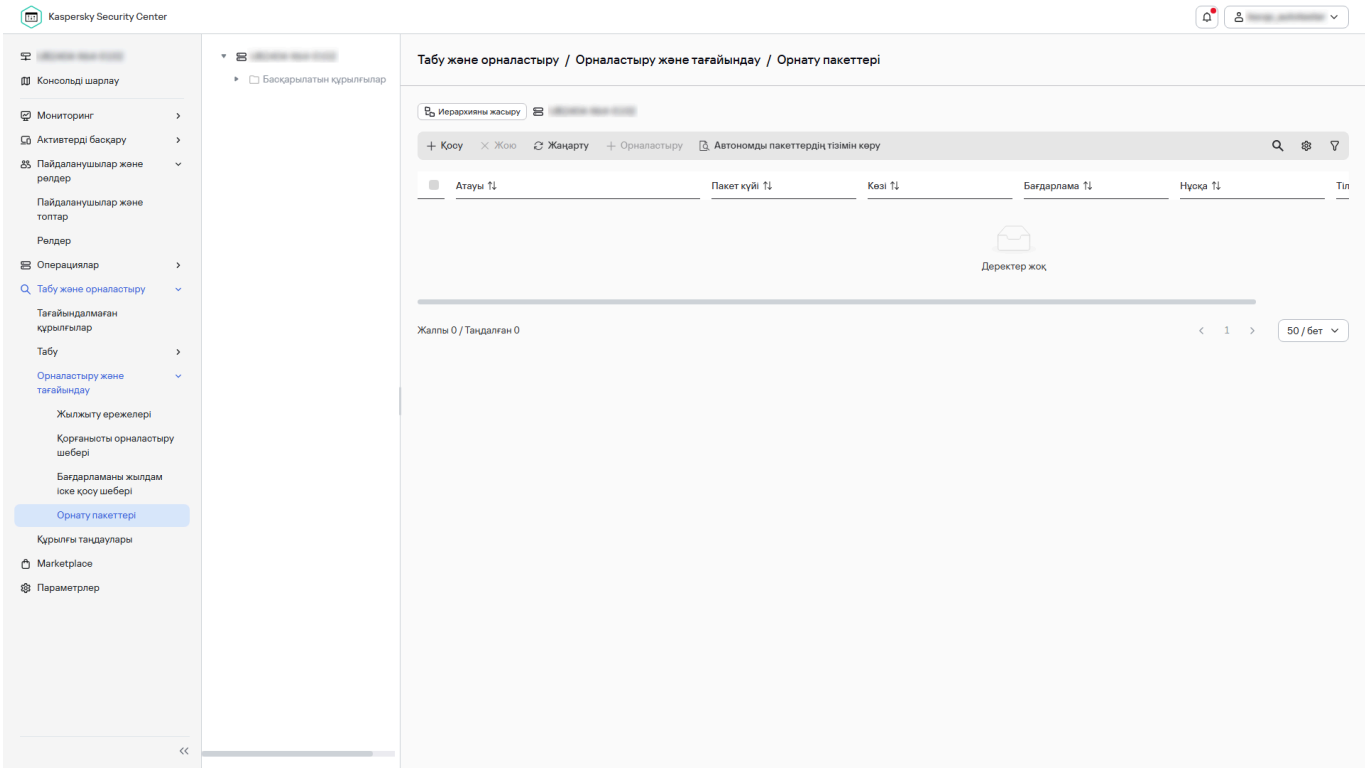


Windows үшін файлдан арнайы орнату пакетін жасау және орналастыру. Бейне

Пайдаланушы орнату пакетін жасау үшін:

1. Бағдарламаның негізгі терезесінде **Бағдарламалық жасақтаманы басқару** → **Орнату пакеттері** бөліміне өтіңіз.

Басқару серверінде қолжетімді орнату пакеттерінің тізімі көрсетіледі.

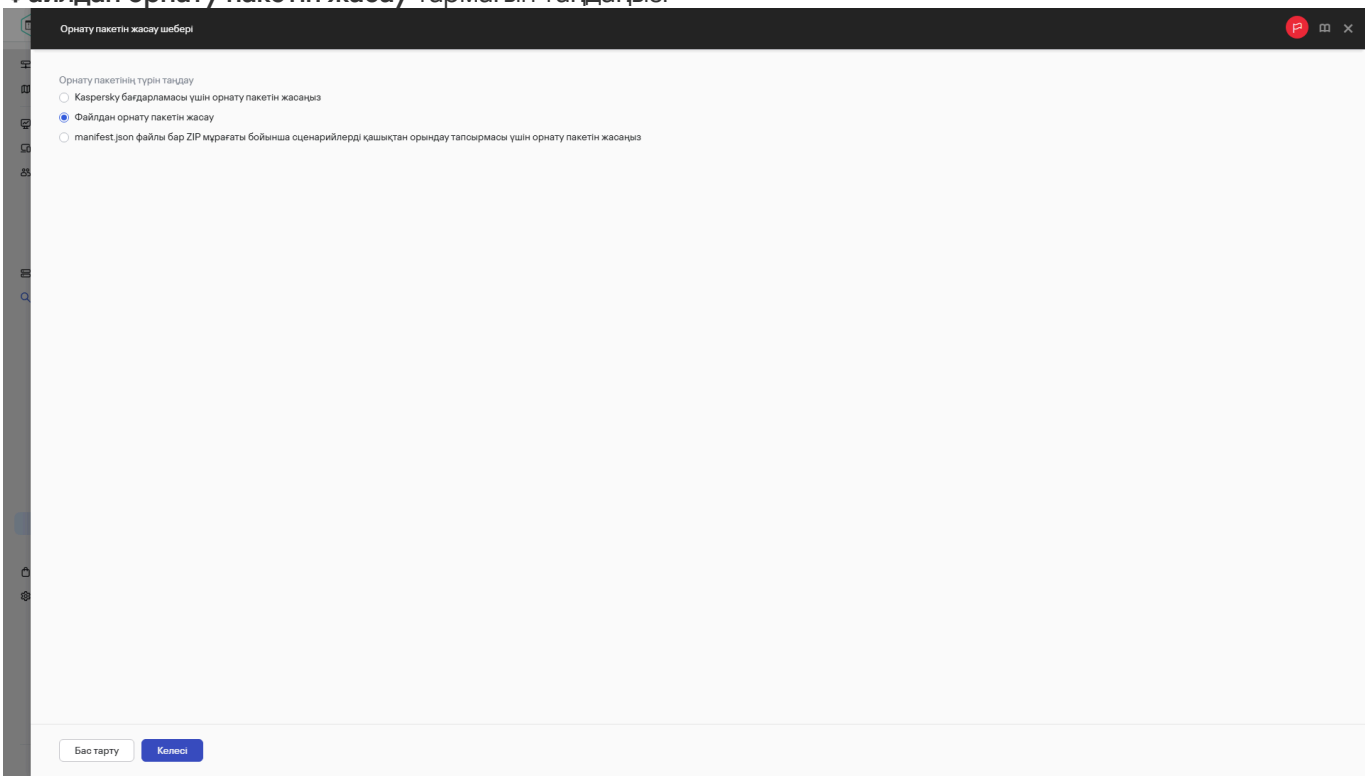


Орнату пакеттерінің тізімі

2. **Қосу** түймесін басыңыз.

   Орнату пакетін жасау шебері іске қосылады. Шебердің жұмысын жалғастыру үшін **Келесі** түймесін басыңыз.

3. **Файлдан орнату пакетін жасау** тармағын таңдаңыз.



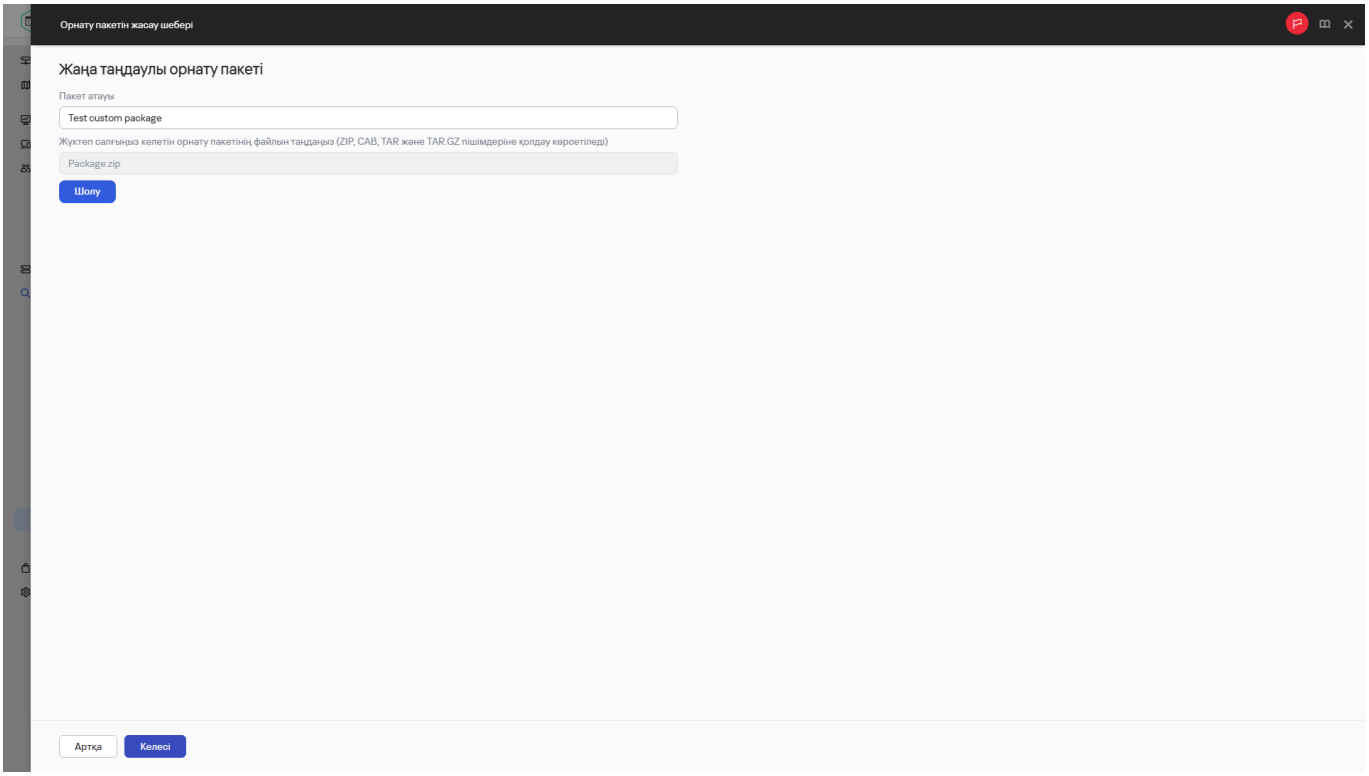
Орнату пакеті түрін таңдау

4. Пакет атауын көрсетіңіз және **Шолу** түймесін басыңыз.

5. Ашылған терезеде қолжетімді дискілерде орналасқан мұрағаттың файлын таңдаңыз.

Сіз ZIP, CAB, TAR немесе TAR.GZ пішіміндегі мұрағаттық файлды жүктей аласыз. SFX (өздігінен шығарылатын мұрағат) файлынан орнату пакетін жасау мүмкін емес.

Файлды Басқару серверіне жүктеу басталады.



Орнату пакеті файлын көрсету

6. Егер сіз Kaspersky бағдарламасының файлын көрсеткен болсаңыз, сізге сол бағдарламаның Лицензиялық келісімін оқып, қабылдау ұсынылуы мүмкін. Жалғастыру үшін Лицензиялық келісімнің шарттарын қабылдауыңыз керек. **Осы Түпкі пайдаланушының лицензиялық келісімінің талаптары мен шарттарын қабылдау** параметрін тек Лицензиялық келісімнің шарттарын толық оқып, түсініп, қабылдаған жағдайда ғана таңдаңыз.

   Сондай-ақ сізге Құпиялық саясатының шарттарын оқып, қабылдау ұсынылады. Жалғастыру үшін Құпиялық саясатының шарттарын қабылдауыңыз керек. Сіздің деректеріңіз Құпиялық саясатында сипатталғандай өңделетінін және берілетінін (соның ішінде үшінші елдерге) түсініп, онымен келіссеңіз ғана **Мен Құпиялық саясатын қабылдаймын** параметрді таңдаңыз.

7. Файлды таңдаңыз (таңдалған мұрағаттық файлдан алынған файлдар тізімінен) және орындалатын файлдың пәрмен жолының параметрлерін көрсетіңіз.

   deb немесе rpm форматында орнату пакетін қалай жасауға болады

   1. Келесі пәрмендермен `.sh` скриптін жасаңыз:

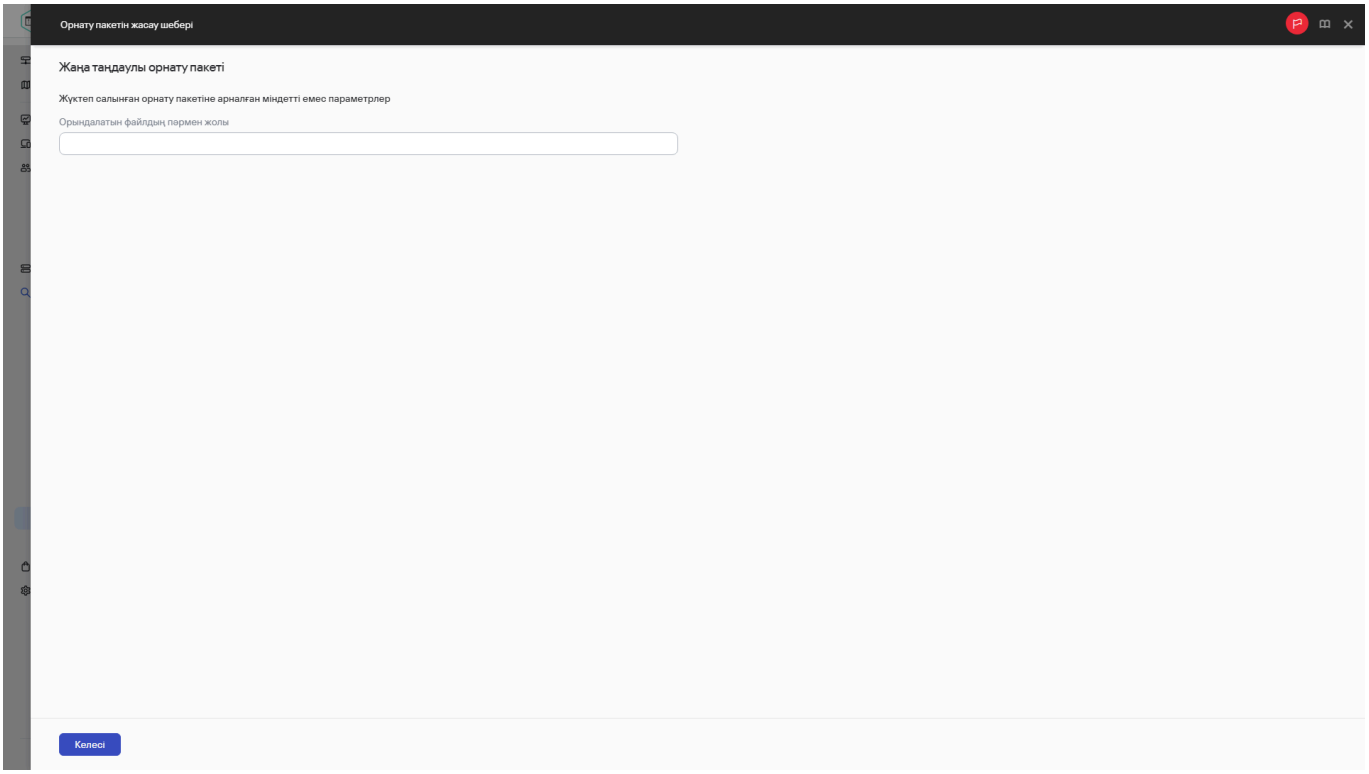
      ```
      #!/bin/sh
      script_dir="$(dirname "$0")"
      apt-get install --yes "$script_dir/<пакеттің_атауы>.deb" </dev/null
      ```

      Скрипт мазмұны мен пәрмендері пакет форматына және басқа мәліметтерге байланысты өзгеруі мүмкін. Скриптті өзіңіздің нақты конфигурацияңызға сәйкес өзгертуге болады.

   2. Жасалған скриптті `.deb` немесе `.rpm` файлымен бірге мұрағатқа орналастырыңыз.

   3. Орнату пакетін жасаған кезде, орындалатын файл ретінде жасалған скриптті таңдаңыз.

Бағдарламаны орнату пакетінен тыныш режимде орнату үшін пәрмен жолының параметрлерін көрсетуге болады. Пәрмен жолының параметрлерін көрсету міндетті емес.



Қосымша пәрмен жолы параметрлерін көрсету

Орнату пакетін жасау процесі басталады.

Шебер терезесінде процестің аяқталуы туралы ақпарат көрсетіледі.

Егер орнату пакеті жасалмаса, тиісті хабарландыру көрсетіледі.

8. Шебер терезесін жабу үшін **Аяқтау** түймесін басыңыз.

Жасалған орнату пакеті Басқару серверінің ортақ қатынасы бар қалтасының Packages салынған қалтасына жүктеледі. Жүктелгеннен кейін, орнату пакеті орнату пакеттерінің тізімінде пайда болады.

Басқару серверінде қолжетімді орнату пакеттері тізімінде, орнату пакетінің атын басу арқылы, келесі әрекеттерді орындай аласыз:

- Орнату пакетінің келесі сипаттарын қарап шыға аласыз:
  - **Атауы**. Орнату пакетінің атауы.
  - **Пакет күйі**. Орнату пакетін жүктеп алу күйі.
  - **Көзі**. Бағдарлама өндірушісінің атауы.
  - **Бағдарлама**. Пайдаланушы орнату пакетіне қапталған бағдарламаның атауы.
  - **Нұсқа**. Бағдарлама нұсқасы.
  - **Тіл**. Пайдаланушы орнату пакетіне қапталған бағдарламаның тілі.
  - **Өлшемі (МБ)**. Орнату пакетінің өлшемі.
  - **ОЖ**. Орнату пакеті арналған операциялық жүйенің түрі.

- **Жасалған күні**. Орнату пакетін жасау күні.
- **Өзгертілген**. Орнату пакетін өзгерту күні.
- **Түрі**. Орнату пакетінің түрі.

- Пәрмен жолының параметрлерін өзгертіңіз.

Автономды орнату пакетін жасау

Сіз және сіздің ұйымыңыздағы құрылғы пайдаланушылары бағдарламаларды құрылғыларға қолмен орнату үшін жеке орнату пакеттерін пайдалана аласыз.

Жеке орнату пакеті, Веб-серверге немесе ортақ қатынасы бар қалтаға орналастыруға, пошта арқылы жіберуге немесе клиент құрылғысына басқа тәсілмен жіберуге болатын орындалатын файл болып саналады. Бағдарламаны Kaspersky Security Center Linux қатысуынсыз орнату үшін, алынған файлды клиент құрылғысында жергілікті түрде іске қосуға болады. Kaspersky бағдарламалары үшін де, үшінші тарап бағдарламалары үшін де жеке орнату пакетін жасауға болады. Үшінші тарап бағдарламалары үшін жеке орнату пакетін жасау үшін, пайдаланушы орнату пакетін жасау керек.

Егер Басқару серверінде интернетке кіру мүмкіндігі болса, **Жаңартуларды Басқару серверінің қоймасына жүктеп алу** тапсырмасы Желілік агенттің автономды орнату пакеттерін жасау үшін қажетті тәуелділіктерді жүктеу үшін пайдаланылады. Басқару серверінде интернетке арнайы мүмкіндіктер болмаса, келесі қадамдарды орындаңыз:

1. RlUtilsArchiveDirUsed жалаушасын жасау үшін келесі пәрменді орындаңыз:

   ```
   /opt/kaspersky/ksc64/sbin/klscflag -fset -pv klserver -n RIUtilsArchiveDirUsed -t d -v 1
   ```

2. Басқару сервері қызметін қайта іске қосу үшін келесі пәрменді орындаңыз:

   ```
   systemctl restart kladminserver_srv.service
   ```

3. Келесі мұрағаттарды Kaspersky веб-сайтынан жүктеп алып, оны /var/opt/kaspersky/klnagent_srv/1093/.working/ri_utils_archives қалтасына салыңыз.

   - ri_utils_win32.zip
   - ri_utils_arm64.zip

   Мұрағаттарды қайта атамаңыз.

Енді Басқару серверінде қажетті тәуелділіктер бар.

Жеке орнату пакетінің үшінші тұлғаларға қолжетімсіз болғанына көз жеткізіңіз.

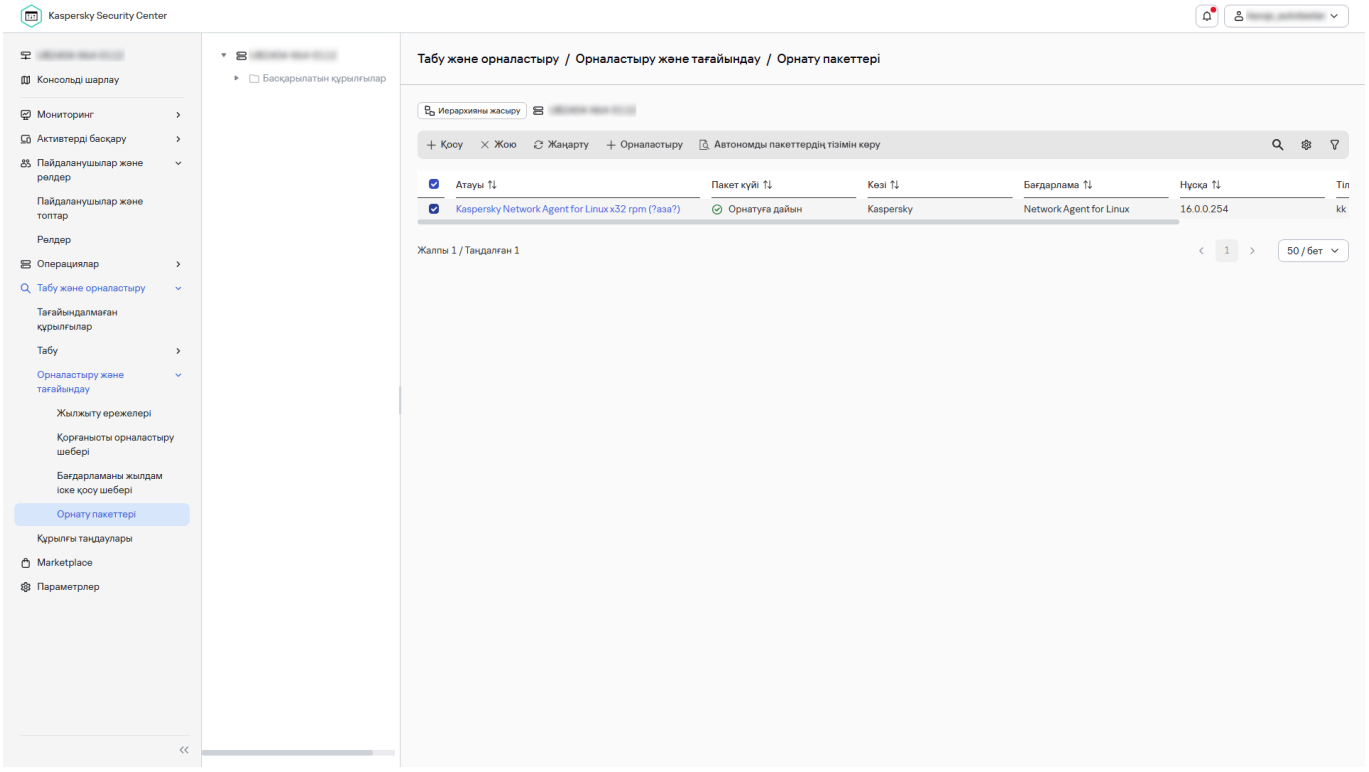
Жеке орнату пакетін жасау үшін:

1. Бағдарламаның негізгі терезесінде **Бағдарламалық жасақтаманы басқару** → **Орнату пакеттері** бөліміне өтіңіз.

   Басқару серверінде қолжетімді орнату пакеттерінің тізімі көрсетіледі.

Өлшемі, файл хэші және жолы туралы ақпарат желілік агент автономды пакеті немесе виртуалды басқару серверлерінде жасалған кез келген пакет үшін орнату пакеттерінің тізімінде қолжетімді емес. Бұл автономды пакеттер жүктеп алу кезінде жасалады.

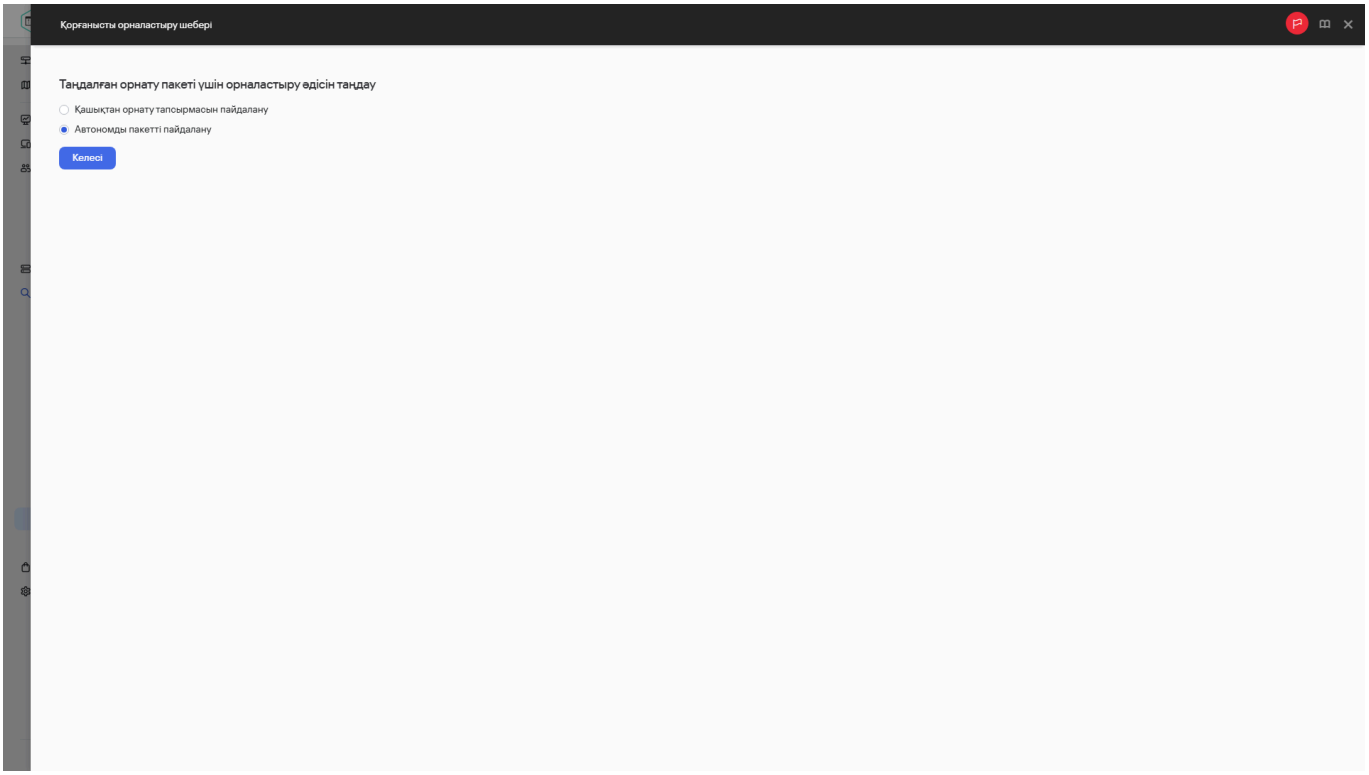
2. Орнату пакеттері тізімінен пакетті таңдап, тізімнің үстінде **Орналастыру** түймесін басыңыз.



Орнату пакеттерінің тізімі

3. **Автономды пакетті пайдалану** параметрін таңдаңыз.

Нәтижесінде, автономды орнату пакетін жасау шебері іске қосылады. Шебердің жұмысын жалғастыру үшін **Келесі** түймесін басыңыз.



Орнату пакеті үшін орналастыру әдісін таңдау

4. Таңдалған бағдарламамен бірге Желілік агентті орнату керек болса, **Желілік агентті осы бағдарламамен бірге орнату** параметрі қосылғанына көз жеткізіңіз.

   Опция автономды орнату пакетін жасайтын қолданбаға байланысты көрсетіледі.

   Әдепкі бойынша, параметр қосулы. Құрылғыда Желілік агенттің орнатылғанына сенімді болмасаңыз, осы параметрді қосу ұсынылады. Желілік агент құрылғыда бұрыннан орнатылған болса, онда Желілік агентпен бірге жеке орнату пакетін орнатқаннан кейін, Желілік агент ең жаңа нұсқасына дейін жаңартылатын болады.

   Осы параметрді өшіретін болсаңыз, Желілік агент құрылғыға орнатылмайды және құрылғы басқарылатын болмайды.

   Егер таңдалған бағдарлама үшін жеке орнату пакеті Басқару серверінде бұрыннан бар болса, шебер бұл туралы хабарды көрсетеді. Бұл жағдайда, келесі әрекеттердің бірін таңдауыңыз керек:

   - **Жеке орнату пакетін жасау**. Бағдарламаның жаңа нұсқасы үшін жеке орнату пакетін жасағыңыз келсе және сіз бұған дейін жасаған бағдарламаның алдыңғы нұсқасы үшін жеке орнату пакетінің қалғанын қаласаңыз, осы параметрді таңдаңыз. Жаңа жеке орнату пакеті басқа қалтада орналасқан.

   - **Бар жеке орнату пакетін пайдалану**. Бар жеке орнату пакетін пайдалануды қаласаңыз, осы параметрді таңдаңыз. Пакет жасау процесі іске қосылмайды.

   - **Бұрыннан бар жеке орнату пакетін қайта құрастыру**. Дәл осы бағдарлама үшін жеке орнату пакетін тағы да жасағыңыз келсе, осы параметрді таңдаңыз. Жеке орнату пакеті дәл осы қалтада орналастырылады.

5. **Басқарылатын құрылғылар тізіміне жылжыту** қадамындағы **Құрылғыларды жылжытпау** параметрі әдепкі бойынша таңдалған. Желілік агентті орнатқаннан кейін, клиент құрылғысын қандай да бір басқару тобына жылжытқыңыз келмесе, осы опцияны таңдалған күйде қалдырыңыз.

   Желілік агентті орнатқаннан кейін, клиент құрылғысын жылжытқыңыз келсе, **Тағайындалмаған құрылғыларды осы топқа жылжыту** параметрін таңдаңыз және клиент құрылғысын жылжытқыңыз келетін басқару тобын көрсетіңіз. Әдепкі бойынша, құрылғылар **Басқарылатын құрылғылар** тобына жылжытылады.



Клиент құрылғысын жылжыту үшін басқару тобын таңдау

6. Автономды орнату пакетін жасау процесі аяқталғаннан кейін, **Аяқтау** түймесін басыңыз.

   Автономды орнату пакетін жасау шебері жабылады.

Жеке орнату пакеті жасалып, Басқару серверінің ортақ қатынасы бар қалтасының PkgInst салынған қалтасына орналастырылған. Орнату пакеттері тізімінің үстінде орналасқан **Автономды пакеттердің тізімін көру** түймесін басып, жеке орнату пакеттері тізімін қарап шыға аласыз.

Желілік агенттің орнату пакетінің параметрлері

Желілік агенттің орнату пакетінің параметрлерін конфигурациялау үшін:

1. Бағдарламаның негізгі терезесінде **Бағдарламалық жасақтаманы басқару** → **Орнату пакеттері** бөліміне өтіңіз.

   Басқару серверінде қолжетімді орнату пакеттерінің тізімі көрсетіледі.

2. Желілік агенттің орнату пакетінің атауын басыңыз.

Желілік агенттің орнату пакетінің сипаттары терезесі ашылады.

Желілік агенттің орнату пакетінің параметрлері келесі қойындыларда топталған:

- **Жалпы** қойындысы

  Бұл қойындыда орнату пакеті туралы келесі ақпарат көрсетілген:

  - Орнату пакетінің атауы
  - Орнату пакеті жасалған бағдарламаның атауы және нұсқасы
  - Орнату пакетінің өлшемі
  - Орнату пакетін жасау күні
  - Орнату пакетін орналастыру қалтасына апаратын жол

- **Параметрлер** қойындысы

  Бұл қойындыда желілік агент орнатылғаннан кейін бірден оның жұмысын қамтамасыз ету үшін қажетті параметрлер берілген.

  - **Параметрлер** бөлімі

    - **Әдепкі қалтаға орнату**

      Осы нұсқа таңдалған болса, Желілік агент <Диск>:\Program Files\Kaspersky Lab\NetworkAgent қалтасына орнатылады. Мұндай қалта болмаса, ол автоматты түрде жасалады.

      Әдепкі бойынша, осы нұсқа таңдалған.

    - **Белгіленген қалтаға орнату**

      Егер бұл нұсқа таңдалса, Желілік агент енгізу өрісінде көрсетілген қалтаға орнатылады.

- **Жою құпиясөзін пайдалану**

  Опция қосулы болса, жою үшін құпиясөзді енгізуге болады (тек Windows операциялық жүйелері бар құрылғылардағы желілік агент үшін қолжетімді).

  Әдепкі бойынша, параметр өшірулі.

- **Желілік агент қызметін рұқсатсыз өшіруден немесе тоқтатудан қорғау және параметрлердегі өзгерістердің алдын алу**

  Желілік агент басқарылатын құрылғыға орнатылғаннан кейін, құрамдасты қажетті құқықтарсыз жою немесе өзгерту мүмкін емес. Желілік агенттің жұмысын тоқтату мүмкін емес. Бұл параметр домен контроллерлеріне әсер етпейді.

  Жергілікті әкімші құқықтарымен басқарылатын жұмыс станцияларында Желілік агентті қорғау үшін осы параметрді қосыңыз.

  Әдепкі бойынша, параметр өшірулі.

- **Белгісіз күйге ие компоненттер үшін қолданылатын жаңартулар мен патчтарды автоматты түрде орнату**

  Бұл опция қосулы болса, басқару серверіне, желілік агентке, Kaspersky Security Center Web Console консолінe және iOS MDM серверіне жүктеп алынған барлық жаңарту мен патч автоматты түрде орнатылады.

  Бұл параметр өшірулі болса, жүктелген жаңартулар мен патчтар, олардың күйін *Расталды* деп өзгерткеннен кейін ғана орнатылатын болады. *Анықталмаған* күйі бар жаңартулар мен патчтар орнатылмайды.

  Әдепкі бойынша, параметр қосулы.

- **Қосылым** бөлімі

  Бұл бөлімде Желілік агенттің Басқару серверіне қосылу параметрлерін конфигурациялауға болады. Қосылымды орнату үшін SSL протоколын немесе UDP протоколын пайдалануға болады. Қосылымды орнату үшін келесі параметрлерді көрсетіңіз:

  - **Басқару серверінің мекенжайы**

    Басқару сервері орнатылған құрылғының мекенжайы.

  - **Порт нөмірі**

    Қосылым орындалатын порт нөмірі.

  - **SSL порты**

    SSL протоколының көмегімен қосылым орындалатын порт нөмірі.

  - **Сервер сертификатын пайдалану**

    Бұл опция қосылса, желілік агенттің басқару серверіне қол жеткізуін авторизациялау үшін **Сертификат файлын таңдау** түймесін басқан кезде көрсетуге болатын сертификат файлы пайдаланылады.

    Бұл опция өшірулі болса, желілік агент **Басқару серверінің мекенжайы** өрісінде көрсетілген мекенжайға бірінші рет қосылған кезде, сертификат файлы басқару серверінен алынады.

    Параметрді өшіру ұсынылмайды, себебі Серверге қосылған кезде Желілік агентпен Басқару серверінің сертификатын автоматты түрде алу қауіпсіз емес болып табылады.

    Әдепкі бойынша, параметр өшірулі.

- **SSL байланысын пайдалану**

  Бұл параметр қосулы болса, Басқару серверіне қосылу SSL протоколының көмегімен, қорғалған порт арқылы орындалатын болады.

  Әдепкі бойынша, параметр өшірулі. Сіздің қосылымыңыз қауіпсіз болып қала беруі үшін, бұл параметрді өшірмеу ұсынылады.

- **UDP портын пайдалану**

  Егер бұл параметр қосулы болса, Желілік агентінің Басқару серверіне қосылуы UDP порты арқылы жүзеге асырылады. Бұл, клиент құрылғыларын басқаруға және олар туралы ақпарат алуға мүмкіндік береді.

  UDP порты Желілік агент орнатылған басқарылатын құрылғыларда ашық болуы керек. Сондықтан бұл параметрді өшірмеу ұсынылады.

  Әдепкі бойынша, параметр қосулы.

- **UDP порты**

  Өрісте Басқару серверін UDP протоколы бойынша Желілік агентке қосу портының нөмірін көрсетуге болады.

  Әдепкі бойынша, UDP портының нөмірі – 15000.

- **Прокси-серверді пайдаланбау**

  Бұл опция қосылса, құрылғыны басқару серверіне қосу үшін тікелей қосылым қолданылады.

- **Прокси-серверді пайдалану**

  Бұл параметр қосылса, прокси сервер параметрлерін көрсетіңіз:

  - **Прокси-сервердің мекенжайы**
  - **Прокси-сервердің порты**

  Егер сіздің прокси серверіңіз аутентификацияны қажет етсе, **Прокси-сервердегі аутентификация** параметрін қосыңыз және прокси серверге қосылым орнатылған тіркелгінің **Пайдаланушы аты** мен **Құпиясөз** көрсетіңіз. Прокси-сервердегі түпнұсқалық растама үшін ғана талап етілетін ең аз құқықтарға ие есептік жазба деректерін беру ұсынылады.

- **Microsoft Windows желілік экранында Желілік агенттің порттарын ашу**

  Параметр қосылса, Желілік агент пайдаланатын порттар Microsoft Windows брандмауэрінің ерекшеліктер тізіміне қосылады.

  Әдепкі бойынша, параметр қосулы.

  > Бұл опция Windows іске қосылған құрылғыларға арналған желілік агенттің орнату пакеттері үшін ғана қолжетімді.

- **Кеңейтілген** бөлімі

  Бұл бөлімде қосылым шлюзін пайдалану жолын конфигурациялауға болады.

Параметрлердің **Қосылым шлюзі** тобында құрылғы мен басқару сервері арасындағы қосылым әдісін конфигурациялауға болады:

- **Желілік агентті DMZ режимінде қосылым шлюзі ретінде пайдалану**

  Бұл опция қосулы болса, басқару серверін қосу, онымен байланыс орнату және деректерді тасымалдау кезінде желілік агенттегі деректерді қорғау үшін демилитаризацияланған аймақта (DMZ) желілік агент қосылым шлюзі ретінде қолданылады.

- **Басқару серверіне қосылу шлюзі арқылы қосылу**

  Бұл опция қосулы болса, басқару серверінің бірнеше қосылымын азайту үшін қосылым шлюзін пайдалану арқылы басқару серверінің қосылымы орнатылады. Бұл жағдайда қосылым шлюзі ретінде қолданылатын құрылғының мекенжайын **Қосылым шлюзінің мекенжайы** өрісіне енгізіңіз.

Желіде виртуалды машиналар болса, параметрлердің **Виртуалды машина** тобында Virtual Desktop Infrastructure (VDI) қосылымын конфигурациялауға болады:

- **VDI үшін динамикалық режимді қосу**

  Параметр қосулы болса, виртуалды машинада орнатылған Желілік агент үшін Virtual Desktop Infrastructure (VDI) үшін динамикалық режим қосылады.

  Әдепкі бойынша, параметр өшірулі.

- **VM параметрлерін оңтайландыру**

  Егер параметр қосулы болса, Желілік агенттің параметрлерінде келесі функциялар өшіріледі:

  - Орнатылған бағдарламалық жасақтама туралы ақпарат алу
  - Аппараттық жасақтама туралы ақпарат алу
  - Осалдықтардың болуы туралы ақпарат алу
  - Қажетті жаңартулар туралы ақпарат алу

  Әдепкі бойынша, параметр өшірулі.

Linux құрылғыларына желілік агентті орнатқаннан кейін, пайдаланушыларға құрылғы иелері ретінде тіркелуге автоматты түрде нұсқау бергіңіз келсе, **Желілік агентті орнатқаннан кейін пайдаланушыны тіркеу утилитасын іске қосуға рұқсат беру** опциясын қосыңыз.

Бұл опция қосылса, желілік агент орнатылғаннан кейін, пайдаланушыны құрылғы иесі ретінде тіркеу утилитасы іске қосылады. Әдепкі бойынша, параметр өшірулі.

- **Тегтер** бөлімі

  Тегтер бөлімінде клиент құрылғыларына Желілік агентті орнатқаннан кейін, оларға қосуға болатын кілт сөздер (тегтер) тізімі көрсетіледі. Сіз тізімдегі тегтерді қоса аласыз және жоя аласыз, сондай-ақ атауын өзгерте аласыз.

  Тегтің жанында жалауша қойылған болса, онда тег, басқарылатын құрылғыларға Желілік агентті орнату кезінде автоматты түрде қосылады.

  Тегтің жанындағы жалауша алынып тасталса, онда тег, басқарылатын құрылғыларға Желілік агентті орнату кезінде автоматты түрде қосылмайды. Бұл тегті құрылғыларға қолмен қосуға болады.

  Тегті тізімнен алып тастаған кезде, тег қосылған барлық құрылғылардан автоматты түрде алынады.

Автоматты тэг енгізу ережелері Linux және macOS жүйесімен жұмыс істейтін құрылғыларға арналған Желілік агенттің орнату пакеттеріне қолданылмайды.

- **Автономды пакеттер** қойындысы

  Бұл қойындыда келесі әрекеттерді орындауға болады:

  - Қолжетімді автономды орнату пакеттерінің тізімін көру.
  - **Жариялау** түймесін пайдаланып, Веб-серверде жеке орнату пакетін жариялау. Жарияланған жеке орнату пакетін, жеке орнату пакетіне сілтеме жіберген пайдаланушыларға жүктеп алуға болады.
  - **Жариялауды болдырмау** түймесін басу арқылы Веб-серверде жеке орнату пакетін жариялаудан бас тарту. Жарияланбаған жеке орнату пакетін тек сізге және басқа әкімшілерге жүктеуге болады.
  - **Жүктеп алу** түймесін басу арқылы құрылғыға жеке орнату пакетін жүктеп алу.
  - **Электрондық пошта арқылы жіберу** түймесін басу арқылы офлайн жеке пакетіне сілтемесі бар электрондық поштаны жіберу.
  - **Жою** түймесін басып, жеке орнату пакетін жою.

- **Тексерістер журналы** қойындысы

  Бұл қойындыда орнату пакетінің тексерістер журналын қарап шығуға болады. Сіз тексерулерді салыстыра аласыз, тексерулерді қарап шыға аласыз, тексерулерді файлға сақтай аласыз, тексерулердің сипаттамасын қоса аласыз және өзгерте аласыз.

Kaspersky Security Center Linux қалыптастырған автономды пакеттерді іске қосу

Желілік агент пен қолданбаларды бастапқы орналастырудың жоғарыда сипатталған тәсілдері барлық қажетті шарттарды орындай алмағандықтан, жүзеге аса бермеуі мүмкін. Мұндай жағдайларда, Kaspersky Security Center Linux құралдарымен орнатудың қажетті параметрлері бар әкімші дайындаған орнату пакеттерінен *жеке орнату пакеті* деп аталатын бірыңғай орындалатын файл жасауға болады. Мұның мәні болса (Веб-серверге құрылғы пайдаланушылары үшін сырттан қатынасу конфигурацияланған), жеке орнату пакеті ішкі Веб-серверде (Kaspersky Security Center Linux құрамына кіретін), сондай-ақ Kaspersky Security Center Web Console құрамына кіретін арнайы орналастырылған Веб-серверде жариялануы мүмкін. Автономды пакеттерді басқа Веб-серверге де көшіруге болады.

Kaspersky Security Center Linux бағдарламасының көмегімен, таңдалған пайдаланушыларға ортақ қатынасы бар қалтадағы осы файлға сілтемені электрондық пошта арқылы (интерактивті түрде немесе "тыныш" орнату "-s" кілтімен) файлды іске қосу туралы өтінішпен бірге таратуға болады. Жеке орнату пакетін, Веб-серверге қатынаса алмайтын құрылғыларды пайдаланушылар үшін электрондық пошта хабаррына тіркеуге болады. Әкімші автономды пакетті алынбалы дискке көшіре алады және пакетті кейін іске қосу мақсатымен қажетті құрылғыға жеткізе алады.

Автономды пакетті Желілік агент пакетінен, басқа қолданба пакетінен (мысалы, қауіпсіздік бағдарламасынан) немесе бірден екі пакеттен де жасауға болады. Егер автономды пакет Желілік агент пен басқа қолданбадан жасалса, онда орнату Желілік агенттен басталады.

Желілік агентпен автономды пакетті жасау кезінде, Желілік агентті орнату аяқталғаннан кейін жаңа құрылғылар (бұрын басқару топтарында орналастырылмаған) автоматты түрде көшірілетін басқару тобын көрсетуге болады.

Автономды пакеттер интерактивті түрде (әдепкі бойынша), оларға кіретін қолданбаларды орнату нәтижесін көрсете отырып немесе "тыныш" режимде ("-s" кілтімен іске қосылғанда) жұмыс істей алады. "Тыныш" режимді кез келген скрипттерден орнату үшін пайдалануға болады (мысалы, операциялық жүйенің кескінін орналастыру аяқталғаннан кейін іске қосылатын скрипттерден және т.с.с.). "Тыныш" режимде орнату нәтижесі процесті қайтару кодымен анықталады.

Бағдарламаларды автономды пакеттердің көмегімен орнату

Kaspersky Security Center бағдарламалардың автономды орнату пакеттерін қалыптастыруға мүмкіндік береді. Жеке орнату пакеті, Веб-серверге орналастыруға, пошта арқылы жіберуге немесе клиент құрылғысына басқа тәсілмен жіберуге болатын орындалатын файл болып саналады. Бағдарламаны Kaspersky Security Center қатысуынсыз орнату үшін, алынған файлды клиент құрылғысында жергілікті түрде іске қосуға болады.

Қолданбаны автономды орнату пакеті арқылы орнату үшін:

1. Бағдарламаның негізгі терезесінде **Бағдарламалық жасақтаманы басқару** → **Орнату пакеттері** бөліміне өтіңіз.

2. Қажетті қолданбаның орнату пакетінің жанындағы ұяшықты белгілеп, **Орналастыру** түймесін басыңыз.

3. Ашылған терезеде **Автономды пакетті пайдалану** опциясын таңдап, **Келесі** түймесін басыңыз.

   Нәтижесінде автономды орнату пакетін жасау шебері іске қосылады. Шебердің жұмысын жалғастыру үшін **Келесі** түймесін басыңыз.

4. **Жеке орнату пакетін жасау** опциясын таңдаңыз.

5. Желілік агент орнатылғаннан кейін, құрылғыларды басқару тобына жылжыту керек пе екенін көрсетіңіз.

6. Шебердің соңғы қадамында автономды орнату пакетін клиенттік құрылғыға тасымалдау әдісін таңдап, шеберді аяқтау үшін **Аяқтау** түймесін басыңыз.

7. Бағдарламаның жеке орнату пакетін клиент құрылғысына жіберіңіз.

8. Жеке орнату пакетін клиент құрылғысында іске қосыңыз.

   Нәтижесінде, бағдарлама автономды пакетте көрсетілген параметрлері бар клиент құрылғысында орнатылады.

Жасау кезінде, жеке орнату пакеті Веб-серверде автоматты түрде жарияланады. Автономды пакетті жүктеу сілтемесі, жасалған автономды орнату пакеттерінің тізімінде көрсетіледі. Қажет болса, таңдалған автономды пакетті жариялауды болдырмай, оны Веб-серверде қайта жариялауыңызға болады. Әдепкі бойынша, автономды орнату пакеттерін жүктеу үшін 8060 порты қолданылады.

Қауіпсіздік бағдарламасының орнату пакетіндегі дерекқорларды жаңартудың орындылығы

Орналастыру алдында, қауіпсіздік бағдарламасының дистрибутивімен бірге таратылатын антивирустық дерекқорларды (автопатч модульдерін қоса) жаңарту мүмкіндігін ескеру қажет. Орналастыруды бастамас бұрын қолданбаның орнату пакетінің құрамындағы дерекқорларды мәжбүрлеп жаңартқан жөн (мысалы, таңдалған орнату пакетінің мәнмәтіндік мәзіріндегі тиісті пәрменді қолдану арқылы). Бұл құрылғыларда қорғанысты орналастыруды аяқтау үшін қажет қайта жүктеу санын азайтады.

Пайдаланушының орнату пакетінің өлшеміне қойылған шектеулерді өзгерту

Таңдаулы орнату пакетін жасау кезінде шығарып алынған деректердің жалпы өлшемі шектеулі. Әдепкі бойынша шектеуі – 1 ГБ.

Егер сіз ағымдағы шектеуден асатын деректерді қамтитын мұрағат файлын жүктеуге тырыссаңыз, қате туралы хабар пайда болады. Үлкен дистрибутивтерден орнату пакеттерін жасау кезінде сізге осы максималды мәнді арттыру қажет болуы мүмкін.

Конфигурацияланатын орнату пакетінің өлшемі үшін максималды мәнді өзгерту үшін:

1. Басқару сервері құрылғысында Басқару серверін орнату үшін пайдаланылған есептік жазбаның астындағы пәрмен жолын іске қосыңыз.

2. Ағымдағы қалтаны Kaspersky Security Center Linux орнату қалтасына өзгертіңіз (әдетте /opt/kaspersky/ksc64/sbin).

3. Басқару серверді орнату түріне байланысты, root есептік жазбасында келесі пәрмендердің бірін енгізіңіз:

   - Кәдімгі жергілікті орнату:

     ```
     klscflag -fset -pv klserver -n MaxArchivePkgSize -t d -v <байттар_саны>
     ```

   - Ақауларға төзімді Kaspersky Security Center Linux кластеріне орнату:

     ```
     klscflag -fset -pv klserver -n MaxArchivePkgSize -t d -v <байттар_саны> --stp klfoc
     ```

   Мұндағы <байттар_саны> – он алтылық немесе ондық пішімдегі байттар саны.

   Мысалы, егер талап етілетін максималды мән 2 ГБ болса, 2147483648 ондық мәнін немесе 0x80000000 он алтылық мәнін көрсетуге болады. Бұл жағдайда, Басқару серверін жергілікті орнату үшін келесі пәрменді пайдалануға болады:

   ```
   klscflag -fset -pv klserver -n MaxArchivePkgSize -t d -v 2147483648
   ```

Орнату пакетінің пайдаланушы деректерінің өлшеміне шектеу өзгертілді.

Орнату пакеттерін қосалқы Басқару серверлеріне тарату

Kaspersky Security Center Linux бағдарламасы сізге Kaspersky бағдарламалары үшін және үшінші тарап бағдарламалары үшін орнату пакеттерін жасауға, сондай-ақ орнату пакеттерін клиент құрылғыларына таратуға және пакеттерден бағдарламалар орнатуға мүмкіндік береді. Негізгі Басқару серверіндегі жүктемені оңтайландыру үшін, орнату пакеттерін қосалқы Басқару серверлеріне таратуға болады. Осыдан кейін, қосалқы Серверлер пакеттерді клиент құрылғыларына жібереді, содан кейін сіз клиент құрылғыларына бағдарламаларды қашықтан орната аласыз.

Орнату пакеттерін қосалқы Басқару серверлеріне тарату үшін:

1. Қосалқы Басқару серверлері негізгі Басқару серверіне қосылғанына көз жеткізіңіз.
2. Бағдарламаның негізгі терезесінде **Тапсырмалар** бөліміне өтіңіз.

   Тапсырмалар тізімі көрсетіледі.
3. **Қосу** түймесін басыңыз.

   Жаңа тапсырма жасау шебері іске қосылады. Содан кейін, шебердің нұсқауларын орындаңыз.
4. **Жаңа тапсырма параметрлері** бетінде, **Бағдарлама** ашылмалы тізімінен **Kaspersky Security Center** тармағын таңдаңыз. Содан соң, **Тапсырма түрі** ашылмалы тізімінен **Орнату пакетін тарату** тармағын таңдап, тапсырманың атауын көрсетіңіз.
5. **Тапсырма ауқымы** бетінде тапсырма тағайындалған құрылғыларды келесі тәсілдердің бірімен таңдаңыз:

   - Егер сіз белгілі бір басқару тобының барлық қосалқы Серверлері үшін тапсырма жасағыңыз келсе, сол топты таңдап, ол үшін топтық тапсырма құруды бастаңыз.
   - Егер сіз белгілі бір қосалқы Басқару серверлері үшін тапсырма жасағыңыз келсе, сол Серверлерді таңдап, олар үшін тапсырма жасаңыз.
6. **Таратылған орнату пакеттері** бетінде қосалқы Басқару серверлеріне көшіру қажет орнату пакеттерін таңдаңыз.
7. Осы есептік жазба астында *Орнату пакетін тарату* тапсырмасын іске қосу үшін есептік жазбаны көрсетіңіз. Сіз өзіңіздің есептік жазбаңызды қолданып, **Әдепкі есептік жазба** параметрін қосулы күйде қалдыра аласыз. Сонымен қатар, тапсырма қажетті қатынасу құқықтары бар басқа есептік жазбада орындалуы керек екенін көрсетуге болады. Ол үшін **Есептік жазбаны көрсету** параметрін таңдап, сол есептік жазбаның есептік деректерін енгізіңіз.
8. **Тапсырманы жасауды аяқтау** бетінде, тапсырма сипаттары терезесін ашу үшін **Жасап болған соң, тапсырма туралы мәліметтерді ашу** параметрін қосып, әдепкі бойынша тапсырма параметрлерін өзгертуге болады. Сондай-ақ, тапсырма параметрлерін кейінірек, кез келген уақытта конфигурациялауға болады.
9. **Аяқтау** түймесін басыңыз.

   Орнату пакеттерін қосалқы Басқару серверлеріне тарату үшін жасалған тапсырма тапсырмалар тізімінде көрсетіледі.
10. Тапсырманы қолмен іске қосыңыз немесе тапсырма параметрлерінде көрсетілген кестеге сәйкес оның іске қосылуын күтіңіз.

Тапсырманы орындағаннан кейін, таңдалған орнату пакеттері көрсетілген қосалқы басқару серверлеріне көшіріледі.

Жеке орнату пакеттері тізімін қарау

Жеке орнату пакеттерінің тізімін және әрбір жеке орнату пакетінің сипаттарын көруге болады.

Барлық орнату пакеттеріне арналған жеке орнату пакеттерінің тізімін көру үшін:

Автономды пакеттердің тізімін көру түймесін басыңыз.

Тізімдегі жеке орнату пакеттерінің сипаттары келесідей көрсетіледі:

- **Пакет атауы**. Пакетке енгізілген бағдарламаның атауынан және нұсқасынан автоматты түрде жасалатын жеке орнату пакетінің атауы.
- **Бағдарлама атауы**. Жеке орнату пакетіне кіретін бағдарламаның атауы.
- **Бағдарламаның нұсқасы**.
- **Желілік агентті орнату пакетінің атауы**. Параметр тек жеке орнату пакетіне Желілік агент қосылған жағдайда ғана көрсетіледі.
- **Желілік агенттің нұсқасы**. Параметр тек жеке орнату пакетіне Желілік агент қосылған жағдайда ғана көрсетіледі.
- **Өлшемі**. Файл өлшемі (МБ).
- **Топ**. Желілік агент орнатылғаннан кейін клиент құрылғысы жылжытылатын топтың аты.
- **Жасалған күні**. Жеке орнату пакетін құру күні мен уақыты.
- **Өзгертілген**. Жеке орнату пакетін өзгерту күні мен уақыты.
- **Жолы**. Жеке орнату пакеті орналасқан қалтаға толық жол.
- **Веб-мекенжай**. Жеке орнату пакетінің орналасқан веб-мекенжайы.
- **Файл хэші**. Параметр, жеке орнату пакетін үшінші тараптар өзгертпегенін және пайдаланушыда сіз жасаған және пайдаланушыға жіберген бірдей файл бар екенін растау үшін пайдаланылады.

Өлшемі, файл хэші және жолы туралы ақпарат желілік агент автономды пакеті немесе виртуалды басқару серверлерінде жасалған кез келген пакет үшін орнату пакеттерінің тізімінде қолжетімді емес. Бұл автономды пакеттер жүктеп алу кезінде жасалады.

Белгілі бір орнату пакеті үшін жеке орнату пакеттерінің тізімін көру үшін,

тізімнен орнату пакетін таңдап, тізімнің үстінен **Автономды пакеттердің тізімін көру** түймесін басыңыз.

Жеке орнату пакеттерінің тізімінде сіз келесі әрекеттерді орындай аласыз:

- **Жариялау** түймесін пайдаланып, Веб-серверде жеке орнату пакетін жариялау. Жарияланған жеке орнату пакетін, жеке орнату пакетіне сілтеме жіберген пайдаланушыларға жүктеп алуға болады.
- **Жариялауды болдырмау** түймесін басу арқылы Веб-серверде жеке орнату пакетін жариялаудан бас тарту. Жарияланбаған жеке орнату пакетін тек сізге және басқа әкімшілерге жүктеуге болады.
- **Жүктеп алу** түймесін басу арқылы құрылғыға жеке орнату пакетін жүктеп алу.
- **Электрондық пошта арқылы жіберу** түймесін басу арқылы офлайн жеке пакетіне сілтемесі бар электрондық поштаны жіберу.
- **Жою** түймесін басып, жеке орнату пакетін жою.

Linux үшін желілік агент орнату

Ұйымның құрылғыларын басқару үшін құрылғыларға Желілік агентті орнату қажет. Ұйымның құрылғыларында Kaspersky Security Center Linux таратылған қолданбасын орналастыру әдетте оларға Желілік агентті орнатудан басталады.

Linux басқарылатын құрылғысына желілік агент орнатудың келесі әдістері бар:

- Басқарылатын құрылғыға SSH арқылы қосылу және қашықтан орнату тапсырмасын орындау арқылы.
- Басқарылатын құрылғыда пакет орнатуды іске қосу арқылы.

Құрылғыға желілік агент орнатылғаннан кейін, осы желілік агент арқылы сол құрылғыда Kaspersky қолданбаларын қашықтан орнатуға болады. Бұл ретте, орнатылатын бағдарламаның дистрибутивін әкімші көрсеткен орнату параметрлерімен бірге жіберу, Желілік агенттер мен Басқару сервері арасындағы байланыс арналары арқылы жүзеге асырылады. Дистрибутивті жіберу үшін тарату нүктелері, көп мекенжайлы таратылым және басқа да құралдар түріндегі аралық тарату орталықтарын пайдалануға болады.

Басқарылатын желіде бағдарламаларды орналастыру тәсілі мен стратегиясын таңдай отырып, бірқатар факторларды назарға алған жөн (тізімі толық емес):

- Ұйым желісінің конфигурациясын.
- Құрылғылардың жалпы саны.
- Ұйым желісінде ешқандай домен мүшесі емес құрылғылардың болуы және мұндай құрылғыларда басқару құқықтары бар біріздендірілген есептік жазбалардың болуы.
- Басқару сервері мен құрылғылар арасында арнаның ені.
- Басқару сервері және қашықтағы ішкі желілер арасындағы байланыс түрі және мұндай ішкі желілердің ішінде желілік арналардың ені.
- Қашықтағы құрылғыларда орналастырудың басында қауіпсіздік параметрлері қолданылады. Бұл параметрлер басқарылатын құрылғыға қашықтан қосылым орнатуға және орнатуды бастауға мүмкіндік береді.

Linux құрылғысын желілік агентті орнатуға дайындау

Желілік агентті Linux құрылғысына орнатпай тұрып, кез келген Linux құрылғысына қажетті дайындық қадамдарын орындау керек.

Linux операциялық жүйесі бар құрылғыны Желілік агентті қашықтан орнатуға дайындау үшін:

1. Linux Желілік агентін орнатқыңыз келетін құрылғыда қолдау көрсетілетін Linux дистрибутивтерінің бірі жұмыс істейтініне көз жеткізіңіз.
2. Желілік агент бағдарламасын AltOS жүйесіне жабық бағдарламалық жасақтама ортасы режимінде орнатқыңыз келсе, орнату бағдарламасы аяқталғанша жабық бағдарламалық жасақтама ортасы режимін өшіріңіз.

3. Web Console интерфейсін пайдаланып немесе Kaspersky веб-сайтынан Желілік агентті орнату пакетін жүктеп алыңыз.

   Сізге glibc 2.5 нұсқасы бар Linux операциялық жүйесін іске қосатын құрылғыға Желілік агентті орнату қажет болса, Web Console интерфейсін пайдаланып немесе Kaspersky веб-сайтынан *Linux үшін Kaspersky Желілік агент Legacy* орнату пакетін жүктеп алуыңыз керек.

4. Linux операциялық жүйесі бар мақсатты құрылғыда келесі бағдарламалық жасақтама орнатылғанына көз жеткізіңіз:

   - Sudo (Ubuntu 10.04 үшін Sudo нұсқасы — 1.7.2p1 немесе одан кейінгі)
   - Perl тілі интерпретаторының 5.10 немесе одан жоғары нұсқасы
   - ps утилитасы

5. Құрылғының конфигурациясын тексеріңіз:

   a. Құрылғыға SSH арқылы қосылуға болатындығын тексеріңіз (мысалы, PuTTY бағдарламасы).

      Құрылғыға қосыла алмасаңыз, `/etc/ssh/sshd_config` файлын ашып, келесі параметрлердің төмендегі мәні бар екеніне көз жеткізіңіз:

      ```
      PasswordAuthentication no
      ChallengeResponseAuthentication yes
      ```

      > Құрылғыға қиындықсыз қосыла алсаңыз, /etc/ssh/sshd_config файлын өзгертпеңіз; әйтпесе қашықтан орнату тапсырмасын орындау кезінде SSH түпнұсқалық растама қатесіне тап болуыңыз мүмкін.

      `sudo service ssh restart` пәрменін қолдана отырып, файлды сақтаңыз (қажет болса) және SSH қызметін қайта іске қосыңыз.

   b. Linux негізіндегі тағайындалмаған құрылғыда TCP 22 портының ашық және қолжетімді екеніне көз жеткізіңіз.

      Linux үшін Желілік агентті сәтті орнату үшін TCP 22 порты қолжетімді болуы керек.

   c. Құрылғы қосылатын пайдаланушы есептік жазбасы үшін sudo құпия сөзін өшіріңіз.

   d. sudoers конфигурациялық файлын ашу үшін sudo `visudo` пәрменін қолданыңыз.

      Сіз ашқан файлда файлдың соңына келесі жолды қосыңыз: `<пайдаланушы аты> ALL = (ALL) NOPASSWD: ALL`. Бұл жағдайда, `<пайдаланушы аты>` — SSH протоколы арқылы құрылғыға қосылу үшін пайдаланылатын пайдаланушы есептік жазбасы. Astra Linux операциялық жүйесін пайдалансаңыз, соңғы жолды /etc/sudoers файлына келесі мәтінмен қосыңыз: `%astra-admin ALL=(ALL:ALL) NOPASSWD: ALL`

   e. sudoers файлын сақтаңыз және жабыңыз.

   f. SSH арқылы құрылғыға қайта қосылыңыз және `sudo whoami` пәрменінің көмегімен, sudo қызметі құпиясөзді қажет етпейтінін тексеріңіз.

6. systemd жұмысқа дайындау жүйесі бар операциялық жүйе іске қосылған құрылғыларға желілік агентті қашықтан орнатқыңыз келсе, `/etc/systemd/logind.conf` файлын ашып, келесі әрекеттердің бірін орындаңыз:

   - `KillUserProcesses` параметрі үшін `no` мәнін көрсетіңіз: `KillUserProcesses=no`.
   - `KillExcludeUsers` параметрі үшін, қашықтан орнату орындалатын есептік жазбаның пайдаланушы атауын енгізіңіз, мысалы, `KillExcludeUsers=root`.

   Astra Linux мақсатты құрылғысы

   Егер мақсатты құрылғы Astra Linux басқаруымен жұмыс істеп тұрса, `export PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin` экспорттау жолын `/home/< пайдаланушы аты >/.bashrc` файлына қосыңыз, мұндағы `< пайдаланушы аты >` – SSH арқылы құрылғыны қосу үшін пайдаланылатын пайдаланушы есептік жазбасы.

   ОСнова мақсатты құрылғысы

   Мақсатты құрылғыда ОСнова жұмыс істеп тұрса, мына қадамдарды орындаңыз:

   a. `/usr/lib/systemd/logind.conf/10-enable-kill-user-processes.conf` файлын ашыңыз және `#KillUserProcess=yes` жолағына түсініктеме беріңіз.

   b. `/usr/lib/NESS/pam-user-session` файлын ашыңыз және `#loginctl terminate-session "$XDG_SESSION_ID"` жолағына түсініктеме беріңіз.

   Өзгертілген параметрді қолдану үшін, Linux басқаруымен жұмыс істейтін құрылғыны қайта іске қосыңыз немесе келесі пәрменді іске қосыңыз:

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

7. SUSE Linux Enterprise Server 15 операциялық жүйесі бар құрылғыларға Желілік агентті орнатқыңыз келсе, алдымен Желілік агентті орнату үшін insserv-compat пакетін орнатыңыз.

8. Жабық бағдарлама ортасы режимінде жұмыс істейтін Astra Linux операциялық жүйесі жұмыс істейтін құрылғыларға Желілік агентті орнатқыңыз келсе, Astra Linux құрылғыларын дайындау үшін қосымша қадамдарды орындаңыз.

9. Ubuntu Server немесе Ubuntu Desktop 10.04 нұсқасы жұмыс істейтін құрылғыларға желілік агентті орнатқыңыз келсе, осы құрылғыларды дайындаудың қосымша қадамдарын орындаңыз.

10. Kaspersky Industrial CyberSecurity for Linux Nodes бағдарламасын glibc 2.5 нұсқасы қамтылған Linux операциялық жүйесі бар құрылғыға орнатқыңыз келсе, мақсатты құрылғыларды дайындау үшін қосымша қадамдарды орындаңыз.

11. Егер сіз AltOS жүйесінде жабық бағдарламалық жасақтама ортасы режимінде Желілік агент орнатып жатсаңыз, жабық бағдарламалық жасақтама ортасы режимін қайта қосыңыз.

12. Желілік агентті RED OS 7.3.4 не одан кейінгі нұсқадағы немесе MSVSPHERE 9.2 не одан кейінгі нұсқадағы операциялық жүйені қолданатын құрылғыларға орнатқыңыз келсе, желілік агенттің дұрыс жұмыс істеуіне арналған libxcrypt-compat пакетін орнатыңыз.

Linux құрылғысы желілік агентті орнатуға дайын. Желілік агентті қашықтан, интерактивті режимде немесе дыбыссыз режимде орнатуға болады.

SUSE Linux Enterprise Server 15 басқаратын құрылғыны Желілік агентті орнатуға дайындау

SUSE Linux Enterprise Server 15 арқылы жұмыс істейтін құрылғыға желілік агентті орнатпай тұрып, екі дайындық процедурасын орындау керек: біреуі төмендегі нұсқауларда сипатталған және Кез келген Linux құрылғысына арналған жалпы дайындық қадамдары.

SUSE Linux Enterprise Server 15 операциялық жүйесі бар құрылғыға Желілік агентті орнату үшін:

Желілік агентті орнатпас бұрын келесі пәрменді іске қосыңыз:

```
sudo zypper install insserv-compat
```

Бұл сізге insserv-compat пакетін орнатуға және Желілік агентті дұрыс конфигурациялауға мүмкіндік береді.

Пакеттің бұған дейін орнатылғанан тексеру үшін `rpm -q insserv-compat` пәрменін орындаңыз.

Егер сіздің желіңізде SUSE Linux Enterprise Server 15 жұмыс істейтін көптеген құрылғылар болса, сіз компанияның инфрақұрылымын конфигурациялау және басқару үшін арнайы бағдарламалық жасақтаманы пайдалана аласыз. Осы бағдарламалық жасақтаманы пайдаланып, insserv-compact пакетін бірден барлық қажетті құрылғыларға автоматты түрде орнатуға болады. Мысалы, сіз Puppet, Ansible, Chef қолдана аласыз немесе скриптті өзіңізге ыңғайлы етіп жасай аласыз.

Құрылғыда SUSE Linux Enterprise үшін GPG қол қою кілттері болмаса, келесі ескертуді көруіңіз мүмкін: `Package header is not signed!` Ескертуді елемеу үшін `i` опциясын таңдаңыз.

Linux құрылғысын дайындағаннан кейін желілік агентті қашықтан, интерактивті режимде немесе дыбыссыз режимде орнатуға болады.

Желілік агентті орнату үшін жабық бағдарлама ортасы режимінде Astra Linux басқаратын құрылғыны дайындау

Жабық бағдарлама ортасы режимінде Astra Linux жұмыс істейтін құрылғыға желілік агентті орнатпас бұрын екі дайындық процедурасын орындау керек: біреуі төмендегі нұсқауларда сипатталған және Linux операциялық жүйесі жұмыс істейтін кез келген құрылғы үшін жалпы дайындық қадамдары.

Осы нұсқаулықтары пәрмендерді root есептік жазбасы астында іске қосыңыз.

Желілік агентті орнату үшін жабық бағдарлама ортасы режимінде Astra Linux жұмыс істейтін құрылғыны дайындау үшін:

1. `/etc/digsig/digsig_initramfs.conf` файлын ашыңыз және келесі параметрлерді көрсетіңіз:

   ```
   DIGSIG_ELF_MODE=1
   ```

2. Пәрмен жолында үйлесімділік пакетін орнату үшін келесі пәрменді енгізіңіз:

   ```
   apt install astra-digsig-oldkeys
   ```

3. Бағдарлама кілті үшін директория жасаңыз:

   ```
   mkdir -p /etc/digsig/keys/legacy/kaspersky/
   ```

4. /opt/kaspersky/klnagent64/share/kaspersky_astra_pub_key.gpg қолданба кілтін алдыңғы қадамда жасалған каталогке қойыңыз:

   ```
   cp kaspersky_astra_pub_key.gpg /etc/digsig/keys/legacy/kaspersky/
   ```

   > Егер Kaspersky Security Center Linux жеткізілім жинағында kaspersky_astra_pub_key.gpg кілті болмаса, бұл кілтті https://media.kaspersky.com/utilities/CorporateUtilities/kaspersky_astra_pub_key.gpg сілтемесінен жүктеп алуға болады.

5. Дискілердің жедел жадын жаңартыңыз:

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

   Жүйені қайта жүктеңіз.

Linux құрылғысы желілік агентті орнатуға дайын. Желілік агентті қашықтан, интерактивті режимде немесе дыбыссыз режимде орнатуға болады.

glibc 2.5 (ескі ОС) бар Linux операциялық жүйесіне Желілік агент орнатуға дайындалуда

Желілік агентті glibc 2.5 нұсқасы (ескі ОЖ) бар Linux операциялық жүйесімен жұмыс істейтін құрылғыға орнатпас бұрын, екі дайындық процедурасын орындау керек: кез келген Linux құрылғысы үшін жалпы дайындық қадамдары және осы мақалада сипатталған процедура.

glibc 2.5 (ескі ОС) нұсқасы бар Linux операциялық жүйесіне Желілік агент бағдарламасын орнату үшін жергілікті орнатуды пайдалануды ұсынамыз. Егер сізге осы сценарий үшін қашықтан орнату тапсырмасын пайдалану қажет болса, төмендегі нұсқаулықта сипатталған қосымша қадамдарды орындауыңыз керек.

> Осы процедурадағы пәрмендерді root есептік жазбасы астында іске қосыңыз.

glibc 2.5 (ескі ОС) нұсқасы бар Linux операциялық жүйесіне Желілік агент бағдарламасын орнату үшін жергілікті орнатуды пайдалануды ұсынамыз. Егер сізге осы сценарий үшін қашықтан орнату тапсырмасын пайдалану қажет болса, төмендегі нұсқаулықта сипатталған қосымша қадамдарды орындауыңыз керек.

1. glibc 2.5 бар Linux операциялық жүйесін іске қосатын құрылғыда кез келген Linux құрылғысы үшін ортақ дайындық қадамдарын орындаңыз.

2. `/etc/sudoers` файлында `Defaults requiretty` жолын алып тастаңыз.

3. glibc 2.5 бар Linux операциялық жүйесін іске қосатын құрылғыда Желілік агентті орнату мақсатымен SSH қосылымдары үшін жарамды шифрлау алгоритмдерінің рұқсат тізімін өшіріңіз.

   Ол үшін Басқару сервері орнатылған құрылғыда немесе мақсатты құрылғыны қамтитын тарату нүктесі ретінде әрекет ететін құрылғыда пәрмен жолында келесі пәрменді орындаңыз:

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

Linux құрылғысы Желілік агентті қашықтан орнатуға дайын.

Жарамды шифрлау алгоритмдерінің рұқсат тізімі өшірілсе, SSH қосылымының қауіпсіздігіне әсер етуі мүмкін. Желілік агент орнату бағдарламасын орнатқаннан кейін бірден жарамды шифрлау алгоритмдерінің рұқсат етілген тізімін қайта қосуд ұсынамыз. Жарамды шифрлау алгоритмдерінің рұқсат етілген тізімін қайта қосу үшін келесі пәрменді орындаңыз:

```
klscflag -fset -pv ".core/.independent" -s "Transport" -n SSH_CLIENT_DISABLE_ALGS_PROTECT
-t d -v 0
```

Желілік агентті орнатып, жарамды шифрлау алгоритмдерінің рұқсат етілген тізімін қайта қосқаннан кейін, glibc 2.5 (ескі ОС) нұсқасы бар Linux операциялық жүйесін іске қосатын құрылғыны енді Басқару сервері басқарады.

OpenSSH 6.4 нұсқасы (ескірген ОЖ) бар Linux операциялық жүйесіне Желілік агентті орнатуға дайындық

OpenSSH 6.4 немесе одан бұрынғы нұсқасын (ескі ОЖ) пайдаланатын құрылғыға Желілік агентті орнату алдында екі дайындық процедурасын орындау керек – кез келген Linux құрылғысы үшін жалпы дайындық қадамдары және осы мақалада сипатталған процедура.

glibc 2.5 (ескі ОС) нұсқасы бар Linux операциялық жүйесіне Желілік агент бағдарламасын орнату үшін жергілікті орнатуды пайдалануды ұсынамыз. Егер сізге осы сценарий үшін қашықтан орнату тапсырмасын пайдалану қажет болса, төмендегі нұсқаулықта сипатталған қосымша қадамдарды орындауыңыз керек.

> Осы нұсқаулықтары пәрмендерді root есептік жазбасы астында іске қосыңыз.

Желілік агентті орнату үшін OpenSSH 6.4 немесе одан бұрынғы нұсқасын пайдаланатын құрылғыны дайындау үшін:

1. OpenSSH 6.4 немесе одан бұрынғы нұсқасын пайдаланатын құрылғыда кез келген Linux құрылғысына ортақ дайындық қадамдарын орындаңыз.

2. OpenSSH 6.4 немесе одан бұрынғы нұсқасы орнатылған құрылғыға желілік агентті орнату үшін SSH қосылымдарына арналған жарамды шифрлау алгоритмдерінің рұқсат тізімін өшіріңіз.

   Ол үшін Басқару сервері орнатылған құрылғыда немесе мақсатты құрылғыны қамтитын тарату нүктесі ретінде әрекет ететін құрылғыда пәрмен жолында келесі пәрменді орындаңыз:

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

Linux құрылғысы Желілік агентті қашықтан орнатуға дайын.

Жарамды шифрлау алгоритмдерінің рұқсат тізімі өшірілсе, SSH қосылымының қауіпсіздігіне әсер етуі мүмкін. Желілік агент орнату бағдарламасын орнатқаннан кейін бірден жарамды шифрлау алгоритмдерінің рұқсат етілген тізімін қайта қосуд ұсынамыз. Жарамды шифрлау алгоритмдерінің рұқсат етілген тізімін қайта қосу үшін келесі пәрменді орындаңыз:

```
klscflag -fset -pv ".core/.independent" -s "Transport" -n SSH_CLIENT_DISABLE_ALGS_PROTECT
-t d -v 0
```

Желілік агентті орнатып, жарамды шифрлау алгоритмдерінің рұқсат етілген тізімін қайта қосқаннан кейін, glibc 2.5 (ескі ОС) нұсқасы бар Linux операциялық жүйесін іске қосатын құрылғыны енді Басқару сервері басқарады.

Linux құрылғысына желілік агентті қашықтан орнату

Желілік агентті Linux негізіндегі құрылғыға орнатпай тұрып, барлық Linux негізіндегі құрылғыға қажетті жалпы дайындық қадамдарын аяқтау керек.

Жалпы қадамдарды орындағаннан кейін, операциялық жүйеңізге тән қосымша нұсқауларды орындауға болады:

- SUSE Linux Enterprise Server 15 арқылы жұмыс істейтін құрылғыны дайындау
- Жабық бағдарламалық жасақтама ортасы режимінде Astra Linux арқылы жұмыс істейтін құрылғыны дайындау
- Ubuntu Server/Desktop 10.04 және 16.04 нұсқалары бар құрылғыны дайындау
- Linux операциялық жүйесі бар glibc 2.5 қамтылған құрылғыны дайындау

Linux операциялық жүйесі бар құрылғыға Желілік агентті орнату үшін:

1. Орнату пакеттерін жүктеп алыңыз және жасаңыз:

   a. Пакетті құрылғыға орнатпас бұрын, онда осы пакетке арналған тәуелділіктер (бағдарламалар, кітапханалар) орнатылғанына көз жеткізіңіз.

   Пакет орнатылатын Linux дистрибутивіне тән утилиталарды қолдана отырып, әр пакетке арналған тәуелділіктерді өзіңіз қарап шыға аласыз. Утилиталар туралы ақпаратпен, өзіңіздің операциялық жүйеңізге қоса берілген құжаттамада таныса аласыз.

   b. Қашықтан орнату пакетін жасау үшін келесі файлдарды пайдаланыңыз:

   - klnagent.kpd;
   - akinstall.sh;
   - Желілік агенттің deb немесе rpm пакеті.

2. Бағдарламаны қашықтан орнату тапсырмасын келесі параметрлермен жасаңыз:

   - Жаңа тапсырма жасау шеберінің **Параметрлер** терезесінде **Басқару сервері арқылы операциялық жүйенің құралдарымен** жалаушасын қойыңыз. Барлық басқа жалаушаларды алып тастаңыз.
   - **Тапсырманы іске қосу үшін есептік жазбаны таңдау** бетінде, құрылғыға SSH арқылы қосылу мақсатымен пайдаланылатын есептік жазба параметрлерін көрсетіңіз.

3. Бағдарламаны қашықтан орнату тапсырмасын іске қосыңыз. Қоршаған ортаны сақтау үшін `su` пәрменіне арналған параметрді пайдаланыңыз: `-m, -p, --preserve-environment`.

Linux үшін Желілік агентті тыныш режимде орнату (жауап файлымен)

Сіз Linux операциялық жүйесі бар құрылғыларға Желілік агентті жауап файлы – орнату параметрлерінің пайдаланушы жиынтығын қамтитын мәтіндік файл: айнымалылар және олардың сәйкес мәндері арқылы орната аласыз. Жауаптар файлын қолдану арқасында орнатуды тыныш режимде, яғни пайдаланушының қатысуынсыз іске қосуға болады.

Желілік агентті Linux негізіндегі құрылғыға орнатпай тұрып, барлық Linux негізіндегі құрылғыға қажетті жалпы дайындық қадамдарын аяқтау керек.

Жалпы қадамдарды орындағаннан кейін, операциялық жүйеңізге тән қосымша нұсқауларды орындауға болады:

- SUSE Linux Enterprise Server 15 арқылы жұмыс істейтін құрылғыны дайындау
- Жабық бағдарламалық жасақтама ортасы режимінде Astra Linux арқылы жұмыс істейтін құрылғыны дайындау
- Ubuntu Server/Desktop 10.04 және 16.04 нұсқалары бар құрылғыны дайындау
- Linux операциялық жүйесі бар glibc 2.5 қамтылған құрылғыны дайындау

Linux үшін Желілік агентті тыныш режимде орнату мақсатында:

1. Лицензиялық келісімді оқып шығыңыз. Лицензиялық келісімнің шарттарын түсініп, қабылдаған жағдайда ғана төмендегі қадамдарды орындаңыз.
2. Жауап файлын (TXT форматында) жасаңыз. Жауап файлына VARIABLE_NAME = variable_value пішіміндегі айнымалылар тізімін қосыңыз, әр айнымалы бөлек жолда тұрады.

   Жауап файлын дұрыс пайдалану үшін оған үш міндетті айнымалының ең аз жиынтығын қосу керек:

   - KLNAGENT_SERVER
   - KLNAGENT_AUTOINSTALL
   - EULA_ACCEPTED

   Қашықтан орнатудың барынша нақты параметрлерін пайдалану үшін кез келген қосымша айнымалыларды қосуға болады. Келесі кестеде жауап файлына енгізуге болатын барлық айнымалылар келтірілген:

   Тыныш режимде Linux үшін Желілік агентті орнату параметрлері ретінде пайдаланылатын жауап файлының айнымалылары

   Тыныш режимде Linux үшін Желілік агентті орнату параметрлері ретінде пайдаланылатын жауап файлының айнымалылары

Айнымалының атауы	Міндетті	Сипаттамасы	Ықтимал мәндер
KLNAGENT_SERVER	Иә	Толық домендік атау (FQDN) немесе IP мекенжайы ретінде ұсынылған Басқару сервері атауын қамтиды.	Құрылғының DNS атауы немесе IP мекенжайы.

KLNAGENT_AUTOINSTALL	Иә	Тыныш орнату режимі қосылғанын анықтайды.	1 – тыныш режим қосулы; орнату кезінде пайдаланушыға ешқандай әрекет ұсынылмайды. Басқасы – тыныш режим өшірулі; орнату кезінде пайдаланушыға әрекеттер ұсынылуы мүмкін.
EULA_ACCEPTED	Иә	Пайдаланушы Желілік агенттің Лицензиялық келісімін қабылдап-қабылдамайтынын анықтайды; егер айнымалы көрсетілмесе, оны Лицензиялық келісімді қабылдамау деп түсіндіруге болады.	1 – Мен осы Түпкі пайдаланушының лицензиялық келісімінің ережелері мен шарттарын толық оқып шықтым, түсіндім және қабылдаймын. Басқа мән немесе белгіленбеген – Лицензиялық келісімнің шарттарымен келіспеймін (орнату жүзеге асырылмайды).
KLNAGENT_PROXY_USE	Жоқ	Басқару серверімен орнатылған қосылым прокси-сервердің параметрлерін қолданады ма екенін анықтайды. Әдепкі бойынша, 0 мәні көрсетілген.	1 – прокси-сервер параметрлері қолданылады. Басқасы – прокси-сервер параметрлері қолданылмайды.
KLNAGENT_PROXY_ADDR	Жоқ	Басқару серверімен байланыс орнату үшін қолданылатын прокси-сервер мекенжайын анықтайды.	Құрылғының DNS атауы немесе IP мекенжайы.
KLNAGENT_PROXY_LOGIN	Жоқ	Прокси-серверге кіру үшін қолданылатын пайдаланушы атын анықтайды.	Кез келген қолданыстағы пайдаланушы аты.
KLNAGENT_PROXY_PASSWORD	Жоқ	Прокси-серверге кіру үшін қолданылатын пайдаланушы құпиясөзін анықтайды.	Операциялық жүйедегі әріптер мен сандардың, пішіммен рұқсат етілген құпиясөздің кез келген жиынтығы.
KLNAGENT_VM_VDI	Жоқ	Динамикалық виртуалды машиналарды жасау үшін кескінге Желілік агенттің орнатылып-орнатылмағанын анықтайды.	1 – Желілік агент динамикалық виртуалды машиналарды жасау үшін қолданылатын кескінге орнатылған. Басқасы – орнату барысында кескін қолданылмайды.
KLNAGENT_VM_OPTIMIZE	Жоқ	Желілік агенттің параметрлері гипервизор үшін оңтайлы ма екенін анықтайды.	1 – Желілік агенттің әдепкі бойынша жергілікті параметрлері, гипервизорда қолдануды оңтайландыра алатындай етіп өзгертілген.
KLNAGENT_TAGS	Жоқ	Желілік агенттің үлгісіне тағайындалған тегтерді атап көрсетеді.	Нүктелі үтірмен бөлінген бір немесе бірнеше тег.
KLNAGENT_UDP_PORT	Жоқ	Желілік агент қолданатын UDP портын анықтайды. Әдепкі бойынша, 15000 мәні көрсетілген.	Кез келген қолданыстағы порт нөмірі.
KLNAGENT_PORT	Жоқ	Желілік агент қолданбайтын портты (TLS емес) анықтайды. Әдепкі бойынша, 14000 мәні көрсетілген.	Кез келген қолданыстағы порт нөмірі.
KLNAGENT_SSLPORT	Жоқ	Желілік агент қолданатын TLS портын анықтайды. Әдепкі бойынша, 13000 мәні көрсетілген.	Кез келген қолданыстағы порт нөмірі.
KLNAGENT_USESSL	Жоқ	Қосылу үшін тасымал деңгейінің (TLS) қауіпсіздігі қолданылады ма екенін анықтайды.	1 (әдепкі бойынша) – TLS қолданылады. Басқасы – TLS қолданылмайды.

KLNAGENT_GW_MODE	Жоқ	Қосылым шлюзі пайдаланылады ма екенін анықтайды.	1 (әдепкі бойынша) – ағымдағы параметрлер өзгертілмейді (бірінші қоңырау кезінде қосылым шлюзі көрсетілмейді). 2 – қосылым шлюзі қолданылмайды. 3 – қосылым шлюзі қолданылады. KLNAGENT_GW_ADDRESS қажет. 4 – Желілік агент үлгісі демилитаризацияланған аймақта (DMZ) қосылым шлюзі ретінде пайдаланылады. Сервер сертификаты қажет.
KLNAGENT_GW_ADDRESS	Жоқ	Қосылым шлюзінің мекенжайын анықтайды. Мән, KLNAGENT_GW_MODE = 3 болса ғана қолданылады.	Құрылғының DNS атауы немесе IP мекенжайы.
KLNAGENT_DEVICEOWNER_REGISTRATION_START	Жоқ	Желілік агентті орнатқаннан кейін пайдаланушыны құрылғы иесі ретінде тіркеу үшін утилитаны іске қосуға мүмкіндік береді. Өшірілген болса, пайдаланушыға құрылғы иесі ретінде тіркелу қолжетімді емес.	1 — пайдаланушыны құрылғы иесінің утилитасы ретінде тіркеу желілік агентті орнатқаннан кейін іске қосылады. Басқа жағдайда — өшірілген.
PTCH_ALLOW_APPLY_NONAPROVED_PATCHES	Жоқ	*Анықталмаған* күйі бар Желілік агент үшін автоматты түрде жүктелген жаңартуларды орнату керек пе екенін анықтайды.	true (әдепкі) – жаңартулар автоматты түрде орнатылады. false – қолданба жаңартулары автоматты түрде орнатылмайды.

3. Желілік агентті орнату пакетін іске қосыңыз. Жауап файлының жолын көрсететін KLAUTOANSWERS ортасының айнымалысы орнату пәрменіне жіберіледі. Келесі пәрмендердің бірін орындаңыз:

   - Желілік агентті RPM пакетінен 32 биттік операциялық жүйеге орнату үшін келесі пәрменді орындаңыз:
     `sudo KLAUTOANSWERS=<жауап файлының жолы> yum install ./klnagent-<құрастыру нөмірі>.i386.rpm`

   - Желілік агентті RPM пакетінен 64 биттік операциялық жүйеге орнату үшін келесі пәрменді орындаңыз:
     `sudo KLAUTOANSWERS=<жауап файлының жолы> yum install ./klnagent64-<құрастыру нөмірі>.x86_64.rpm`

   - Желілік агентті RPM пакетінен Arm архитектурасына арналған 64 биттік операциялық жүйеге орнату үшін келесі пәрменді орындаңыз:
     `sudo KLAUTOANSWERS=<жауап файлының жолы> yum install ./klnagent64-<құрастыру нөмірі>.aarch64.rpm`

   - Желілік агентті DEB пакетінен 32 биттік операциялық жүйеге орнату үшін келесі пәрменді орындаңыз:
     `sudo KLAUTOANSWERS=<жауап файлының жолы> apt install ./klnagent_<құрастыру нөмірі>_i386.deb`

   - Желілік агентті DEB пакетінен 64 биттік операциялық жүйеге орнату үшін келесі пәрменді орындаңыз:
     `sudo KLAUTOANSWERS=<жауап файлының жолы> apt install ./klnagent64_<құрастыру нөмірі>_amd64.deb`

   - Желілік агентті DEB пакетінен Arm архитектурасына арналған 64 биттік операциялық жүйеге орнату үшін келесі пәрменді орындаңыз:
     `sudo KLAUTOANSWERS=<жауап файлының жолы> apt install ./klnagent64_<құрастыру нөмірі>_arm64.deb`

Операциялық жүйе конфигурациясына байланысты желілік агентті орнату үшін rpm, dpkg немесе dnf пакет менеджерлерін де пайдалануға болады.

Linux үшін Желілік агентті орнату тыныш режимде басталады; пайдаланушыдан процесс кезінде ешқандай әрекеттерді орындау сұралмайды.

Linux үшін Желілік агентті интерактивті режимде орнату

Бұл мақалада орнату параметрлерін кезең-кезеңімен көрсете отырып, Linux операциялық жүйесімен жұмыс істейтін құрылғыларға Желілік агентті интерактивті режимде орнату жолы сипатталады. Сондай-ақ, жауап файлын – орнату параметрлерінің пайдаланушы белгілеген баптауларын қамтитын мәтіндік файлды пайдалануға болады: айнымалылар және олардың сәйкес мәндері. Жауаптар файлын қолдану арқасында орнатуды тыныш режимде, яғни пайдаланушының қатысуынсыз іске қосуға болады.

Желілік агентті Linux негізіндегі құрылғыға орнатпай тұрып, барлық Linux негізіндегі құрылғыға қажетті жалпы дайындық қадамдарын аяқтау керек.

Жалпы қадамдарды орындағаннан кейін, операциялық жүйеңізге тән қосымша нұсқауларды орындауға болады:

- SUSE Linux Enterprise Server 15 арқылы жұмыс істейтін құрылғыны дайындау
- Жабық бағдарламалық жасақтама ортасы режимінде Astra Linux арқылы жұмыс істейтін құрылғыны дайындау
- Ubuntu Server/Desktop 10.04 және 16.04 нұсқалары бар құрылғыны дайындау
- Linux операциялық жүйесі бар glibc 2.5 қамтылған құрылғыны дайындау

Желілік агентті интерактивті режимде орнату үшін:

1. Желілік агентті орнату пакетін іске қосыңыз. Linux дистрибутивіңізге байланысты келесі пәрмендердің бірін орындаңыз:

   - 32 разрядты операциялық жүйесі бар құрылғыға RPM бумасынан Желілік агентті орнату үшін:

     ```
     # yum -i klnagent-<құрастыру нөмірі>.i386.rpm
     ```

   - 64 разрядты операциялық жүйесі бар құрылғыға RPM бумасынан Желілік агентті орнату үшін:

     ```
     # yum -i klnagent64-<құрастыру нөмірі>.x86_64.rpm
     ```

   - Arm архитектурасына арналған 64 разрядты операциялық жүйесі бар құрылғыға RPM бумасынан Желілік агентті орнату үшін:

     ```
     # yum -i klnagent64-<құрастыру нөмірі>.aarch64.rpm
     ```

   - 32 разрядты операциялық жүйесі бар құрылғыға DEB бумасынан Желілік агентті орнату үшін:

     ```
     # apt install ./klnagent_<құрастыру нөмірі>_i386.deb
     ```

   - 64 разрядты операциялық жүйесі бар құрылғыға DEB бумасынан Желілік агентті орнату үшін:

     ```
     # apt install ./klnagent64_<құрастыру нөмірі>_amd64.deb
     ```

   - Arm архитектурасына арналған 64 разрядты операциялық жүйесі бар құрылғыға DEB бумасынан Желілік агентті орнату үшін:

     ```
     # apt install ./klnagent64_<құрастыру нөмірі>_arm64.deb
     ```

2. Желілік агентті конфигурациялауды іске қосыңыз:

   ```
   # /opt/kaspersky/klnagent64/lib/bin/setup/postinstall.pl
   ```

3. Лицензиялық келісімді оқып шығыңыз. Мәтін пәрмен жолы терезесінде көрсетіледі. Мәтіннің келесі бөлігін көру үшін бос орын пернесін басыңыз. Сұрау көрсетілген кезде келесі мәндердің бірін енгізіңіз:

   - Лицензиялық келісімнің шарттарын түсініп, қабылдасаңыз, `y` енгізіңіз.
   - Лицензиялық келісімнің шарттарын қабылдамасаңыз, `n` енгізіңіз. Желілік агентті қолдану үшін Лицензиялық келісімнің шарттарын қабылдауыңыз қажет.
   - Лицензиялық келісімді қайта көрсету үшін `r` теріңіз.

4. Басқару серверінің DNS атын немесе IP мекенжайын енгізіңіз.
5. Басқару сервері портының нөмірі енгізіңіз. Әдепкі бойынша порт нөмірі – 14000.
6. Басқару сервері SSL портының нөмірін енгізіңіз. Әдепкі бойынша порт нөмірі – 13000.
7. Желілік агент және Басқару сервері арасындағы трафик үшін SSL шифрлауын пайдаланғыңыз келсе, `y` енгізіңіз. Болмаса, `n` енгізіңіз.
8. Желілік агентті конфигурациялаудың келесі тәсілдерінің бірін таңдаңыз:

   - `[1]` – қосылым шлюзін конфигурацияламаңыз.

     Құрылғыңыз қосылу шлюзі ретінде әрекет етпейді және қосылу шлюзі арқылы Басқару серверіне қосылмайды.

   - `[2]` – қосылу шлюзін пайдаланбау.

     Құрылғыңыз Басқару серверіне қосылу шлюзі арқылы қосылмайды.

   - `[3]` – қосылу шлюзі арқылы Серверге қосылыңыз.

     Құрылғыңыз Басқару серверіне қосылу шлюзі арқылы қосылады.

   - `[4]` – қосылу шлюзі ретінде пайдалану.

     Құрылғыңыз қосылу шлюзі ретінде әрекет етеді.

Желілік агент Linux операциялық жүйесімен жұмыс істейтін құрылғыда орнатылған.

Желілік агенті бар құрылғылар үшін файлдық жүйені шегіндіруді қолдау

Kaspersky Security Center Linux қолданбасы таратылған бағдарлама болып саналады. Желілік агенті орнатылған құрылғылардың бірінде файлдық жүйені алдыңғы күйге шегіндіру деректерді синхрондамауға және Kaspersky Security Center Linux дұрыс жұмыс істемеуіне әкеледі.

Файлдық жүйені (немесе оның бір бөлігін) алдыңғы күйге шегіндіру келесі жағдайларда болуы мүмкін:

- қатты дискінің кескінін көшіру кезінде;
- виртуалды инфрақұрылым арқылы виртуалды машинаның күйін қалпына келтіру кезінде;
- сақтық көшірмеден немесе қалпына келтіру нүктесінен деректерді қалпына келтіру кезінде.

Желілік агент орнатылған құрылғылардағы үшінші тараптың бағдарламалық жасақтамасы /var/opt/kaspersky/klnagent каталогіне әсер ететін жағдайлар — Kaspersky Security Center Linux үшін жалғыз критикалық жағдайлар. Сондықтан, мүмкіндік болса, бұл қалтаны қалпына келтіру процедурасынан әрқашан алып тастап отыру керек.

Бірқатар ұйымдарда жұмыс регламенті құрылғылардың файлдық жүйесінің күйін шегіндіруді көздейтіндіктен, Kaspersky Security Center Linux бағдарламасында, 10 Maintenance Release 1 нұсқасынан бастап (Басқару сервері мен Желілік агенттер нұсқасы 10 Maintenance Release 1 немесе одан жоғары болуы керек), Желілік агенті орнатылған құрылғыларда файлдық жүйенің шегіндірілуін анықтауды қолдау мүмкіндігі қосылды. Табылған жағдайда, мұндай құрылғылар деректерді толық тазалаумен және толық синхрондаумен бірге Басқару серверіне автоматты түрде қайта қосылады.

Kaspersky Security Center Linux нұсқасында файлдық жүйенің шегіндірілуін анықтауды қолдау әдепкі бойынша қосылады.

Желілік агент орнатылған құрылғыларда /var/opt/kaspersky/klnagent каталогіне қайтаруға жол бермеңіз, себебі деректерді қайта синхрондау үшін көп ресурс қажет.

Басқару сервері орнатылған құрылғы үшін жүйенің күйін шегіндіруге жол берілмейді. Басқару сервері пайдаланатын дерекқордың алдыңғы күйіне шегіндіру де қолайсыз.

Сақтық көшірмеден Басқару серверінің күйін тек штаттық klbackup утилитасын пайдаланып қалпына келтіруге болады.

Windows үшін желілік агент орнату

Сондай-ақ басқару сервері арқылы басқару үшін желілік агентті ұйымның Windows негізіндегі құрылғыларына орнатуға болады.

Microsoft Windows XP-де желілік агент келесі операцияларды дұрыс орындамауы мүмкін: жаңартуларды тікелей Kaspersky серверлерінен жүктеп алу (тарату нүктесі ретінде); KSN прокси-сервері ретінде жұмыс істеу (тарату нүктесі ретінде); және үшінші тараптар осалдықтарын анықтау (осалдықтар мен патчтарды басқаруды қолданған кезде).

Microsoft Windows on Arm жұмыс істейтін құрылғыға Желілік агентті орнатпас бұрын, Microsoft Windows x86-64 үшін ешқандай Желілік агент орнатылмағанына көз жеткізіңіз. Әйтпесе, орнату бағдарламасы сәтсіз аяқталады.

Windows басқаратын құрылғысына желілік агентті орнатудың келесі әдістері бар:

- Windows тарату нүктесінде қашықтан орнату тапсырмасын орындау арқылы.

  Windows тағайындалмаған құрылғысына қашықтан орнатуды орындамас бұрын, Windows негізіндегі тарату нүктесі мақсатты құрылғының операциялық жүйе түрін анықтау үшін UDP портын 137 автоматты түрде тексереді. Егер UDP порты 137 қолжетімді болмаса, тарату нүктесі орнатуды орындау үшін қажетті мақсатты құрылғыдағы 445 TCP портына қосылуға тырысады.

- Қолданбаларды қашықтан орнатуға арналған үшінші тарап құралдарымен бірге Желілік агент үшін Windows орнату бағдарламасы пакетін (MSI) пайдалану арқылы.

- Басқарылатын құрылғыда қолданба орнатушысын іске қосу арқылы.

- Құрылғы пайдаланушыларына Kaspersky Security Center Linux жасаған дербес пакеттер сілтемелерін жіберу арқылы. Автономды пакеттер, параметрлері конфигурацияланған таңдалған бағдарламалардың дистрибутивтерін қамтитын орындалатын модульдер болып табылады.

Windows үшін желілік агентті өзара әрекет режимінде орнату

Құрылғыға Желілік агентті жергілікті түрде орнату үшін:

1. Құрылғыда интернет арқылы алынған дистрибутивтен ksc_<нұсқа нөмірі>.<құрастыру нөмірі>_full_<орналасу тілі>.exe файлын іске қосыңыз.

   Орнату үшін Kaspersky бағдарламалары таңдалатын терезе ашылады.

2. Бағдарлама таңдау терезесінде **Kaspersky Security Center Желілік агентін ғана орнатыңыз** сілтемесі бойынша желілік агентті орнату шеберін іске қосыңыз. Содан кейін, шебердің нұсқауларын орындаңыз.

   Орнату шебері жұмыс істеп тұрған кезде, Желілік агенттің қосымша параметрлерін конфигурациялауға болады (төменде қараңыз).

3. Құрылғыны таңдалған басқару топтың қосылым шлюзі ретінде пайдалану үшін орнату шеберінің **Қосылым шлюзі** терезесінде **Желілік агентті DMZ режимінде қосылым шлюзі ретінде пайдалану** опциясын таңдаңыз.

4. Виртуалды машинаға орнатқан кезде Желілік агентті конфигурациялау үшін:

   a. Егер сіз виртуалды машина кескіндерінен динамикалық түрде виртуалды машиналар жасауды жоспарласаңыз, виртуалды Virtual Desktop Infrastructure (VDI) үшін Желілік агенттің динамикалық режимін қосыңыз. Ол үшін **Қосымша параметрлер** орнату шебері терезесінде **VDI үшін динамикалық режимді қосу** параметрін таңдаңыз.

      Егер сіз виртуалды машина кескіндерінен динамикалық түрде виртуалды машиналар жасауды жоспарламасаңыз, бұл қадамды өткізіп жіберіңіз.

   b. Виртуалды инфрақұрылым үшін Желілік агенттің жұмысын оңтайландырыңыз. Ол үшін **Қосымша параметрлер** орнату шебері терезесінде **VM параметрлерін оңтайландыру** параметрін таңдаңыз.

      Нәтижесінде, құрылғы іске қосылған кезде орындалатын файлдардың осалдығын тексеру өшіріледі. Сондай-ақ, келесі ақпаратты Басқару серверіне жіберу өшіріледі:

      - Жабдық тізімдемесі
      - Құрылғыда орнатылған бағдарламалар туралы

- Жергілікті клиент құрылғысына орнатылатын Microsoft Windows жаңартулары туралы
- Жергілікті клиент құрылғысында табылған бағдарламалық жасақтаманың осалдықтары туралы

Болашақта, сіз бұл ақпаратты Желілік агент сипаттарында немесе Желілік агент саясатының параметрлерінде жіберуді қоса аласыз.

Орнату шеберінің жұмысы аяқталғаннан кейін, құрылғыға Желілік агент орнатылады.

Сіз Желілік агент қызметінің сипаттарын көре аласыз, сонымен қатар Microsoft Windows стандартты құралдары: Компьютерді басқару\Қызметтер арқылы Желілік агенттің белсенділігін іске қоса, тоқтата және бақылай аласыз.

Windows үшін Желілік агентті тыныш режимде орнату

Желілік агентті тыныш режимде орнатуға болады, яғни орнату параметрлерін интерактивті түрде енгізбестен. Тыныш орнату үшін Желілік агенттің Windows Installer пакеті (MSI) қолданылады. MSI файлы Kaspersky Security Center Linux қолданбасының дистрибутивінде Packages\NetAgent\exec қалтасында орналасқан.

MSI пакетінен желілік агентті тек тыныш режимде орнатуға болады, MSI пакетінен интерактивті орнатуға қолдау көрсетілмейді.

Жергілікті құрылғыда Желілік агентті тыныш режимде орнату үшін:

1. Лицензиялық келісімді оқып шығыңыз. Лицензиялық келісімді оқып шықсаңыз және оның шарттарын қабылдасаңыз, төмендегі пәрменді қолданыңыз.

2. Келесі пәрменді орындаңыз:
   ```
   msiexec /i "Kaspersky Network Agent.msi" /qn <setup_parameters>
   ```
   мұндағы `setup_parameters` – бір-бірінен бос орын арқылы бөлінген параметрлер мен олардың мәндерінің тізімі (`PROP1=PROP1VAL PROP2=PROP2VAL`).

   Параметрлер тізіміне `EULA=1` параметрін қосуыңыз керек. Әйтпесе, Желілік агент орнатылмайды.

Егер сіз қашықтағы құрылғыларда Kaspersky Security Center және Желілік агент үшін стандартты қосылым параметрлерін қолдансаңыз, келесі пәрменді орындаңыз:

```
msiexec /i "Kaspersky Network Agent.msi" /qn /l*vx c:\windows\temp\nag_inst.log
SERVERADDRESS=kscserver.mycompany.com EULA=1
```

`/l*vx` – оқиғалар журналына жазу кілті. Оқиғалар журналы Желілік агентті орнатқан кезде жасалады және C:\windows\temp\nag_inst.log қалтасында сақталады.

nag_inst.log файлынан басқа, бағдарлама орнату оқиғаларының журналын қамтитын $klssinstlib.log файлын жасайды. Бұл файл %windir%\temp немесе %temp% қалтасында сақталады. Ақауларды жою үшін сізге немесе Kaspersky Техникалық қолдау қызметінің маманына екі журнал файлы қажет болуы мүмкін – nag_inst.log және $klssinstlib.log.

Басқару серверіне қосылу үшін портты қосымша көрсету қажет болса, келесі пәрменді енгізіңіз:

```
msiexec /i "Kaspersky Network Agent.msi" /qn /l*vx c:\windows\temp\nag_inst.log
SERVERADDRESS=kscserver.mycompany.com EULA=1 SERVERPORT=14000
```

`SERVERPORT` параметрі Басқару серверіне қосылу портының нөміріне сәйкес келеді.

Желілік агентті тыныш режимде орнату кезінде қолдануға болатын параметрлердің аттары мен ықтимал мәндері Желілік агентті орнату параметрлері бөлімінде келтірілген.

Windows Installer көмегімен желі агентін жаңартқыңыз келсе, келесі пәрменді орындаңыз:

```
msiexec /i "Kaspersky Network Agent.msi" /qn /l*vx c:\windows\temp\nag_inst.log
REINSTALL=ALL REINSTALLMODE=vomus /norestart
```

Құрылғының бейнесін қармау және көшіру арқылы енгізу

Егер операциялық жүйені және басқа бағдарламалық жасақтаманы орнату (немесе қайта орнату) жүргізілетін құрылғыларға Желілік агентті орнату керек болса, құрылғының үлгісін қармау және көшіру механизмін қолдануға болады.

Қатты дискті қармау және көшіру арқылы орналастыруды орындау үшін:

1. Желілік агентті және қауіпсіздік бағдарламасын қоса, орнатылған операциялық жүйемен және жұмысқа қажетті бағдарламалық жасақтаманың жиынтығымен эталондық құрылғыны жасау.

2. "Эталондық" құрылғының үлгісін қармау және одан әрі бұл үлгіні Kaspersky Security Center Linux тапсырмасы арқылы жаңа құрылғыларға тарату.

   Диск кескіндерін түсіру және орнату үшін ұйымыңызда қолжетімді үшінші тарап құралдарын пайдаланыңыз.

Бөтен құралдармен қатты дисктің үлгісін көшіру

Желілік агенті орнатылған құрылғы үлгісін қармау үшін бөтен құралдарды қолданған кезде келесі әдістердің бірінші қолдану керек:

- Эталондық құрылғыда Желілік агенттің қызметін тоқтатыңыз және `-dupfix` кілтімен klmover утилитасын іске қосыңыз. klmover утилитасы Желілік агенттің орнату пакетінің құрамына кіреді. Одан әрі тіпті үлгіні қармау операциясын орындауға дейін Желілік агенттің қызметін іске қосуға жол бермеңіз.

- klmover утилитасы іске қосылғанына көз жеткізіңіз де, мақсатты құрылғыларда Желілік агент қызметін бірінші рет іске қоспас бұрын `-dupfix` кілтін басыңыз. Бұл міндетті талап және кескін орналастырылғаннан кейін операциялық жүйені бірінші рет іске қосқан кезде орындалуы керек. klmover утилитасы Желілік агенттің орнату пакетінің құрамына кіреді.

- Желілік агенттің дискісін клондау режимін пайдалану.

Егер қатты диск үлгісі қате көшірілсе, сіз бұл мәселені шеше аласыз.

Сондай-ақ, Желілік агент орнатылмай-ақ құрылғы кескінін түсіруге болады. Бұл әрекетті орындау үшін кескінді мақсатты құрылғыларға орналастырып, одан кейін Желілік агентті орнатыңыз. Бұл әдісті пайдаланған кезде құрылғыдан автономды орнату пакеттері бар желілік қалтаға кіруді беріңіз.

Желілік агенттің дискісін клондау режимі

"Эталонды" құрылғының қатты дискісін клондау, бағдарламалық жасақтаманы жаңа құрылғыларға орнатудың кеңінен таралған тәсілі болып табылады. Клондау барысында "эталонды" құрылғының қатты дискісіндегі Желілік агент әдеттегі режимде жұмыс істесе, келесі мәселе туындайды:

Желілік агенттің эталонды үлгідегі дискісі көмегімен жаңа құрылғыларға орналастырғаннан кейін, бұл құрылғылар Kaspersky Security Center Web Console консолінде бір құрылғы ретінде көрсетіледі. Клондау кезінде жаңа құрылғыларда Басқару серверге құрылғыны Kaspersky Security Center Web Console консолиндегі белгішемен байланыстыруға мүмкіндік беретін бірдей ішкі деректер сақталатындықтан, мәселе туындайды.

Клондағаннан кейін Kaspersky Security Center Web Console консолінде жаңа құрылғыларды дұрыс көрсетпеумен байланысты мәселелерді болдырмау үшін арнайы *желілік агент дискісін клондау* режимі көмектеседі. Бағдарламалық жасақтаманы жаңа құрылғыларға дискіні клондау арқылы енгізіп жатсаңыз (Желілік агентпен бірге), осы режимді қолданыңыз.

Дискіні клондау режимінде, Желілік агент жұмыс істеп тұрғанымен, Басқару серверіне қосылмайды. Клондау режимінен шығу кезінде Желілік агент ішкі деректерді жояды, олардың болуынан Басқару сервер бірнеше құрылғыны Kaspersky Security Center Web Console консолиндегі бір жазбамен байланыстырады. Эталондық құрылғы кескінін клондау аяқталғаннан кейін, жаңа құрылғылар әдетте Kaspersky Security Center Web Console консолінде дұрыс көрсетіледі (бөлек жазбалар ретінде).

Желілік агент дискісін клондау режимін қолдану сценарийі

1. Әкімші Желілік агентті "эталонды" құрылғыда орнатады.
2. Әкімші Желілік агенттің Басқару серверіне қосылуын "klnagchk" утилитасы арқылы тексереді.
3. Әкімші Желілік агент дискісін клондау режимін қосады.
4. Әкімші құрылғыға бағдарламалық жасақтаманы, патчтарды орнатады және құрылғыны қайта жүктеудің кез келген санын орындайды.
5. Әкімші "эталонды" құрылғының қатты дискісін құрылғылардың кез келген санына клондайды.
6. Әрбір клондалған көшірме үшін келесі шарттар орындалуы тиіс:
   a. құрылғының атауы өзгертілген;
   b. құрылғы қайта жүктелген;
   c. дискіні клондау режимі өшірулі.

Дискіні klmover утилитасы көмегімен клондау режимін қосу және өшіру

Желілік агент дискісін клондау режимін қосу немесе өшіру үшін:

1. Клондау қажет болған Желілік агенті орнатылған құрылғыда klmover утилитасын іске қосыңыз.

   klmover утилитасы Желілік агентті орнату қалтасында орналасқан.

2. Дискіні клондау режимін қосу үшін Linux пәрмен қабықшасына келесі пәрменді енгізіңіз:

   ```
   ./klmover -cloningmode 1
   ```

   Желілік агент дискіні клондау режиміне ауысады.

3. Дискіні клондау режимінің ағымдағы күйін сұрау үшін пәрмен жолына келесі пәрменді енгізіңіз:

   ```
   ./klmover -cloningmode
   ```

   Нәтижесінде, утилитаның терезесінде дискіні клондау режимінің қосулы немесе өшірулі екені туралы ақпарат көрсетіледі.

4. Дискіні клондау режимін өшіру үшін утилитаның пәрмен жолына келесі пәрменді енгізіңіз:

   ```
   ./klmover -cloningmode 0
   ```

Желілік агентті орнату параметрлері

Төмендегі кестеде, Желілік агентті орнату кезінде конфигурациялауға болатын MSI сипаттары сипатталған. EULA және SERVERADDRESS қоспағанда, барлық параметрлер міндетті емес.

Желілік агентті тыныш режимде орнату параметрлері

MSI сипаты	Сипаттамасы	Қолжетімді мәндері
EULA	Лицензиялық келісімнің шарттарымен келісу	• 1 – мен осы Түпкі пайдаланушының лицензиялық келісімінің шарттары мен талаптарын толықтай оқып шығып, түсінгенімді растаймын және қабылдаймын. • 0 – Лицензиялық келісімнің шарттарын қабылдамаймын (орнату орындалмайды). • Мән белгіленбеген – Лицензиялық келісімнің шарттарын қабылдамаймын (орнату орындалмайды).
DONT_USE_ANSWER_FILE	Жауап файлынан орнату параметрлерін оқу.	• 1 – Қолданбау. • басқа мән немесе белгіленбеген – оқу.
INSTALLDIR	Желілік агентті орнату қалтасына апаратын жол.	Жол мәні.
SERVERADDRESS	Басқару серверінің мекенжайы (міндетті параметр).	Жол мәні.
SERVERPORT	Басқару серверіне қосылу портының нөмірі.	Сандық мән.
SERVERSSLPORT	SSL протоколын пайдаланып Басқару серверіне қауіпсіз қосылуға арналған порт нөмірі.	Сандық мән.
USESSL	SSL байланысын пайдалану керек пе.	• 1 – пайдалану; • басқа мән немесе белгіленбеген – пайдаланбау.
OPENUDPPORT	UDP портын ашу керек пе.	• 1 – ашу; • басқа мән немесе белгіленбеген – ашпау.

MSI сипаты	Сипаттамасы	Қолжетімді мәндері
UDPPORT	UDP портының нөмірі.	Сандық мән.
USEPROXY	Прокси-серверді пайдалану керек пе.	• 1 – пайдалану; • басқа мән немесе белгіленбеген – пайдаланбау.
PROXYLOCATION (PROXYADDRESS:PROXYPORT)	Прокси-сервер мекенжайы және прокси-серверге қосылуға арналған порт нөмірі.	Жол мәні.
PROXYLOGIN	Прокси-серверге қосылуға арналған есептік жазба.	Жол мәні.
PROXYPASSWORD	Прокси-серверге қосылуға арналған есептік жазбаның құпиясөзі (орнату пакеттерінің параметрлерінде артықшылықты есептік жазбалардың деректерін көрсетіңіз).	Жол мәні.
GATEWAYMODE	Қосылым шлюзін пайдалану режимі.	• 0 – қосылымдар шлюзін пайдаланбау; • 1 – бұл Желілік агентті қосылым шлюзі ретінде пайдалану; • 2 – Басқару серверіне қосылым шлюзі арқылы қосылу.
GATEWAYADDRESS	Қосылым шлюзі мекенжайы.	Жол мәні.
CERTSELECTION	Сертификат алу тәсілі.	• GetOnFirstConnection – Басқару серверінен сертификат алу; • GetExistent — бар сертификатты таңдау. Бұл опция таңдалса, CERTFILE сипаты көрсетілуі керек.
CERTFILE	Сертификат файлының жолы.	Жол мәні.
VMVDI	VDI үшін динамикалық режимді қосу керек пе.	• 1 – қосу; • 0 – қоспау; • Мән белгіленбеген – қоспау.
LAUNCHPROGRAM	Желілік агент қызметін орнатқаннан кейін іске қосу керек пе. VMVDI=1 болса, параметр еленбейді.	• 1 – іске қосу; • басқа мән немесе белгіленбеген – іске қоспау.
NAGENTTAGS	Желілік агентке арналған тег (жауап файлында көрсетілген тегтен басым).	Жол мәні.

Қашықтан орнату тапсырмасын пайдаланып бағдарламаларды орнату

Kaspersky Security Center Linux қашықтан орнату тапсырмаларын пайдаланып құрылғыларға бағдарламаларды қашықтан орнатуға мүмкіндік береді. Тапсырмалар шебердің көмегімен жасалады және құрылғыларға тағайындалады. Құрылғыларға (ең көбі 1000 құрылғы) тапсырманы тезірек және оңай тағайындау үшін құрылғы шебері терезесінде өзіңізге ыңғайлы түрде көрсете аласыз:

- **Басқару тобына тапсырманы белгілеу**. Бұл жағдайда, тапсырма бұрын жасалған басқару тобына кіретін құрылғыларға тағайындалады.

- **Құрылғының мекенжайларын қолмен белгілеу немесе тізімнен импорттау**. Сіз DNS атауларын, IP мекенжайларын, сондай-ақ тапсырманы тағайындауды қажет ететін құрылғылардың IP мекенжайы ауқымдарын белгілей аласыз.

- **Құрылғы таңдауына тапсырманы белгілеу**. Бұл жағдайда, тапсырма бұрын жасалған таңдауды құрайтын құрылғыларға тағайындалады. Сіз әдепкі бойынша жасалған таңдауды немесе өзіндік таңдауды көрсете аласыз. 1000 құрылғыдан асырмай таңдауға болады.

Желілік агент орнатылмаған клиент құрылғысына қолданбаны орнату кезінде туындауы мүмкін мәселелерге жол бермеу үшін Kaspersky Security Center Linux қашықтан орнату тапсырмасымен мәжбүрлі түрде орналастыру процедурасында сипатталғандай әрекет етуіңіз керек.

Kaspersky Security Center Linux қолданбаларын қашықтан орнату тапсырмалары туралы

Kaspersky Security Center Linux қолданбаларды қашықтан орнату тапсырмалары түрінде іске асырылған қолданбаларды қашықтан орнатудың әртүрлі механизмдерін ұсынады (күшпен орнату, қатты дисктің үлгісін көшіру арқылы орнату). Қашықтықтан орнату тапсырмасын көрсетілген басқару топ үшін де, құрылғылар жиынтығы үшін де немесе құрылғыларды таңдау үшін де орындауға болады (мұндай тапсырмалар Kaspersky Security Center Web Console консолінде **Тапсырмалар** қалтасында көрсетіледі). Тапсырманы жасау кезінде, сіз осы тапсырманы пайдаланып, орнатылатын орнату пакеттерін (Желілік агент және/немесе басқа қолданба) таңдай аласыз, сонымен қатар қашықтан орнату тәсілін анықтайтын бірқатар параметрлерді орната аласыз. Сонымен қатар, қолданбаларды қашықтан орнату шеберін қолдануға болады, оның негізінде қолданбаларды қашықтан орнату тапсырмасын жасау және нәтижелерді мониторингтеу жатыр.

Басқару топтарына арналған тапсырмалар тек осы топқа жататын құрылғыларда ғана емес, таңдалған топтың барлық ішкі топтарының барлық құрылғыларында да жұмыс істейді. Егер тапсырма параметрлерінде тиісті параметр қосылса, тапсырма осы топта немесе оның ішкі топтарында орналасқан қосалқы Басқару серверлерінің құрылғыларына қолданылады.

Құрылғылар жиынтығына арналған тапсырмалар, тапсырманы іске қосу кезінде құрылғыларды таңдау құрамына сәйкес әрбір рет іске қосу кезінде клиент құрылғыларының тізімін жаңартады. Егер құрылғыларды таңдауда қосалқы Басқару серверлеріне қосылған құрылғылар болса, тапсырма осы құрылғыларда да іске қосылады. Бұл параметрлер және орнату тәсілдері туралы толығырақ осы бөлімде кейін айтылады.

Қосалқы Басқару серверіне қосылған құрылғыларда қашықтан орнату тапсырмасының сәтті жұмысы үшін ауыстыру тапсырмасымен сәйкес қосалқы Басқару серверлеріне тапсырма қолданатын орнату пакеттерін алдын ала ауыстыру керек.

Бағдарламаны қашықтан орнату

Бұл бөлімде басқару тобындағы құрылғыларға, белгілі бір мекенжайлары бар құрылғыларға немесе құрылғы таңдауларына бағдарламаны қашықтан орнату туралы ақпарат бар.

Бағдарламаны таңдалған құрылғыларға орнату үшін:

1. Бағдарламаның негізгі терезесінде **Тапсырмалар** бөліміне өтіңіз.
2. **Қосу** түймесін басыңыз.

   Жаңа тапсырма жасау шебері іске қосылады.
3. **Тапсырма түрі** өрісінде **Бағдарламаны қашықтан орнату** таңдаңыз.

4. Келесі нұсқалардың бірін таңдаңыз:

- **Басқару тобына тапсырманы белгілеу**

  Тапсырма бұрын жасалған басқару тобына кіретін құрылғыларға тағайындалады. Бар топтардың бірін көрсетуге немесе жаңа топ құруға болады.

  Мысалы, хабар белгілі бір басқару тобындағы құрылғыларға арналған болса, пайдаланушыларға хабар жіберу тапсырмасын іске қосу үшін осы параметрді пайдалануға болады.

  Тапсырма Басқару тобына тағайындалса, **Қауіпсіздік** қойындысы тапсырма сипаттары терезесінде көрсетілмейді, себебі топтық тапсырмалар олар тиесілі болып саналатын қауіпсіздік топтарының параметрлеріне бағынады.

- **Құрылғының мекенжайларын қолмен белгілеу немесе тізімнен импорттау**

  Сіз DNS атауларын, IP мекенжайларын, сондай-ақ тапсырманы тағайындауды қажет ететін құрылғылардың IP мекенжайы ауқымдарын белгілей аласыз.

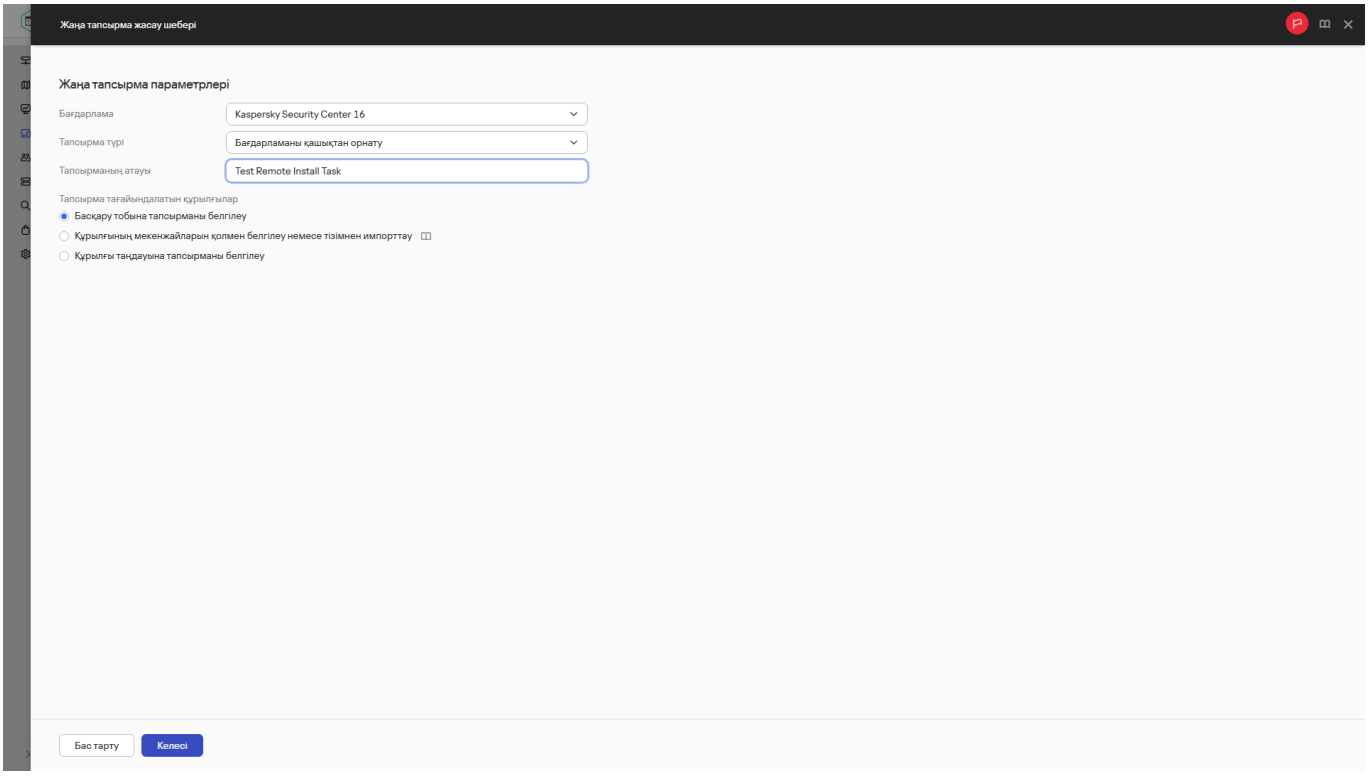
  Бұл параметрді белгіленген ішкі желі үшін тапсырманы орындау үшін пайдалануға болады. Мысалы, сіз бухгалтерлердің құрылғыларына белгілі бір бағдарламаны орната аласыз немесе вирус жұқтыруы мүмкін ішкі желідегі құрылғыларды тексере аласыз.

- **Құрылғы таңдауына тапсырманы белгілеу**

  Тапсырма құрылғы таңдауларына кіретін құрылғыларға тағайындалады. Қолданыстағы таңдаулардың бірін көрсетуге болады.

  Мысалы, операциялық жүйенің белгілі бір нұсқасы бар құрылғыларда тапсырманы іске қосу үшін осы параметрді пайдалануға болады.

Бағдарламаны қашықтан орнату тапсырмасы көрсетілген құрылғылар үшін жасалды. **Басқару тобына тапсырманы белгілеу** параметрін таңдаған болсаңыз, тапсырма топтық болып саналады.



Бағдарламаны қашықтан орнату тапсырмасын жасау

5. **Тапсырма ауқымы** қадамында басқару тобын, нақты мекенжайлары бар құрылғыларды немесе құрылғылар таңдауын көрсетіңіз.

   Қолжетімді параметрлер алдыңғы қадамда таңдалған параметрлерге байланысты.

6. **Орнату пакеттері** қадамында келесі параметрлерді көрсетіңіз:

- Орнатылуы қажет бағдарламаның орнату пакетін **Орнату пакетін таңдау** өрісінен таңдаңыз.
- **Орнату пакетін мәжбүрлеп жүктеп алу** параметрлер блогында бағдарламаны орнату үшін қажетті файлдарды клиент құрылғыларына жеткізу тәсілін таңдаңыз:
  - **Желілік агенттің көмегімен**

    Егер бұл параметр қосылса, орнату пакеттерін клиент құрылғыларына жеткізуді клиент құрылғыларына орнатылған Желілік агент жүзеге асырады.

    Егер бұл параметр өшірулі болса, орнату пакеттері клиент құрылғысының операциялық жүйесі құралдарының көмегімен жеткізіледі.

    Егер тапсырма Желілік агенттер орнатылған құрылғыларға тағайындалса, бұл параметрді қосу ұсынылады.

    Әдепкі бойынша, параметр қосулы.

  - **Тарату нүктелері арқылы операциялық жүйе ресурстарының көмегімен**

    Егер бұл параметр қосылса, орнату пакеттері тарату нүктелері арқылы операциялық жүйенің көмегімен клиент құрылғыларына беріледі. Егер желіде кем дегенде бір тарату нүктесі болса, бұл нұсқаны таңдауға болады.

    Желілік агент көмегімен параметрі қосылса, онда файлдар, операциялық жүйенің құралдарымен Желілік агент құралдарын пайдалану мүмкін болмаған жағдайда ғана жеткізіледі.

    Әдепкі бойынша, параметр виртуалды Басқару серверінде жасалған қашықтан орнату тапсырмалары үшін қосылған.

    Windows жүйесіне арналған бағдарламаны (Windows жүйесіне арналған Желілік агентті қоса) Желілік агент орнатылмаған құрылғыға орнатудың жалғыз жолы – бұл Windows операциялық жүйесі бар тарату нүктесін пайдалану болып табылады. Сондықтан Windows жүйесіне арналған бағдарламаны орнату кезінде:
    - Осы параметрді таңдаңыз.
    - Тарату нүктесі мақсатты клиенттік құрылғыларға тағайындалғанын көз жеткізіңіз.
    - Тарату нүктесінде Windows операциялық жүйесі орнатылғанына көз жеткізіңіз.

  - **Басқару сервері арқылы операциялық жүйе ресурстарының көмегімен**

    Бұл параметр қосылса, файлдар Басқару сервері көмегімен клиент құрылғыларының операциялық жүйесі арқылы клиент құрылғыларына жеткізіледі. Бұл параметрді клиент құрылғысында Желілік агент орнатылмаған, бірақ клиент құрылғысы Басқару серверімен бір желіде орналасқан кезде қосуға болады.

    Әдепкі бойынша, параметр қосулы.

- Басқару сервері файлдарды бір уақытта жібере алатын клиент құрылғыларының рұқсат етілген ең көп санын **Бір уақытта орындалатын жүктеулердің ең көп саны** өрісінде көрсетіңіз.
- Орнату бағдарламасын іске қосуға рұқсат етілген ең көп санын **Орнату әрекеттерінің максималды саны** өрісінде көрсетіңіз.

  Тапсырма параметрлерінде көрсетілген әрекеттер саны асып кетсе, Kaspersky Security Center Linux енді құрылғыдағы орнату бағдарламасын іске қоспайды. *Бағдарламаны қашықтан орнату* тапсырмасын қайта іске қосу үшін **Орнату әрекеттерінің максималды саны** параметрінің мәнін арттырыңыз және тапсырманы орындаңыз. Сондай-ақ, сіз *Бағдарламаны қашықтан орнату* тапсырмасының басқасын жасай аласыз.

- Деректерді бір Kaspersky қолданбасынан екіншісіне тасымалдап жатсаңыз және ағымдағы қолданбаңыз құпиясөзбен қорғалған болса, **Kaspersky ағымдағы бағдарламасын жою үшін құпиясөз** өрісіне құпиясөзді енгізіңіз. Ағымдағы Kaspersky қолданбасы деректерді тасымалдау кезінде жойылатынын ескеріңіз.

  Kaspersky ағымдағы бағдарламасын жою үшін құпиясөз өрісі, **Орнату пакетін мәжбүрлеп жүктеп алу** параметрлер тобында **Желілік агенттің көмегімен** параметрін таңдаған жағдайда ғана қолжетімді болады.

  Жою құпиясөзін тек Қолданбаларды қашықтан орнату тапсырмасының көмегімен Kaspersky Endpoint Security for Windows орнату кезінде Kaspersky Security for Windows Server деректерін Kaspersky Endpoint Security for Windows қолданбасына көшіру сценарийі үшін ғана қолдана аласыз. Басқа компоненттерді орнату кезінде деинсталляция құпиясөзін пайдалану салдарынан орнату қателері туындауы мүмкін.

  Деректерді тасымалдау сценарийін сәтті аяқтау үшін келесі алғышарттардың орындалғанына көз жеткізіңіз:

  - Сіз Windows жүйесіне арналған Kaspersky Security Center Желілік агенті 14.2 немесе одан жоғары нұсқасын пайдаланып жатырсыз.
  - Сіз қолданбаны Windows басқаруымен жұмыс істейтін құрылғыларға орнатып жатырсыз.

- Қосымша параметрді конфигурациялаңыз:

  - **Бұрын орнатылып қойған жағдайда, бағдарламаны қайта орнатпау**

    Егер бұл параметр қосылса, таңдалған бағдарлама клиент құрылғысында орнатылған болса, қайта орнатылмайды.

    Егер бұл параметр өшірулі болса, бағдарлама кез келген жағдайда орнатылады.

    Әдепкі бойынша, параметр қосулы.

  - **Жүктеп алмас бұрын операциялық жүйенің түрін тексеру**

    Файлдарды клиент құрылғыларына жібермес бұрын, Kaspersky Security Center Linux бағдарламасы орнату утилитасының параметрлері клиент құрылғысының операциялық жүйесіне қолданылатындығын тексереді. Егер параметрлер қолданылмаса, Kaspersky Security Center Linux бағдарламасы файлдарды жібермейді және бағдарламаны орнатуға тырыспайды. Мысалы, әртүрлі операциялық жүйелері бар құрылғыларды қамтитын басқару тобының құрылғыларынан кейбір бағдарламаларды орнату үшін басқару тобына орнату тапсырмасын тағайындауға болады, содан кейін қажеттіден басқа операциялық жүйесі бар құрылғыларды өткізіп жіберу үшін осы параметрді қосуға болады.

    Желілік агентті тағайындалмаған құрылғыларға қашықтан орнатқан кезде, Kaspersky Security Center Linux немесе тарату нүктесі құрылғының операциялық жүйесінің түрін, **Жүктеп алмас бұрын операциялық жүйенің түрін тексеру** қарамастан, автоматты түрде анықтайды.

  - **Active Directory топтық саясаттарында пакет орнатуды тағайындау**

    Егер бұл параметр қосылса, орнату пакеті Active Directory топтық саясаттары арқылы орнатылады.

    Егер Желілік агенттің орнату пакеті таңдалса, параметр қолжетімді.

    Әдепкі бойынша, параметр өшірулі.

- **Пайдаланушылардан іске қосылған бағдарламаларды жабуды сұрайды**

  Іске қосылған бағдарламалар клиент құрылғысын қайта жүктеуге мүмкіндік бермеуі мүмкін. Мысалы, егер мәтіндік редакторда құжатпен жұмыс жасалса және өзгертулер сақталмаса, бағдарлама құрылғыны қайта жүктеуге мүмкіндік бермейді.

  Егер бұл параметр қосулы болса, құрылғыны қайта іске қоспас бұрын бұғатталған құрылғылардағы мұндай бағдарламалар мәжбүрлі түрде жабылады. Нәтижесінде, пайдаланушылар сақталмаған жұмысын жоғалтуы мүмкін.

  Егер бұл параметр өшірулі болса, бұғатталған құрылғы қайта жүктелмейді. Бұл құрылғыдағы тапсырманың күйі құрылғыны қайта іске қосу қажеттілігін көрсетеді. Пайдаланушылар бұғатталған құрылғыларда жұмыс істейтін барлық бағдарламаларды қолмен жауып, сол құрылғыларды қайта іске қосуы керек.

  Әдепкі бойынша, параметр өшірулі.

- Бағдарламаны орнатқыңыз келетін құрылғыларды таңдаңыз:

  - **Барлық құрылғыларда орнату**

    Бағдарлама тіпті басқа Басқару серверлері басқаратын құрылғыларға орнатылады.

    Әдепкі бойынша, осы нұсқа таңдалады. Желіде тек бір Басқару сервері болса, бұл параметрді өзгертудің қажеті жоқ.

  - **Тек осы Басқару сервері арқылы басқарылатын құрылғыларда орнату**

    Бағдарлама тек осы Басқару сервері басқаратын құрылғыларға орнатылады. Егер сіздің желіңізде бірнеше Басқару сервері орнатылған болса және олардың арасындағы қайшылықтардан аулақ болғыңыз келсе, осы параметрді таңдаңыз.

- Орнатудан кейін, құрылғыларды басқару тобына жылжыту керектігін көрсетіңіз:

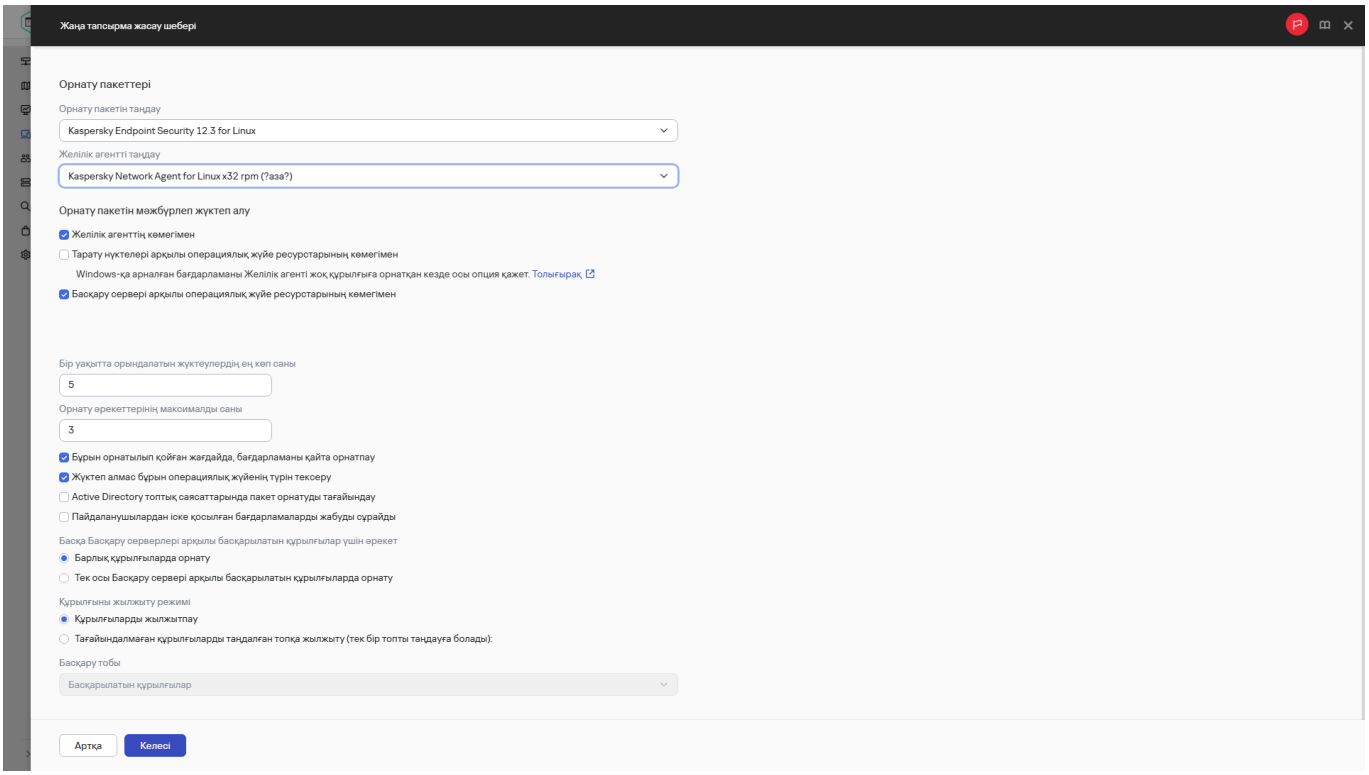
  - **Құрылғыларды жылжытпау**

    Құрылғылар тиесілі болып саналатын топтарда қалады. Топтардың ешқайсысына жатпайтын құрылғылар таратылмаған болып қалады.

  - **Тағайындалмаған құрылғыларды таңдалған топқа жылжыту (тек бір топты таңдауға болады)**

    Құрылғылар сіз таңдаған басқару тобына жылжытылады.

  Әдепкі бойынша **Құрылғыларды жылжытпау** нұсқасының таңдалғанын ескеріңіз. Қауіпсіздік тұрғысынан, сіз құрылғыларды қолмен жылжытуды таңдай аласыз.



Тапсырма параметрлерін көрсету

7. Шебердің осы қадамында бағдарламаларды орнату кезінде құрылғыны қайта жүктеу талап етілетін көрсетіңіз:

   - **Құрылғыны қайта іске қоспау**

     Осы нұсқа таңдалған болса, онда қауіпсіздік бағдарламасы орнатылғаннан кейін, құрылғы қайта іске қосылмайды.

   - **Құрылғыны қайта іске қосу**

     Осы нұсқа таңдалған болса, онда қауіпсіздік бағдарламасы орнатылғаннан кейін, құрылғы қайта іске қосылады.

8. Қажет болса, кезең-кезеңімен **Құрылғыларға қатынасу үшін есептік жазбаларды таңдау** қадамында *Бағдарламаны қашықтан орнату* тапсырмасын орындау үшін пайдаланылатын есептік жазбаларды қосыңыз:

   - **Есептік жазба қажет емес (Желілік агент орнатылды)**

     Егер бұл нұсқа таңдалса, бағдарлама инсталляторын іске қосуға негіз болып саналатын есептік жазбаны көрсетудің қажеті жоқ. Тапсырма, Басқару сервері қызметі жұмыс істейтін есептік жазба астында іске қосылады.

     Желілік агент клиент құрылғыларында орнатылмаған болса, бұл нұсқа қолжетімді емес.

- **Есептік жазба қажет (Желілік агент пайдаланылмайды)**

  Егер сіз қашықтан орнату тапсырмасын тағайындайтын құрылғыларда Желілік агент орнатылмаған болса, осы нұсқаны таңдаңыз. Бұл жағдайда бағдарламаны орнату үшін пайдаланушы есептік жазбасын немесе SSH сертификатын көрсетуге болады.

  - **Жергілікті немесе домен есептік жазбасы**. Егер бұл нұсқа таңдалса, бағдарлама инсталляторын іске қосуға негіз болатын есептік жазбаны көрсетіңіз. **Қосу** түймесін басыңыз, **Жергілікті немесе домен есептік жазбасы** опциясын таңдаңыз және пайдаланушының есептік жазбасының деректерін көрсетіңіз.

    Тапсырма тағайындалған барлық құрылғыларда олардың ешқайсысы қажетті құқықтарға ие болмаса, бірнеше есептік жазбаны көрсетуге болады. Бұл жағдайда, тапсырманы іске қосу үшін барлық қосылған есептік жазбалар бірізді түрде, жоғарыдан төменге қарай қолданылады.

  - **SSH сертификаты**. Бағдарламаны Linux басқаратын клиенттік құрылғыға орнатқыңыз келсе, пайдаланушы есептік жазбасының орнына SSH сертификатын көрсетуге болады. **Қосу** түймесін басыңыз, **SSH сертификаты** опциясын таңдаңыз және сертификаттың жеке және ашық кілттерін көрсетіңіз.

    Жеке кілт жасау үшін ssh-keygen утилитасын пайдалануға болады. Kaspersky Security Center Linux жеке кілттердің PEM форматына қолдау көрсететінін ескеріңіз, бірақ ssh-keygen утилитасы SSH кілттерін әдепкісінше OPENSSH форматында жасайды. OPENSSH форматына Kaspersky Security Center Linux қолдау көрсетпейді. PEM қолдау көрсетілетін пішімінде жабық кілт жасау үшін -m PEM параметрін ssh-keygen пәрменіне қосыңыз. Мысалы:

    ```
    ssh-keygen -m PEM -t rsa -b 4096 -C "<пайдаланушының электрондық поштасы>"
    ```

9. Тапсырма жасау және шеберді абу үшін **Тапсырманы жасауды аяқтау** қадамында **Аяқтау** түймесін басыңыз.

   Жасап болған соң, тапсырма туралы мәліметтерді ашу параметрі қосулы болса, тапсырма параметрлері терезесі ашылады. Бұл терезеде тапсырма параметрлерін тексеруге, оларды өзгертуге немесе қажет болса, тапсырманы іске қосу кестесін конфигурациялауға болады.

10. Тапсырмалар тізімінде жасалған тапсырманы таңдап, **Іске қосу** түймесін басыңыз.

    Немесе тапсырма параметрлерінде көрсетілген кестеге сәйкес тапсырманың іске қосылуын күтіңіз.

Қашықтан орнату тапсырмасын орындағаннан кейін, таңдалған бағдарлама көрсетілген құрылғылар жиынтығына орнатылады.

Қолданбаларды macOS құрылғыларына қашықтан орнату

Қашықтан орнату тапсырмасын пайдаланып, macOS жүйесі бар құрылғыларға қолданбаларды орнату үшін:

1. Орнату пакеті мен .sh орнату сценарийінен тұратын мұрағат жасаңыз.

2. Жаңа тапсырма шеберіндегі **Жүктеп алмас бұрын операциялық жүйенің түрін тексеру** опциясын өшіріңіз.

Болмаса **Скрипттерді қашықтан орындау** тапсырмасын пайдалануға болады. Келесі мақалада осы тапсырма үшін файлдарды конфигурациялау жолы сипатталған: Скриптілерді қашықтан орындау тапсырмасын пайдаланып, құрылғыларға қолданбаларды қашықтан орнату.

Қосалқы Басқару серверлеріне бағдарламаларды орнату

Басқару серверінің нұсқасы 15.4 немесе одан кейінгі нұсқа болса, өосымша басқару серверінің нұсқасы 15.4 немесе одан кейінгі нұсқа болса ғана, қосымша басқару серверіне қолданбаларды орнатуға болады.

Бағдарламаны қосалқы Басқару серверлеріне орнату үшін:

1. Өзіңізге қажетті қосалқы Басқару серверлерін басқаратын Басқару серверіне қосылыңыз.

2. Орнатылған бағдарламаға сәйкес орнату пакеті таңдалған қосалқы Басқару серверлерінің әрқайсысында екеніне көз жеткізіңіз. Егер сіз кез келген Серверден орнату пакетін таба алмасаңыз, оны таратыңыз. Бұл үшін **Орнату пакетін тарату** тапсырма түрі бар тапсырманы жасаңыз.

3. Қосалқы Басқару серверлеріне бағдарламаны қашықтан орнату тапсырмасын жасаңыз. **Қосалқы Басқару серверіне бағдарламаны қашықтан орнату** тапсырма түрін таңдаңыз.

   Жаңа тапсырма жасау шебері жұмысының нәтижесінде таңдалған қосалқы Басқару серверлеріне таңдалған бағдарламаны қашықтан орнату тапсырмасы жасалады.

4. Тапсырманы қолмен іске қосыңыз немесе тапсырма параметрлерінде көрсетілген кестеге сәйкес оның іске қосылуын күтіңіз.

Қашықтан орнату тапсырмасын орындағаннан кейін, таңдалған бағдарлама қосалқы Басқару серверлеріне орнатылады.

Желілік агенті орнатылған құрылғыларға бағдарламаларды қашықтан орнату

Егер құрылғыда негізгі Басқару серверіне немесе оның қосалқы Серверлерінің біріне қосылған жұмысқа жарамды Желілік агент орнатылған болса, онда осы құрылғыда Желілік агенттің нұсқасын жаңартуға, сондай-ақ Желілік агенттің көмегімен кез келген қолдау көрсетілетін қолданбаларды орнатуға, жаңартуға немесе жоюға болады.

Бұл функция, қолданбаларды қашықтан орнату тапсырмасының сипаттарында **Желілік агенттің көмегімен** параметрі тарапынан қосылады.

Параметр таңдалған болса, құрылғыларға әкімші белгілеген орнату параметрлері бар орнату пакеттерін жіберу, Желілік агент пен Басқару сервері арасындағы байланыс арналары арқылы жүзеге асырылады.

Басқару серверіне түсетін жүктемені оңтайландыру және Басқару сервері мен құрылғылар арасындағы трафикті азайту үшін, әрбір қашықтағы желіде немесе әрбір кеңінен тарататын доменде тарату нүктелерін тағайындаған жөн ("Тарату нүктелері туралы" және "Басқару топтары құрылымын құру және тарату нүктелерін тағайындау" бөлімдерін қараңыз). Бұл жағдайда, орнату пакеттері мен инсталлятор параметрлерін тарату, құрылғыларға Басқару серверінен тарату нүктелері арқылы жүзеге асырылады.

Сондай-ақ, тарату нүктелерін қолдана отырып, бағдарламаларды орналастыру барысында желілік трафикті бірнеше есе төмендетуге мүмкіндік беретін орнату пакеттерін кеңінен (көп мекенжайға) таратуға болады.

Орнату пакеттерін құрылғыларға желілік агенттер мен басқару сервері арасында байланыс арналары арқылы жіберген кезде, жіберуге дайындалған орнату пакеттері /var/opt/kaspersky/klnagent_srv/1093/.working/ қалтасында қосымша түрде кэштеледі. Үлкен өлшемдегі әртүрлі орнату пакеттерінің көп бөлігін қолдану кезінде және тарату нүктелерінің көп санында осы қалтаның өлшемі айтарлықтай ұлғаюы мүмкін.

FTServer қалтасындағы файлдарды жоюға болмайды. Бастапқы орнату пакеттерін жою кезінде, тиісті деректер FTServer қалтасынан да автоматты түрде жойылатын болады.

Тарату нүктелері қабылайтын деректер /var/opt/kaspersky/klnagent_srv/1103/ қалтасында сақталады.

$FTCITmp қалтасындағы файлдарды жоюға болмайды. Қалтадағы деректерді қолданатын тапсырмаларды аяқтау шамасына қарай, осы қалтаның ішіндегісі автоматты түрде жойылады.

Орнату пакеттері, желі арқылы беру үшін оңтайландырылған аралық қоймадан Басқару сервері мен Желілік агент арасындағы байланыс арналары бойынша таратылатындықтан, орнату пакетінің бастапқы қалтасындағы орнату пакеттеріне өзгеріс енгізуге болмайды. Мұндай өзгерістерді Басқару сервері автоматты түрде ескермейді. Орнату пакеттерінің файлдарын қолмен өзгерту қажет болса (мұны жасау ұсынылмайды), Kaspersky Security Center Web Console консоліндегі орнату пакетінің қандай да бір параметрлерін міндетті түрде өзгерту керек. Kaspersky Security Center Web Console консоліндегі орнату пакетінің параметрлерін өзгерту, Басқару серверін құрылғыға жіберуге дайындалған кештегі пакет кескінін жаңартуға мәжбүрлейді.

Сервер қашықтан орнату кезінде мақсатты құрылғыға ICMP жаңғырық сұрауларын (ping пәрменімен бірдей) жібереді.

Қашықтан орнату тапсырмасында құрылғыларды қайта жүктеуді басқару

Жиі қолданбаларды қашықтан орнатуды аяқтау үшін (әсіресе Windows платформасында) құрылғыны қайта іске қосу қажет.

Егер Kaspersky Security Center Linux қолданбаларды қашықтан орнату тапсырмасы қолданылса, жаңа тапсырма жасау шеберінде немесе жасалған тапсырма сипаттарының терезесінде (**Операциялық жүйені қайта іске қосу** бөлімі) Windows құрылғысы қайта іске қосуды қажет еткенде орындалатын әрекетті таңдауға болады:

- **Құрылғыны қайта іске қоспау**. Бұл жағдайда автоматты қайта іске қосу орындалмайды. Орнатуды аяқтау үшін құрылғыны қайта іске қосу керек (мысалы, қолмен немесе құрылғыларды басқару тапсырмасы көмегімен). Қайта іске қосу қажеттілігі туралы ақпарат тапсырманы орындау нәтижелерінде және құрылғы күйінде сақталады. Бұл нұсқа серверлерге және үздіксіз жұмыс критикалық түрде маңызды басқа құрылғыларға орнату тапсырмалары үшін қолайлы.

- **Құрылғыны қайта іске қосу**. Бұл жағдайда, егер қайта іске қосу орнатуды аяқтау үшін қажет болса, қайта іске қосу автоматты түрде орындалады. Бұл нұсқа жұмыста мерзімді үзілістерге жол берілетін (сөндіру, қайта іске қосу) құрылғыларға арналған орнату тапсырмаларына қолайлы.

- **Пайдаланушыдан әрекетті орындауды сұрау**. Клиент құрылғысының экранында құрылғыны қолмен қайта жүктеу керек деген хабар пайда болады. Бұл нұсқа үшін қосымша параметрлерді конфигурациялауға болады: пайдаланушыға арналған хабар мәтіні, хабардың жиілігі, сондай-ақ қайта жүктеу мәжбүрлі түрде орындалатын уақыт (пайдаланушының растауынсыз). **Пайдаланушыдан әрекетті орындауды сұрау** нұсқасы пайдаланушылары қайта іске қосу үшін анағұрлым қолайлы сәтті таңдау мүмкіндігіне ие болуы тиіс жұмыс станцияларына анағұрлым қолайлы.

Kaspersky Security Center Linux қолданбаларын қашықтан орнату тапсырмасы арқылы мәжбүрлеп орналастыру

Желілік агентті немесе басқа қолданбаларды бастапқы орналастыру үшін әрбір құрылғыда жергілікті әкімші құқықтары бар пайдаланушы есептік жазбалары болған жағдайда, Kaspersky Security Center Linux қашықтан орнату тапсырмасымен таңдалған орнату пакеттерін мәжбүрлі түрде орнатуға болады.

Күшпен орнату құрылғылар тікелей Басқару серверіне қолжетімді болмаған жағдайда қолданылуы мүмкін: мысалы, құрылғылар оқшауланған желілерде орналасқан немесе құрылғылар жергілікті желіде, ал Басқару сервері - демилитаризацияланған аймақта орналасқан.

Бастапқы енгізу кезінде желілік агент орнатылмайды. Сондықтан қашықтан орнату тапсырмасының параметрлерінде Желілік агент көмегімен қолданбаны орнату үшін қажетті файлдарды таратуды таңдау мүмкін емес. Файлдарды басқару сервері немесе тарату нүктесі көмегімен операциялық жүйе ресурстарын пайдаланып қана тарата аласыз.

Басқару серверінің қызметі мақсатты құрылғыларда әкімші құқықтары бар есептік жазбамен іске қосылуы керек. Сондай-ақ қашықтан орнату тапсырмасы параметрлерінде admin$ жалпы қатынасы бар әкімшілік ресурстарына кіре алатын есептік жазбаны көрсетуге болады.

Әдепкісінше қашықтан орнату тапсырмасы құрылғыларға басқару сервері іске қосылған есептік жазбаның тіркелгі деректері көмегімен қосылады. Бұл қашықтан орнату тапсырмасы орындалатын есептік жазба емес, admin$ жалпы қатынасы бар әкімшілік ресурстарына кіру үшін қолданылатын есептік жазба екенін ескеріңіз. Орнату LocalSystem есептік жазбасында орындалады.

Мақсатты құрылғыларды олар тиесілі Kaspersky Security Center Linux басқару тобын таңдау арқылы анық (тізіммен) ашық көрсетуге; немесе белгілі бір критерийге негізделген құрылғыларды таңдау арқылы көрсетуге болады. Орнатуды іске қосу уақыты тапсырма кестесімен анықталады. Тапсырманың сипаттарында **Өткізіп алынған тапсырмаларды іске қосу** параметрі қосулы болса, тапсырма құрылғыларды қосу кезінде немесе оларды мақсатты басқару тобына көшіру кезінде бірден іске қосылуы мүмкін.

Мәжбүрлеп орнату әрекеті, орнату пакеттерін мақсатты құрылғыларға жеткізу, содан соң файлдарды құрылғылардың әрқайсысының admin$ басқару ресурсына көшіру және оларға көмекші қызметтерді қашықтан тіркеу арқылы жүзеге асырылады. Орнату пакеттерін мақсатты құрылғыларға жеткізу әрекеті желілік өзара әрекеттесуге жауап беретін Kaspersky Security Center Linux функциясы арқылы жүзеге асырылады. Бұл жағдайда, келесі шарттар орындалуы керек:

- Мақсатты құрылғыларға басқару серверінен немесе тарату нүктесінен қол жеткізуге болады.
- Желіде құрылғыларға арналған атаулар рұқсаты дұрыс жұмыс істеп жатыр.
- Мақсатты құрылғыларда admin$ жалпы қатынасын басқару ресурстары қосулы.
- Мақсатты құрылғыларда келесі жүйелік қызметтер іске қосылған:
  - Сервер (LanmanServer).

    Әдепкі бойынша бұл қызмет іске қосылған.
  - DCOM Server Process Launcher (DcomLaunch).

- RPC Endpoint Mapper (RpcEptMapper).
- Қашықтағы процедураны шақыру (Remote Procedure Call, RpcSs).

- TCP 445 порты Windows басқару құралдары көмегімен қашықтан қол жеткізуге рұқсат беру үшін мақсатты құрылғыларда ашық.

  > TCP 139, UDP 137 және UDP 138 ескі протоколдармен пайдаланылады және енді ағымдағы бағдарламаларға қажет емес.

  Басқару серверін және тарату нүктелерін мақсатты құрылғыларға қосу үшін желілік экранда динамикалық шығыс кіру порттарына рұқсат берілуі керек.

- Желілік агентті енгізу кезінде Active Directory домен саясатының қауіпсіздік параметрлерінде NTLM протоколының жұмысын қамтамасыз етуге рұқсат берілді.
- Microsoft Windows XP басқаратын мақсатты құрылғыларда Simple File Sharing режимі өшірулі.
- Мақсатты құрылғыларда *классикалық бөлісу және қауіпсіздік моделінің параметрлері орнатылған — жергілікті пайдаланушылар өздерін аутентификациялайды.* Мұндай модель *тек қонақ болуы мүмкін емес – жергілікті пайдаланушылар қонақ ретінде аутентификациялайды.*
- Құрылғылар домен мүшелері болып табылады немесе құрылғыларда басқару құқықтары бар бірегейлендірілген есептік жазбалар алдын ала жасалған.

> Windows Server 2003 немесе одан жоғары операциялық жүйе нұсқасы орнатылған Active Directory доменіне қосылмаған құрылғыда желілік агент немесе басқа бағдарламаларды сәтті енгізу үшін сол құрылғыда қашықтағы UAC өшіру керек. Қашықтағы UAC — жергілікті әкімші есептік жазбаларының admin$-ке қол жеткізе алмауы себептерінің бірі, бұл желілік агентті және басқа бағдарламаларды мәжбүрлі түрде енгізу үшін қажет. Қашықтағы UAC өшіру жергілікті UAC-ге әсер етпейді.

Kaspersky Security Center Linux басқару топтарында әлі орналастырылмаған жаңа құрылғыларға орнатқан кезде, қашықтан орнату тапсырмасының сипаттарында Желілік агентті орнату аяқталғаннан кейін құрылғылар көшірілетін басқару тобын белгілеуге болады.

> Топтық тапсырманы жасау кезінде, топтық тапсырма таңдалған топтың барлық салынған ішкі топтарының құрылғыларына әсер ететінін есте ұстаған жөн. Сондықтан, орнату тапсырмаларын ішкі топтарда қайталамау керек.

Бағдарламаларды мәжбүрлі түрде орнату үшін тапсырмаларды жасаудың жеңіл жолы — автоматты түрде орнату. Ол үшін басқару тобының сипаттарында орнату пакеттерінің тізімін ашып, осы топтың құрылғыларына орнатылуы керек пакеттерді таңдау керек. Нәтижесінде, осы топтың және оның ішкі топтарының барлық құрылғыларында, таңдалған орнату пакеттері автоматты түрде орнатылады. Пакеттер орнатылатын кезең, желінің өткізу қабілетіне және желідегі құрылғылардың жалпы санына байланысты.

Орнату пакеттерін мақсатты құрылғыларға тарату кезінде басқару серверіндегі жүктемені азайту үшін орнату тапсырмасында тарату нүктелерін пайдаланып, орнатуды таңдауға болады. Орнатудың бұл тәсілі, тарату нүктелерімен тағайындалған құрылғыларға елеулі жүктеме түсіретінін ескеру қажет. Тарату нүктелеріне қойылатын талаптарға сай құрылғыларды таңдау ұсынылады. Тарату нүктелерін пайдалансаңыз, олардың мақсатты құрылғыларды орналастыратын оқшауланған ішкі желілердің әрқайсысында болуын қамтамасыз ету керек.

Жергілікті орнату орталықтары ретінде тарату нүктелерін қолдану ішкі желі ішінде құрылғылар арасында кең байланыс арнасы бар болған кезде тар байланыс арнасымен Басқару серверіне қосылған ішкі желілерде құрылғыларға орнату үшін де ыңғайлы болуы мүмкін.

/var/opt/kaspersky/KSC_Backups* қалтасы бар бөлімдегі бос орын өлшемі орнатылатын қолданбалар дистрибутивтерінің жалпы өлшемінен бірнеше есе асып түсуі керек.

Бағдарламаларды тыныш режимде орнату

Бағдарламаны тыныш режимде орнату үшін:

1. Бағдарламаның негізгі терезесінде **Бағдарламалық жасақтаманы басқару** → **Орнату пакеттері** бөліміне өтіңіз.

2. Қажетті қолданбаның орнату пакетінің жанындағы ұяшықты белгілеңіз немесе сол қолданба үшін жаңасын жасаңыз.

   Орнату пакеті Басқару серверінде Packages қызметтік қалтасындағы ортақ қатынасы бар қалтада сақталады. Бұл жағдайда, әрбір орнату пакетіне жеке салынған қалта сәйкес келеді.

3. Қажетті орнату пакетінің қалтасын келесі тәсілдердің бірімен ашыңыз:

   - Қажетті орнату пакетіне сәйкес қалтаны Басқару серверінен клиент құрылғысына көшіріңіз. Содан кейін, клиент құрылғысында көшірілген қалтаны ашыңыз.

   - Клиент құрылғысынан Басқару серверінде қажетті орнату пакетіне сәйкес келетін ортақ қатынасы бар қалтаны ашыңыз.

   Егер ортақ қатынасы бар қалта Microsoft Windows Vista операциялық жүйесі орнатылған құрылғыларда орналасқан болса, **Пайдаланушылардың есептік жазбаларын басқару: барлық әкімшілер әкімшінің мақұлдауы режимінде жұмыс істейді** параметрі үшін **Өшірулі** мәнін белгілеу керек (**Бастау** → **Басқару тақтасы** → **Басқару** → **Жергілікті қауіпсіздік саясаты** → **Қауіпсіздік параметрлері**).

4. Таңдалған бағдарламаға байланысты келесі әрекеттерді орындаңыз:

   - Kaspersky Anti-Virus for Windows Workstations, Kaspersky Anti-Virus for Windows Servers және Kaspersky Security Center үшін салынған exec қалтасына өтіп, /s кілті бар орындалатын файлды (exe кеңейтімі бар файлды) іске қосыңыз.

   - Kaspersky қалған бағдарламалары үшін /s кілті бар орындалатын файлды (exe кеңейтімі бар файлды) ашық қалтадан іске қосыңыз.

`EULA=1` және `PRIVACYPOLICY=1` кілттері бар орындалатын файлды іске қосу, сіз сәйкесінше Лицензиялық келісім мен Құпиялық саясатын толығымен оқып шыққаныңызды, түсінгеніңізді және олардың ережелерін қабылдайтыныңызды білдіреді. Сондай-ақ, сіздің деректеріңіз Құпиялылық саясатында сипатталғандай өңделетінін және жіберілетінін (соның ішінде үшінші елдерге) білесіз. Лицензиялық келісімнің мәтіні және Құпиялылық саясатының мәтіні Kaspersky Security Center Linux жеткізу жиынтығына кіреді. Лицензиялық келісім мен Құпиялылық саясатының ережелерімен келісу, бағдарламаны орнату үшін немесе бағдарламаның алдыңғы нұсқасын жаңарту үшін қажетті шарт болып табылады.

macOS операциялық жүйесі бар құрылғыны Желілік агентті қашықтан орнатуға дайындау

MacOS басқарылатын құрылғысына желілік агентті орнатудың келесі әдістері бар:

- macOS тарату нүктесінде қашықтан орнату тапсырмасын орындау арқылы.
- Құрылғы пайдаланушыларына Kaspersky Security Center Linux жасаған дербес пакеттер сілтемелерін жіберу арқылы. Автономды пакеттер, параметрлері конфигурацияланған таңдалған бағдарламалардың дистрибутивтерін қамтитын орындалатын модульдер болып табылады.

macOS операциялық жүйесі бар құрылғыны Желілік агентті қашықтан орнатуға дайындау үшін:

1. macOS операциялық жүйесі бар мақсатты құрылғыда sudo бағдарламасы орнатылғанына көз жеткізіңіз.
2. Құрылғының конфигурациясын тексеріңіз:
   a. Клиент құрылғысында 22-порттың ашық екеніне көз жеткізіңіз. Бұл үшін, **Жүйелік конфигурациялар** бөлімінде **Алмасу** тақтасын ашып, **Қашықтан кіру** жалаушасының қойылғанына көз жеткізіңіз.

      Сіз клиент құрылғысына Secure Shell (SSH) протоколы бойынша тек 22-порт арқылы қосыла аласыз. Сіз порт нөмірін өзгерте алмайсыз.

      macOS құрылғысына қашықтан кіру үшін `ssh <құрылғы_аты>` пәрменін қолдана аласыз. macOS құрылғысына қатынасуға рұқсат алған пайдаланушылардың әрекет ету аумағын белгілеу үшін **Ортақ қатынас** тақтасында **Қатынасты рұқсат ету** параметрін қолдана аласыз.

   b. Құрылғы қосылатын пайдаланушы есептік жазбасы үшін sudo құпия сөзін өшіріңіз.

      Терминалда sudoers конфигурациялық файлын ашу үшін `sudo visudo` пәрменін қолданыңыз. Сіз ашқан файлда, `Пайдаланушы артықшылықтары ерекшеліктері` өрісінде келесіні көрсетіңіз: `username ALL = (ALL) NOPASSWD: ALL`. Бұл жағдайда, `username` – құрылғыға SSH протоколы арқылы қосылу үшін қолданылатын пайдаланушы есептік жазбасы болып табылады.

   c. sudoers файлын сақтаңыз және жабыңыз.

   d. SSH арқылы құрылғыға қайта қосылыңыз және `sudo whoami` пәрменінің көмегімен, sudo қызметі құпиясөзді қажет етпейтінін тексеріңіз.

3. Орнату пакеттерін жүктеп алыңыз және жасаңыз:

   a. Желілік агенттің орнату пакетін келесі тәсілдердің бірімен жүктеп алыңыз:

      - Қолданба интерфейсін пайдалану арқылы
      - Желілік агенттің тиісті нұсқасын техникалық қолдау қызметінің https://support.kaspersky.com/ веб-сайтынан жүктеп алу арқылы
      - Техникалық қолдау қызметі мамандарынан орнату пакетін сұрау арқылы

   b. Қашықтан орнату пакетін жасау үшін келесі файлдарды пайдаланыңыз:

      - klnagent.kud
      - install.sh
      - klnagentmac.dmg

4. Бағдарламаны қашықтан орнату тапсырмасын келесі параметрлермен жасаңыз:

   - Жаңа тапсырма жасау шеберінің **Параметрлер** терезесінде **Басқару сервері арқылы операциялық жүйе ресурстарының көмегімен** жалаушасын қойыңыз. Барлық басқа жалаушаларды алып тастаңыз.
   - **Тапсырманы іске қосу үшін есептік жазбаны таңдау** терезесінде, тапсырманы іске қосу үшін құрылғыға SSH арқылы қосылу мақсатымен пайдаланылатын есептік жазба параметрлерін көрсетіңіз.

Клиент құрылғысы сіз жасаған тиісті тапсырманы пайдаланып Желілік агентті қашықтан орнатуға дайын.

Виртуалды инфрақұрылым

Kaspersky Security Center Linux бағдарламасы виртуалды машиналармен жұмыс істеуді қолдайды. Сіз әр виртуалды машинада Желілік агент пен қауіпсіздік бағдарламаларын орната аласыз, сонымен қатар виртуалды машиналарды гипервизор деңгейінде қорғай аласыз. Бірінші жағдайда, виртуалды машиналарды қорғау үшін қарапайым қауіпсіздік бағдарламасын да, Kaspersky Security for Virtualization Light Agent бағдарламасын да қолдануға болады. Екінші жағдайда, Kaspersky Security for Virtualization Agentless бағдарламасын қолдана аласыз.

Kaspersky Security Center Linux бағдарламасы виртуалды машиналарды алдыңғы күйге шегіндіру мүмкіндігін қолдайды.

Виртуалды машиналарға түсетін жүктемені азайту бойынша ұсынымдар

Желілік агентті виртуалды машинаға орнатқан жағдайда, виртуалды машиналар үшін өте пайдалы емес Kaspersky Security Center Linux функционалдығының бір бөлігін өшіру туралы ойлану керек.

Желілік агентті виртуалды машинаға немесе болашақта виртуалды машиналар алынатын үлгіге орнатқан кезде келесі әрекеттерді орындау ұсынылады:

- қашықтан орнату орындалып жатса, Желілік агенттің орнату пакетінің сипаттар терезесінде (**Кеңейтілген** бөлімінде) **VDI параметрлерін оңтайландыру** параметрін таңдаңыз;
- егер шебердің көмегімен интерактивті орнату орындалып жатса, шебер терезесінде **Виртуалды инфрақұрылым үшін Желілік агент параметрлерін оңтайландыру** параметрін таңдаңыз.

Параметрлерді таңдау, Желілік агенттің параметрлерін, әдепкі бойынша (саясатты қолданар алдында) келесі функциялар өшірілетіндей етіп өзгертеді:

- Орнатылған бағдарламалық жасақтама туралы ақпарат алу
- Аппараттық жасақтама туралы ақпарат алу
- Осалдықтардың болуы туралы ақпарат алу
- Қажетті жаңартулар туралы ақпарат алу

Әдетте, аталған функциялар виртуалды машиналарда қажет емес, өйткені олардағы бағдарламалық жасақтама мен виртуалды аппараттық жасақтама біркелкі.

Функцияларды өшіру қайтымды. Егер өшірулі функциялардың кез келгені қажет болса, оны Желілік агент саясаты немесе Желілік агенттің жергілікті параметрлері арқылы қосуға болады. Желілік агенттің жергілікті параметрлері Kaspersky Security Center Web Console консоліндегі сәйкес құрылғының контекстік мәзірінен қолжетімді.

Динамикалық виртуалды машиналарды қолдау

Kaspersky Security Center Linux динамикалық виртуалды машиналарды қолдайды. Егер ұйымның желісінде виртуалды инфрақұрылым орналастырылған болса, онда кейбір жағдайларда динамикалық (уақытша) виртуалды машиналар қолданылуы мүмкін. Мұндай машиналар, әкімші алдын ала дайындаған үлгіден ерекше атаулармен жасалады. Пайдаланушы жасалған машинамен біраз уақыт жұмыс істейді, ал виртуалды машина өшірілгеннен кейін виртуалды инфрақұрылымнан жойылады. Егер ұйымның желісінде Kaspersky Security Center Linux орналастырылған болса, оған орнатылған Желілік агенті бар виртуалды машина Басқару серверінің дерекқорына қосылады. Виртуалды машинаны өшіргеннен кейін, ол туралы жазба Басқару сервері дерекқорынан да жойылуы керек.

Виртуалды машина жазбаларын автоматты түрде жою функционалдығы жұмыс істеуі үшін Желілік агентті динамикалық виртуалды машиналар жасалатын үлгіе орнатқан кезде **VDI үшін динамикалық режимді қосу** параметрін таңдау керек:

- қашықтан орнату жағдайында – Желілік агенттің орнату пакетінің сипаттары терезесінде (**Кеңейтілген** бөлімі);
- интерактивті орнату жағдайында – Желілік агентті орнату шеберінде.

VDI үшін динамикалық режимді қосу параметрі Желілік агентті физикалық құрылғыларға орнатқан кезде таңдалмауы керек.

Машиналар жойылғаннан кейін Динамикалық виртуалды машиналардағы оқиғалар біраз уақыт бойы Басқару серверінде сақталуы керек болса, онда Басқару сервері сипаттары терезесінде, **Оқиғалар қоймасы** бөлімінде **Құрылғылар жойылғаннан кейін оқиғаларды сақтау** параметрін таңдап, күндердегі оқиғаларды сақтаудың ең ұзақ уақытын көрсету керек.

Динамикалық виртуалды машиналарда дискіні шифрлауды қосуға кеңес бермейміз.

Виртуалды машиналарды көшіруді қолдау

Виртуалды машинаны орнатылған Желілік агентімен бірге көшіру немесе оны орнатылған Желілік агентпен бірге үлгіден жасау – қатты дискінің кескінін түсіру және көшіру арқылы Желілік агенттерді орналастыруға тең келеді. Сондықтан, жалпы жағдайда, виртуалды машиналарды көшіру кезінде диск кескінін көшіру арқылы орналастыру сияқты әрекеттерді орындау қажет.

Алайда, төменде сипатталған екі жағдайда Желілік агент көшіру фактісін автоматты түрде анықтайды. Сондықтан, "Құрылғының қатты дискісін түсіру және көшіру" бөлімінде сипатталған күрделі әрекеттерді орындау міндетті емес:

- Желілік агентті орнату кезінде **VDI үшін динамикалық режимді қосу** параметрі таңдалды: операциялық жүйені әрбір рет қайта іске қосқаннан кейін мұндай виртуалды машина, оны көшіру фактісіне қарамастан, жаңа құрылғы болып саналатын болады.
- Келесі гипервизорлардың бірі қолданылады: VMware™, HyperV® немесе Xen®: Желілік агент виртуалды машинаны көшіру фактісін виртуалды аппараттық жасақтаманың өзгерген идентификаторлар бойынша анықтайды.

Виртуалды аппараттық жасақтаманың өзгерістерін талдау мүлдем сенімді емес. Бұл әдісті кеңінен қолданбас бұрын, оның жұмысқа жарамдылығын ұйымда қолданылатын гипервизордың нұсқасы үшін аздаған виртуалды машиналарда алдын ала тексеріп алу керек.

Unix басқаруымен жұмыс істейтін құрылғыларда қашықтан орнату параметрлерін көрсету

Бағдарламаны Unix басқаруымен жұмыс істейтін құрылғыға қашықтан орнату тапсырмасы арқылы орнатқан кезде, сіз осы тапсырма үшін Unix-ке тән параметрлерді көрсете аласыз. Бұл параметрлер тапсырма жасалғаннан кейін, оның сипаттарында қолжетімді.

Қашықтан орнату тапсырмасы үшін Unix-ке тән параметрлерді көрсету үшін:

1. Бағдарламаның негізгі терезесінде **Тапсырмалар** бөліміне өтіңіз.
2. Unix-ке тән параметрлерді көрсеткіңіз келетін қашықтан орнату тапсырмасының атын басыңыз.

   Тапсырма сипаттары терезесі ашылады.
3. **Бағдарлама параметрлері** → **Unix жүйесіне тән параметрлер** бөліміне өтіңіз.

4. Келесі параметрлерді белгілеңіз:

   - **Түбірлік есептік жазба үшін құпиясөз орнатыңыз (тек SSH арқылы орналастыру үшін)**

     `sudo` пәрменін мақсатты құрылғыда құпиясөзді көрсетпей қолдануға болмаса, осы параметрді таңдаңыз, содан соң root есептік жазбасы үшін құпиясөзді көрсетіңіз. Kaspersky Security Center Linux бағдарламасы құпиясөзді мақсатты құрылғыға шифрланған түрде жібереді, құпиясөзді шифрсыздайды, содан кейін орнату процедурасын құпиясөзі көрсетілген root есептік жазбасы атынан іске қосады.

     > Kaspersky Security Center Linux бағдарламасы SSH қосылымын жасау үшін есептік жазбаны немесе көрсетілген құпиясөзді пайдаланбайды.

   - **Мақсатты құрылғыда Рұқсатты орындау арқылы уақытша қалтаға жолды көрсетіңіз (тек SSH арқылы орналастыру үшін)**

     Егер мақсатты құрылғыдағы /tmp қалтасының Орындау құқығы болмаса, осы параметрді таңдап, содан кейін Орындау құқықтары бар қалта жолын көрсетіңіз. Kaspersky Security Center Linux аталған қалтаны SSH арқылы қатынасу үшін уақытша қалта ретінде пайдаланады. Бағдарлама орнату пакетін қалтаға орналастырады және орнату процедурасын бастайды.

5. **Сақтау** түймесін басыңыз.

Көрсетілген тапсырма параметрлері сақталған.

Орналастыру мониторингі

Kaspersky Security Center Linux жүйесін орналастыруды бақылау және қауіпсіздік қолданбасы мен Желілік агент басқарылатын құрылғыларда орнатылғанына көз жеткізу үшін бақылау және есеп функцияларын пайдаланыңыз:

- Нақты уақытта орналастыруды бақылау үшін бақылау тақтасында орналастыру веб-виджетін пайдаланыңыз.
- Толық ақпарат алу үшін есептерді пайдаланыңыз.

Kaspersky бағдарламаларын іске қосу және тоқтату

Басқарылатын құрылғыларда Kaspersky қолданбаларын іске қосу және тоқтату үшін *қолданбаны іске қосу немесе тоқтату* тапсырмасын пайдалануға болады.

Қолданбаны іске қосу немесе тоқтату тапсырмасын жасау үшін:

1. Бағдарламаның негізгі терезесінде **Тапсырмалар** бөліміне өтіңіз.
2. **Қосу** түймесін басыңыз.

   Жаңа тапсырма жасау шебері іске қосылады. Шебердің жұмысын жалғастыру үшін **Келесі** түймесін басыңыз.

3. Ашылатын **Бағдарлама** тізімінен тапсырма жасағыңыз келетін қолданбаны таңдаңыз.

   Осы қолданбаларды басқаруға арналған веб-плагиндерді бұрын қосқан болсаңыз, Kaspersky қолданбалары тізімде пайда болады.

4. **Тапсырма түрі** тізімінде **Бағдарламаны белсендіру** тапсырмасын таңдаңыз.

5. **Тапсырманың атауы** өрісіне жаңа тапсырманың атын енгізіңіз.

   Тапсырма атауы 100 таңбадан асуы және арнайы таңбаларды ("*<>?\:|) қамтуы мүмкін емес.

6. Тапсырмалар тағайындалатын құрылғыларды таңдаңыз.

7. **Бағдарламалар** терезесінде келесі әрекеттерді орындаңыз:

   - Тапсырма жасағыңыз келетін қолданбалардың атауларының жанындағы құсбелгілерді қойыңыз.
   - **Бағдарламаны іске қосу** немесе **Бағдарламаны тоқтату** параметрін таңдаңыз.

8. **Жасап болған соң, тапсырма туралы мәліметтерді ашу** қадамында **Тапсырманы жасауды аяқтау** параметрін қоссаңыз, әдепкі бойынша белгіленген тапсырма параметрлері мәндерін өзгерте аласыз. Егер сіз бұл параметрді қоспасаңыз, тапсырма әдепкі бойынша белгіленген параметр мәндерімен жасалады. Әдепкі бойынша параметр мәндерін кейінірек кез келген уақытта өзгертуге болады.

9. **Аяқтау** түймесін басыңыз.

   Тапсырма жасалып, тапсырмалар тізімінде көрсетіледі.

10. Тапсырма сипаттары терезесін ашу үшін жасалған тапсырманың атын басыңыз.

11. Тапсырма сипаттары терезесінде өзіңіздің талаптарыңызға сай тапсырманың жалпы параметрлерін көрсетіп, параметрлерді сақтаңыз.

Тапсырма жасалды және конфигурацияланды.

Тапсырманы іске қосу үшін тапсырмалар тізімінен тапсырманы таңдап, **Іске қосу** түймесін басыңыз.

Үшінші тарап қауіпсіздік бағдарламаларын алмастыру

Kaspersky қауіпсіздік бағдарламаларын Kaspersky Security Center Linux құралдарымен орнату үшін, орнатылатын бағдарламамен үйлеспейтін үшінші тарап бағдарламалық жасақтамасын жою қажет болуы мүмкін. Kaspersky Security Center Linux, үшінші тарап бағдарламаларын жоюдың бірнеше тәсілін ұсынады.

Бағдарламаны қашықтан орнатуды кезінде үйлесімсіз бағдарламаларды жою

Қорғанысты орналастыру шеберінде қауіпсіздік бағдарламасын қашықтан орнату кезінде **Үйлесімсіз бағдарламаларды автоматты түрде жою** параметрін қосуға болады. Егер бұл параметр қосулы болса, Kaspersky Security Center Linux бағдарламасы басқарылатын құрылғыға қауіпсіздік бағдарламасын орнатпас бұрын, үйлесімсіз бағдарламаларды жояды.

Үйлесімсіз бағдарламаларды бөлек тапсырма арқылы жою

Үйлесімсіз қолданбаларды жою үшін *Бағдарламаны қашықтан жою* тапсырмасы қолданылады. Тапсырма қауіпсіздік бағдарламасын орнату тапсырмасынан бұрын, құрылғыларда іске қосылуы керек. Мысалы, орнату тапсырмасында **Басқа тапсырманы аяқтағанда** түріндегі кестені таңдауға болады, онда басқа тапсырма *Бағдарламаны қашықтан жою* тапсырмасы болып табылады.

Бұл жою тәсілі, қауіпсіздік бағдарламасы инсталляторы үйлесімсіз бағдарламалардың ешқайсысын сәтті жоя алмаған жағдайда қолданылғаны жөн.

Бағдарламаларды немесе бағдарламалық жасақтама жаңартуларын қашықтан жою

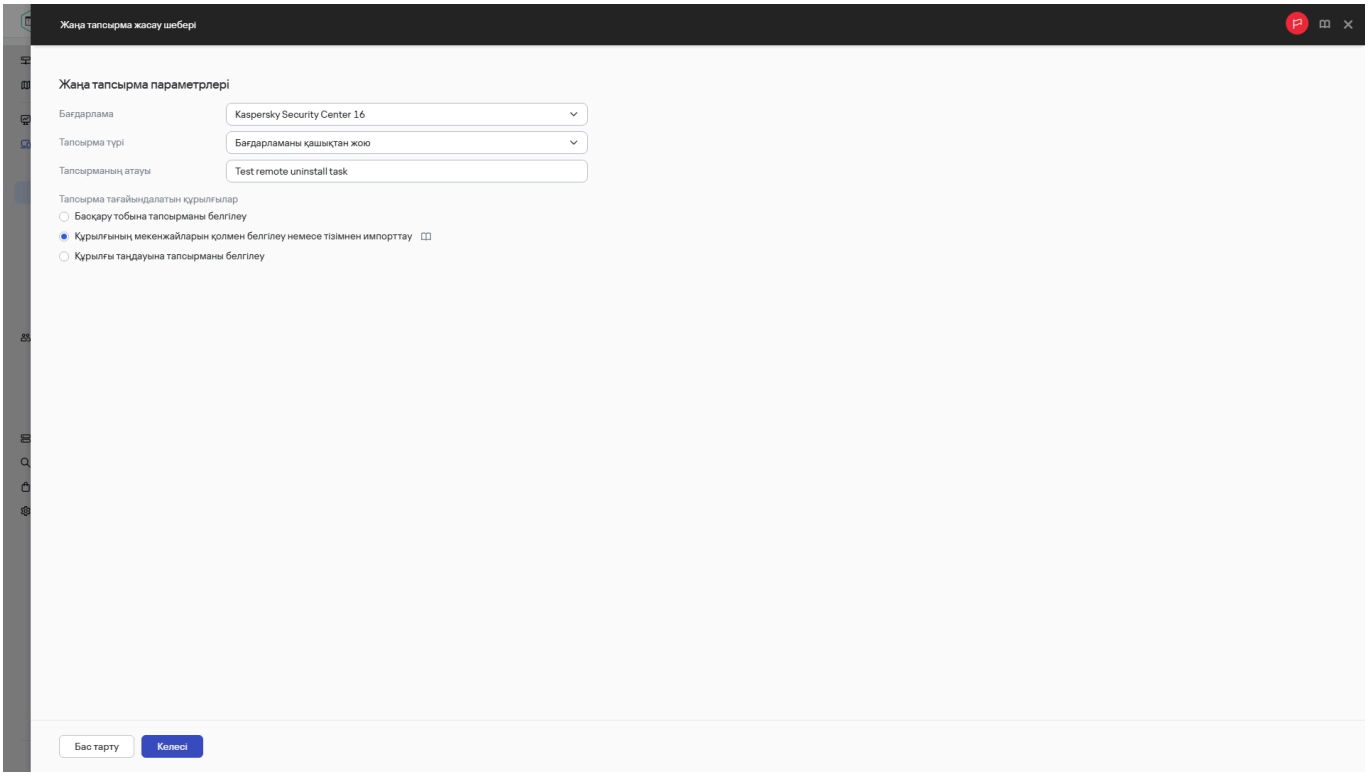
Сіз тек Желілік агент көмегімен Linux жұмыс істейтін басқарылатын құрылғылардағы бағдарламаларды немесе бағдарламалық жасақтама жаңартуларын қашықтан жоюға болады.

Бағдарламаларды немесе бағдарламалық жасақтама жаңартуларын қашықтан жою үшін:

1. Бағдарламаның негізгі терезесінде **Тапсырмалар** бөліміне өтіңіз.
2. **Қосу** түймесін басыңыз.

   Жаңа тапсырма жасау шебері іске қосылады. Шебердің жұмысын жалғастыру үшін **Келесі** түймесін басыңыз.
3. **Бағдарлама** ашылмалы тізімінде Kaspersky Security Center Linux опциясын таңдаңыз.
4. **Тапсырма түрі** тізімінде **Бағдарламаны қашықтан жою** тапсырма түрін таңдаңыз.
5. **Тапсырманың атауы** өрісіне жаңа тапсырманың атын енгізіңіз.

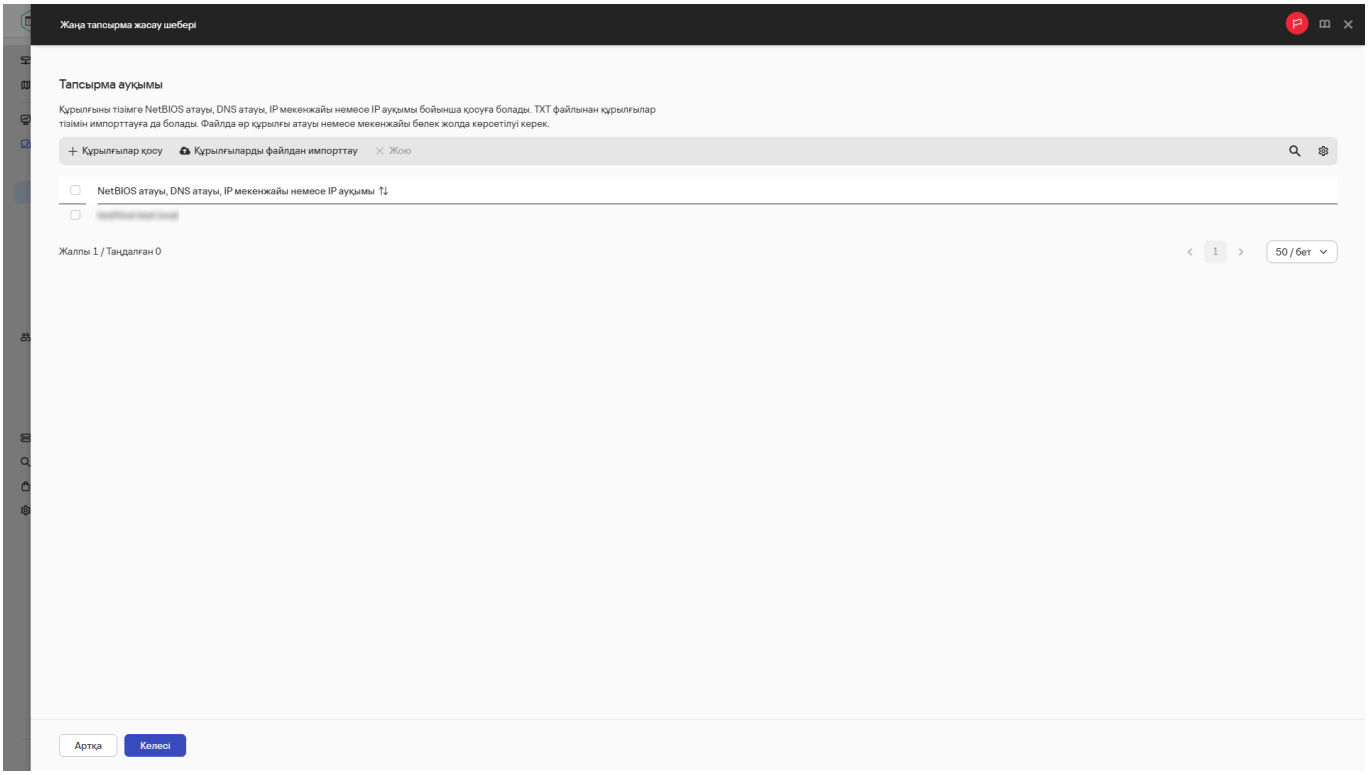
Тапсырма атауы 100 таңбадан асуы және арнайы таңбаларды ("*<>?\:|) қамтуы мүмкін емес.



Бағдарламаны қашықтан жою тапсырмасын жасау

6. Тапсырмалар тағайындалатын құрылғыларды таңдаңыз.

   Шебердің келесі қадамына өтіңіз.



Тапсырма ауқымын көрсету

7. Қандай бағдарламаны жойғыңыз келетінін таңдаңыз, содан кейін жойғыңыз келетін бағдарламаларды, жаңартуларды немесе патчтарды таңдаңыз:

- **Басқарылатын бағдарламаны жою**

  Kaspersky бағдарламалары тізімі көрсетіледі. Жойғыңыз келетін бағдарламаны таңдаңыз.

- **Үйлесімсіз бағдарламаны жою**

  Kaspersky немесе Kaspersky Security Center Linux қауіпсіздік бағдарламаларына сәйкес келмейтін бағдарламалардың тізімі көрсетіледі. Жойғыңыз келетін бағдарламаларға қарама-қарсы жалаушалар қойыңыз.

- **Бағдарламаны бағдарламалар тізімдемесінен жою**

  Әдепкі бойынша, Желілік агенттер басқарылатын құрылғыларда орнатылған бағдарламалар туралы ақпаратты Басқару серверіне жібереді. Орнатылған бағдарламалар тізімі бағдарламалар тізімдемесінде сақталады.

  Бағдарламалар тізімдемесінен бағдарламаны таңдау үшін:

  a. **Жойылатын бағдарлама** өрісіне басып, жойғыңыз келетін бағдарламаны таңдаңыз.

  > Егер сіз Kaspersky Security Center Желілік агентін таңдаған болсаңыз, тапсырма басталған кезде *Сәтті түрде аяқталды* күйі жою процесінің басталғанын көрсетеді. Kaspersky Security Center Желілік агент бағдарламасын жойған кезде күй өзгермейді. Тапсырма істен шыққан жағдайда күй *Ақау* деп өзгереді.

  b. Жою параметрлерін көрсетіңіз:

  - **Жою режимі**

    Бағдарламаны қалай жойғыңыз келетінін таңдаңыз:

    - **Жою пәрменін автоматты түрде анықтау**

      Егер бағдарламада бағдарлама өндірушісі белгілеген жою пәрмені болса, Kaspersky Security Center Linux бұл пәрменді пайдаланады. Осы нұсқаны таңдау ұсынылады.

    - **Жою пәрменін белгілеу**

      Бағдарламаны жою үшін пәрменіңізді көрсеткіңіз келсе, осы нұсқаны таңдаңыз.

      > Алдымен бағдарламаны **Жою пәрменін автоматты түрде анықтау** параметрімен жоюға тырысқан жөн. Егер автоматты түрде анықталған пәрменнің көмегімен жою сәтсіз болса, өз пәрменіңізді пайдаланыңыз.

      Осы өріске орнату пәрменін енгізіп, келесі параметрді көрсетіңіз:

      Әдепкі пәрмен автоматты түрде анықталмаса, әдепкі пәрменді тек жою үшін қолданыңыз

      Kaspersky Security Center Linux бағдарламасы таңдалған бағдарламада бағдарлама өндірушісі белгілеген жою пәрмені бар-жоғын тексереді. Егер команда табылса, Kaspersky Security Center Linux бағдарламасы оны **Бағдарламаны жою пәрмені** өрісінде көрсетілген пәрменнің орнына пайдаланады.

      Бұл параметрді қосу ұсынылады.

- **Бағдарлама сәтті жойылған соң қайта іске қосуды орындаңыз**

  Егер бағдарламаны жойғаннан кейін басқарылатын құрылғыда операциялық жүйені қайта іске қосу қажет болса, операциялық жүйе автоматты түрде қайта іске қосылады.

- **Көрсетілген бағдарламаны жаңартуды, патчты немесе өзге бағдарламаны жою**

  Үшінші тарап жаңартуларының, патчтарының және бағдарламаларының тізімі көрсетіледі. Жойғыңыз келетін нысанды таңдаңыз.

  Көрсетілетін тізім, бағдарламалар мен жаңартулардың жалпы тізімі болып табылады және ол басқарылатын құрылғыларда орнатылған бағдарламалар мен жаңартуларға сәйкес келмейді. Нысанды таңдамас бұрын, тапсырманың әрекет ету ауқымында анықталған құрылғыларда бағдарламаның немесе жаңартудың орнатылғанына көз жеткізген жөн. Сипаттар терезесінде бағдарлама немесе жаңарту орнатылған құрылғылардың тізімін көруге болады.

  Құрылғылар тізімін көру үшін:

  a. Бағдарламаның немесе жаңартулардың атын басыңыз.

  Сипаттар терезесі ашылады.

  b. **Құрылғылар** бөлімін ашыңыз.

  Сондай-ақ, құрылғы сипаттары терезесінде орнатылған бағдарламалар мен жаңартулар тізімін көруге болады.

8. Клиент құрылғылары жою утилитасын қалай жүктейтінін көрсетіңіз:

- **Желілік агенттің көмегімен**

  Файлдарды клиент құрылғыларына осы клиент құрылғыларында орнатылған Желілік агент жеткізеді.

  Егер бұл параметр өшірулі болса, файлдар Linux операциялық жүйесі құралдарының көмегімен жеткізіледі.

  Егер тапсырма Желілік агенттер орнатылған құрылғыларға тағайындалса, бұл параметрді қосу ұсынылады.

- **Басқару сервері арқылы операциялық жүйе ресурстарының көмегімен**

  > Параметр ескірген. **Желілік агенттің көмегімен** параметрін немесе осы параметрдің орнына **Тарату нүктелері арқылы операциялық жүйе ресурстарының көмегімен** пайдаланыңыз.

  Файлдар Басқару серверінің операциялық жүйесінің құралдарын пайдаланып клиент құрылғыларына жіберіледі. Бұл параметрді клиент құрылғысында Желілік агент орнатылмаған, бірақ клиент құрылғысы Басқару серверімен бір желіде орналасқан кезде қосуға болады.

- **Тарату нүктелері арқылы операциялық жүйе ресурстарының көмегімен**

  Файлдар тарату нүктелері арқылы операциялық жүйенің құралдарын қолдана отырып, клиент құрылғыларына жіберіледі. Егер желіде кем дегенде бір тарату нүктесі болса, бұл параметрді қосуға болады.

  Желілік агенттің көмегімен параметрі қосылса, онда файлдар, операциялық жүйенің құралдарымен Желілік агент құралдарын пайдалану мүмкін болмаған жағдайда ғана жеткізіледі.

- **Бір уақытта орындалатын жүктеулердің ең көп саны**

  Басқару сервері файлдарды бір уақытта жібере алатын клиент құрылғыларының рұқсат етілген ең көп саны. Бұл сан неғұрлым көп болса, бағдарлама соғұрлым тезірек жойылады, бірақ Басқару серверіне жүктеме артады.

- **Жою әрекеттерінің максималды саны**

  Бағдарламаны қашықтан жою тапсырмасын іске қосу кезінде, бағдарламаны басқарылатын құрылғыдан параметрлерде көрсетілген орнатуды іске қосу саны ішінде жоюға мүмкін болмаса, Kaspersky Security Center Linux бағдарламасы осы басқарылатын құрылғыға жою утилитасын жеткізуді тоқтатады және бұдан былай орнатушыны құрылғыда іске қоспайды.

  Жою әрекеттерінің максималды саны параметрі басқарылатын құрылғы ресурстарын сақтауға, сондай-ақ трафикті азайтуға мүмкіндік береді (жою, MSI файлын іске қосу және қате туралы хабарлар).

  Тапсырманы бірнеше рет іске қосу әрекеттері жоюға кедергі келтіретін құрылғыдағы ақаулықты көрсетуі мүмкін. Әкімші жою әрекеттерінің көрсетілген саны ішінде мәселені шешіп, тапсырманы қайта іске қосуы керек (қолмен немесе кесте бойынша).

  Егер жою орындалмаса, мәселе шешілмейтін болып саналады және кез келген кейінгі іске қосу әрекеттері ресурстар мен трафиктің қажетсіз шығыны тұрғысынан қымбат болып саналады.

  Тапсырма жасалғаннан кейін, орнату әрекеттерінің саны `0`-ге тең болады. Құрылғыдағы қатені қайтаратын әрбір орнатуды іске қосу есептегіштің көрсеткіштерін арттырады.

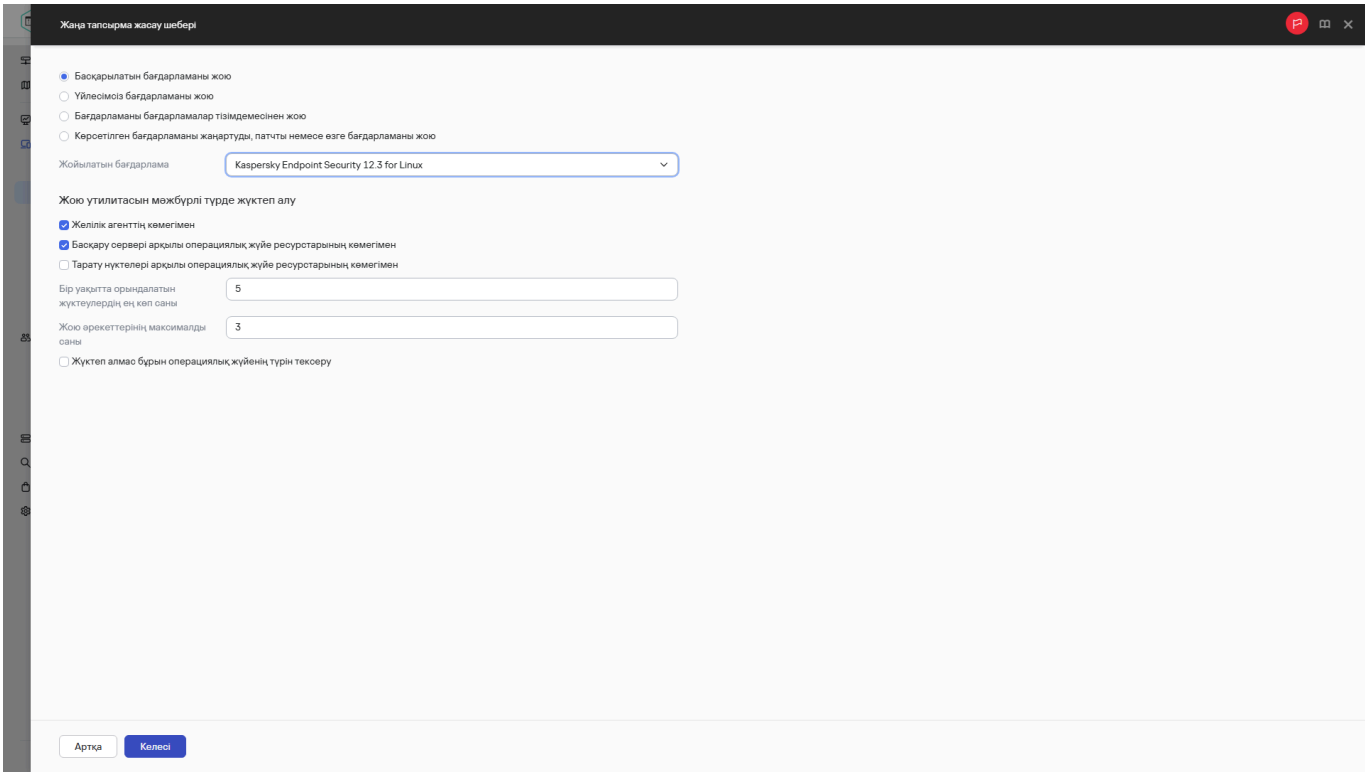
  Егер тапсырма параметрлерінде көрсетілген жою әрекеттерінің саны асып кетсе және құрылғы бағдарламаны жоюға дайын болса, сіз **Жою әрекеттерінің максималды саны** параметрінің мәнін арттырып, бағдарламаны жою тапсырмасын орындай аласыз. Сондай-ақ, басқа *Бағдарламаны қашықтан жою* тапсырмасын жасай аласыз.

- **Жүктеп алмас бұрын операциялық жүйенің түрін тексеру**

  Файлдарды клиент құрылғыларына жібермес бұрын, Kaspersky Security Center Linux бағдарламасы орнату утилитасының параметрлері клиент құрылғысының операциялық жүйесіне қолданылатындығын тексереді. Егер параметрлер қолданылмаса, Kaspersky Security Center Linux бағдарламасы файлдарды жібермейді және бағдарламаны орнатуға тырыспайды. Мысалы, әртүрлі операциялық жүйелері бар құрылғыларды қамтитын басқару тобының құрылғыларынан кейбір бағдарламаларды орнату үшін басқару тобына орнату тапсырмасын тағайындауға болады, содан кейін қажеттіден басқа операциялық жүйесі бар құрылғыларды өткізіп жіберу үшін осы параметрді қосуға болады.

  Желілік агентті тағайындалмаған құрылғыларға қашықтан орнатқан кезде, Kaspersky Security Center Linux немесе тарату нүктесі құрылғының операциялық жүйесінің түрін, **Жүктеп алмас бұрын операциялық жүйенің түрін тексеру** қарамастан, автоматты түрде анықтайды.

Шебердің келесі қадамына өтіңіз.



Тапсырма параметрлерін көрсету

9. Операциялық жүйені қайта іске қосу параметрлерін көрсетіңіз:

- **Құрылғыны қайта іске қоспау**

  Операция аяқталғаннан кейін, клиент құрылғылары автоматты түрде қайта жүктелмейді. Операцияны аяқтау үшін құрылғыны қайта қосу қажет (мысалы, қолмен немесе құрылғыны басқару тапсырмасы арқылы). Қайта жүктеу қажеттілігі туралы ақпарат тапсырманы орындау нәтижелерінде және құрылғы күйінде сақталады. Бұл нұсқа, үздіксіз жұмыс өте маңызды болып саналатын серверлердегі және басқа құрылғылардағы тапсырмалар үшін жарамды.

- **Құрылғыны қайта іске қосу**

  Бұл жағдайда, операцияны аяқтау үшін қайта жүктеу қажет болса, қайта жүктеу әрқашан автоматты түрде орындалады. Бұл нұсқа, мезгіл-мезгіл үзілістерге (өшіру, қайта жүктеу) рұқсат етілген құрылғылардағы тапсырмалар үшін жарамды.

- **Пайдаланушыдан әрекетті орындауды сұрау**

  Клиент құрылғысының экранында құрылғыны қолмен қайта жүктеу керек деген хабар пайда болады. Бұл нұсқа үшін қосымша параметрлерді конфигурациялауға болады: пайдаланушыға арналған хабар мәтіні, хабардың жиілігі, сондай-ақ қайта жүктеу мәжбүрлі түрде орындалатын уақыт (пайдаланушының растауынсыз). Бұл нұсқа жұмыс станциялары үшін оңтайлы болып табылады, сондықтан пайдаланушылар қайта жүктеудің ең қолайлы уақытын таңдай алады.

  Әдепкі бойынша, осы нұсқа таңдалған.

  - **Сұрауды қайталау жиілігі (мин)**

  - **Келесі уақыттан кейін қайта іске қосу (мин)**

- **Бұғатталған сеанстардағы бағдарламалардың мәжбүрлі жабылуы**

  Іске қосылған қолданбалар клиент құрылғысын қайта жүктеуге мүмкіндік бермеуі мүмкін. Мысалы, егер мәтіндік редакторда құжатпен жұмыс жасалса және өзгертулер сақталмаса, бағдарлама құрылғыны қайта жүктеуге мүмкіндік бермейді.

  Егер бұл параметр қосулы болса, құрылғыны қайта іске қоспас бұрын бұғатталған құрылғылардағы мұндай бағдарламалар мәжбүрлі түрде жабылады. Нәтижесінде, пайдаланушылар сақталмаған жұмысын жоғалтуы мүмкін.

  Егер бұл параметр өшірулі болса, бұғатталған құрылғы қайта жүктелмейді. Бұл құрылғыдағы тапсырманың күйі құрылғыны қайта іске қосу қажеттілігін көрсетеді. Пайдаланушылар бұғатталған құрылғыларда жұмыс істейтін барлық бағдарламаларды қолмен жауып, сол құрылғыларды қайта іске қосуы керек.

  Әдепкі бойынша, параметр өшірулі.

Шебердің келесі қадамына өтіңіз.

10. Қажет болса, қашықтан жою тапсырмасын орындау үшін пайдаланылатын есептік жазбаларды қосыңыз:

    - **Есептік жазба қажет емес (Желілік агент орнатылды)**

      Егер бұл нұсқа таңдалса, бағдарлама инсталляторын іске қосуға негіз болып саналатын есептік жазбаны көрсетудің қажеті жоқ. Тапсырма, Басқару сервері қызметі жұмыс істейтін есептік жазба астында іске қосылады.

      Желілік агент клиент құрылғыларында орнатылмаған болса, бұл нұсқа қолжетімді емес.

    - **Есептік жазба қажет (Желілік агент пайдаланылмайды)**

      Егер сіз *Бағдарламаны қашықтан жою* тапсырмасын тағайындайтын құрылғыларда Желілік агент орнатылмаған болса, осы нұсқаны таңдаңыз. Бұл жағдайда қолданбаны орнату үшін пайдаланушы есептік жазбасын немесе SSH сертификатын көрсетуге болады.

      - **Жергілікті немесе домен есептік жазбасы**. Егер бұл нұсқа таңдалса, бағдарлама инсталляторын іске қосуға негіз болатын есептік жазбаны көрсетіңіз. **Қосу** түймесін басыңыз, **Жергілікті немесе домен есептік жазбасы** опциясын таңдаңыз және пайдаланушының есептік жазбасының деректерін көрсетіңіз.

        Тапсырма тағайындалған барлық құрылғыларда олардың ешқайсысы қажетті құқықтарға ие болмаса, бірнеше есептік жазбаны көрсетуге болады. Бұл жағдайда, тапсырманы іске қосу үшін барлық қосылған есептік жазбалар бірізді түрде, жоғарыдан төменге қарай қолданылады.

      - **SSH сертификаты**. Қолданбаны Linux басқаратын клиент құрылғысына орнатқыңыз келсе, пайдаланушы есептік жазбасының орнына SSH сертификатын көрсетуге болады. **Қосу** түймесін басыңыз, **SSH сертификаты** опциясын таңдаңыз және сертификаттың жеке және ашық кілттерін көрсетіңіз.

        Жеке кілт жасау үшін ssh-keygen утилитасын пайдалануға болады. Kaspersky Security Center Linux жеке кілттердің PEM форматына қолдау көрсететінін ескеріңіз, бірақ ssh-keygen утилитасы SSH кілттерін әдепкісінше OPENSSH форматында жасайды. OPENSSH форматына Kaspersky Security Center Linux қолдау көрсетпейді. PEM қолдау көрсетілетін пішімінде жабық кілт жасау үшін -m PEM параметрін ssh-keygen пәрменіне қосыңыз.

        Мысалы:

        ```
        ssh-keygen -m PEM -t rsa -b 4096 -C "<пайдаланушының электрондық поштасы>"
        ```

11. **Тапсырманы жасауды аяқтау** қадамында **Жасап болған соң, тапсырма туралы мәліметтерді ашу** параметрін қоссаңыз, тапсырма параметрлерінің орнатылған әдепкі мәндерін өзгертуге болады.

    Егер сіз бұл параметрді қоспасаңыз, тапсырма әдепкі бойынша белгіленген параметр мәндерімен жасалады. Орнатылған әдепкі параметрлер мәндерін кейінірек өзгертуге болады.

12. **Аяқтау** түймесін басыңыз.

    Шебер жұмысының нәтижесінде тапсырма жасалды. **Жасап болған соң, тапсырма туралы мәліметтерді ашу** параметрі қосулы болса, тапсырма параметрлерінің терезесі автоматты түрде ашылады. Бұл терезеде тапсырманың жалпы параметрлерін көрсетуге және қажет болса, тапсырма жасағаннан кейін көрсетілген параметрлерді өзгертуге болады.

    > Тапсырмалар тізіміндегі жасалған тапсырма атауын басу арқылы тапсырма сипаттарының терезесін ашуға да болады.

    Тапсырма жасалады, теңшеледі және тапсырмалар тізімінде, **Тапсырмалар** бөлімінде көрсетіледі.

13. Тапсырманы іске қосу үшін тапсырмалар тізімінен тапсырманы таңдап, **Іске қосу** түймесін басыңыз.

    Сондай-ақ тапсырма сипаттары терезесіндегі **Кесте** қойындысында тапсырманы іске қосу кестесін жасауға да болады.

    Кесте бойынша іске қосу параметрлерінің толық сипаттамасын тапсырманың жалпы параметрлерінен қараңыз.

Тапсырма аяқталғаннан кейін, таңдалған бағдарлама таңдалған құрылғыларда жойылады.

Қашықтан жою мәселелері

Үшінші тарап қолданбаларын қашықтан жойған кезде, кейде "Қашықтан жою осы құрылғыда ескертулермен аяқталды: жойылатын қолданба орнатылмаған" деген ескертумен аяқталуы мүмкін. Бұл мәселе жойылатын қолданба әлдеқашан жойылған немесе тек жеке пайдаланушы үшін орнатылған кезде орын алады. Жеке пайдаланушы үшін орнатылған қолданбалар (бір пайдаланушыға арналған қолданбалар деп те аталады) көрінбейтін болады және пайдаланушы жүйеге кірмеген жағдайда, оларды қашықтан жою мүмкін болмайды.

Бұл әрекет бір құрылғыда бірнеше пайдаланушының қолданысына арналған қолданбалардан (бір құрылғыға арналған қолданбалар ретінде де белгілі) өзгеше. Бір құрылғыға арналған қолданбаларды құрылғының барлық пайдаланушысы көріп, пайдалана алады.

Сондықтан бір пайдаланушыға арналған қолданбаларды пайдаланушы жүйеге кірген кезде ғана жою керек.

Орнатылған қолданбалар туралы ақпарат көзі

Желілік агент Windows құрылғыларына орнатылған бағдарламалық жасақтама туралы ақпаратты келесі тіркеу кілттерінен алады:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall

  Барлық пайдаланушы үшін орнатылған қолданбалар туралы ақпаратты қамтиды.

- HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall

  Барлық пайдаланушы үшін орнатылған қолданбалар туралы ақпаратты қамтиды.

- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Uninstall

  Ағымдағы пайдаланушы үшін орнатылған қолданбалар туралы ақпаратты қамтиды.

- HKEY_USER<...>\Software\Microsoft\Windows\CurrentVersion\Uninstall

  Нақты пайдаланушылар үшін орнатылған қолданбалар туралы ақпаратты қамтиды.

Windows басқаратын құрылғыны қашықтан орнатуға дайындау

Клиент құрылғысына бағдарламаны қашықтан орнату келесі себептерге байланысты қатемен аяқталуы мүмкін:

- Тапсырма бұған дейін осы құрылғыда сәтті орындалды.

  Бұл жағдайда, оны қайта орындау қажет емес.

- Тапсырманы іске қосу кезінде құрылғы өшірілді.

  Бұл жағдайда, құрылғыны қосып, тапсырманы қайтадан іске қосу қажет.

- Клиент құрылғысында орнатылған Басқару сервері мен Желілік агент арасында байланыс жоқ.

  Мәселенің себебін анықтау үшін клиент құрылғысын қашықтан диагностикалау утилитасын (klactgui) пайдалануыңызға болады.

- Құрылғыда желілік агент орнатылмаған болса, қашықтан орнату кезінде келесі мәселелер туындауы мүмкін:

  - Клиент құрылғысында **Файлдарға қарапайым жалпы қатынасты өшіру** опциясы қосылған.
  - Клиент құрылғысында Server қызметі жұмыс істемейді.
  - Клиент құрылғысында қажетті порттар жабық.
  - Тапсырма орындалып жатқан есептік жазбаның құқықтары жеткіліксіз.

  Желілік агент орнатылмаған клиент құрылғысына қолданбаны орнату кезінде туындауы мүмкін мәселелерге жол бермеу үшін Kaspersky Security Center Linux қашықтан орнату тапсырмасымен мәжбүрлі түрде орналастыру процедурасында сипатталғандай әрекет етуіңіз керек.

Бұрын riprep утилитасы құрылғыны қашықтан орнатуға дайындау үшін пайдаланылды. Бұл енді операциялық жүйелерді реттеудің ескірген әдісі болып саналады. Riprep утилитасын Windows XP және Windows Server 2003 R2 нұсқасынан жаңа операциялық жүйелерде пайдалану ұсынылмайды.

Скрипттерді қашықтан орындау тапсырмасын жасау

Клиенттік құрылғыда орнату пакетін орындау және қолданбаны қашықтан орнату үшін *Скрипттерді қашықтан орындау* тапсырмасын жасауға болады.

Орнату пакетінде клиент құрылғыларында орындауға арналған скрипттер жинағы бар ZIP мұрағаты, сондай-ақ manifest.json файлы бар. Орнату пакетінің осы түрін жасау туралы қосымша ақпарат алу үшін мақаланы қараңыз.

Бұл тапсырма тек Linux үшін Желілік агенті бар құрылғыларда іске қосылуы керек.

Скрипттерді қашықтан орындау тапсырмасын іске қосу үшін:

1. **Жаңа тапсырма жасау шебері** өтіңіз және **Скрипттерді қашықтан орындау** тапсырма түрін таңдаңыз.
2. Тапсырманың атауын енгізіп, тапсырма тағайындалатын құрылғыларды таңдаңыз. **Келесі** түймесін басыңыз.
3. Қашықтан орындау үшін manifest.json файлы бар ZIP мұрағатына негізделген орнату пакетін таңдаңыз.

   Тапсырманы ол бұрыннан іске қосылған құрылғыларда қайта іске қосқыңыз келмесе, **Бұл тапсырманы ол ақталып қойған құрылғыларда бастамаңыз** параметрін қосыңыз.
4. Тапсырманы іске қосу үшін есептік жазбаны таңдаңыз.

   Әдепкі есептік жазбаны таңдасаңыз, тапсырманы Желілік агент (root есептік жазбасы) орындайды.

   Скрипттерді қашықтан орындау тапсырмасын іске қосқанда, тапсырмаға тағайындалған есептік жазбаны өзгерте алмайсыз. Тапсырма тағайындалған есептік жазбаны өзгерту үшін тапсырма параметрлерінде тапсырманы тоқтатып, қажетті есептік жазбамен тапсырманы қайта жасаңыз.
5. **Жасап болған соң, тапсырма туралы мәліметтерді ашу** бетінде **Тапсырманы жасауды аяқтау** параметрін қоссаңыз, әдепкі бойынша белгіленген тапсырма параметрлері мәндерін өзгерте аласыз. Егер сіз бұл параметрді қоспасаңыз, тапсырма әдепкі бойынша белгіленген параметр мәндерімен жасалады. Әдепкі бойынша параметр мәндерін кейінірек кез келген уақытта өзгертуге болады.
6. **Аяқтау** түймесін басыңыз.

   Скрипттерді қашықтан орындау тапсырмасы жасалды және тапсырмалар тізімінде көрсетіледі.

Скрипттерді қашықтан орындау тапсырмасынан деректерді алғаннан кейін, Желілік агент тапсырма параметрлерінде көрсетілген әкімші мен пайдаланушыдан басқа барлық пайдаланушылар үшін алынған деректерге кіруді шектейді.

Манифест-файлы негізінде орнату пакетін жасау

Манифест-файлы негізінде орнату пакетін жасау үшін:

1. Бағдарламаның негізгі терезесінде **Бағдарламалық жасақтаманы басқару → Орнату пакеттері** бөліміне өтіңіз.

   Басқару серверінде қолжетімді орнату пакеттерінің тізімі көрсетіледі.
2. **Қосу** түймесін басыңыз.

   Орнату пакетін жасау шебері іске қосылады. Шебердің жұмысын жалғастыру үшін **Келесі** түймесін басыңыз.

3. **manifest.json файлы бар ZIP мұрағаты бойынша сценарийлерді қашықтан орындау тапсырмасы үшін орнату пакетін жасаңыз** параметрін таңдаңыз.

4. Пакет атауын көрсетіңіз және **Шолу** түймесін басыңыз.

   Ашылған терезеде орнату пакетін жасау үшін файлды таңдаңыз.

5. Қолжетімді дискілерде орналасқан мұрағаттық файлды таңдаңыз. Бұл тапсырма үшін мұрағатты қалай дайындау керектігі туралы ақпаратты мақаланы қараңыз.

   Файл Kaspersky Security Center Linux Басқару серверіне жүктеле бастайды.

   Орнату пакетін жасау процесі басталады.

   Шебер терезесінде процестің аяқталуы туралы ақпарат көрсетіледі.

   Егер орнату пакеті жасалмаса, тиісті хабарландыру көрсетіледі.

6. Шебер терезесін жабу үшін **Аяқтау** түймесін басыңыз.

Жасалған орнату пакеті Басқару серверінің ортақ қатынасы бар қалтасының Packages салынған қалтасына жүктеледі. Жүктелгеннен кейін, орнату пакеті орнату пакеттерінің тізімінде пайда болады.

Басқару серверінде қолжетімді орнату пакеттері тізімінде, орнату пакетінің атын басу арқылы, келесі әрекеттерді орындай аласыз:

- Орнату пакетінің келесі сипаттарын қарап шыға аласыз:
  - **Атауы.** Орнату пакетінің атауы.
  - **Көзі.** Бағдарлама өндірушісінің атауы.
  - **Нұсқа.** Бағдарлама нұсқасы.
  - **Жасалған күні.** Орнату пакетін жасау күні.
  - **Өзгертілген.** Орнату пакетін өзгерту күні.
  - **Жолы.** Басқару серверіндегі пайдаланушы орнату пакетіне апаратын жол.
- Пакеттің атын және пәрмен жолының параметрлерін өзгертіңіз. Бұл функция тек Kaspersky қолданбалары негізінде жасалмаған пакеттер үшін қолжетімді.

Скрипттерді қашықтан орындау тапсырмасы үшін мұрағатты дайындау

manifest.json файлына негізделген *Скрипттерді қашықтан орындау* тапсырмасына арналған мұрағат келесі талаптарға сай болуы керек:

- Мұрағат пішімі: ZIP.
- Жалпы көлемі: 1 ГБ аспайды.
- Мұрағаттағы файлдар мен қалталардың саны шектелмейді.

- Мұрағаттық манифест файлы төмендегі схемаға сәйкес болуы және manifest.json деп аталуы керек. Схема құрылғыда тапсырма орындалып жатқанда ғана тексеріледі.

  Манифест файлының JSON схемасы және массивтердің сипаттамасы

  JSON схемасы

```
{
 "$schema": "http://json-schema.org/draft-07/schema#",
  "title": "Schema for execute scripts task",
   "type": "object",
    "properties": {
        "version": {
            "type": "integer",
            "enum": [1]
        },
        "actions":{
            "type": "array",
            "items": {
                "type": "object",
                "properties": {
                    "type": {
                        "type": "string",
                        "enum": ["execute"]
                    },
                    "path": {
                        "type": "string"
                    },
                    "args": {
                        "type": "string"
                    },
                    "results":{
                        "type": "array",
                        "items": {
                            "type": "object",
                            "properties": {
                                "code": {
                                    "type": "integer",
                                    "minimum": -255,
                                    "maximum": 255
                                },
                                "next":{
                                    "type": "string",
                                    "enum": ["break", "continue"]
                                }
                            },
                            "required": [
                                "code",
                                "next"
                            ]
                        }
                    },
                    "default_next":{
                        "type": "string",
```

```
                        "enum": ["break", "continue"]
                    }
                },
                "required": [
                    "type",
                    "path",
                    "default_next"
                ]
            }
        }
    },
    "required": [
        "version",
        "actions"
    ]
}
```

Манифест файлының мысалы

```
{
  "version": 1,
  "actions": [
    {
      "type": "execute",
      "path": "scripts/run1.cmd",
      "args": "testArg",
      "results": [
        {
          "code": 0,
          "next": "continue"
        }
      ],
      "default_next": "break"
    },
    {
      "type": "execute",
      "path": "scripts/run2.cmd",
      "results": [
        {
          "code": 0,
          "next": "continue"
        }
      ],
      "default_next": "break"
    },
    {
      "type": "execute",
      "path": "scripts/run3.cmd",
      "results": [
        {
          "code": 0,
          "next": "continue"
        }
      ],
      "default_next": "break"
    }
  ]
}
```

- Мұрағат келесі құрылымға ие болуы керек:

  `manifest.json`

  `<file1>`

  `<file2>`

  `<folder1>/<file3>`

  `<folder2>/<folder3>/<file4>`

  `...`

  `<fileX>`

  manifest.json – тапсырма манифест файлы.

  `<file1>, ...., <fileX>` – орындалуы қажет скрипттері бар файлдар жинағы.

Скрипттерді қашықтан орындау тапсырмасын пайдаланып құрылғыларға қолданбаларды қашықтан орнату

Скрипттерді қашықтан орындау тапсырмасы пайдаланушы орнату пакетін жасау арқылы клиент құрылғысында қолданбаны қашықтан орнату үшін пайдаланылуы мүмкін.

Бұл тапсырма үшін мұрағатты қалай дайындау керектігі туралы ақпаратты мақаланы қараңыз.

Клиент құрылғысында қолданбаны қашықтан орнату үшін орнату пакетін жасау үшін келесі файлдар осы тапсырма үшін жүктеп алғыңыз келетін мұрағатта болуы керек:

- `<package name>.deb`
- **install.sh**

  `sudo apt-get install <пакет атауы>.deb`

- **manifest.json**

  Қашықтағы қолданбаны орнатуға арналған JSON схемасы

```
{
  "version": 1,
  "actions": [
    {
      "type": "execute",
      "path": "install.sh",
      "args": "<қажет болса, аргументтерді енгізіңіз>",
      "results": [
        {
          "code": 0,
          "next": "continue"
        }
      ],
      "default_next": "break"
    }
```

```
  ]
}
```

Массивтердің сипаттамасы

1. `version` – манифест пен тапсырма файлының нұсқасы.

   Қазіргі уақытта жалғыз рұқсат етілетін мән – 1.

2. `actions` массивінің элементтері тапсырмадағы скрипттердің құрамы мен орындалу ретін анықтайды.

   Скрипттің орындалу реті массивтегі элементтің индексіне (жайғасымына) сәйкес келеді.

3. `actions` массивінің әрбір элементі үшін келесі элементтер анықталады.

   a. `type` – скрипттерден орындалатын пәрмен түрі. Қазіргі уақытта мән әрқашан `execute`.

   b. `path` – мұрағаттағы скрипт файлына апаратын жол.

   c. `args` – орындалатын пәрменнің бөлігі ретінде скриптке жіберілетін аргументтер.

   d. `results` – тапсырманың нәтижесіне байланысты келесі әрекеттерді анықтайтын массив.

      1. `code` – скриптті қайтаратын мән.

      2. `next` – келесі орындалатын әрекет. `continue` әрекеті келесі скриптіні орындауға жалғасады (`actions` массивіндегі элемент); `break` әрекеті тапсырманы тоқтатады.

   e. `default_next` – скрипт `results`-та жоқ мәнді қайтарса, орын алатын әрекет.

Скрипттерді қашықтан орындау тапсырмасын іске қосқан кезде, Желілік агент клиент құрылғысына қолданбамен бірге орнату пакетін жүктеп алады. Клиент құрылғысы орнату пакетін алған кезде, осы құрылғыдағы Желілік агент manifest.json файлын талдайды және нәтижеге байланысты сценарийлер мен әрекеттердің орындалу ретін анықтайды, содан кейін орындауды бастайды.

Скрипттерді қашықтан орындау тапсырмасы аяқталғаннан кейін қолданба клиент құрылғысына орнатылады.

Скрипттерді қашықтан орындау тапсырмасы үшін хабарландыруларды конфигурациялау және бақылау

Скрипттерді қашықтан орындау тапсырмасы үшін оқиғаны сақтау кезіндегі бақылауды, жүріс-тұрысты және хабарландыруларды конфигурациялауға болады.

Скрипттерді қашықтан орындау тапсырмасының күйін көру үшін:

1. Бағдарламаның негізгі терезесінде **Тапсырмалар** бөліміне өтіңіз.

   Тапсырмалар тізімі көрсетіледі.

2. Тапсырманы таңдап, **Құрылғыдағы әрекеттер журналы** түймесін басыңыз.

   Тапсырманың орындалу барысы көрсетіледі.

Оқиғаны сақтау кезіндегі жүріс-тұрысты конфигурациялау үшін:

1. Тапсырмалар тізімінде тапсырма атын басып, **Параметрлер** қойындысына өтіңіз.
2. **Хабарландырулар** бөлімінде **Параметрлер** түймесін басыңыз.
3. Тапсырманы орындағаннан кейін, қолданба жүріс-тұрысының келесі нұсқаларының бірін таңдаңыз:
   - **Барлық оқиғаларды сақтау**.
   - **Тапсырманы орындау барысына қатысты оқиғаларды сақтау**.
   - **Тек тапсырманы орындау нәтижелерін сақтау**.
     Оқиғалар **Құрылғыдағы әрекеттер журналы** және **Оқиғалар қоймасы** бөлімдерінде сақталады.
     Әдепкі бойынша тапсырманың нәтижелері ғана сақталады.

     > **Барлық оқиғаларды сақтау** тармағын таңдасаңыз, тапсырманың нәтижелері ғана сақталады.
4. Оқиғаларды Басқару сервері дерекқорында, Басқару серверіндегі оқиғалар журналында немесе құрылғыда сақтағыңыз келсе, сәйкес параметрді қосыңыз.

Хабарландыруларды реттеу туралы қосымша ақпарат алу үшін осы мақаланы қараңыз.

Бағдарламаны лицензиялау

Бұл бөлімде келесі ақпарат бар:

- Kaspersky Security Center Linux лицензиясына қатысты жалпы түсініктер.
- Kaspersky басқарылатын қолданбаларына арналған лицензияларды басқару нұсқаулары.

Kaspersky Security Center Linux лицензиясы

Бұл бөлімде Kaspersky Security Center Linux лицензиялаумен байланысты негізгі түсініктер туралы ақпарат бар.

Лицензиялық келісім туралы

Лицензиялық келісім – бағдарламаны қандай шарттарда пайдалана алатыныңыз көрсетілген, сіз бен АО "Лаборатория Касперского" арасында жасалған заңды келісім.

Бағдарламамен жұмыс жасамас бұрын, Лицензиялық келісімнің шарттарын мұқият оқып шығыңыз.

Kaspersky Security Center Linux және оның құрамдастары, мысалы, Желілік агент, өздерінің Лицензиялық келісімдеріне ие.

Сіз Kaspersky Security Center Linux үшін Лицензиялық келісімнің шарттарымен келесі тәсілдер арқылы таныса аласыз:

- Kaspersky Security Center орнату кезінде.
- Kaspersky Security Center жеткізу жиынтығына қосылған license.txt құжатын оқығаннан кейін.
- Kaspersky Security Center орнату қалтасындағы license.txt құжатын оқығаннан кейін.
- Kaspersky сайтынан license.txt файлын жүктеп алу арқылы.

Сіз Linux үшін Желілік агентке арналған Лицензиялық келісімнің шарттарымен келесі тәсілдер арқылы таныса аласыз:

- Желілік агенттің дистрибутивін Kaspersky веб-серверлерінен жүктеу кезінде.
- Linux үшін Желілік агентті орнату кезінде.
- Linux үшін Желілік агентті жеткізу жиынтығына кіретін license.txt құжатын оқу арқылы.
- Linux үшін Желілік агентті орнату қалтасындағы license.txt құжатын оқу арқылы.
- Kaspersky сайтынан license.txt файлын жүктеп алу арқылы.

Сіз бағдарламаны орнату кезінде Лицензиялық келісімнің мәтінімен келіскеніңізді растай отырып, Лицензиялық келісімнің шарттарын қабылдайсыз. Егер сіз Лицензиялық келісімнің шарттарымен келіспесеңіз, бағдарламаны орнатуды тоқтатып, бағдарламаны пайдаланбауыңыз керек.

Лицензия туралы

Лицензия – бұл Лицензиялық келісім негізінде сізге берілген Kaspersky Security Center Linux бағдарламаны пайдалану үшін уақыт бойынша шектелген құқық.

Көрсетілетін қызметтердің көлемі және бағдарламаны пайдалану мерзімі бағдарлама қолданылатын лицензияға байланысты.

Лицензиялардың келесі түрлері қарастырылған:

- *Сынақ*.

  Бағдарламамен танысуға арналған тегін лицензия. Сынақ лицензиясының жарамдылық мерзімі қысқа.

  Сынақ лицензиясының мерзімі аяқталғаннан кейін, Kaspersky Security Center Linux бағдарламасы өзінің барлық функцияларын орындауды тоқтатады. Бағдарламаны пайдалануды жалғастыру үшін сізге коммерциялық лицензия сатып алу қажет.

  Бағдарламаны сынақ лицензиясы бойынша тек бір сынақ мерзімінде пайдалануға болады.

- *Коммерциялық*.

  Ақылы лицензия.

  Коммерциялық лицензияның қолданылу мерзімі аяқталғаннан кейін, бағдарлама өзінің негізгі функцияларын орындауды тоқтатады. Kaspersky Security Center бағдарламасын пайдалануды жалғастыру үшін коммерциялық лицензияның жарамдылық мерзімін ұзарту қажет. Коммерциялық лицензияның мерзімі аяқталғаннан кейін, бағдарламаны енді пайдалана алмайсыз және оны құрылғыңыздан жоюыңыз керек.

  Компьютерлік қауіпсіздік қатерлерінен үздіксіз қорғауды қамтамасыз ету үшін лицензияның жарамдылық мерзімін оның аяқталу күнінен кешіктірмей ұзарту ұсынылады.

Лицензиялық сертификат туралы

Лицензиялық сертификат – бұл кілт файлы немесе белсендіру кодымен бірге сізге берілетін құжат.

Лицензиялық сертификатта, ұсынылатын лицензия туралы келесі ақпарат бар:

- Лицензия идентификаторы немесе тапсырыс нөмірі
- Лицензия берілетін пайдаланушы туралы ақпарат
- Берілетін лицензия бойынша белсендіруге болатын бағдарлама туралы ақпарат
- Лицензиялау бірліктерінің санына қойылатын шектеу (мысалы, берілетін лицензия бойынша бағдарламаны пайдалануға болатын құрылғылар)
- Лицензияның қолданылу мерзімі басталған күн

- Лицензияның жарамдылық мерзімінің аяқталу күні немесе лицензияның қолданылу мерзімі
- Лицензия түрі

Лицензиялық кілт туралы

Лицензиялық кілт – Лицензиялық келісім шарттарына сәйкес бағдарламаны белсендіріп, пайдалануға мүмкіндік беретін биттер тізбегі. Лицензиялық кілтті Kaspersky мамандары жасайды.

Бағдарламаға лицензиялық кілтті келесі тәсілдердің бірімен қосуға болады: *кілт файлын* қолдану немесе *белсендіру кодын* енгізу. Лицензиялық кілт бағдарламаның интерфейсінде, оны бағдарламаға қосқаннан кейінгі бірегей әріптік-цифрлық реттілік түрінде көрсетіледі.

Лицензиялық келісімнің шарттары бұзылған жағдайда, лицензиялық кілтті Kaspersky бұғаттауы мүмкін. Егер лицензиялық кілт бұғатталған болса, бағдарлама жұмыс істеуі үшін басқа лицензиялық кілтті қосу қажет.

Лицензиялық кілт белсенді және қосымша (резервтік) болуы мүмкін.

Белсенді лицензиялық кілт – ағымдағы сәтте бағдарламаның жұмыс істеуі үшін қолданылатын лицензиялық кілт. Белсенді кілт ретінде, сынақ немесе коммерциялық лицензия үшін лицензиялық кілтті қосуға болады. Бағдарламада бірден артық белсенді лицензиялық кілт болуы мүмкін емес.

Қосымша (резервттегі) лицензиялық кілт – бағдарламаны қолдану құқығын растайтын, бірақ ағымдағы сәтте қолданылмайтын лицензиялық кілт. Ағымдағы белсенді лицензиялық кілтпен байланысты лицензияның мерзімі аяқталғалы жатқан кезде қосымша лицензиялық кілт автоматты түрде белсенді болады. Қосымша лицензиялық кілтті тек белсенді лицензиялық кілт болған жағдайда ғана қосуға болады.

Сынақ лицензиясының лицензиялық кілті тек белсенді лицензиялық кілт ретінде қосылуы мүмкін. Сынақ лицензиясының лицензиялық кілтін қосымша лицензиялық кілт ретінде қосу мүмкін емес.

Құпиялылық саясатын қарау

Құпиялық саясаты интернетте https://www.kaspersky.ru/products-and-services-privacy-policy бетінде қолжетімді.

Құпиялық саясаты автономды режимде де қолжетімді:

- Kaspersky Security Center Linux жүйесін орнатпас бұрын Құпиялылық саясатын оқуға болады.
- Құпиялық саясатының мәтіні Kaspersky Security Center Linux орнату қалтасындағы license.txt файлында орналасқан.
- privacy_policy.txt файлы Желілік агент қалтасындағы басқарылатын құрылғыда қолжетімді.
- privacy_policy.txt файлын Желілік агент дистрибутивінан шығаруға болады.

Kaspersky Security Center лицензиялау нұсқалары

Kaspersky Security Center келесі режимдерде жұмыс істей алады:

- **Басқару консолінің негізгі функциясы**

  Kaspersky Security Center, бағдарлама іске қосылғанша немесе коммерциялық лицензияның қолданылу мерзімі аяқталғанға дейін осы режимде жұмыс істейді. Басқару консолінің негізгі функциясын қолдайтын Kaspersky Security Center бағдарламасы ұйымның желісін қорғауға арналған Kaspersky бағдарламаларының құрамында жеткізіледі. Бұдан бөлек, ол Kaspersky веб-сайтынан жүктеу үшін қолжетімді.

- **Коммерциялық лицензия**

  Басқару консолінің базалық функционалдылығына кірмейтін қосымша функционалдылық қажет болса, коммерциялық лицензияны сатып алу қажет.

  Басқару сервері сипаттары терезесіне лицензиялық кілт қосқанда, Kaspersky Security Center Linux пайдалануға мүмкіндік беретін лицензиялық кілтті қосқаныңызға көз жеткізіңіз. Сіз бұл ақпаратты Kaspersky сайтынан таба аласыз. Әрбір шешім бетінде осы шешімге енгізілген бағдарламалардың тізімі бар. Басқару сервері Kaspersky Endpoint Security Cloud лицензия кілті сияқты қолдау көрсетілмейтін лицензия кілттерін қабылдай алады, бірақ мұндай лицензия кілттері Басқару консолінің базалық функционалдылығынан басқа ешқандай жаңа мүмкіндіктерді ұсынбайды.

Функция немесе сипат	Kaspersky Security Center Linux жұмыс режимі	
	Лицензия жоқ	Коммерциялық лицензия
Басқару консолінің негізгі функциясы Келесі функциялар қолжетімді: • Қашықтағы кеңселер немесе ұйым-клиенттер желісін басқару үшін виртуалды Басқару серверлерін құру. • Құрылғылар жиынтығын тұтастай басқару үшін басқару топтарының иерархиясын құру. • Бағдарламаларды қашықтан орнату. • Клиент құрылғыларында орнатылған бағдарлама параметрлерін орталықтандырылған конфигурациялау. • Ұйымның антивирустық қауіпсіздігінің күйін бақылау. • Пайдаланушы рөлдерін басқару. • Бағдарламалардың статистикасы мен есептерін, сондай-ақ критикалық оқиғалар туралы хабарландыруларды алу. • Карантинге немесе сақтық көшірмелеуге орналастырылған файлдармен, сондай-ақ өңделуі кейінге қалдырылған файлдармен орталықтандырылған жұмыс. • Деректерді шифрлау және қорғау процесін басқару. • Желі сауалнамасы нәтижесінде табылған жабдықтар тізімін қолмен қарау және өңдеу. • Қашықтан орнатуға болатын операциялық жүйе кескіндерінің тізімін қарау.	✓	✓

Функция немесе сипат	Kaspersky Security Center Linux жұмыс режимі	
	Лицензия жоқ	Коммерциялық лицензия
Осалдықтар мен патчтарды басқару: базалық функционалдылық Келесі тапсырмалар коммерциялық лицензияны қажет етпейді: • *Осалдықтарды және қажетті жаңартуларды іздеу* тапсырмасы Осы тапсырмасының көмегімен Kaspersky Security Center Linux қолданбасы басқарылатын құрылғыларға орнатылған үшінші тарап бағдарламалары үшін табылған осалдықтар мен қажетті жаңартулар тізімдерін алады. • *Осалдықтарды түзету* тапсырмасы *Осалдықтарды түзету* тапсырмасы үшінші тарап бағдарламалары үшін ұсынылған Microsoft бағдарламаларының түзетулері мен пайдаланушылық түзетулерді пайдаланады. Бұл тапсырманы пайдалану мақсатында, тапсырма параметрлерінде осалдықтарды түзету үшін пайдаланушылық түзетулерді қолмен көрсету қажет.	✓	✓
Осалдықтар мен патчтарды басқару: қосымша функционалдылық Бағдарламалық жасақтама жаңартуларын автоматты түрде қашықтан белгілеу және осалдықтарды автоматты түзету ережелерін анықтауға болады.	—	✓
Жүйелерді басқару Келесі функциялар қолжетімді: • Microsoft Windows "Қашықтағы жұмыс үстеліне қосылу орындалуда" құрамдасы арқылы клиент құрылғыларына қосылуға қашықтан рұқсат беру. • Windows компьютерлік бөлісу қызметі арқылы клиент құрылғыларына қашықтан қосылу.	—	✓
Оқиғаларды SIEM жүйелеріне экспорттау: Syslog протоколы арқылы Syslog протоколы бойынша Kaspersky Security Center Басқару серверінде және басқарылатын құрылғыларды орнатылған Kaspersky бағдарламаларында орын алған кез келген оқиғаларды жіберуге болады. Syslog протоколы – хабарларды тіркеудің стандартты протоколы. Сіз осы протоколды оқиғаларды кез келген SIEM жүйесіне экспорттау үшін қолдана аласыз.	✓	✓
Дабылдарды біріктіру және Active directory, KASAP және Kaspersky TIP Sandbox арқылы жауап әрекеттерін орындау	—	✓

Кілт файлы туралы

Кілт файлы – Kaspersky сізге ұсынатын key кеңейтімі бар файл. Кілт файлы бағдарламаны белсендіретін лицензиялық кілтті қосуға арналған.

Сіз Kaspersky Security Center бағдарламасын сатып алғаннан немесе Kaspersky Security Center сынақ нұсқасына тапсырыс бергеннен кейін, өзіңіз көрсеткен электрондық пошта мекенжайы бойынша кілт файлын аласыз.

Бағдарламаны кілт файлы арқылы белсендіру үшін Kaspersky белсендіру серверлеріне қосылудың қажет емес.

Егер кілт файлы кездейсоқ жойылса, оны қалпына келтіруге болады. Сізге кілт файлы қажет болуы мүмкін, мысалы, Kaspersky CompanyAccount порталында тіркелу үшін.

Кілт файлын қалпына келтіру үшін келесі әрекеттердің бірін орындау керек:

- Лицензия сатушысына хабарласу.
- Қолда бар белсендіру коды негізінде Kaspersky веб-сайтынан кілт файлын алу.

Деректерді беру туралы

Үшінші тараптарға берілетін деректер

Android операциялық жүйесі іске қосылған құрылғыларға push хабарландыру механизмі арқылы пәрмендерді уақтылы жеткізу мақсатына бағдарламалық жасақтаманың мобильдік құрылғыны басқару функциясын пайдаланған кезде, Google Firebase Cloud Messaging қызметі қолданылады. Пайдаланушы Google Firebase Cloud Messaging қызметін пайдалануды реттеген болса, пайдаланушы келесі ақпаратты Google Firebase Cloud Messaging қызметіне автоматты режимде беруге келіседі:

- Дана идентификаторы
- Google Firebase Cloud Messaging қызметіндегі бағдарламалық жасақтама идентификаторы
- Орнатылған бағдарламалық жасақтама нұсқасы
- Бағдарламалық жасақтаманың толық нұсқасы
- Google Play нұсқасы
- Бағдарламалық жасақтама дистрибутивінің атауы
- Беріліп жатқан деректерге арналған схема нұсқасы
- Операциялық жүйе нұсқасы
- Бағдарламалық жасақтама идентификаторы

Google Firebase Cloud Messaging қызметімен ақпарат алмасуды бұғаттау үшін, Пайдаланушы Google Firebase Cloud Messaging қызметін пайдалану конфигурацияларын бастапқы мәнге келтіруі керек.

iOS операциялық жүйесі іске қосылған құрылғыларға push хабарландыру механизмі арқылы пәрмендерді уақтылы жеткізу мақсатына бағдарламалық жасақтаманың мобильдік құрылғыны басқару функциясын пайдаланған кезде, Apple Push Notification Service (APN) қызметі қолданылады. Егер Пайдаланушы iOS MDM серверіне APNs сертификатын орнатқан болса, iOS ұялы құрылғыларын Бағдарламалық жасақтамаға қосу параметрлерінің жиынтығымен iOS MDM профилін қалыптастырса және осы iOS MDM профилін ұялы құрылғыларға орнатса, Пайдаланушы автоматты режимде APNs сервисіне келесі ақпаратты ұсынуға келіседі:

- Токен – құрылғының push-токені. Сервер құрылғыға push хабарландыруларын жіберген кезде осы токенді пайдаланады.
- PushMagic – push хабарландыруына қосылуы керек жол. Жолдың мәні құрылғы арқылы жасалады.

Деректер Kaspersky Lab АҚ-ға жіберіледі

Пайдаланушыға Kaspersky Extended Detection and Response Optimum функциясы қолжетімді болса, Kaspersky Security Center Linux келесі жағдайларда деректерді тасымалдайды:

- Қызметкерге оқыту курсын тағайындау үшін Kaspersky Security Center Linux келесі деректерді Kaspersky Automated Security Awareness Platform (KASAP) жүйесіне тасымалдайды: пайдаланушының электрондық мекенжайы, пайдаланушының балама электрондық поштасы (бар болса), KASAP жүйесіндегі пайдаланушы идентификаторы, оқыту тобының идентификаторы.

- Касперский Cloud Sandbox қызметін пайдалану арқылы зиянды әрекетті автоматты түрде орындау және анықтау үшін басқарылатын Kaspersky қолданбасы карантинге салынған нысандарды және тасымалданған нысандарды орындау кезінде жасалған файлдарды басқару серверінен желілік агент арқылы, содан кейін Kaspersky Security Center Web Console арқылы Kaspersky Cloud Sandbox қызметіне тасымалдайды.

Жергілікті түрде өңделетін деректер

Kaspersky Security Center Linux бағдарламасы ұйымның желісін қорғау жүйесін басқару және қызмет көрсету жөніндегі негізгі тапсырмаларды орталықтандырылған шешуге арналған. Kaspersky Security Center Linux әкімшіге ұйым желісінің қауіпсіздік деңгейі туралы егжей-тегжейлі ақпаратқа қатынасуға мүмкіндік береді және Kaspersky бағдарламалары негізінде құрылған қорғаныстың барлық құрамдастарын конфигурациялауға мүмкіндік береді. Kaspersky Security Center Linux келесі негізгі функцияларды орындайды:

- Ұйымның желісінде құрылғылар мен олардың пайдаланушыларын анықтау

- Құрылғыларды басқару үшін басқару топтарының иерархиясын қалыптастыру

- Құрылғыларға Kaspersky бағдарламаларын орнату

- Орнатылған бағдарламалардың жұмыс параметрлері мен тапсырмаларын басқару

- Kaspersky және басқа өндірушілер бағдарламаларының жаңартуларын басқару, осалдықтарды іздеу және түзету

- Құрылғыларда Kaspersky бағдарламаларын белсендіру

- Пайдаланушы есептік жазбаларын басқару

- Құрылғылардағы Kaspersky бағдарламаларының жұмысы туралы ақпаратты қарау

- Есептерді қарау

- Kaspersky қызметтерімен интеграцияны қосу

Өзінің негізгі функцияларын орындау үшін Kaspersky Security Center Linux бағдарламасы келесі ақпаратты қабылдай алады, сақтай алады және өңдей алады:

- Ұйым желісіндегі құрылғылар туралы ақпарат домен контроллерлерін (Active Directory, Samba, FreeIPA және ALD Pro) сканерлеу немесе IP аралықтарын сканерлеу арқылы алынады. Басқару сервері деректерді өз бетінше алады немесе оларды оған Желілік агент жібереді.

- Ұйым бөлімшелері, домендер, пайдаланушылар және топтар туралы домен контроллерлерінен (Active Directory, Samba, FreeIPA және ALD Pro) алынған ақпарат. Басқару сервердің өзі деректерді қабылдайды немесе оны тарату нүктесі ретінде әрекет ететін Желілік агент жібереді.

- Басқарылатын құрылғылар туралы деректер. Желілік агент құрылғыдан Басқару серверіне төменде келтірілген деректерді жібереді. Пайдаланушы құрылғының көрсетілетін атауы мен сипаттамасын Kaspersky Security Center Web Console интерфейсіне енгізеді:

  - Құрылғыны анықтау үшін қажетті басқарылатын құрылғы мен оның құрамдастарының техникалық сипаттамалары, яғни құрылғының көрсетілетін атауы мен сипаттамасы, Windows домен атауы мен түрі (Windows доменіне тиесілі құрылғылар үшін), Windows ортадағы құрылғы атауы (Windows доменіне тиесілі құрылғылар үшін), DNS домені және DNS атауы, IPv4 мекенжайы, IPv6 мекенжайы, желілік орналасуы, MAC мекенжайы, сериялық нөмірі, операциялық жүйенің түрі, құрылғының виртуалды машина болып табылатыны және гипервизор түрі, құрылғының VDI бөлігі ретінде динамикалық виртуалды машина болып табылатыны.

  - Басқарылатын құрылғыларды тексеру үшін және қандай да бір патчтар мен жаңартуларды қолдануға жарамдылық туралы шешімдерді қабылдау үшін қажетті басқарылатын құрылғылардың және олардың құрамдастарының басқа сипаттамалары: операциялық жүйе архитектурасы, операциялық жүйе жеткізушісі, операциялық жүйені құрастыру нөмірі, операциялық жүйенің шығарылым идентификаторы, операциялық жүйенің орналасу қалтасы, егер құрылғы виртуалды машина болса, виртуалды машина түрі, Құрылғыны басқаратын виртуалды Басқару серверінің атауы.

  - Басқарылатын құрылғылардағы әрекеттер туралы егжей-тегжейлі деректер: соңғы рет жаңартылған күні мен уақыты, құрылғы желіде соңғы рет көрінген уақыт, қайта іске қосуды күту күйі, құрылғыны қосу уақыты.

  - Құрылғылардың пайдаланушыларының есептік жазбалары және олардың жұмыс сеанстары туралы деректер.

- Басқарылатын құрылғыда қашықтағы диагностиканы іске қосу кезінде алынған деректер: трассалау файлдары, жүйелік ақпарат, құрылғыда орнатылған Kaspersky қолданбасы туралы ақпарат, дамп файлдары, оқиғалар журналдары, Kaspersky техникалық қолдау қызметінен алынған диагностикалық скриптілерді іске қосу нәтижелері.

- Егер құрылғы тарату нүктесі болса, тарату нүктесінің жұмыс статистикасы. Желілік агент деректерді құрылғыдан Басқару серверіне жібереді.

- Пайдаланушы Kaspersky Security Center Web Console жүйесіне енгізетін тарату нүктесінің параметрлері.

- Ұялы құрылғыларды Басқару серверіне қосу үшін қажетті деректер: сертификат, ұялы құрылғыларды қосу порты, Басқару серверіне қосылу мекенжайы. Пайдаланушы деректерді Kaspersky Security Center Web Console интерфейсінде енгізеді.

- Мобильдік қосылым протоколы бойынша жіберілетін мобильдік құрылғылар туралы деректер. Төменде атап көрсетілген деректер ұялы құрылғыдан Басқару серверіне беріледі:

  - Қолданба туралы ақпарат: қолданба атауы, қолданбаның толық нұсқасы, қолданбаны орнату күні мен уақыты, құрылғының нақты уақыттағы қорғаныс күйі, сеанс идентификаторы.

  - Қолданба пайдаланатын лицензиялық кілттер туралы ақпарат: лицензиялық кілттің сериялық нөмірі және лицензия түрі, лицензиялық кілт күйі, лицензиялық кілттің жарамдылық мерзімі (күн), лицензиялық кілт жасалған күн және соңғы мерзімі, лицензия берілген компанияның атауы, жазылым қолданылған жағдайда, қосымша ақпарат (жазылым жалаушасы, жарамдылық мерзімі және жазылым мерзімін созу үшін қолжетімді күндер саны, жазылым провайдерінің веб-мекенжайы, ағымдағы жазылым күйі және бұл күйді алу себебі), жазылымның қолданбада іске қосылған күні мен уақыты, құрылғыдағы лицензия мерзімі өтетін күн мен уақыт.

  - Басқарылатын құрылғы туралы ақпарат: құрылғы атауы, құрылғы идентификаторы, құрылғы түрі, құрылғы IMEI (бар болса), құрылғының сериялық нөмірі (бар болса), құрылғы өндірушісі, құрылғы процессорлары тобының атауы, құрылғы иесі куәлігінің саусақ ізі, операциялық жүйе түрі, операциялық жүйе нұсқасы, операциялық жүйенің атауы, құрылғыдағы дискілік кеңістіктің жалпы көлемі, құрылғыға тиесілі сервердің атауы, құрылғының IP мекенжайы, құрылғылар тобының атауы, пайдаланушының ерекше аты, доменнің ерекше атауы, бір реттік құпиясөз немесе домен құпиясөзі.

  - Пайдаланушы пәрмендерін орындау нәтижелері туралы ақпарат: пәрмен идентификаторы, пәрменнің орындалу күйі, пәрменнің орындалу нәтижесі; құрылғының орналасқан жерін анықтау пәрмені үшін: құрылғының ендігі, бойлығы, биіктігі және жылдамдығы; суретке түсіру пәрмені үшін: құрылғы құлпын ашу әрекеті кезінде мобильдік құрылғының алдыңғы камерасы түсірген фотосуреттер.

  - Құрылғыны тексеру туралы ақпарат: құрылғыны соңғы тексеру күні мен уақыты; тексеру басталған файлдық жүйедегі толық жол; тексерілген нысандар саны; анықталған зиянды нысандар саны; бұғатталған, жойылған және зарарсыздандырылған нысандар саны; зарарсыздандырылмаған нысандар саны; тексеру қателерінің саны; аяқталған процестер саны.

  - Оқиғалар түрінде ұсынылған әрбір қосымша құрамдастың жұмыс істеуі және әрбір тапсырманың орындалуы туралы ақпарат:

    - Оқиға идентификаторы.

    - Маңыздылық деңгейі.

    - Оқиға атауы және түрі.

    - Оқиға себебінің сипаттамасы.

    - Оқиға болған күн мен уақыт.

    - Ұрлыққа қарсы әрекет оқиғалары туралы ақпарат (құрылғы құлпын ашу коды, құрылғы координаттары, пәрменді жеткізу әдісі, жойылған деректер тізімі).

    - Анықталған нысанды немесе әрекетті өңдеу нәтижелері (құрылғыдағы файл атауы; қолданба атауы; қауіп атауы; қауіп түрі; файлда орындалатын әрекет түрі; әрекеттің нәтижесі; егер орын алса, қате коды).

    - Іске қосылған сәйкестік ережесі туралы ақпарат (ереже критерийі; қолданылған әрекет; әрекетті қолданған кездегі орын алған қатенің сипаттамасы).

    - Қолданба қатесі туралы ақпарат (қолданба нұсқасы, ОЖ нұсқасы, құрылғы атауы, қате сипаттамасы).

    - Samsung KNOX қатесі туралы ақпарат (қате коды, файлды жүктеп алу мүмкін емес URL).

- Қолданбаға берілген рұқсаттар туралы ақпарат.
- Басқарылатын құрылғыда орнатылған әрбір қолданба туралы ақпарат (бағдарлама атауы, орнату күйі).
- Жаһандық лицензиялық келісімді қабылдау туралы ақпарат: лицензиялық келісім идентификаторы, лицензиялық келісімнің уақыт белгісі, лицензиялық келісім мәтіні.
- Google Firebase Cloud Messaging параметрлері: Sender ID, құрылғыны тіркеу идентификаторы.

- Құрылғының жалпы IP мекенжайы туралы ақпарат.

- iOS MDM протоколы бойынша жіберілетін ұялы құрылғылар туралы деректер. Төменде атап көрсетілген деректер ұялы құрылғыдан Басқару серверіне беріледі:
  - Құрылғыны анықтау үшін қажетті мобильдік құрылғы мен оның құрамдастарының техникалық сипаттамалары: құрылғының атауы, үлгісі, операциялық жүйе атауы, нұсқасы және құрастырылым нөмірі, құрылғы үлгісінің нөмірі, IMEI нөмірі, UDID, MEID нөмірі, сериялық нөмірі, толық және қолжетімді жад көлемі, модем шағын бағдарламасының нұсқасы, Bluetooth MAC мекенжайы, Wi-Fi MAC мекенжайы және SIM картасының деректері (SIM картасы идентификаторының бөлігі ретіндегі ICCID коды).
  - Ұялы құрылғы пайдаланатын ұялы байланыс желісі туралы деректер: ұялы байланыс желісінің түрі, пайдаланылатын ұялы байланыс желісінің атауы, үйдегі ұялы байланыс желісінің атауы, ұялы байланыс желісі операторы параметрлерінің нұсқасы, дауыстық роуминг және деректер роумингі күйі, үй желісіне арналған ел коды, орналасу елінің коды, пайдаланылатын желінің ел коды және шифрлау деңгейі.
  - Мобильдік құрылғының қауіпсіздік параметрлері: құпиясөзді пайдалану және оның саясат параметрлеріне сәйкестігі, орнатылған сертификаттар тізімі, қолданбалар тізімі және конфигурация профильдері.
  - Басқару серверімен соңғы рет синхрондау күні және құрылғыны басқару күйі.

- WebRTC хаттамасын пайдаланып берілетін мобильді құрылғы деректерінің мәліметтері: құрылғы экранының кескіні.

- Мобильдік құрылғыларға тасымалдау үшін көрсетілген файлдар туралы мәліметтер. Пайдаланушы деректерді Kaspersky Security Center Web Console интерфейсінде енгізеді.

- Құрылғыда орнатылған Kaspersky бағдарламалары туралы деректер. Басқарылатын бағдарлама деректерді құрылғыдан Басқару серверіне Желілік агент арқылы жібереді:
  - Басқарылатын құрылғыда орнатылған Kaspersky бағдарламаларының параметрлері: Kaspersky бағдарламасының атауы мен нұсқасы, күйі, тұрақты қорғау күйі, құрылғыны соңғы тексеру күні мен уақыты, анықталған қауіптер саны, зарарсыздандыру орындалмаған нысандар саны, бағдарлама компоненттерінің болуы және күйі, Kaspersky бағдарламасының параметрлері мен тапсырмалары туралы ақпарат, белсенді және резервтегі лицензиялық кілттер туралы ақпарат, бағдарламаны орнату күні мен идентификаторы.
  - Бағдарлама жұмысының статистикасы: басқарылатын құрылғыдағы Kaspersky бағдарламасының құрамдастары күйінің өзгерістерімен және бағдарламалық құрамдастар бастаған тапсырмаларды орындаумен байланысты оқиғалар.
  - Kaspersky бағдарламасы айқындаған құрылғының күйі.
  - Kaspersky бағдарламасы беретін тегтер.

- Kaspersky Security Center Linux құрамдастары және Kaspersky басқарылатын бағдарламалары оқиғаларында қамтылған деректер. Желілік агент деректерді құрылғыдан Басқару серверіне жібереді.
- Kaspersky Security Center Linux бағдарламасын оқиғаларды экспорттауға арналған SIEM жүйесімен біріктіру үшін қажетті деректер. Пайдаланушы деректерді Kaspersky Security Center Web Console интерфейсінде енгізеді.
- Kaspersky Security Center Linux жүйесін домен контроллерлерімен (Active Directory, Samba, FreeIPA және ALD Pro) интеграциялау үшін қажет деректер. Пайдаланушы деректерді Kaspersky Security Center Web Console интерфейсінде енгізеді.
- Kerberos бірыңғай кіру (SSO) көмегімен қосылуға арналған пернетақта файлдары. Пайдаланушы деректерді Kaspersky Security Center Web Console интерфейсінде енгізеді.
- Интернетке қосылу үшін прокси-серверге қосылымды конфигурациялау үшін қажет деректер. Пайдаланушы деректерді Kaspersky Security Center Web Console интерфейсінде енгізеді.
- Саясат және саясат профильдері түрінде ұсынылған Kaspersky Security Center Linux құрамдастарының және Kaspersky басқарылатын бағдарламаларының конфигурациялары. Пайдаланушы деректерді Kaspersky Security Center Web Console интерфейсінде енгізеді.
- Kaspersky Security Center Linux құрамдастары және Kaspersky басқарылатын бағдарламалары тапсырмаларының конфигурациялары. Пайдаланушы деректерді Kaspersky Security Center Web Console интерфейсінде енгізеді.
- Осалдықтар мен патчтарды басқару функциясы өңдейтін деректер. Желілік агент құрылғыдан Басқару серверіне келесі ақпаратты жібереді:
  - Басқарылатын құрылғыларда табылған жабдық туралы ақпарат (Жабдық тізімдемесі).

    Желілік агент Windows жүйесімен жұмыс істейтін құрылғыға орнатылған болса, ол басқару серверіне құрылғының аппараттық жасақтамасы туралы келесі ақпаратты жібереді:
    - ЖЖҚ
    - Жаппай сақтау құрылғылары
    - Негізгі тақта
    - Процессор
    - Желілік адаптерлер
    - Мониторлар
    - Бейне адаптері
    - Дыбыстық карта

    Желілік агент Linux немесе macOS жүйесімен жұмыс істейтін құрылғыға орнатылған болса, ол басқару серверіне құрылғының аппараттық жасақтамасы туралы келесі ақпаратты жібереді (бұл ақпаратты операциялық жүйе қамтамасыз етсе):
    - Жалпы ЖЖҚ көлемі
    - Жаппай сақтау құрылғыларының жалпы көлемі

- Негізгі тақта
- Процессор
- Желілік адаптерлер

- Басқарылатын құрылғыларда орнатылған бағдарламалар мен патчтар туралы деректер (Бағдарламалар тізімдемесі). Қолданбаларды басқарылатын құрылғыларда Қолданбаларды бақылау функциясымен табылған орындалатын файлдар туралы ақпаратпен байланыстыруға болады.

- Басқарылатын құрылғыларда анықталған үшінші тарап бағдарламалық жасақтамасының осалдықтары туралы деректер.

- Басқарылатын құрылғыларда орнатылған үшінші тарап бағдарламалары үшін қолжетімді жаңарту туралы деректер.

- Басқарылатын құрылғылардағы үшінші тарап бағдарламаларындағы осалдықтарды түзету үшін жаңартуларды оқшауланған Басқару серверіне жүктеу үшін қажетті деректер. Пайдаланушы Басқару серверінің klscflag утилитасын пайдаланып, деректерді енгізеді және жібереді.

- Реттелмелі бағдарламалар санаттары. Пайдаланушы деректерді Kaspersky Security Center Web Console интерфейсінде енгізеді.

- Бағдарламаны басқару функциясы арқылы басқарылатын құрылғыларда анықталған орындалатын файлдар туралы деректер. Басқарылатын бағдарлама деректерді құрылғыдан Басқару серверіне Желілік агент арқылы жібереді. Деректердің толық тізімі тиісті қолданбаның анықтамасында келтірілген.

- Сақтық көшірмелеуге орналастырылған файлдар туралы деректер. Басқарылатын бағдарлама деректерді құрылғыдан Басқару серверіне Желілік агент арқылы жібереді. Деректердің толық тізімі тиісті бағдарламаның анықтамасында келтірілген.

- Карантинге орналастырылған файлдар туралы деректер. Басқарылатын бағдарлама деректерді құрылғыдан Басқару серверіне Желілік агент арқылы жібереді. Деректердің толық тізімі тиісті бағдарламаның анықтамасында келтірілген.

- Егжей-тегжейлі талдау үшін Kaspersky мамандары сұраған файлдар туралы деректер. Басқарылатын бағдарлама деректерді құрылғыдан Басқару серверіне Желілік агент арқылы жібереді. Деректердің толық тізімі тиісті бағдарламаның анықтамасында келтірілген.

- Аномалияларды бейімделумен басқару ережелерінің күйі және іске қосылуы туралы деректер. Басқарылатын бағдарлама деректерді құрылғыдан Басқару серверіне Желілік агент арқылы жібереді. Деректердің толық тізімі тиісті бағдарламаның анықтамасында келтірілген.

- Басқарылатын құрылғыға орнатылған немесе қосылған және Құрылғыны басқару функциясы анықтаған сыртқы құрылғылар (жад құрылғылары, ақпаратты беру құралдары, ақпаратты қатты көшірмеге айналдыру құралдары, қосылым шиналары) туралы деректер. Басқарылатын бағдарлама деректерді құрылғыдан Басқару серверіне Желілік агент арқылы жібереді. Деректердің толық тізімі тиісті бағдарламаның анықтамасында келтірілген.

- Windows операциялық жүйесі бар құрылғыларды шифрлау және шифрлау күйлері туралы ақпарат. Басқарылатын бағдарлама деректерді құрылғыдан Басқару серверіне Желілік агент арқылы жібереді.

- Құрылғылардағы деректерді шифрлау қателері туралы ақпарат. Шифрлау Kaspersky бағдарламаларын деректерді шифрлау функциясы арқылы орындалады. Басқарылатын бағдарлама деректерді құрылғыдан Басқару серверіне Желілік агент арқылы жібереді. Деректердің толық тізімі тиісті бағдарламаның онлайн анықтамасында келтірілген.

- Басқарылатын бағдарламаланатын логикалық контроллерлер (БЛК) тізімі. Басқарылатын бағдарлама деректерді құрылғыдан Басқару серверіне Желілік агент арқылы жібереді. Деректердің толық тізімі тиісті бағдарламаның анықтамасында келтірілген.

- Қауіптердің даму тізбегін жасауға арналған деректер. Басқарылатын бағдарлама деректерді құрылғыдан Басқару серверіне Желілік агент арқылы жібереді. Деректердің толық тізімі тиісті бағдарламаның анықтамасында келтірілген.

- Ұйым қызметкерлерінің бұлттық сервистерге қол жеткізу әрекеттері туралы ақпарат. Басқарылатын бағдарлама деректерді құрылғыдан Басқару серверіне Желілік агент арқылы жібереді. Деректердің толық тізімі тиісті бағдарламаның анықтамасында келтірілген.

- Kaspersky Security Center бағдарламасын Kaspersky Managed Detection and Response қызметімен біріктіруге қажетті деректер (Kaspersky Security Center Web Console үшін арнайы плагин орнатылуы тиіс): біріктіруді бастау токені, біріктіру токені және пайдаланушы сеансы токені. Пайдаланушы біріктіруді бастау токені арқылы Kaspersky Security Center Web Console интерфейсіне кіреді. Kaspersky MDR қызметі арнайы плагин арқылы біріктіру токенін және пайдаланушы сеансы токенін береді.

- Kaspersky Security Center Linux жүйесін Kaspersky Cloud Sandbox және Kaspersky Threat Intelligence Portal-мен интеграциялау үшін қажетті деректер (Kaspersky Security Center Web Console үшін сәйкес плагинді орнату қажет): интеграция токені, авторизация токені. Пайдаланушы интеграция токенін Kaspersky Security Center Web Console интерфейсінде енгізеді. Kaspersky Security Center Web Console сұраудағы авторизация токенін Kaspersky Cloud Sandbox API интерфейсіне тасымалдайды.

- Kaspersky Security Center Linux жүйесін Kaspersky Automated Security Awareness Platform (KASAP) қызметімен интеграциялау үшін қажетті деректер: KASAP Open API, URL мекенжайы (Open API арқылы KASAP жүйесіне кіруге арналған сілтеме).

- Енгізілген белсендіру кодтары немесе кілт файлдары туралы толық ақпарат. Пайдаланушы деректерді Kaspersky Security Center Web Console интерфейсінде енгізеді.

- Пайдаланушылардың есептік жазбалары: атауы, сипаттамасы, толық атауы, электрондық пошта мекенжайы, негізгі телефон нөмірі, құпиясөзі, Басқару сервері жасаған құпия кілті және екі факторлы аутентификация үшін бір реттік құпиясөз. Пайдаланушы деректерді Kaspersky Security Center Web Console интерфейсінде енгізеді.

- Басқару нысандарының тексерістер журналы. Пайдаланушы деректерді Kaspersky Security Center Web Console интерфейсінде енгізеді.

- Пайдаланушы тексеріс жасаған құрылғының IP мекенжайы. IP мекенжайын Басқару сервері автоматты түрде анықтайды.

- Жойылған басқару нысандары тізімдемесі. Пайдаланушы деректерді Kaspersky Security Center Web Console интерфейсінде енгізеді.

- Файлдан жасалған орнату пакеттері және орнату параметрлері. Пайдаланушы деректерді Kaspersky Security Center Web Console интерфейсінде енгізеді.

- Kaspersky хабарландыруларын Kaspersky Security Center Web Console веб-консолінде көрсетуге қажетті деректер. Пайдаланушы деректерді Kaspersky Security Center Web Console интерфейсінде енгізеді.

- Kaspersky Security Center Web Console веб-консолінде басқарылатын бағдарлама плагиндерінің жұмыс істеуі үшін қажетті және күнделікті жұмыс барысында Басқару сервері деректорында плагиндер сақтайтын деректер. Сипаттама және деректерді беру тәсілдері тиісті бағдарламаның анықтама файлдарында келтірілген.

- Kaspersky Security Center Web Console пайдаланушы конфигурациялары: локализация тілі және пайдаланушы интерфейсі тақырыбы, бақылау тақтасын көрсету конфигурациялары, нотификациялар күйі туралы ақпарат (оқылған/оқылмаған), кестелердегі бағандардың күйі (жасыру/көрсету), оқу режимінің өту барысы. Пайдаланушы деректерді Kaspersky Security Center Web Console интерфейсінде енгізеді.

- Басқарылатын құрылғыларды Kaspersky Security Center Linux құрамдастарына қауіпсіз қосу сертификаты. Пайдаланушы Басқару серверінің klsetsrvcert утилитасын пайдаланып, деректерді енгізеді және жібереді.

- Ұйымның ішкі веб-ресурстарына сенім орнатуға арналған сертификаттар. Пайдаланушы деректерді Kaspersky Security Center Web Console интерфейсінде енгізеді.

- Пайдаланушының Kaspersky ұйымымен жасалған заңды келісімдердің шарттарын қабылдауы туралы ақпарат.

- Пайдаланушы Kaspersky Security Center Web Console интерфейсіне немесе Kaspersky Security Center OpenAPI бағдарламалық интерфейсіне енгізетін Басқару серверінің деректері.

- Пайдаланушы Kaspersky Security Center Web Console интерфейсіне енгізетін кез келген деректер.

Жоғарыда атап көрсетілген деректер Kaspersky Security Center Linux-ке келесі тәсілдермен кіруі мүмкін:

- Пайдаланушы деректерді Kaspersky Security Center Web Console интерфейсінде енгізеді.

- Желілік агент құрылғыдан деректерді өз бетінше алады және Басқару серверіне жібереді.

- Желілік агент Kaspersky бағдарламасы арқылы жиналған деректерді алады және Басқару серверіне жібереді. Kaspersky басқарылатын бағдарламалары өңдейтін деректер тізбесі тиісті бағдарламалардың анықтамаларында келтірілген.

- Басқару сервері желілік құрылғылар туралы ақпаратты өз бетінше алады немесе оны тарату нүктесі ретінде әрекет ететін желілік агент жібереді.

- Деректер мобильдік құрылғыдан басқару серверіне iOS MDM немесе мобильдік байланыс протоколы арқылы беріледі.

Атап көрсетілген деректер Басқару сервері дерекқорында сақталады. Құпиясөз хэштері шифрланған түрде сақталады.

Жоғарыда аталған барлық деректерді Kaspersky бағдарламасына тек Kaspersky Security Center Linux құрамдастарының дамп файлдары, трассалау файлдары немесе журнал файлдары, соның ішінде инсталляторлар мен утилиталар жасайтын журналдар файлдары арқылы беруге болады.

Kaspersky Security Center Linux құрамдастарының дамп файлдары, трассалау файлдары немесе журнал файлдары Басқару серверінен, Желілік агенттен және Kaspersky Security Center Web Console-інен ерікті деректерді қамтиды. Бұл файлдарда дербес және басқа да құпия деректер болуы мүмкін. Қоқыс файлдары, трассалау файлдары немесе оқиғалар журналының файлдары құрылғыларда шифрланбаған күйде сақталады. Қоқыс файлдары, трассалау файлдары немесе журнал файлдары Kaspersky бағдарламасына автоматты түрде берілмейді, алайда, әкімші осы файлдарды Kaspersky бағдарламасына Техникалық қолдау қызметінің сұрауы бойынша Kaspersky Security Center Linux жұмысындағы мәселелерді шешу үшін қолмен жібере алады.

Kaspersky барлық алынған деректерді заңнамаға және Kaspersky қолданыстағы ережелеріне сәйкес қорғауды қамтамасыз етеді. Деректер қауіпсіз байланыс арналары бойынша беріледі.

Сілтемелер арқылы Kaspersky Security Center Web Console веб-консоліне өту арқылы, Пайдаланушы келесі деректерді автоматты түрде жіберуге келіседі:

- Kaspersky Security Center Linux коды
- Kaspersky Security Center Linux нұсқасы
- Kaspersky Security Center Linux локализациясы
- Лицензия идентификаторы
- Лицензия түрі
- Серіктес арқылы лицензияны сатып алу белгісі

Әрбір сілтеме бойынша ұсынылатын деректер тізімі сілтеменің мақсаты мен орналасқан жеріне байланысты.

Kaspersky алынған деректерді жасырын түрде және тек жалпы статистика мақсатында пайдаланады. Жиынтық статистика алынған бастапқы ақпараттан автоматты түрде қалыптастырылады және қандай да бір дербес немесе өзге де құпия деректерді қамтымайды. Жаңа деректер жинақталған кезде алдыңғы деректер жойылады (жылына бір рет). Жиынтық статистика шектелмеген уақыт бойы сақталады.

Жазылым туралы

Kaspersky Security Center Linux-ке жазылым – бұл параметрлері таңдалған бағдарламаны қолдануға тапсырыс беру (жазылымның аяқталу күні, қорғалатын құрылғылардың саны). Kaspersky Security Center Linux-ке жазылымды провайдерде (мысалы, интернет-провайдерде) тіркеуге болады. Жазылымды қолмен немесе автоматты режимде ұзартуға немесе одан бас тартуға болады.

Жазылым шектеулі (мысалы, бір жылға) немесе шектеусіз (аяқталу күні жоқ) болуы мүмкін. Шектеулі жазылым аяқталғаннан кейін Kaspersky Security Center жұмысын жалғастыру үшін, оны жаңарту қажет. Провайдерге алдын ала төлем уақтылы енгізілген жағдайда, шектеусіз жазылым автоматты түрде ұзартылады.

Егер жазылым шектеулі болса, жазылым аяқталғаннан кейін жазылымды ұзарту үшін жеңілдік кезеңі берілуі мүмкін, оның барысында бағдарламаның функционалдығы сақталады. Жеңілдік кезеңінің болуы мен ұзақтығын провайдер айқындайды.

Kaspersky Security Center Linux жазылымын пайдалану үшін провайдер ұсынған белсендіру кодын қолдану қажет.

Жазылым аяқталғаннан немесе одан бас тартқаннан кейін ғана Kaspersky Security Center Linux пайдалану үшін басқа белсендіру кодын қолдануға болады.

Провайдерге байланысты жазылымды басқаруға арналған ықтимал әрекеттер жиынтығы әртүрлі болуы мүмкін. Провайдер бағдарламаның функционалдығы сақталатын жазылымның мерзімін ұзарту үшін жеңілдік кезеңін ұсынбауы мүмкін.

Жазылым арқылы сатып алынған белсендіру кодтарын Kaspersky Security Center бағдарламасының алдыңғы нұсқаларын белсендіру үшін пайдалану мүмкін емес.

Жазылым бағдарламасын пайдалану кезінде, Kaspersky Security Center Linux бағдарламасы автоматты түрде белсендіру серверіне жазылымның аяқталу күніне дейін белгілі бір уақыт аралығында жүгінеді. Жүйелік DNS арқылы серверге қатынасу мүмкін болмаса, бағдарлама жалпыға ортақ DNS серверлерін пайдаланады. Сіз жазылымды провайдердің веб-сайтында ұзарта аласыз.

Kaspersky Security Center Linux-ті белсендіру

Қосымша функцияларын пайдалану үшін Kaspersky Security Center Linux бағдарламасын белсендіруге болады. Бұл тапсырманы екі жолмен орындауға болады: басқару серверінің бастапқы орнату шеберін пайдалану немесе басқару сервері параметрлерін конфигурациялау.

Kaspersky Security Center Linux белсендіру үшін:

1. Негізгі мәзірдегі басқару серверінің атауын басыңыз.

   Басқару серверінің сипаттары терезесі ашылады.

2. **Жалпы** қойыншасында **Лицензиялық кілттер** бөлімін таңдаңыз.

3. **Ағымдағы лицензия** бөлімінде **Таңдау** түймесін басыңыз.

4. Ашылған терезеде Kaspersky Security Center Linux қызметін іске қосу үшін пайдаланғыңыз келетін лицензия кілтін таңдаңыз. Лицензия кілті тізімде болмаса, **Жаңа лицензия кілтін қосу** түймесін басып, жаңа лицензия кілтін көрсетіңіз.

5. Қажет болса, сақтық көшірменің лицензия кілтін де қосуға болады. Ол үшін **Резервттегі лицензиялық кілт** бөлімінде **Таңдау** түймесін басып, бар лицензия кілтін таңдаңыз немесе кілтті қосыңыз. Белсенді лицензия кілті болмаса, резервтік лицензия кілтін қоса алмайтыныңызды ескеріңіз.

6. **Сақтау** түймесін басыңыз.

Kaspersky басқарылатын қолданбаларын лицензиялау

Бұл бөлімде Kaspersky Security Center бағдарламасының Kaspersky басқарылатын бағдарламаларының лицензиялық кілттерімен жұмыс істеу мүмкіндіктері сипатталған.

Kaspersky Security Center Linux бағдарламасы Kaspersky бағдарламаларының лицензиялық кілттерін клиент құрылғыларына орталықтан таратуға, кілттердің қолданылуын бақылауға және лицензиялардың жарамдылық мерзімін ұзартуға мүмкіндік береді.

Kaspersky Security Center көмегімен лицензиялық кілт қосылған кезде лицензиялық кілттің сипаттары Басқару серверінде сақталады. Осы ақпарат негізінде бағдарлама лицензиялық кілттерді пайдалану туралы есепті қалыптастырады және әкімшіге лицензиялардың жарамдылық мерзімінің аяқталғаны және лицензиялық кілттердің сипаттарында қойылған лицензиялық шектеулердің асып кеткені туралы хабарлайды. Басқару сервері параметрлері құрамындағы лицензиялық кілттерді пайдалану туралы хабарландыру параметрлерін конфигурациялауға болады.

Басқарылатын бағдарламаларды лицензиялау

Басқарылатын құрылғыларда орнатылған Kaspersky бағдарламалары, бағдарламалардың әрқайсысына кілт файлын немесе белсендіру кодын қолдану арқылы іске қосылуы керек. Кілт файлы немесе белсендіру коды келесі тәсілдермен таратылуы мүмкін:

- Автоматты түрде тарату
- Басқарылатын бағдарламаның орнату пакетін пайдалану
- Басқарылатын бағдарламаның Лицензиялық кілтін қосу тапсырмасы арқылы
- Басқарылатын бағдарламаны қолмен белсендіру

Жоғарыда аталған тәсілдердің кез келгенімен белсенді немесе сақтық лицензиялық кілтті қосуға болады. Kaspersky бағдарламасы қазіргі уақытта белсенді болып саналатын кілтті пайдаланады және белсенді кілттің әрекет ету мерзімі аяқталғаннан кейін қолданылатын резервттегі лицензиялық кілтті сақтайды. Лицензиялық кілті қосылып жатқан бағдарлама кілттің белсенді немесе резервтік екенін анықтайды. Кілтті анықтау лицензиялық кілтті қосу үшін қолданылатын тәсілге байланысты емес.

Автоматты түрде тарату

Егер сіз әртүрлі басқарылатын бағдарламаларды қолдансаңыз және белгілі бір кілт файлын немесе белсендіру кодын құрылғыларға тарату маңызды болса, белсендіру кодын немесе кілтті таратудың басқа тәсілдерін қолданыңыз.

Kaspersky Security Center қолда бар лицензиялық кілттерді құрылғыларға автоматты түрде таратуға мүмкіндік береді. Мысалы, Басқару сервері қоймасында үш лицензиялық кілт бар. Барлық үш лицензиялық кілт үшін **Автоматты түрде таратылған лицензиялық кілт** параметрін қосу керек. Ұйымның құрылғыларында Kaspersky қауіпсіздік бағдарламасы, мысалы, Kaspersky Endpoint Security for Linux орнатылған. Лицензиялық кілтті тратуды қажет ететін жаңа құрылғы табылды. Бағдарлама бұл құрылғыға не сәйкес келетінін анықтайды, мысалы, қоймадан екі лицензиялық кілт, *Кілт_1* лицензиялық кілті және *Кілт_2* лицензиялық кілті. Құрылғыға жарамды лицензиялық кілттердің бірі қолданылады. Бұл жағдайда, осы екі лицензиялық кілттің қайсысы осы құрылғыға қолданылатынын болжау мүмкін емес, өйткені лицензиялық кілттерді автоматты түрде тарату әкімшінің араласуын қамтымайды.

Лицензиялық кілтті құрылғыларға таратқан кезде осы лицензиялық кілт үшін құрылғылар есептеледі. Лицензиялық кілт қолданылатын құрылғылардың саны лицензиялық шектен аспайтынына көз жеткізуіңіз керек. Егер құрылғылардың саны лицензиялық шектен асып кетсе, мұндай құрылғыларға *Критикалық* күйі беріледі.

Таратпас бұрын, кілт файлы немесе белсендіру коды Басқару сервері қоймасына қосылуы керек.

Нұсқаулар:

- Лицензиялық кілтті Басқару серверінің қоймасына қосу
- Лицензиялық кілтті автоматты түрде тарату

Келесі жағдайларда автоматты түрде таратылатын лицензиялық кілт виртуалды Басқару серверінің қоймасында көрінбеуі мүмкін екенін ескеріңіз:

- Лицензиялық кілт бағдарлама үшін жарамсыз.
- Виртуалды Басқару серверінде басқарылатын құрылғылар жоқ.
- Лицензиялық кілт басқа виртуалды Басқару сервері басқаратын құрылғылар үшін әлдеқашан қолданыста және құрылғылар санының лицензиялық шегіне жетті.

Басқарылатын бағдарламаның орнату пакетіне кілт файлын немесе белсендіру кодын қосу.

Қауіпсіздік тұрғысынан, бұл параметрді пайдалану ұсынылмайды. Орнату пакетіне қосылған кілт файлы немесе белсендіру коды бұзылуы мүмкін.

Басқарылатын бағдарламаны орнату пакеті арқылы орнатқан жағдайда, белсендіру кодын немесе кілт файлын орнату пакетінде немесе сол бағдарламаның саясатында көрсетуге болады. Лицензиялық кілт, құрылғыны Басқару серверімен кезекті рет синхрондау кезінде басқарылатын құрылғыларға қолданылады.

Нұсқаулар: Лицензиялық кілтті орнату пакетіне қосу.

Лицензиялы бағдарламалардың лицензиялық кілтін қосу тапсырмасы арқылы тарату

Басқарылатын бағдарламаның лицензиялық кілтін қосу тапсырмасын пайдаланған жағдайда, сіз құрылғыларға таратылатын лицензиялық кілтті таңдап, құрылғыларды өзіңізге ыңғайлы тәсілмен таңдай аласыз, мысалы, басқару тобын немесе құрылғылар таңдауын таңдау арқылы.

Таратпас бұрын, кілт файлы немесе белсендіру коды Басқару сервері қоймасына қосылуы керек.

Нұсқаулар:

- Лицензиялық кілтті Басқару серверінің қоймасына қосу
- Лицензиялық кілтті клиент құрылғыларына тарату

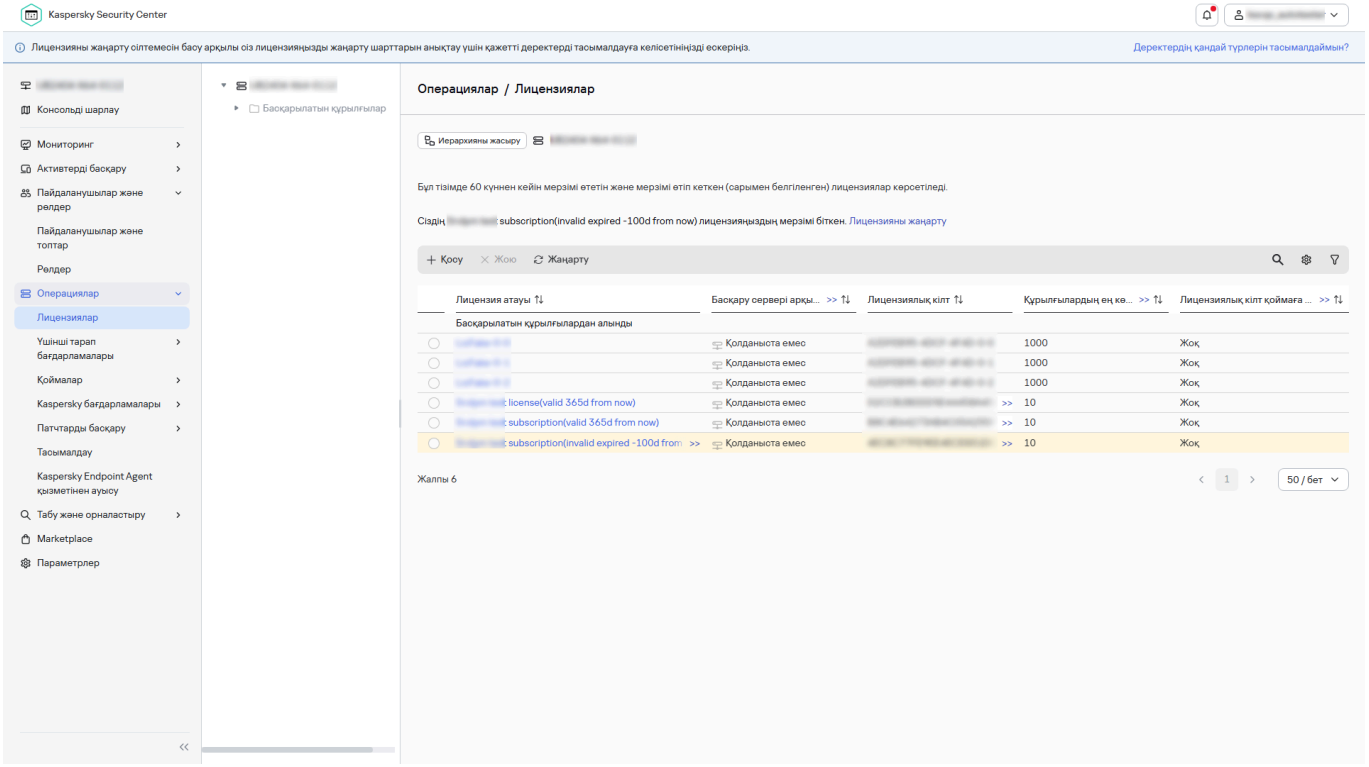
Құрылғыларға белсендіру кодын немесе кілт файлын қолмен қосу.

Орнатылған Kaspersky бағдарламасын жергілікті түрде қосу үшін бағдарлама құралдарын пайдалануға болады. Кеңейтілген ақпаратты орнатылған бағдарламаларға арналған құжаттамадан қараңыз.

Лицензиялық кілтті Басқару серверінің қоймасына қосу

Басқару сервері қоймасына лицензиялық кілтті қосу үшін:

1. Қолданбаның негізгі терезесінде **Операциялар** → **Лицензиялар** лицензиялары бөліміне өтіңіз.



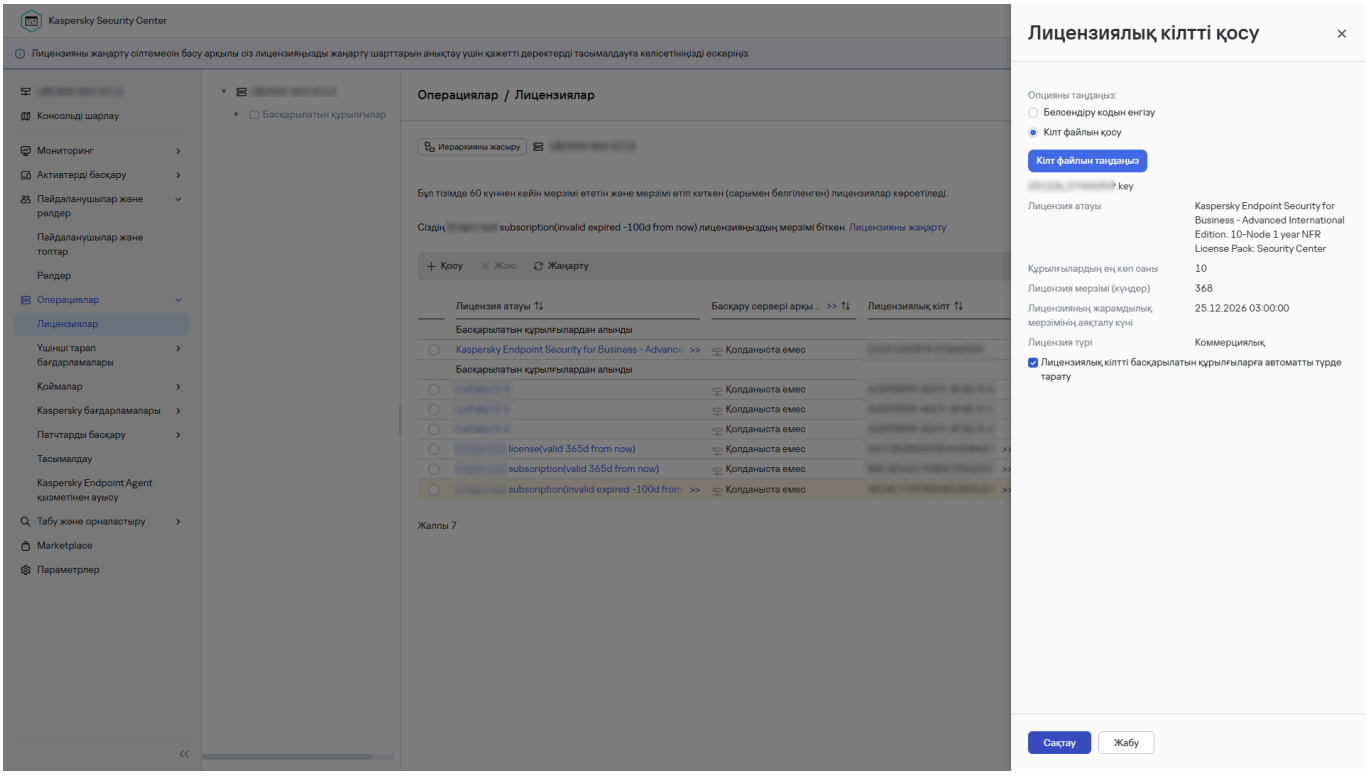
Қосылған Kaspersky лицензиялары кілттерінің тізімі

2. **Қосу** түймесін басыңыз.

3. Қосқыңыз келетін нәрсені таңдаңыз:

- **Кілт файлын қосу**

  Кілт файлын таңдаңыз түймесін басып, қосқыңыз келетін .key файлын таңдаңыз.



Кілт файлын қолдану арқылы лицензия кілтін қосу

- **Белсендіру кодын енгізу**

  Мәтін жолағында белсендіру кодын көрсетіңіз және **Жіберу** түймесін басыңыз.

4. **Жабу** түймесін басыңыз.

Басқару сервері қоймасына лицензиялық кілт немесе бірнеше лицензиялық кілт қосылады.

Лицензиялық кілтті клиент құрылғыларына тарату

Kaspersky Security Center Web Console қолданбасы лицензиялық кілтті клиент құрылғыларына автоматты түрде немесе **Бағдарламаны белсендіру** тапсырмасы арқылы таратуға мүмкіндік береді. Құрылғылардың белгілі бір тобына кілттерді тарату үшін тапсырманы пайдалануға болады. Лицензиялық кілтті тапсырманың көмегімен тарату кезінде құрылғылар санына қойылатын лицензиялық шектеу ескеріледі. Лицензия шегіне жеткенде лицензия кілтін таратуды автоматты түрде тоқтату үшін автоматты кілтті таратуды пайдаланыңыз.

Лицензия кілтін автоматты түрде таратуды қосқан болсаңыз, лицензия кілтін клиент құрылғыларына тарату үшін **Бағдарламаны белсендіру** тапсырмасын жасамаңыз. Әйтпесе, жиі синхрондауға байланысты Басқару серверіне түсетін жүктеме артады.

Таратпас бұрын лицензиялық кілтті Басқару серверінің қоймасына қосыңыз.

*Лицензиялық кілтті клиент құрылғыларына **Бағдарламаны белсендіру** тапсырмасы арқылы тарату үшін:*

1. Бағдарламаның негізгі терезесінде **Тапсырмалар** бөліміне өтіңіз.

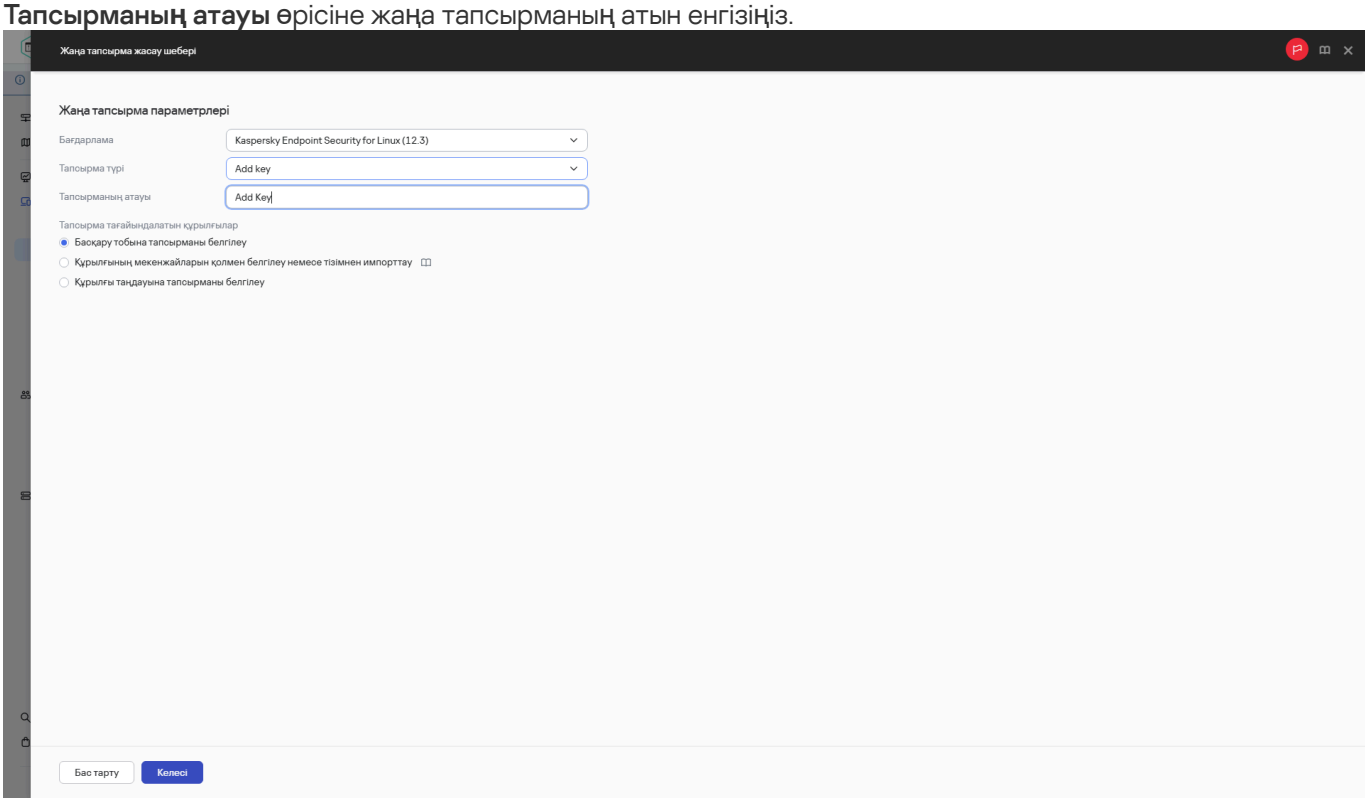
2. **Қосу** түймесін басыңыз.

   Жаңа тапсырма жасау шебері іске қосылады. Шебердің жұмысын жалғастыру үшін **Келесі** түймесін басыңыз.

3. **Бағдарлама** ашылмалы тізімінде лицензия кілтін қосқыңыз келетін бағдарламаны таңдаңыз.

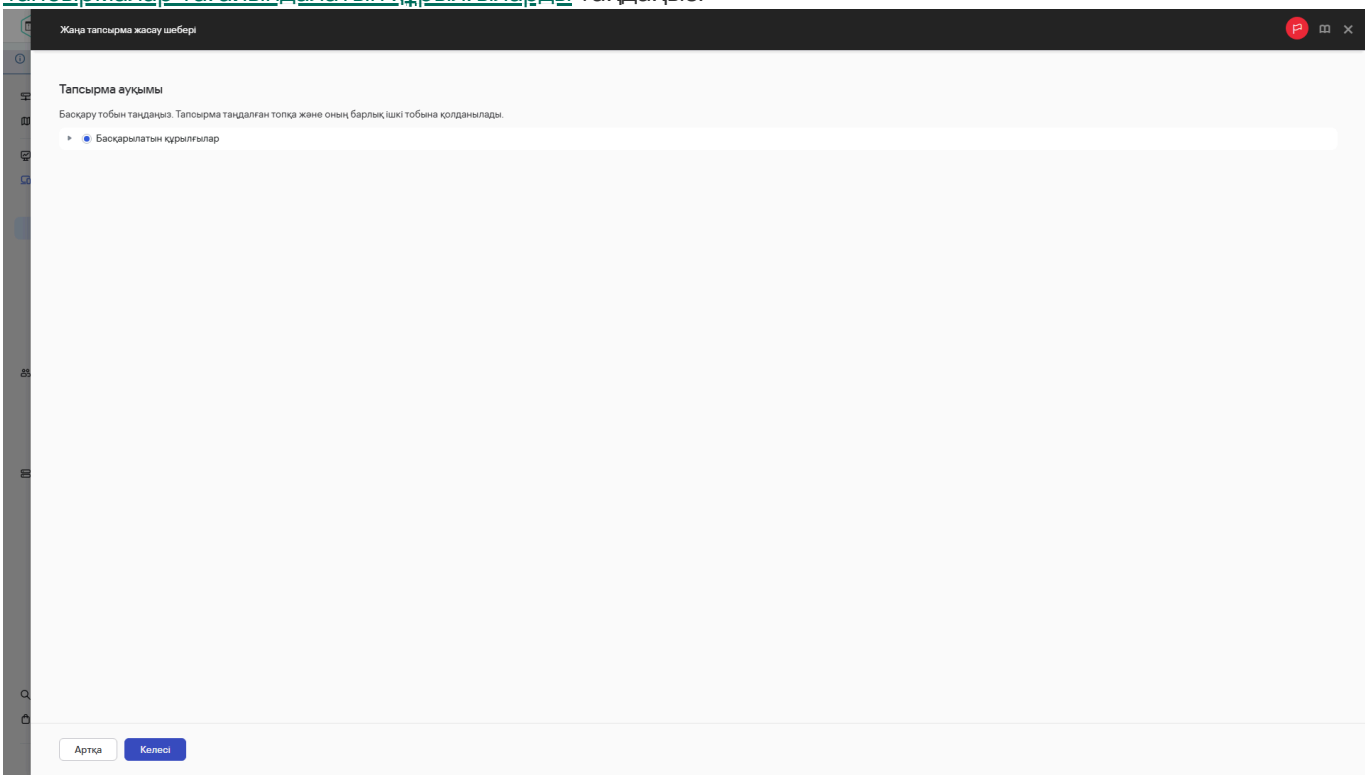
4. **Тапсырма түрі** тізімінде **Бағдарламаны белсендіру** тапсырмасын таңдаңыз.

5. **Тапсырманың атауы** өрісіне жаңа тапсырманың атын енгізіңіз.



Кілт қосу тапсырмасын жасау

6. Тапсырмалар тағайындалатын құрылғыларды таңдаңыз.



Тапсырма ауқымын көрсету

7. **Лицензия кілтін таңдау** шеберінің қадамында лицензия кілтін қосу үшін **Кілт қосу** сілтемесіне өтіңіз.

8. Кілт қосу тақтасында келесі параметрлердің бірін пайдаланып, лицензиялық кілт қосыңыз:

> **Бағдарламаны белсендіру** тапсырмасын жасағанға дейін басқару серверінің қоймасына лицензиялық кілтті қоспасаңыз ғана, лицензиялық кілтті қосу қажет.

- Белсендіру кодын енгізу үшін **Белсендіру кодын енгізу** параметрін таңдаңыз, содан кейін келесі әрекеттерді орындаңыз:

  a. Белсендіру кодын көрсетіңіз және **Жіберу** түймесін басыңыз.

  Лицензиялық кілт туралы ақпарат кілтті қосу тақтасында көрсетіледі.

  b. **Сақтау** түймесін басыңыз.

  > Лицензия кілтін басқарылатын құрылғыларға автоматты түрде таратуды қаласаңыз, **Лицензиялық кілтті басқарылатын құрылғыларға автоматты түрде тарату** параметрін қосыңыз.

  Кілт қосу тақтасы жабық.

- Кілт файлын қосу үшін **Кілт файлын қосу** параметрін таңдаңыз, содан кейін келесі әрекеттерді орындаңыз:

  a. **Кілт файлын таңдаңыз** түймесін басыңыз.

  b. Ашылған терезеде кілт файлын таңдап, **Ашу** түймесін басыңыз.

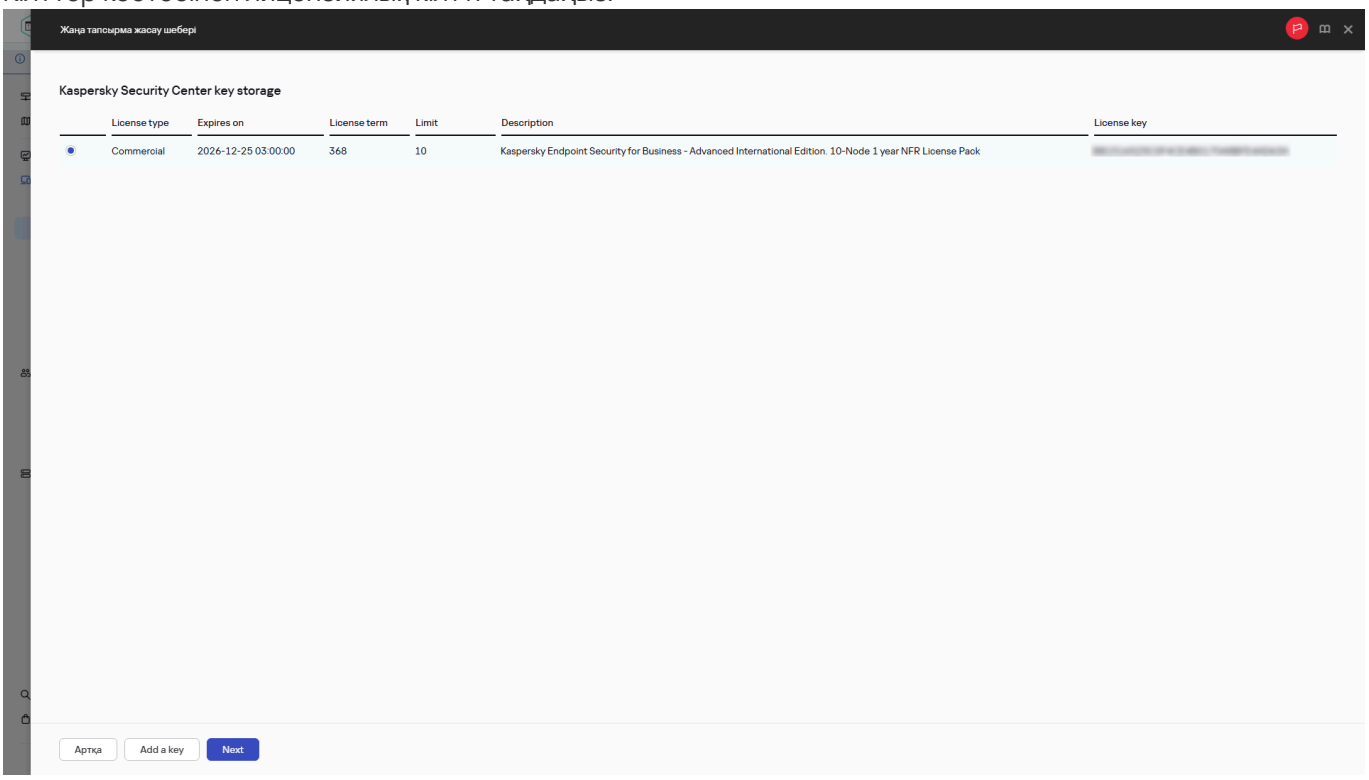
  Лицензиялық кілт туралы ақпарат лицензиялық кілтті қосу тақтасында көрсетіледі.

c. **Сақтау** түймесін басыңыз.

> Лицензиялық кілтті басқарылатын құрылғыларға автоматты түрде таратуды қаласаңыз, **Лицензиялық кілтті басқарылатын құрылғыларға автоматты түрде тарату** параметрін қосыңыз.

Кілт қосу тақтасы жабық.

9. Кілттер кестесінен лицензиялық кілтті таңдаңыз.

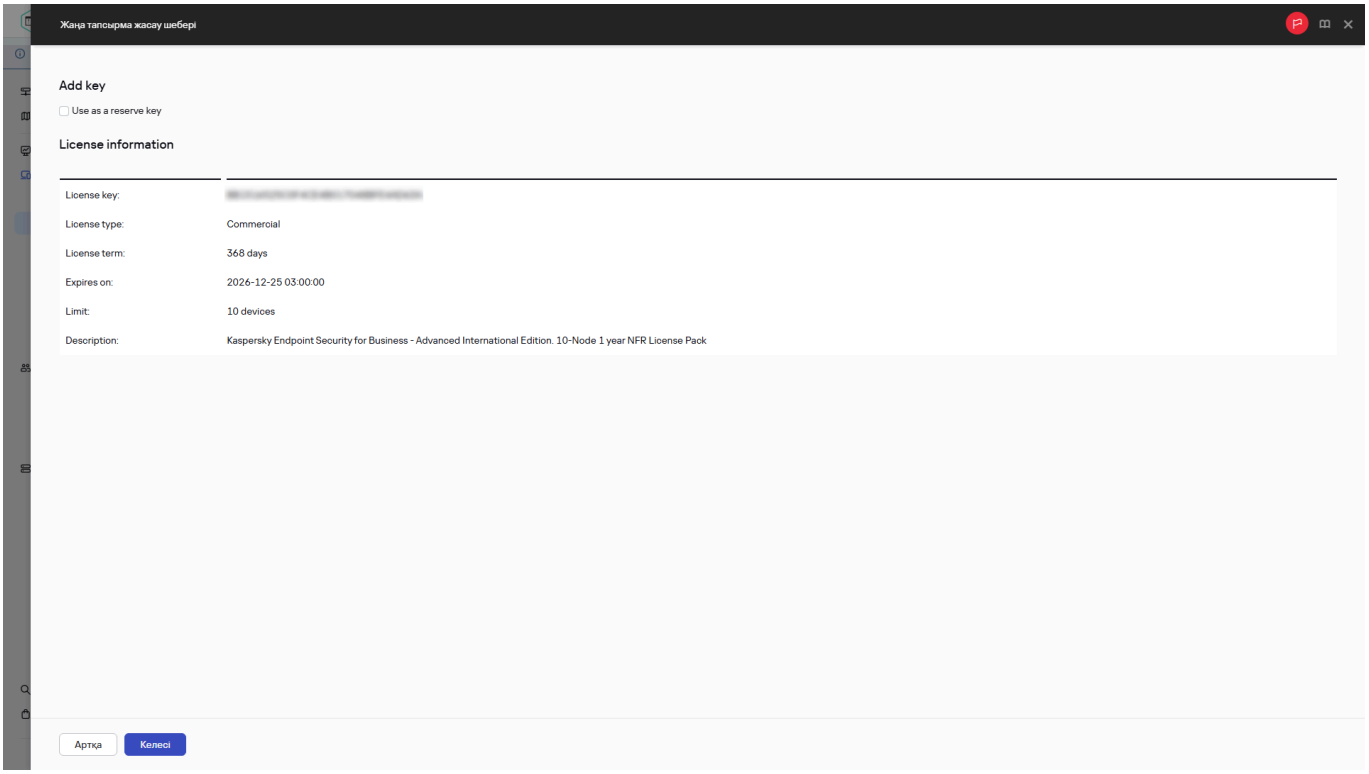


Лицензия кілтін таңдау

10. Шебердің **Лицензия туралы ақпарат** қадамында белсенді лицензия кілтін ауыстырғыңыз келсе, әдепкі **Резервтік лицензия кілті ретінде пайдалану** құсбелгі ұяшығын алып тастаңыз.

    Мысалы, бұл ұйымыңыз өзгергенде және құрылғыда басқа ұйымның кілті қажет болғанда немесе кілт қайта шығарылған болса және ағымдағы лицензияның мерзімі біткенге дейін жаңа лицензияның мерзімі бітетін болса қажет. Қателерге жол бермеу үшін **Резервтегі лицензия кілті ретінде пайдалану** жалаушасын алып тастаңыз.

Kaspersky Security Center қолданбасына кілт қосу кезінде туындауы мүмкін мәселелер және оларды шешу жолдары туралы көбірек білгіңіз келсе, Kaspersky Security Center білім қорын қараңыз.



Резервтік лицензия кілтін көрсету

11. **Тапсырманы жасауды аяқтау** қадамында **Жасап болған соң, тапсырма туралы мәліметтерді ашу** параметрін қоссаңыз, тапсырма параметрлерінің орнатылған әдепкі мәндерін өзгертуге болады.

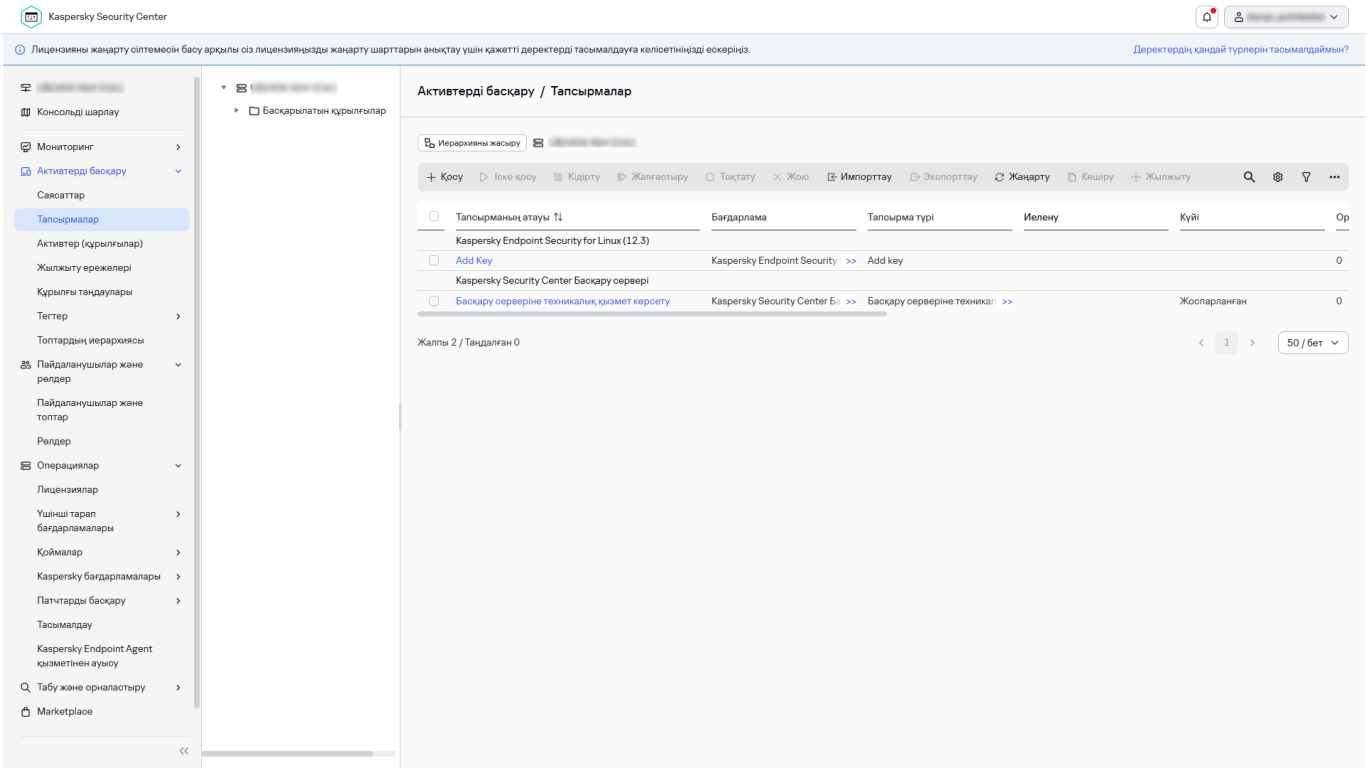
    Егер сіз бұл параметрді қоспасаңыз, тапсырма әдепкі бойынша белгіленген параметр мәндерімен жасалады. Орнатылған әдепкі параметрлер мәндерін кейінірек өзгертуге болады.

12. **Аяқтау** түймесін басыңыз.

    Шебер жұмысының нәтижесінде тапсырма жасалды. **Жасап болған соң, тапсырма туралы мәліметтерді ашу** параметрі қосулы болса, тапсырма параметрлерінің терезесі автоматты түрде ашылады. Бұл терезеде тапсырманың жалпы параметрлерін көрсетуге және қажет болса, тапсырма жасаған кезде көрсетілген параметрлерді өзгертуге болады.

Тапсырмалар тізіміндегі жасалған тапсырма атауын басу арқылы тапсырма сипаттарының терезесін ашуға да болады.

Тапсырма жасалып, орнатылып, тапсырмалар тізімінде көрсетіледі.



Тапсырмалар тізімі

13. Тапсырманы іске қосу үшін тапсырмалар тізімінен тапсырманы таңдап, **Іске қосу** түймесін басыңыз.

    Сондай-ақ тапсырма сипаттары терезесіндегі **Кесте** қойындысында тапсырманы іске қосу кестесін жасауға да болады.

    Кесте бойынша іске қосу параметрлерінің толық сипаттамасын тапсырманың жалпы параметрлерінен қараңыз.

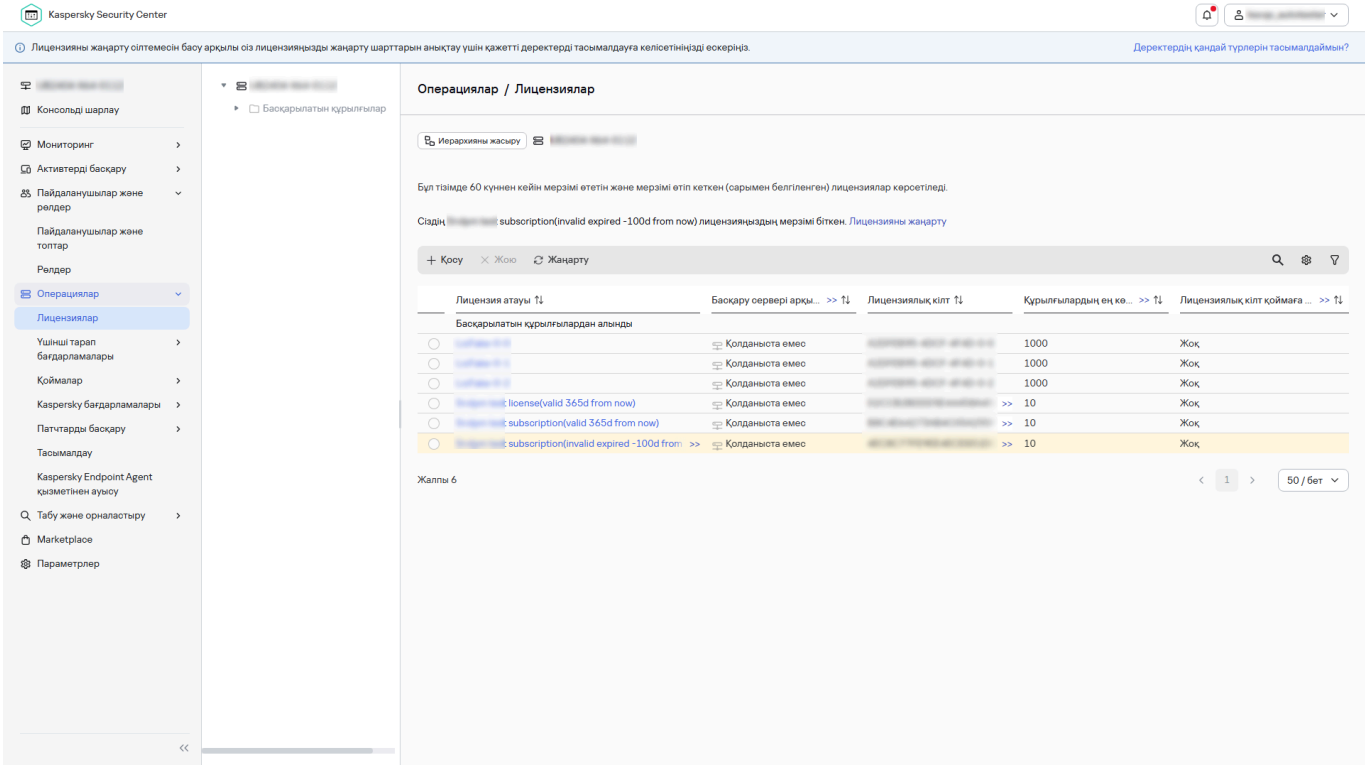
Тапсырманы аяқтағаннан кейін, лицензиялық кілт таңдалған құрылғыларға таратылады.

Лицензиялық кілтті автоматты түрде тарату

Kaspersky Security Center Linux бағдарламасы Басқару серверіндегі кілттер қоймасында орналастырылған лицензиялық кілттерді басқарылатын құрылғыларға автоматты түрде таратуға мүмкіндік береді.

Лицензиялық кілтті басқарылатын құрылғыларға автоматты түрде тарату үшін

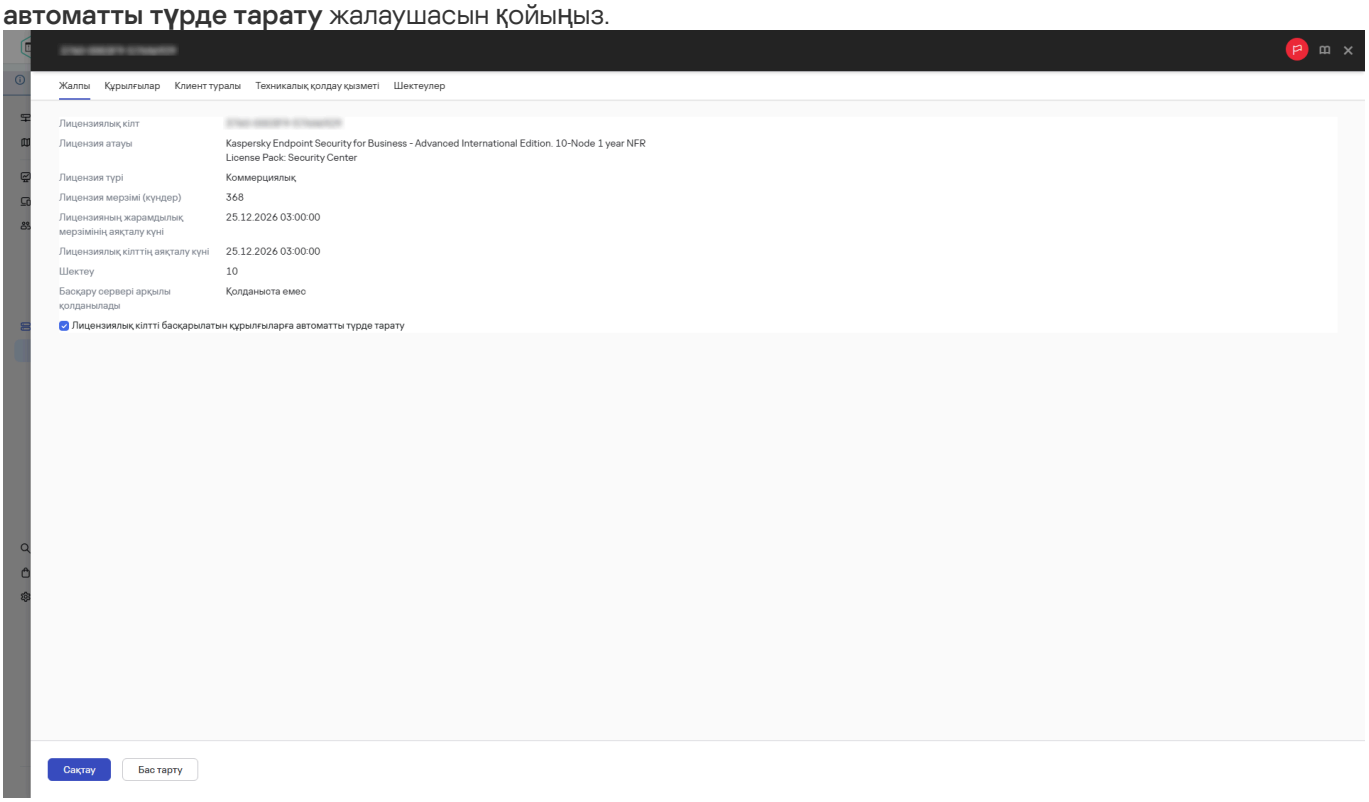
1. Бағдарламаның негізгі терезесінде **Операциялар** → **Лицензиялау** → **Лицензиялар** бөліміне өтіңіз.



Лицензиялар тізімі

2. Құрылғыларға автоматты түрде таратқыңыз келетін лицензиялық кілттің атауын түртіңіз.

3. Ашылған лицензиялық кілттің сипаттары терезесінде **Лицензиялық кілтті басқарылатын құрылғыларға автоматты түрде тарату** жалаушасын қойыңыз.



Лицензия кілтінің сипаттар терезесі

4. **Сақтау** түймесін басыңыз.

Лицензиялық кілт сай келетін құрылғыларға автоматты түрде таратылатын болады.

Лицензиялық кілтті тарату Желілік агенттің құралдарымен орындалады. Бұл арада, бағдарлама үшін резервттегі лицензиялық кілтті тарату тапсырмалары жасалмайды.

Лицензиялық кілтті автоматты түрде тарату кезінде құрылғылар санына қойылатын лицензиялық шектеу ескеріледі. Лицензиялық шектеу лицензиялық кілттің сипаттарында белгіленген. Егер лицензиялық шектеуге қол жеткізілсе, лицензиялық кілтті құрылғыларға тарату автоматты түрде тоқтатылады.

Келесі жағдайларда автоматты түрде таратылатын лицензиялық кілт виртуалды Басқару серверінің қоймасында көрінбеуі мүмкін екенін ескеріңіз:

- Лицензиялық кілт бағдарлама үшін жарамсыз.
- Виртуалды Басқару серверінде басқарылатын құрылғылар жоқ.
- Лицензиялық кілт басқа виртуалды Басқару сервері басқаратын құрылғылар үшін әлдеқашан қолданыста және құрылғылар санының лицензиялық шегіне жетті.

Виртуалды Басқару сервері лицензиялық кілттерді өзінің қоймасынан және Басқару сервері қоймасынан автоматты түрде таратады. Ұсынылады:

- Құрылғыларға қолданғыңыз келетін лицензия кілтін таңдау үшін *Лицензия кілтін қосу* тапсырмасын пайдаланыңыз.
- Виртуалды Басқару серверінің параметрлеріндегі **Осы виртуалды Басқару серверінен өзінің құрылғыларына лицензиялық кілттерді автоматты түрде орналастыруға рұқсат беру** параметрін өшірмеңіз. Әйтпесе, виртуалды Басқару сервері лицензиялық кілттерді құрылғыларға, соның ішінде Басқару сервері қоймасынан лицензиялық кілттерді таратпайды.

Лицензиялық кілт сипаттары терезесінде **Лицензиялық кілтті басқарылатын құрылғыларға автоматты түрде тарату** жалаушасын қойылған болса, лицензиялық кілт сіздің желіңізде дереу таратылатын болады. Бұл параметрді таңдамасаңыз, лицензия кілтін тарату тапсырмасын кейінірек пайдалануға болады.

Негізгі Басқару серверінде конфигурацияланған лицензия кілттерін автоматты түрде тарату виртуалды емес қосалқы Басқару серверлері басқаратын құрылғыларды қамтымайды.

Қолданылатын лицензиялық кілттер туралы ақпаратты қарап шығу

Басқару сервері қоймасына қосылған лицензиялық кілттердің тізімін көру үшін:

Бағдарламаның негізгі терезесінде **Операциялар** → **Лицензиялау** → **Лицензиялар** бөліміне өтіңіз.

Басқару сервері қоймасына қосылған кілт файлдары мен белсендіру кодтарының тізімі көрсетіледі.

Лицензиялық кілт туралы толық ақпаратты көру үшін:

1. Бағдарламаның негізгі терезесінде **Операциялар** → **Лицензиялау** → **Лицензиялар** бөліміне өтіңіз.
2. Қажетті лицензиялық кілттің атын басыңыз.

Ашылған лицензиялық кілттің сипаттары терезесінде сіз келесіні көре аласыз:

- **Жалпы** қойыншасында – лицензиялық кілт туралы негізгі ақпарат.
- **Құрылғылар** қойыншасында – орнатылған Kaspersky бағдарламасын белсендіру үшін лицензиялық кілт қолданылған клиент құрылғыларының тізімі.
- **Шектеулер** қойындысында — лицензия шектеулерінің тізімі

  Басқару серверін Kaspersky Security: Бизнеске арналған Кәсіби лицензиясы бойынша белсендірсеңіз, **Шектеулер** қойындысында **Қосылған XDR-О** өрісі көрсетіледі.

Таңдалған клиент құрылғысында қандай лицензиялық кілттердің жиі кездесетінін көру үшін:

1. Бағдарламаның негізгі терезесінде **Активтерді басқару** → **Активтер (құрылғылар)** бөліміне өтіңіз.
2. Қажетті құрылғының атауын басыңыз.
3. Ашылған құрылғы сипаттары терезесінде **Бағдарламалар** қойыншасын таңдаңыз.

4. Таратылған лицензиялық кілт туралы ақпаратты көргіңіз келетін бағдарламаның атауын басыңыз.

5. Ашылған бағдарлама сипаттары терезесінде **Жалпы** қойыншасына өтіп, **Лицензия** бөлімін ашыңыз.

Белсенді және сақтық лицензиялық кілттер туралы негізгі ақпарат көрсетіледі.

Виртуалды Басқару серверінің лицензиялық кілттерінің өзекті параметрлерін анықтау үшін Басқару сервері тәулігіне бір реттен сиретпей Kaspersky белсендіру серверлеріне сұрау жібереді. Жүйелік DNS арқылы серверлерге қатынасу мүмкін болмаса, бағдарлама жалпыға ортақ DNS серверлерін пайдаланады.

Лицензия шектеуден асып кету оқиғалары

Kaspersky Security Center Linux, клиент құрылғыларында орнатылған Kaspersky бағдарламаларының лицензия шектеулерінен асып кету оқиғалары туралы ақпарат алуға мүмкіндік береді.

Лицензия шектеуден асып кету туралы оқиғалардың маңыздылық деңгейі мынадай ережелер бойынша айқындалады:

- Бір лицензияның пайдаланылатын лицензиялық бірліктерінің саны осы лицензияның лицензиялық бірліктерінің жалпы санының 90%–100% аралығында болса, **Ақпараттық хабарлар** маңыздылық деңгейі бар оқиға жарияланады.

- Бір лицензияның пайдаланылатын лицензиялық бірліктерінің саны осы лицензияның лицензиялық бірліктерінің жалпы санының 100%–110% аралығында болса, **Ескерту** маңыздылық деңгейі бар оқиға жарияланады.

- Бір лицензияның пайдаланылатын лицензиялық бірліктерінің саны осы лицензияның лицензиялық бірліктерінің жалпы санының 110%-нан асатын болса, **Критикалық оқиға** маңыздылық деңгейі бар оқиға жарияланады.

Лицензиялық кілтті қоймадан жою

Басқарылатын құрылғыларға таратылған белсенді лицензиялық кілт жойылған кезде, бағдарламалар басқарылатын құрылғыларда жұмысын жалғастырады.

Басқару сервері қоймасынан кілт файлын немесе белсендіру кодын жою үшін:

1. Басқару сервері сіз жойғыңыз келетін кілт немесе белсендіру кодын пайдаланбайтынына көз жеткізіңіз. Басқару сервері осындай кілтті қолданса, сіз кілтті жоя алмайсыз. Тексеруді орындау үшін:

   a. Негізгі мәзірдегі басқару серверінің атауын басыңыз.

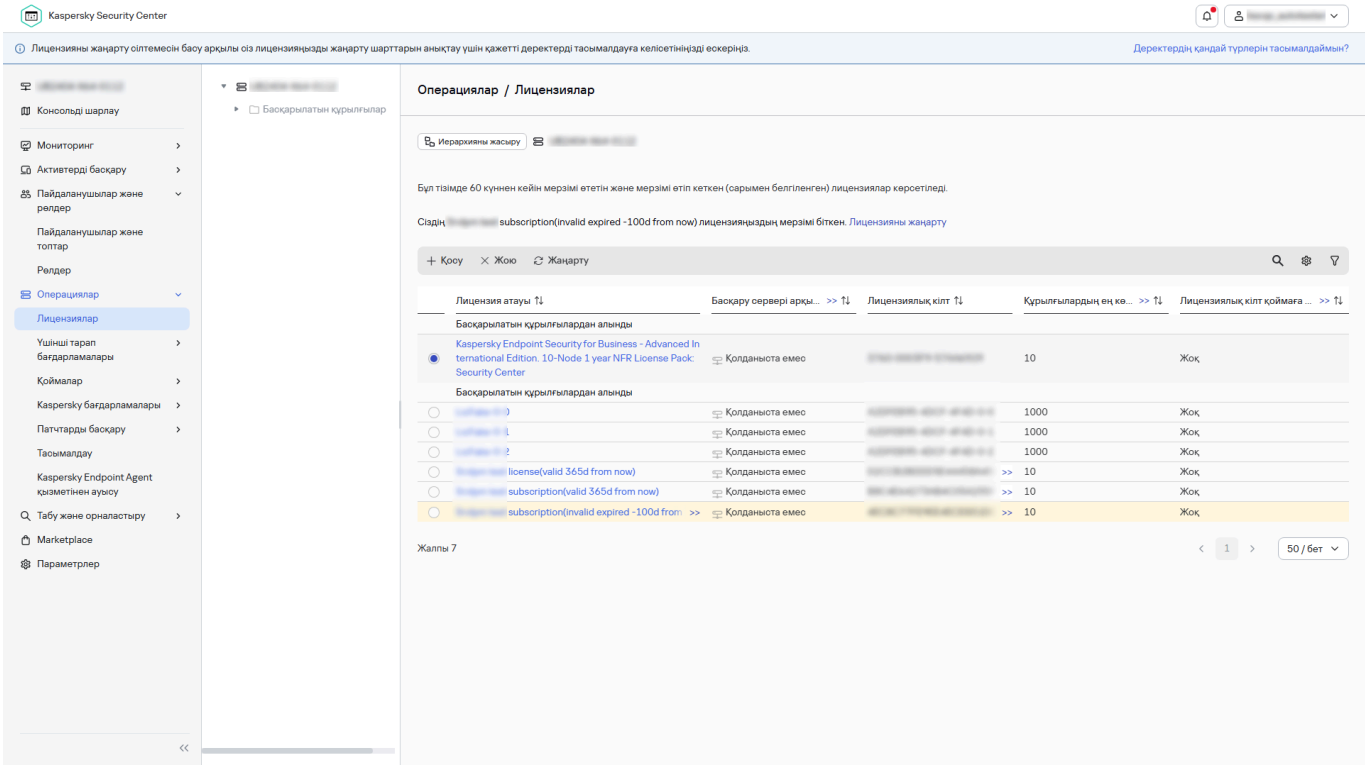
      Басқару серверінің сипаттары терезесі ашылады.

b. **Жалпы** қойыншасында **Лицензиялық кілттер** бөлімін таңдаңыз.

c. Егер ашылған бөлімде қажетті кілт файлы немесе белсендіру коды көрсетілсе, **Белсенді кілтті жою** түймесін басып, операцияны растаңыз. Осыдан кейін, Басқару сервері қашықтағы лицензиялық кілтті пайдаланбайды, кілт Басқару сервері қоймасында қалады. Егер қажетті кілт файлы немесе белсендіру коды көрсетілмесе, Басқару сервері оны пайдаланбайды.

2. Бағдарламаның негізгі терезесінде **Операциялар** → **Лицензиялау** → **Лицензиялар** бөліміне өтіңіз.

3. Қажетті кілт файлын немесе белсендіру кодын таңдап, **Жою** түймесін басыңыз.



Лицензиялар тізімі

Таңдалған кілт файлы немесе белсендіру коды қоймадан жойылады.

Жойылған лицензиялық кілтті қайта қосуға немесе басқа лицензиялық кілтті қосуға болады.

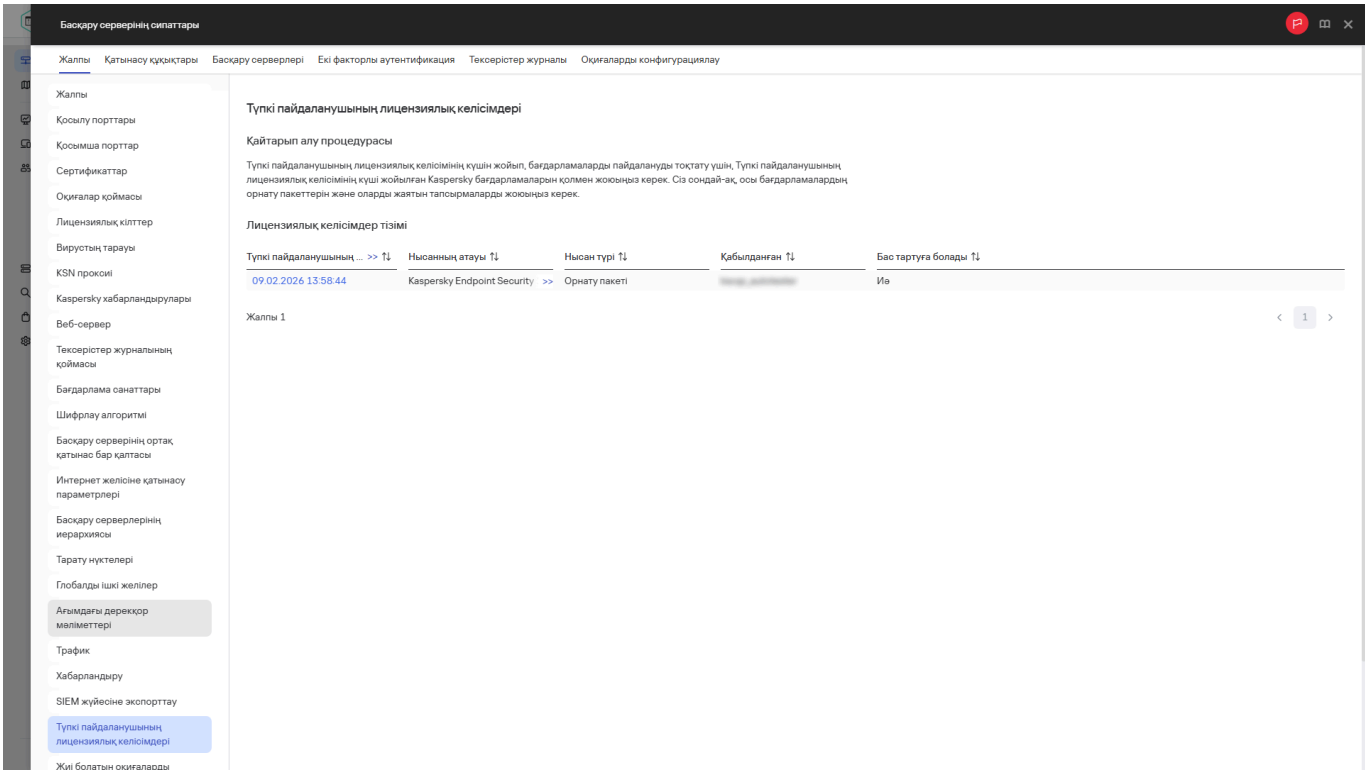
Лицензиялық келісімге берілген келісімді кері қайтарып алу

Егер сіз кейбір клиент құрылғыларын қорғауды тоқтатуды шешсеңіз, Kaspersky кез келген басқарылатын бағдарламасы үшін Лицензиялық келісімді кері қайтарып ала аласыз. Лицензиялық келісімді қайтарып алмас бұрын таңдалған бағдарламаны жою керек.

Kaspersky басқарылатын бағдарламалары үшін Лицензиялық келісімді кері қайтарып алу үшін:

1. Басқару сервері сипаттары терезесін ашып, **Жалпы** қойындысында **Түпкі пайдаланушының лицензиялық келісімдері** бөлімін таңдаңыз.

Орнату пакеттерін жасау, жаңартуларды орнату немесе Kaspersky Security for Mobile қолданбасын орналастыру кезінде қабылданған Лицензиялық келісімдердің тізімі көрсетіледі.



EULA тізімі

2. Тізімнен қайтарып алғыңыз келетін Лицензиялық келісімдерді таңдаңыз.

   Лицензиялық келісімдердің келесі сипаттарын көруге болады:

   - Лицензиялық келісімді қабылдау күні.
   - Лицензиялық келісімді қабылдаған пайдаланушы аты.

3. Келесі деректерді көрсететін сипаттар терезесін ашу үшін кез келген Лицензиялық келісімнің қабылданған күнін басыңыз:

   - Лицензиялық келісімді қабылдаған пайдаланушы аты.
   - Лицензиялық келісімді қабылдау күні.
   - Лицензиялық келісімнің бірегей идентификаторы (UID).
   - Лицензиялық келісімнің толық мәтіні.
   - Лицензиялық келісімге қатысты нысандардың тізімі (орнату пакеттері, жаңартулар, ұялы қолданбалар) және олардың тиісті атаулары мен түрлері.

4. Лицензиялық келісімнің сипаттары терезесінің төменгі жағында **Лицензиялық келісімді қайтару** түймесін басыңыз.

   Лицензиялық келісімді қайтарып алуға мүмкіндік бермейтін қандай да бір нысандар (орнату пакеттері және олардың тиісті тапсырмалары) болса, тиісті хабарландыру көрсетіледі. Сіз бұл нысандарды жоймайынша, қайтарып алуды жалғастыра алмайсыз.

Ашылған терезеде алдымен осы Лицензиялық келісімге сәйкес келетін Kaspersky бағдарламасын жою қажет екендігі туралы хабар көрсетіледі.

5. Лицензияны қайтарып алуды растайтын түймесін басыңыз.

Лицензиялық келісім қайтарып алынды. Лицензиялық келісім енді **Түпкі пайдаланушының лицензиялық келісімдері** бөліміндегі Лицензиялық келісімдер тізімінде көрсетілмейді. Лицензиялық келісімнің сипаттары терезесі жабылады; бағдарлама енді орнатылмайды.

Kaspersky бағдарламалары лицензиясының әрекет ету мерзімін ұзарту

Сіз мерзімі біткен немесе жақын арада аяқталатын (30 күннен аз) Kaspersky бағдарламасының лицензиясының жарамдылық мерзімін ұзарта аласыз.

Жарамдылық мерзімі жақын арада аяқталатын немесе аяқталған лицензияның мерзімін ұзарту үшін:

1. Келесі әрекеттердің бірін орындаңыз:

   - Бағдарламаның негізгі терезесінде **Операциялар** → **Лицензиялау** → **Лицензиялар** бөліміне өтіңіз.
   - Бағдарламаның негізгі терезесінде **Мониторинг** → **Бақылау тақтасы** бөліміне өтіңіз және хабарландырудың жанындағы **Жарамдылық мерзімі өтіп кеткен лицензияларды қарау** сілтемесінен өтіңіз.

   Лицензиялар терезесі ашылып, онда лицензияның жарамдылық мерзімін қарай аласыз және ұзарта аласыз.

2. Қажетті лицензияның жанындағы **Лицензияны жаңарту** сілтемесінен өтіңіз.

   Лицензияның жарамдылық мерзімін ұзарту сілтемесін басу арқылы сіз Kaspersky бағдарламасына келесі Kaspersky Security Center Linux деректерін беруге келісесіз: сіз қолданатын нұсқа, локализация, бағдарламалық жасақтама лицензиясының идентификаторы (яғни сіз мерзімін ұзартып жатқан лицензия идентификаторы), сондай-ақ сіз лицензияны серіктес компания арқылы сатып алдыңыз ба, жоқ па.

3. Лицензияның жарамдылық мерзімін ұзартудың ашылған терезесінде нұсқауларды орындаңыз.

   Лицензияның жарамдылық мерзімі ұзартылды.

Kaspersky Security Center Web Console бағдарламасында хабарландырулар лицензияның жарамдылық мерзімінің аяқталуы келесі кесте бойынша жақындаған кезде көрсетіледі:

- жарамдылық мерзімінің аяқталу күніне дейін 30 күн бұрын;
- жарамдылық мерзімінің аяқталу күніне дейін 7 күн бұрын;
- жарамдылық мерзімінің аяқталу күніне дейін 3 күн бұрын;
- жарамдылық мерзімінің аяқталу күніне дейін 24 сағат бұрын;
- лицензия мерзімі өтіп кеткен кезде.

Бизнес шешімдерін таңдау үшін Kaspersky Marketplace пайдалану

Marketplace – Kaspersky бизнес-шешімдерінің барлық спектрін көруге, өзіңізге қажет шешімдерді таңдауға және Kaspersky сайтында сатып алуға өтуге мүмкіндік беретін бас мәзір бөлімі. Сіз сүзгілерді ұйымыңызға және ақпараттық қауіпсіздік жүйеңіздің талаптарына сәйкес келетін шешімдерді ғана көру үшін пайдалана аласыз. Шешімді таңдаған кезде, Kaspersky Security Center Linux бағдарламасы сізді Kaspersky веб-сайтындағы тиісті бетке қайта бағыттайды, осылайша сіз шешім туралы көбірек біле алатын боласыз. Әрбір веб-бет сатып алуға өтуге мүмкіндік береді немесе сатып алу процесі туралы нұсқауларды қамтиды.

Marketplace бөлімінде Kaspersky шешімдерін келесі критерийлер бойынша сүзуге болады:

- Сіз қорғағыңыз келетін құрылғылардың саны (соңғы нүктелер, серверлер және активтердің басқа түрлері):
  - 50–250
  - 250–1000
  - 1000-нан артық
- Сіздің ұйымыңыздың ақпараттық қауіпсіздік тобының тәжірибе деңгейі:
  - **Foundations**

    Бұл деңгей тек АТ командасы бар кәсіпорындарға тән. Қауіптердің ең көп саны автоматты түрде бұғатталады.
  - **Optimum**

    Бұл деңгей АТ командасында нақты АТ қауіпсіздік функциясы бар кәсіпорынға тән. Бұл деңгейде компаниялар қолданыстағы алдын алу тетіктерін айналып өту үшін тауарлық қауіптер мен қауіптерге қарсы тұруға мүмкіндік беретін шешімдерді қажет етеді.
  - **Expert**

    Бұл деңгей күрделі және таратылған АТ ортасы бар кәсіпорындарға тән. АТ қауіпсіздік тобы тәжірибелі мамандардан тұрады немесе компанияда SOC (Security Operations Center) тобы бар. Қажетті шешімдер компанияларға кешенді қауіптер мен мақсатты шабуылдарға қарсы тұруға мүмкіндік береді.
- Қорғағыңыз келетін актив түрлері:
  - **Соңғы нүктелер**: қызметкерлердің жұмыс станциялары, физикалық және виртуалды машиналар, кіріктірілетін жүйелер.
  - **Серверлер**: физикалық және виртуалды серверлер.
  - **Cloud**: жария, жеке немесе гибридті бұлтты орталар; бұлттық қызметтер.
  - **Желі**: жергілікті желі, АТ инфрақұрылымы.
  - **Қызмет**: Kaspersky ұсынатын қауіпсіздікпен байланысты қызметтер.

Kaspersky бизнес шешімін табу және сатып алу үшін:

1. Бағдарламаның негізгі терезесінде **Marketplace** бөліміне өтіңіз.

   Әдепкі бойынша, бөлімде Kaspersky барлық қолжетімді бизнес-шешімдері көрсетіледі.

2. Ұйымыңызға сәйкес келетін шешімдерді ғана көру үшін сүзгілердегі қажетті мәндерді таңдаңыз.

3. Сатып алғыңыз келетін немесе көбірек білгіңіз келетін шешімді басыңыз.

Сіз шешімнің веб-бетіне қайта бағытталасыз. Сатып алуға өту үшін экрандағы нұсқауларды орындаңыз.

Kaspersky қолданбаларын конфигурациялау

Бұл бөлімде саясат пен тапсырмаларды қолмен конфигурациялау туралы, пайдаланушы рөлдері туралы, басқару топтарының құрылымын құру туралы және тапсырмалар иерархиясы туралы ақпарат бар.

Сценарий: Желі қорғанысын конфигурациялау

Бағдарламаны жылдам іске қосу шебері әдепкі бойынша параметрлері бар саясаттар мен тапсырмаларды жасайды. Бұл параметрлер ұйымда оңтайлы емес немесе тіпті тыйым салынған болуы мүмкін. Сондықтан, осы саясаттар мен тапсырмаларды конфигурациялау және сіздің желіңіз үшін қажет болса, қосымша саясаттар мен тапсырмаларды жасау ұсынылады.

Алдын ала талаптар

Бастамас бұрын, келесі әрекеттерді орындағаныңызға көз жеткізіңіз:

- Kaspersky Security Center Linux Басқару серверін орнаттыңыз
- Kaspersky Security Center Web Console веб-консолін орнаттыңыз
- Kaspersky Security Center Linux орнатудың негізгі сценарийі аяқталған
- Бағдарламаны жылдам іске қосу шебері аяқталды немесе келесі саясаттар мен тапсырмалар **Басқарылатын құрылғылар** басқару тобында қолмен жасалған:
  - Kaspersky Endpoint Security саясаты
  - Kaspersky Endpoint Security жаңарту топтық тапсырмасы
  - Желілік агент саясаты
  - *Осалдықтарды және қажетті жаңартуларды іздеу* тапсырмасы

Кезеңдер

Желі қорғанысын конфигурациялау келесі кезеңдерден тұрады:

1. **Kaspersky бағдарламалары үшін саясаттар мен саясат профильдерін конфигурациялау және тарату**

   Басқарылатын құрылғыларда орнатылған Kaspersky бағдарламаларының параметрлерін конфигурациялау және тарату үшін қауіпсіздікті басқарудың екі түрлі тәсілдемесін қолдануға болады: пайдаланушыға бағытталған және құрылғыға бағытталған. Осы екі тәсілдемені біріктіруге болады.

2. **Kaspersky бағдарламаларын қашықтан басқару үшін тапсырмаларды конфигурациялау**

Бағдарламаны жылдам іске қосу шеберімен жасалған тапсырмаларды тексеріп, қажет болған жағдайда олардың параметрлерін оңтайландырыңыз.

Нұсқаулар: Kaspersky Endpoint Security үшін топтық жаңарту тапсырмасын орнату, Осалдықтарды және қажетті жаңартуларды іздеу тапсырмасын жасау.

Қажет болса, клиент құрылғыларында орнатылған Kaspersky бағдарламаларын басқарудың қосымша тапсырмаларын жасаңыз.

3. **Дерекқорға оқиғаларды жүктеуді бағалау және шектеу**

   Басқарылатын қолданбалар жұмысы кезінде пайда болатын оқиғалар туралы ақпарат клиент құрылғысынан тасымалданады және басқару серверінің дерекқорына тіркеледі. Басқару серверіне түсетін жүктемені азайту үшін дерекқорда сақталуы мүмкін оқиғалардың ең көп санын бағалаңыз және шектеңіз.

   Нұсқаулар: Оқиғалар қоймасындағы оқиғалар санын конфигурациялау.

Нәтижелер

Осы сценарий аяқталғаннан кейін, сіздің желіңіз Kaspersky бағдарламаларын, Басқару сервері алатын тапсырмалар мен оқиғаларды конфигурациялау арқылы қорғалады:

- Kaspersky бағдарламалары саясаттар мен саясат профильдеріне сай конфигурацияланған.
- Бағдарламаларды басқару тапсырмалар жиынтығының көмегімен жүзеге асырылады.
- Дерекқорда сақталуы мүмкін оқиғалардың ең көп саны белгіленген.

Желі қорғанысын конфигурациялап болғаннан кейін, сіз Kaspersky бағдарламалары мен дерекқорының тұрақты емес жаңартуларын конфигурациялауға кірісе аласыз.

Құрылғыларға және пайдаланушыларға бағытталған қауіпсіздікті басқару тәсілдемелері

Қауіпсіздік параметрлерін құрылғының функциялары мен пайдаланушы рөлдері жайғасымынан басқаруға болады. Бірінші тәсілдемесі *құрылғыларға бағытталған қауіпсіздікті басқару*, екіншісі тәсілдемесі *пайдаланушыларға бағытталған қауіпсіздікті басқару* деп аталады. Қолданбалардың әртүрлі параметрлерін әртүрлі құрылғыларға қолдану үшін, сіз тіркесімдегі бір немесе екі басқару түрін қолдана аласыз.

Құрылғыға бағытталған қауіпсіздікті басқару құрылғының ерекшеліктеріне байланысты басқарылатын құрылғыларға қауіпсіздік бағдарламасының әртүрлі параметрлерін қолдануға мүмкіндік береді. Мысалы, әртүрлі басқару топтарында орналасқан құрылғыларға әртүрлі параметрлерді қолдануға болады.

Пайдаланушыға бағытталған қауіпсіздікті басқару қауіпсіздік бағдарламаларының әртүрлі параметрлерін әртүрлі пайдаланушы рөлдеріне қолдануға мүмкіндік береді. Сіз бірнеше пайдаланушы рөлдерін жасай аласыз, әр пайдаланушыға сәйкес келетін пайдаланушы рөлін тағайындай аласыз және әртүрлі рөлдері бар пайдаланушыларға тиесілі құрылғылар үшін әртүрлі бағдарлама параметрлерін анықтай аласыз. Мысалы, бағдарламалардың әртүрлі параметрлерін бухгалтерлердің құрылғыларына және кадрлар бөлімі мамандарының құрылғыларына қатысты қолдануға болады. Пайдаланушыларға бағытталған қауіпсіздікті басқаруды енгізу нәтижесінде, әрбір бөлім – бухгалтерия бөлімі мен кадрлар бөлімі – Kaspersky бағдарламаларымен жұмыс істеуге арналған параметрлердің өзіндік конфигурациясын алады. Параметрлер конфигурациясы бағдарламаның қандай параметрлерін пайдаланушылар өзгерте алатынын, ал қайсысын әкімші мәжбүрлеп орнатып, бұғаттай алатынын анықтайды.

Пайдаланушыларға бағытталған қауіпсіздікті басқару жекелеген пайдаланушылар үшін белгіленген қолданба параметрлерін қолдануға мүмкіндік береді. Бұл, қызметкерге ұйымда бірегей рөл тағайындалса немесе белгілі бір қызметкерге қатысты қауіпсіздік мәселелерін бақылау керек болса, қажет болуы мүмкін. Бұл қызметкердің компаниядағы рөліне байланысты, бағдарламаның параметрлерін өзгерту үшін, оның құқықтарын кеңейтуге немесе қысқартуға болады. Мысалы, жергілікті кеңседе клиент құрылғыларын басқаратын жүйелік әкімшінің құқықтарын кеңейту қажет болуы мүмкін.

Сондай-ақ, сіз пайдаланушыларға бағытталған және құрылғыларға бағытталған қауіпсіздікті басқару тәсілдемелерін біріктіре аласыз. Мысалы, әрбір басқару тобы үшін әртүрлі саясаттарды конфигурациялауға, содан кейін ұйымыңыздың бір немесе бірнеше пайдаланушы рөлі үшін саясат профильдерін қосымша түрде жасауға болады. Бұл жағдайда, саясаттар мен саясат профильдері келесі тәртіпте қолданылады:

1. Құрылғыларға бағытталған қауіпсіздікті басқару үшін жасалған саясаттар қолданылады.
2. Олар саясат профильдерінің параметрлеріне сәйкес саясат профильдерімен түрлендіріледі.
3. Саясаттар пайдаланушы рөлдерімен байланысты саясат профильдерімен түрлендіріледі.

Саясаттарды конфигурациялау және тарату: құрылғыларға бағытталған тәсілдеме

Осы сценарий аяқталғаннан кейін, қолданбалар сіз анықтайтын қолданба саясаттары мен саясат профильдеріне сәйкес барлық басқарылатын құрылғыларда конфигурацияланады.

Алдын ала талаптар

Kaspersky Security Center Linux Басқару серверін және Kaspersky Security Center Web Console веб-консолін орнатқаныңызға көз жеткізіңіз. Сондай-ақ, пайдаланушыға бағытталған қауіпсіздікті басқаруды балама немесе қосымша мүмкіндік ретінде қарастырғыңыз келуі мүмкін. Басқарудың екі тәсілдемесі туралы көбірек біліңіз.

Кезеңдер

Құрылғыларға бағытталған Kaspersky бағдарламаларын басқару сценарийі келесі қадамдарды қамтиды:

1. **Бағдарламалар саясаттарын конфигурациялау**

   Әр бағдарлама үшін саясат жасау арқылы басқарылатын құрылғыларда орнатылған Kaspersky бағдарламаларының параметрлерін конфигурациялаңыз. Бұл саясат жиынтығы клиент құрылғыларына қолданылады.

   Бағдарламаны жылдам іске қосу шебері арқылы желі қорғанысын конфигурациялау кезінде Kaspersky Security Center Linux бағдарламасы келесі бағдарламалар үшін әдепкі бойынша саясатты жасайды:

   - Kaspersky Endpoint Security for Linux – Linux операциялық жүйесі бар клиент құрылғылары үшін
   - Kaspersky Endpoint Security for Windows – Windows операциялық жүйесі бар клиент құрылғылары үшін

Егер сіз осы шебердің көмегімен конфигурациялау процесін аяқтаған болсаңыз, сізге бұл бағдарлама үшін жаңа саясат жасаудың қажеті жоқ.

Егер сізде бірнеше Басқару серверінің және/немесе басқару топтарының иерархиялық құрылымы болса, қосалқы Басқару серверлері мен еншілес басқару топтары саясатты әдепкі бойынша негізгі Басқару серверінен иеленеді. Саясат параметрлерін иерархия бойынша төмен қарай өзгертуге тыйым салу үшін параметрлерді еншілес топтар мен қосалқы Басқару серверлеріне мәжбүрлеп иелендіруге болады. Егер сіз параметрлердің тек бір бөлігін иеленуге рұқсат бергіңіз келсе, оларды саясат иерархиясы бойынша жоғары деңгейде құлыптай аласыз. Басқа құлыпталмаған параметрлер иерархия бойынша төменгі саясатты өзгерту үшін қолжетімді болады. Құрылған саясат иерархиясы басқару топтарындағы құрылғыларды тиімді басқаруға мүмкіндік береді.

Нұсқаулар: саясатты жасау

2. **Саясат профильдерін жасау (қажет болса)**

Егер сіз бір басқару тобындағы құрылғыларға әртүрлі саясат параметрлерін қолданғыңыз келсе, сол құрылғылар үшін саясат профильдерін жасаңыз. Саясат профилі, саясат параметрлерінің аталған ішкі жиынтығы болып табылады. Параметрлердің осы ішкі жиынтығы құрылғыларға саясатпен бірге таралады және келесі шартты – *профильді белсендіру шартын* орындаған кезде саясатты толықтырады. Профильдер басқарылатын құрылғыда әрекет ететін "негізгі" саясаттан ерекшеленетін параметрлерді ғана қамтиды.

Профильді белсендіру шарттарын пайдалана отырып, әртүрлі саясат профильдерін қолдануға болады, мысалы, арнайы бағдарламалық жасақтама конфигурациясы немесе берілген тегтері бар құрылғыларға. Белгілі бір өлшемшарттарға сәйкес келетін құрылғыларды сүзгілеу үшін тегтерді пайдаланыңыз. Мысалы, сіз *CentOS* тегін жасай аласыз, оны CentOS операциялық жүйесі басқаратын барлық құрылғыларға тағайындай аласыз, содан кейін бұл тегті саясат профилін белсендіру ережелерінде көрсете аласыз. Нәтижесінде, CentOS операциялық жүйесі басқаратын құрылғыларда орнатылған Kaspersky бағдарламалары өздерінің саясат профилімен басқарылатын болады.

Нұсқаулар:

- Саясат профилін жасау
- Саясатын профилін белсендіру ережесін жасау

3. **Саясаттар мен саясат профильдерін басқарылатын құрылғыларға тарату**

Әдепкі бойынша, басқарылатын құрылғыларды Басқару серверімен синхрондау 15 минут сайын бір рет жүзеге асырылады. Синхрондау кезінде басқарылатын құрылғыларға жаңа немесе өзгертілген саясат пен саясат профильдері қолданылады. Автоматты синхрондауды өткізіп жіберіп, синхрондауды Мәжбүрлеп синхрондау пәрмені арқылы қолмен іске қосуға болады. Синхрондау аяқталғаннан кейін, саясаттар мен саясат профильдері жеткізіліп, Kaspersky белгіленген бағдарламаларына қолданылады.

Саясаттар мен саясат профильдерінің құрылғыға жеткізілгенін тексеруге болады. Kaspersky Security Center Linux бағдарламасы құрылғының сипаттарында жеткізу күні мен уақытын анықтайды.

Нұсқаулар: Мәжбүрлеп синхрондау.

Нәтижелер

Құрылғыларға бағытталған сценарий аяқталғаннан кейін, Kaspersky бағдарламалары саясат иерархиясы арқылы көрсетілген және таралған параметрлерге сәйкес конфигурацияланады.

Бағдарлама саясаттары мен саясат профильдері басқару топтарына қосылған жаңа құрылғыларға автоматты түрде қолданылады.

Саясаттарды конфигурациялау және тарату: пайдаланушыларға бағытталған тәсілдеме

Бұл бөлімде басқарылатын құрылғыларда орнатылған Kaspersky бағдарламаларын орталықтандырылған конфигурациялауға арналған пайдаланушыға бағытталған сценарий сипатталған. Осы сценарий аяқталғаннан кейін, бағдарламалар сіз анықтайтын бағдарлама саясаттары мен саясат профильдеріне сәйкес барлық басқарылатын құрылғыларда конфигурацияланады.

Алдын ала талаптар

Kaspersky Security Center Linux Басқару серверін және Kaspersky Security Center Web Console веб-консолін сәтті орнатқаныңызға және негізгі орналастыру сценарийін аяқтағаныңызға көз жеткізіңіз. Сондай-ақ, құрылғыға бағытталған қауіпсіздікті басқаруды пайдаланушыға бағытталған тәсілдемеге балама немесе қосымша мүмкіндік ретінде қарастырғыңыз келуі мүмкін. Басқарудың екі тәсілдемесі туралы көбірек біліңіз.

Процесс

Пайдаланушыға бағытталған Kaspersky бағдарламаларын басқару сценарийі келесі қадамдарды қамтиды:

1. **Бағдарламалар саясаттарын конфигурациялау**

   Әр бағдарлама үшін саясат жасау арқылы басқарылатын құрылғыларда орнатылған Kaspersky бағдарламаларының параметрлерін конфигурациялаңыз. Бұл саясат жиынтығы клиент құрылғыларына қолданылады.

   Бағдарламаны жылдам іске қосу шебері арқылы желі қорғанысын конфигурациялау кезінде Kaspersky Security Center Linux бағдарламасы Kaspersky Endpoint Security үшін әдепкі бойынша саясатты жасайды. Егер сіз осы шебердің көмегімен конфигурациялау процесін аяқтаған болсаңыз, сізге бұл бағдарлама үшін жаңа саясат жасаудың қажеті жоқ.

   Егер сізде бірнеше Басқару серверінің және/немесе басқару топтарының иерархиялық құрылымы болса, қосалқы Басқару серверлері мен еншілес басқару топтары саясатты әдепкі бойынша негізгі Басқару серверінен иеленеді. Саясат параметрлерін иерархия бойынша төмен қарай өзгертуге тыйым салу үшін параметрлерді еншілес топтар мен қосалқы Басқару серверлеріне мәжбүрлеп иелендіруге болады. Егер сіз параметрлердің тек бір бөлігін иеленуге рұқсат бергіңіз келсе, оларды саясат иерархиясы бойынша жоғары деңгейде құлыптай аласыз. Басқа құлыпталмаған параметрлер иерархия бойынша төменгі саясатты өзгерту үшін қолжетімді болады. Құрылған саясат иерархиясы басқару топтарындағы құрылғыларды тиімді басқаруға мүмкіндік береді.

   Нұсқаулар: саясатты жасау

2. **Пайдаланушыларды құрылғы иелері ретінде көрсетіңіз**

   Басқарылатын құрылғыларды сәйкес пайдаланушыларға тағайындаңыз.

   Нұсқаулар: Пайдаланушыны құрылғының иесі етіп тағайындау.

3. **Ұйымыңызға тән пайдаланушы рөлдерін анықтау**

   Ұйымыңыздың қызметкерлері әдетте орындайтын әртүрлі жұмыс түрлері туралы ойланыңыз. Сіз барлық қызметкерлерді олардың рөлдеріне сәйкес бөлуіңіз керек. Мысалы, сіз оларды бөлімдерге, кәсіптерге немесе лауазымдарға бөле аласыз. Осыдан кейін, сізге әр топ үшін пайдаланушы рөлін жасау қажет болады. Бұл жағдайда, әрбір пайдаланушы рөлінде осы рөлге тән бағдарлама параметрлерін қамтитын өзіндік саясат профилі болады.

4. **Пайдаланушы рөлдерін жасау**

   Алдыңғы қадамда сіз анықтаған әрбір қызметкерлер тобы үшін пайдаланушы рөлін жасаңыз және конфигурациялаңыз немесе алдын ала анықталған рөлдерді пайдаланыңыз. Пайдаланушы рөлдерінде бағдарлама мүмкіндіктеріне қатынасу құқықтарының жиынтығы бар.

   Нұсқаулар: Пайдаланушы рөлін жасау.

5. **Әрбір пайдаланушы рөлі үшін аймақты анықтау**

   Әрбір жасалған пайдаланушы рөлі үшін пайдаланушыларды және/немесе қауіпсіздік топтарын және басқару топтарын анықтаңыз. Пайдаланушы рөліне қатысты параметрлер тек осы рөл тағайындалған пайдаланушыларға тиесілі құрылғыларға қолданылады және бұл құрылғылар осы рөл тағайындалған топтарға, соның ішінде еншілес топтарға жататын болса ғана қолданылады.

   Нұсқаулар: Пайдаланушы рөлі үшін аймақты өзгерту.

6. **Саясат профилін жасау**

   Ұйымыңыздың әрбір пайдаланушы рөлі үшін саясат профилін жасаңыз. Саясат профильдері әр пайдаланушының рөліне байланысты пайдаланушы құрылғыларында орнатылған бағдарламаларға қандай параметрлерді қолдану керектігін анықтайды.

   Нұсқаулар: Саясат профилін жасау.

7. **Саясат профилінің пайдаланушы рөлдерімен байланысы**

   Саясат профилінің профилін пайдаланушы рөлдерімен байланыстырыңыз. Осыдан кейін, саясат профилі осы рөл анықталған пайдаланушылар үшін белсенді болады. Саясат профилінің параметрлері пайдаланушының құрылғыларында орнатылған Kaspersky бағдарламаларына қолданылады.

   Нұсқаулар: Саясат профильдерінің рөлдермен байланысы.

8. **Саясаттар мен саясат профильдерін басқарылатын құрылғыларға тарату**

   Әдепкі бойынша, Kaspersky Security Center Linux бағдарламасын Басқару серверімен синхрондау 15 минут сайын бір рет жүзеге асырылады. Синхрондау кезінде басқарылатын құрылғыларға жаңа немесе өзгертілген саясат пен саясат профильдері қолданылады. Автоматты синхрондауды өткізіп жіберіп, синхрондауды Мәжбүрлеп синхрондау пәрмені арқылы қолмен іске қосуға болады. Синхрондау аяқталғаннан кейін, саясаттар мен саясат профильдері жеткізіліп, Kaspersky белгіленген бағдарламаларына қолданылады.

   Саясаттар мен саясат профильдерінің құрылғыға жеткізілгенін тексеруге болады. Kaspersky Security Center Linux бағдарламасы құрылғының сипаттарында жеткізу күні мен уақытын анықтайды.

   Нұсқаулар: Мәжбүрлеп синхрондау.

Нәтижелер

Пайдаланушыға бағытталған сценарий аяқталғаннан кейін, Kaspersky бағдарламалары саясаттар иерархиясы мен саясат профильдері арқылы көрсетілген және таралған параметрлерге сәйкес конфигурацияланады.

Жаңа пайдаланушы үшін, сізге есептік жазба жасау, пайдаланушыға жасалған пайдаланушы рөлдерінің бірін тағайындау және құрылғыларды пайдаланушыға тағайындау қажет. Бағдарлама саясаттары мен саясат профильдері сол пайдаланушының құрылғыларына автоматты түрде қолданылады.

Саясаттар және профильдер

Kaspersky Security Center Web Console бағдарламасында Kaspersky бағдарламаларына арналған саясаттарды жасауға болады. Бұл бөлімде саясаттар және профильдер сипатталған, сондай-ақ оларды жасау және өзгерту бойынша нұсқаулар келтірілген.

Саясаттар мен саясат профильдері туралы

Саясат – басқару тобы мен оның ішкі тобына қатысты қолданылатын Kaspersky бағдарламасының параметрлері жиынтығы. Kaspersky бағдарламаларының бірнешеуін басқару тобының құрылғыларына орната аласыз. Kaspersky Security Center бағдарламасы басқару тобындағы Kaspersky бағдарламасының әрқайсысы үшін бір саясаттан ұсынады. Саясат келесі мәртебелердің біріне ие:

Саясат күйі

Күй	Сипаттамасы
Белсенді	Бұл, құрылғыға қатысты қолданылатын ағымдағы саясат. Kaspersky бағдарламасы үшін әрбір басқару тобында тек бір саясат белсенді болуы мүмкін. Kaspersky бағдарламасының белсенді саясаты параметрлерінің мәндері құрылғыға қатысты қолданылады.
Белсенді емес	Қазіргі уақытта құрылғыға қатысты қолданылмайтын саясат.
Автономды пайдаланушылар үшін	Егер бұл нұсқа таңдалса, құрылғы ұйым желісінен шыққан кезде саясат күшіне енеді.

Саясаттар келесі ережелер бойынша әрекет етеді:

- Бір бағдарлама үшін түрлі мәндері бар бірнеше саясатты конфигурациялауға болады.
- Бір бағдарлама үшін тек бір саясат белсенді болуы мүмкін.
- Саясаттың еншілес саясаттары болуы мүмкін.

Сіз вирустық шабуыл сияқты төтенше жағдайларға дайындалу үшін саясатты қолдана аласыз. Мысалы, USB флеш-дискілері арқылы шабуыл орын алса, флеш-дискілерге қатынасуға тыйым салатын саясатты іске қосуға болады. Бұл жағдайда, ағымдағы белсенді саясат автоматты түрде белсенді емес болады.

Көптеген саясаттарды қолдамау үшін, мысалы, әртүрлі жағдайларда бірнеше параметрлерді ғана өзгерту қажет болғанда, сіз саясат профильдерін қолдана аласыз.

Саясат профилі – саясат параметрлерін алмастыратын аталған саясат параметрлері ішкі жиынтығы. Саясат профилі басқарылатын құрылғының тиімді параметрлерін қалыптастыруға әсер етеді. *Тиімді параметрлер* – қазіргі уақытта құрылғыға қатысты қолданылатын саясат параметрлері, саясат профилі параметрлері және жергілікті бағдарлама параметрлері жиынтығы.

Саясат профильдері келесі ережелер бойынша жұмыс істейді:

- Саясат профилі белгіленген белсендіру шарты туындаған кезде күшіне енеді.
- Саясат профильдері саясат параметрлерінен ерекшеленетін параметр мәндерін қамтиды.

- Саясат профилін белсендіру кезінде басқарылатын құрылғының тиімді параметрлері өзгереді.
- Саясатта ең көбі 100 профиль болуы мүмкін.

Бұғаттау (құлып) және бұғатталған параметрлер

Әрбір саясат параметрінде (🔒) құлып белгішесі бар. Төмендегі кестеде құлып белгішесінің күйлері көрсетілген:

Құлып белгішесінің күйлері

Күй	Сипаттамасы
Undefined	Егер параметрдің жанында ашық құлып белгішесі пайда болса және қосқыш өшірулі болса, параметр саясатта көрсетілмейді. Пайдаланушы бұл параметрлерді басқарылатын бағдарлама интерфейсінде өзгерте алады. Мұндай параметрлер *құлпы ашылған* деп аталады.
Enforce	Егер параметрдің жанында жабық құлып белгішесі көрсетілсе және қосқыш қосулы болса, параметр саясат қолданылатын құрылғыларға қолданылады. Пайдаланушы басқарылатын бағдарлама интерфейсіндегі осы параметрлердің мәндерін өзгерте алмайды. Мұндай параметрлер *құлыпталған* деп аталады.

Басқарылатын құрылғыларға қолданғыңыз келетін саясат параметрлерін құлыптау ұсынылады. Құлпы ашылған саясат параметрлері басқарылатын құрылғыдағы Kaspersky бағдарламасының параметрлерімен қайта тағайындалуы мүмкін.

Келесі әрекеттерді орындау үшін құлып белгішесін пайдалануға болады:

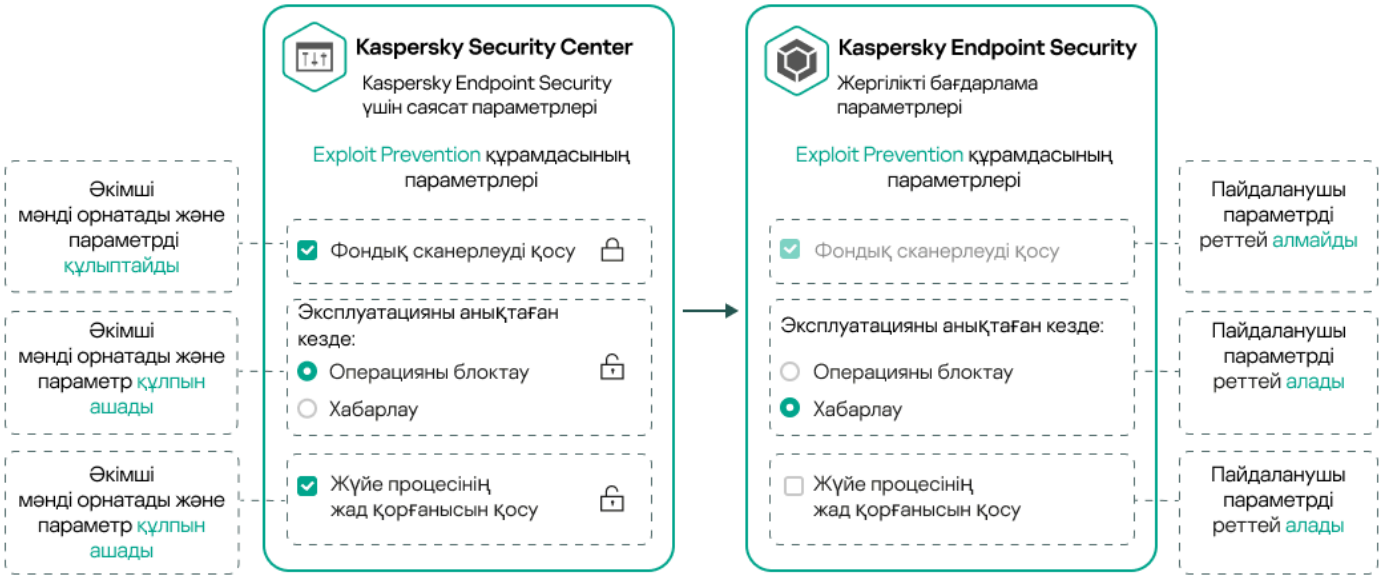
- Басқару ішкі тобы саясаты үшін параметрлерді құлыптау.
- Басқарылатын құрылғыдағы Kaspersky бағдарламасының параметрлерін құлыптау.

Осылайша, құлыпталған параметр басқарылатын құрылғыдағы тиімді параметрлерде қолданылады.

Тиімді параметрлерді қолдану келесі әрекеттерді қамтиды:

- Басқарылатын құрылғы Kaspersky бағдарламасының параметрлерінің мәндерін қолданады.
- Басқарылатын құрылғы саясат параметрлерінің құлыпталған мәндерін қолданады.

Саясат және Kaspersky басқарылатын бағдарламасы бірдей параметрлер жиынтығын қамтиды. Саясат параметрлерін конфигурациялау кезінде Kaspersky бағдарламасының параметрлері басқарылатын құрылғыдағы мәндерді өзгертеді. Басқарылатын құрылғыда құлыпталған параметрлерді өзгерту мүмкін емес (төмендегі суретті қараңыз):



Kaspersky бағдарламасының құлыптары мен параметрлері

Саясат пен саясат профильдерін иелену

Бұл бөлімде, саясаттар және профильдер иерархиясы және оларды иелену туралы ақпарат келтірілген.

Саясаттар иерархиясы

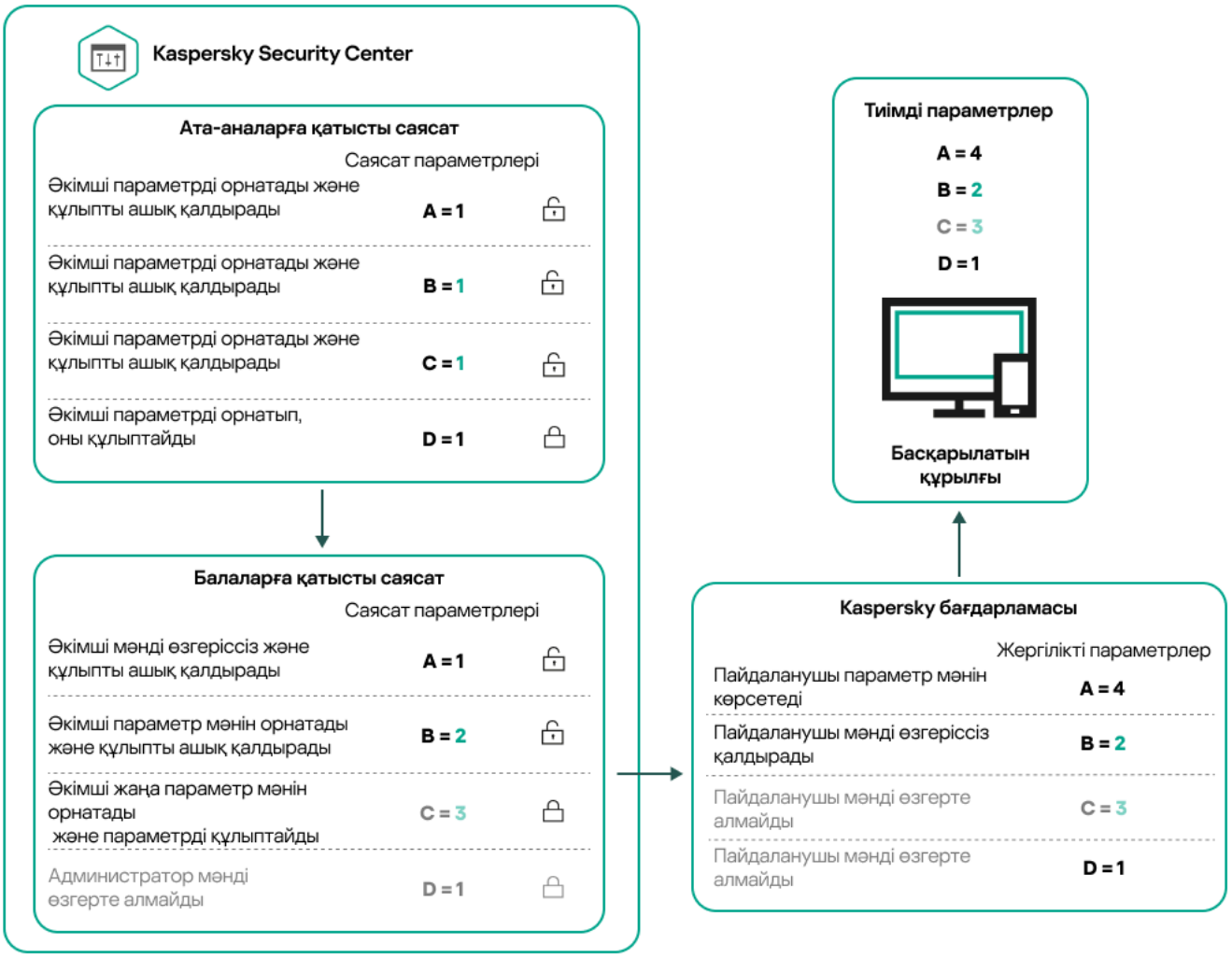
Түрлі құрылғылар үшін түрлі параметрлер керек болса, сіз құрылғыларды басқару топтарына біріктіре аласыз.

Сіз бөлек басқару тобына арналған саясатты көрсете аласыз. Саясат параметрлерін *мұралауға* болады. Иелену – (тектік) басқару тобының жоғары тұрған саясатынан ішкі топтарда (еншілес топтарда) саясат параметрлері мәндерін алу.

Тектік топ үшін жасалған саясат *тектік саясат* деп те аталады. Ішкі топ (еншілес топ) үшін жасалған саясат *еншілес саясат* деп те аталады.

Әдепкі бойынша, Басқару серверінде басқарылатын құрылғылардың кемінде бір басқару тобы бар. Егер сіз басқару топтарын құрғыңыз келсе, олар Басқарылатын құрылғылар тобында ішкі топтар (еншілес топтар) ретінде құрылады.

Бір бағдарламаның саясаттары басқару топтарының иерархиясы бойынша бір-біріне әсер етеді. Жоғары тұрған (тектік) басқару тобының саясатынан бұғатталған параметрлер ішкі топтың саясат параметрлерінің мәндерін қайта тағайындайды (төмендегі суретті қараңыз).

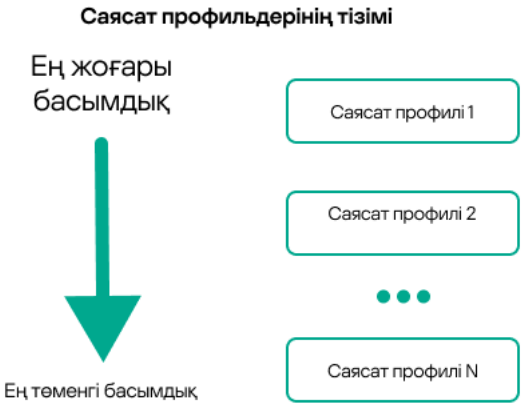


Саясаттар иерархиясы

Саясаттар иерархиясындағы саясат профильдері

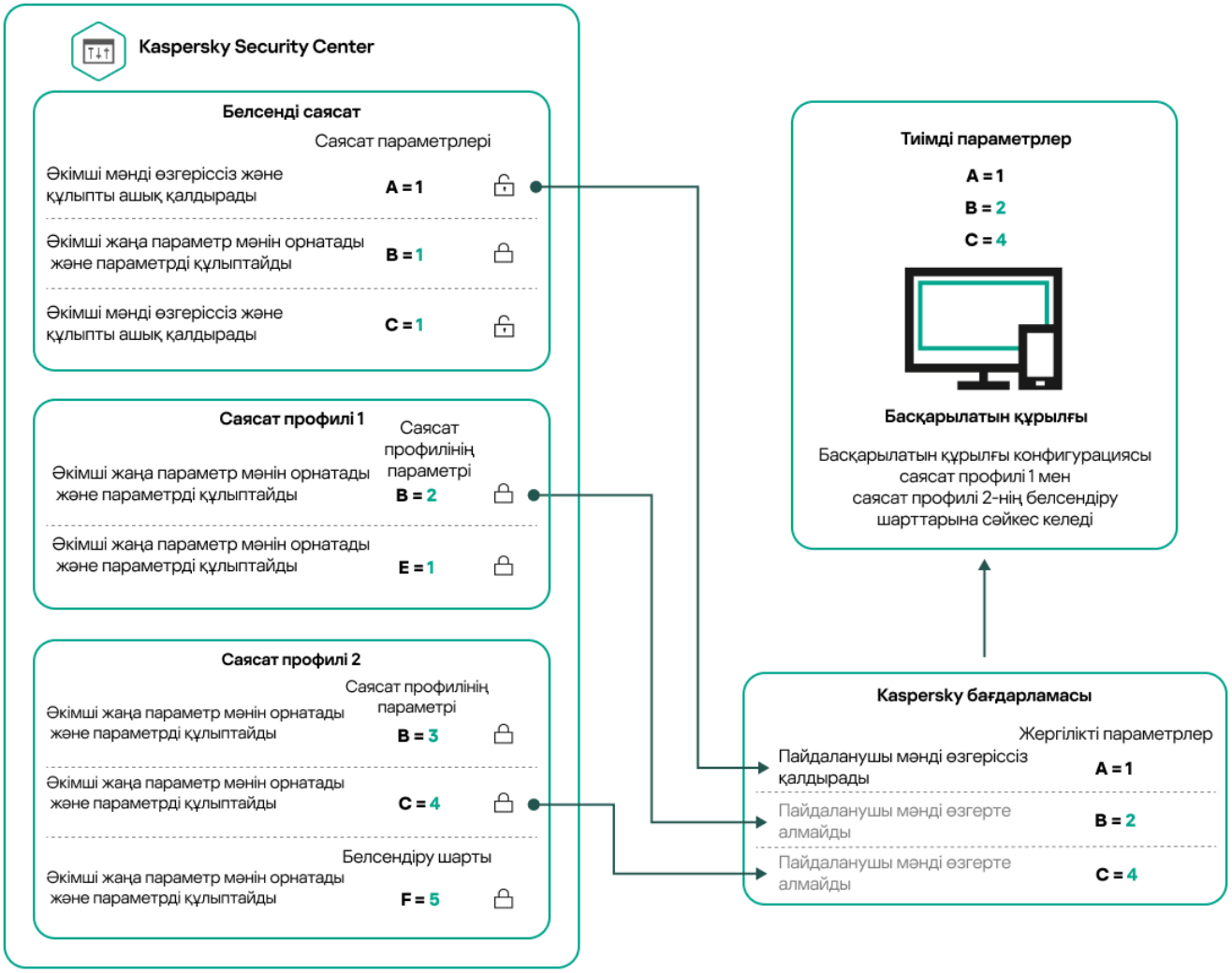
Саясат профильдерінде басымдықты тағайындаудың келесі шарттары бар:

- Саясат профильдерінің тізіміндегі профильдің орны оның басымдылығын білдіреді. Саясат профилінің басымдылығын өзгертуге болады. Тізімдегі ең жоғары жайғасым ең жоғары басымдықты білдіреді (төмендегі суретті қараңыз).



Саясат профилі басымдығын анықтау

- Саясат профильдерін белсендіру шарттары бір-біріне тәуелді емес. Бір уақытта бірнеше саясат профильдерін белсендіруге болады. Егер бірнеше саясат профильдері бірдей параметрге әсер етсе, құрылғы ең жоғары басымдығы бар саясат профиліндегі параметр мәнін пайдаланады (төмендегі суретті қараңыз).



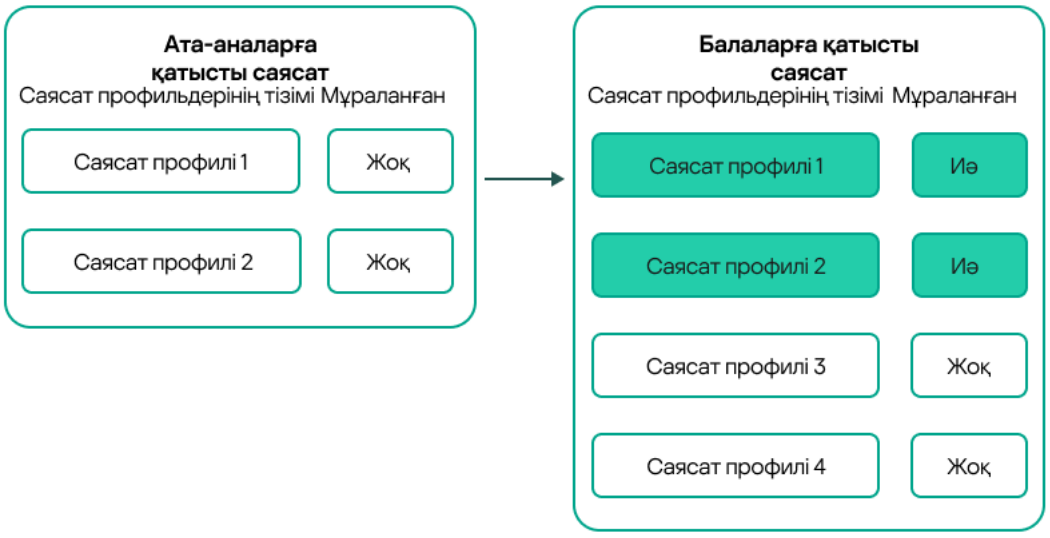
Басқарылатын құрылғының конфигурациясы бірнеше саясат профильдерін белсендіру шарттарына сәйкес келеді

Иелену иерархиясындағы саясат профильдері

Иерархияның әртүрлі деңгейлерінің саясаттарындағы саясат профильдері келесі шарттарға сәйкес келеді:

- Төменгі деңгейдегі саясат аса жоғары деңгейдегі саясаттан саясат профильдерін алады. Жоғары деңгейдегі саясаттан иеленген саясат профилі бастапқы саясат профилінің деңгейіне қарағанда жоғары басымдыққа ие болады.

- Сіз иеленген саясат профилінің басымдылығын өзгерте алмайсыз (төмендегі суретті қараңыз).

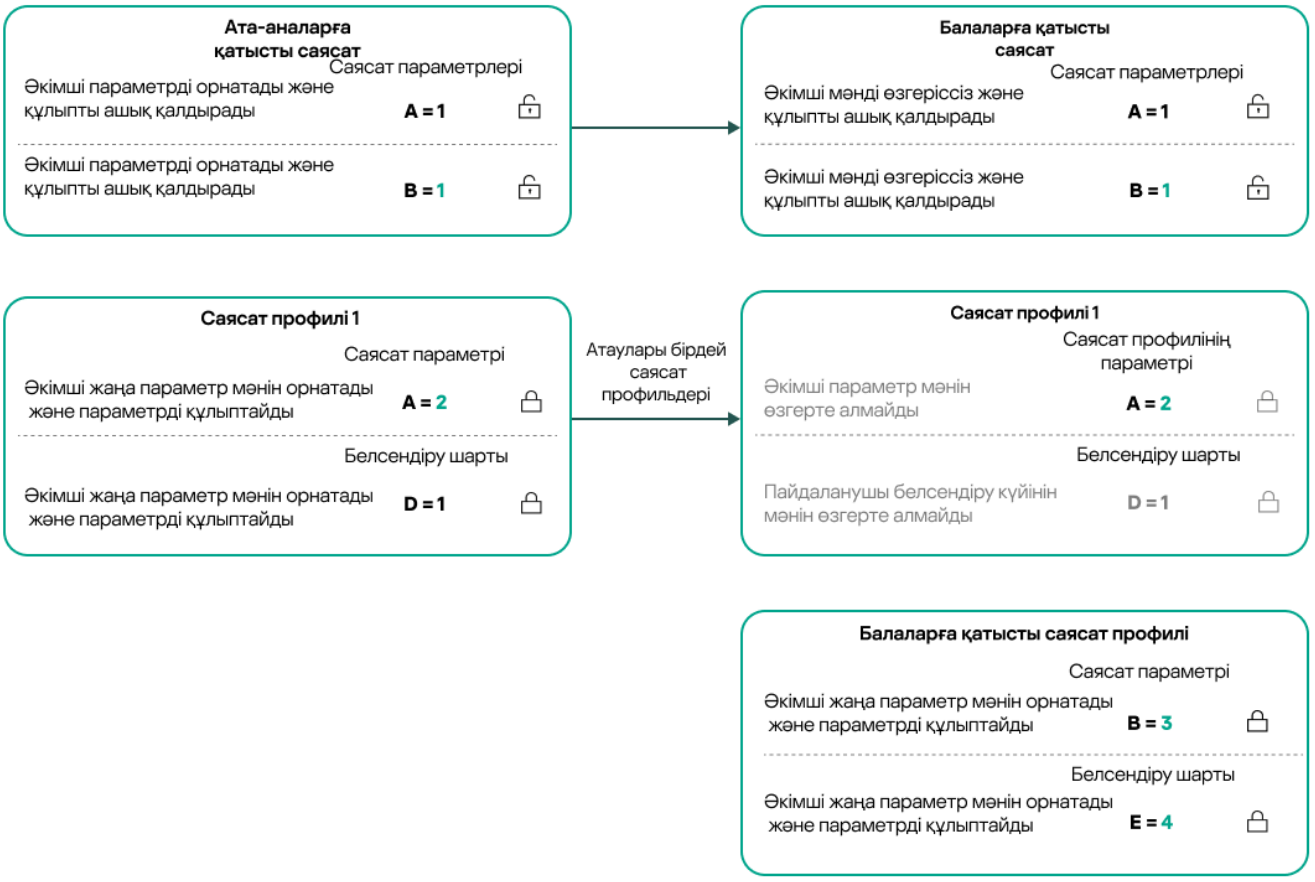


Саясат профильдерінің параметрлерін иелену

Атауы бірдей саясат профильдері

Егер иерархияның әртүрлі деңгейлерінде атаулары бірдей екі саясат болса, бұл саясаттар келесі ережелерге сәйкес жұмыс істейді:

- Аса жоғары деңгейлі саясат профилі үшін құлыпталған параметрлер мен профильді белсендіру шарты ең төменгі деңгейдегі саясат профилі үшін профильді белсендіру параметрлері мен шарттарын өзгертеді (төмендегі суретті қараңыз).



Еншілес профиль тектік саясат профилінен параметрлердің мәндерін алады

- Аса жоғары деңгейлі саясат профилі үшін құлпы ашылған параметрлер мен профильді белсендіру шарты ең төменгі деңгейдегі саясат профилі үшін профильді белсендіру параметрлері мен шарттарын өзгертеді.

Басқарылатын құрылғының параметрлері қалай іске асырылады

Басқарылатын құрылғыда тиімді параметрлердің қолданылуын келесідей сипаттауға болады:

- Барлық құлыпталмаған параметрлердің мәндері саясаттан алынады.
- Содан кейін, олар басқарылатын бағдарлама параметрлерінің мәндерімен қайта жазылады.
- Әрі қарай, қолданыстағы саясаттан бұғатталған параметр мәндері қолданылады. Құлыпталған параметрлердің мәндері құлпы ашылған қолданыстағы параметрлердің мәндерін өзгертеді.

Саясатты басқару

Бұл бөлім саясатты басқаруды сипаттайды және саясат тізімін қарау, саясатты жасау, саясатты өзгерту, саясатты көшіру, саясатты жылжыту, мәжбүрлеп синхрондау, саясатты тарату күйінің диаграммасын қарау және саясатты жою туралы ақпарат береді.

Саясаттар тізімін қарап шығу

Басқару серверінде немесе кез келген басқару тобында жасалған саясаттардың тізімін көре аласыз.

Саясаттар тізімін қарап шығу үшін:

1. Бағдарламаның негізгі терезесінде **Активтерді басқару** → **Топтардың иерархиясы** бөліміне өтіңіз.
2. Басқару топтары тізімінен саясат тізімін қарап шыққыңыз келетін басқару тобын таңдаңыз.

Саясаттар кесте түрінде көрсетіледі. Саясаттар болмаса, бос кесте көрсетіледі. Сіз кестенің бағандарын көрсете немесе жасыра аласыз, олардың ретін өзгерте аласыз, тек сіз көрсеткен мәнді қамтитын жолдарды көре аласыз немесе іздеуді қолдана аласыз.

Саясатты жасау

Сіз саясаттар жасай аласыз; қолданыстағы саясаттарды өзгертуге немесе жоюға да болады.

Саясат жасау үшін:

1. Бағдарламаның негізгі терезесінде **Активтерді басқару** → **Саясаттар** бөліміне өтіңіз.
2. Саясат жасау қажет басқару тобын таңдаңыз:
   - Түбірлік топ үшін.

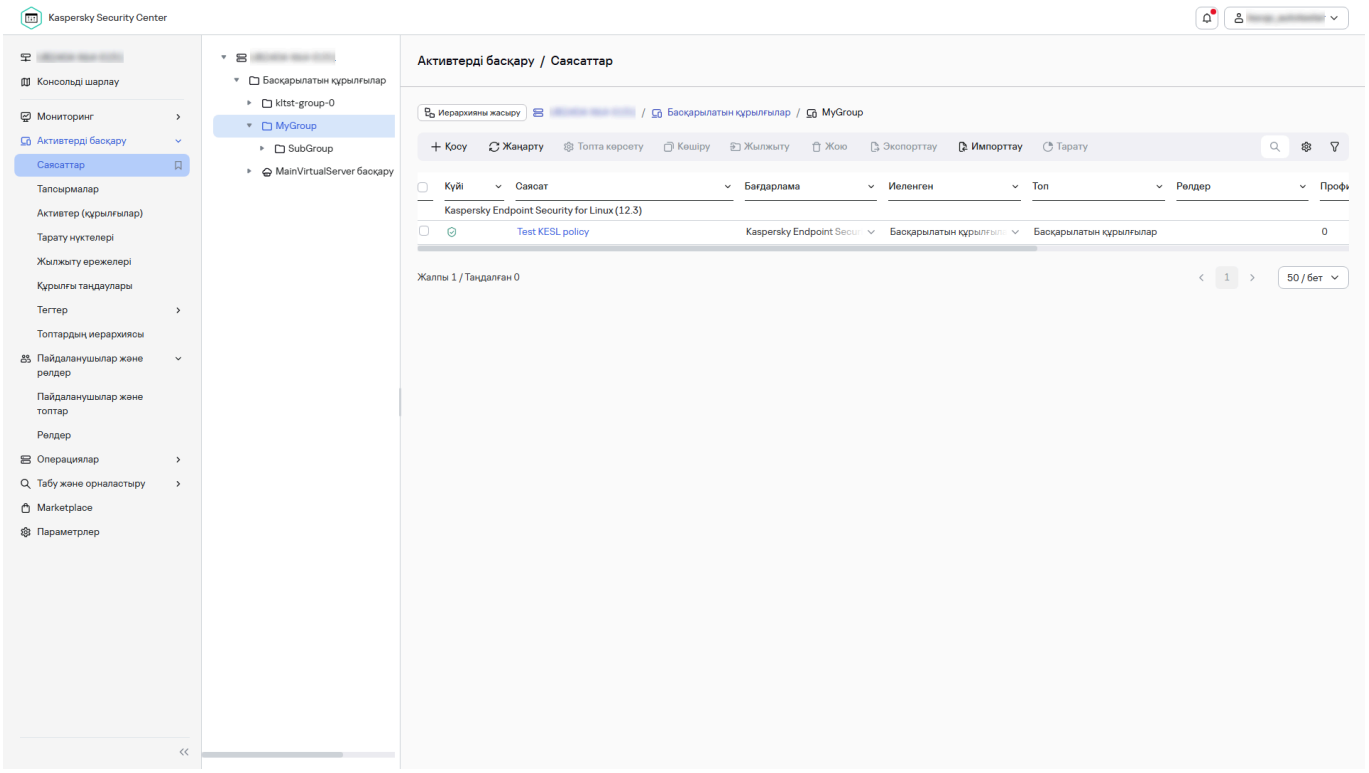
     Бұл жағдайда келесі қадамға өтуге болады.
   - Ішкі топ үшін:

     a. Беттің жоғарғы жағындағы **Иерархияны көрсету** түймесін басыңыз.

     Түйме атауы **Иерархияны жасыру** деп өзгереді.

     b. Ашылған терезеде қажетті ішкі топтың атын басыңыз.

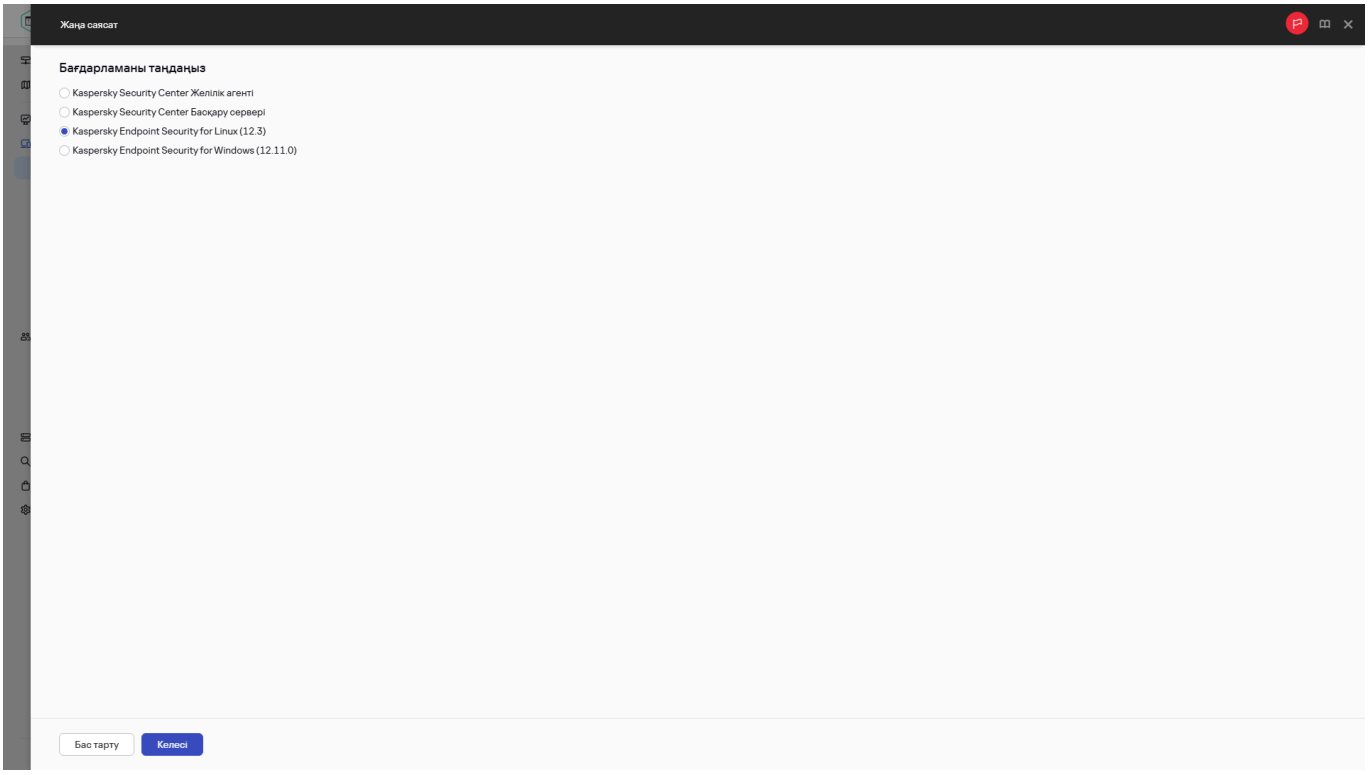
Таңдалған топ жолы беттің жоғарғы жағында көрсетіледі. Қажет болса, топқа өту үшін басқару тобының атауы бар сілтемені басуға болады. Әдепкісінше жолдағы соңғы сілтеме белсенді емес. Сондай-ақ **Иерархияны жасыру** түймесін басу арқылы иерархия терезесін жабуға болады.



Саясаттар тізімі

3. **Қосу** түймесін басыңыз.

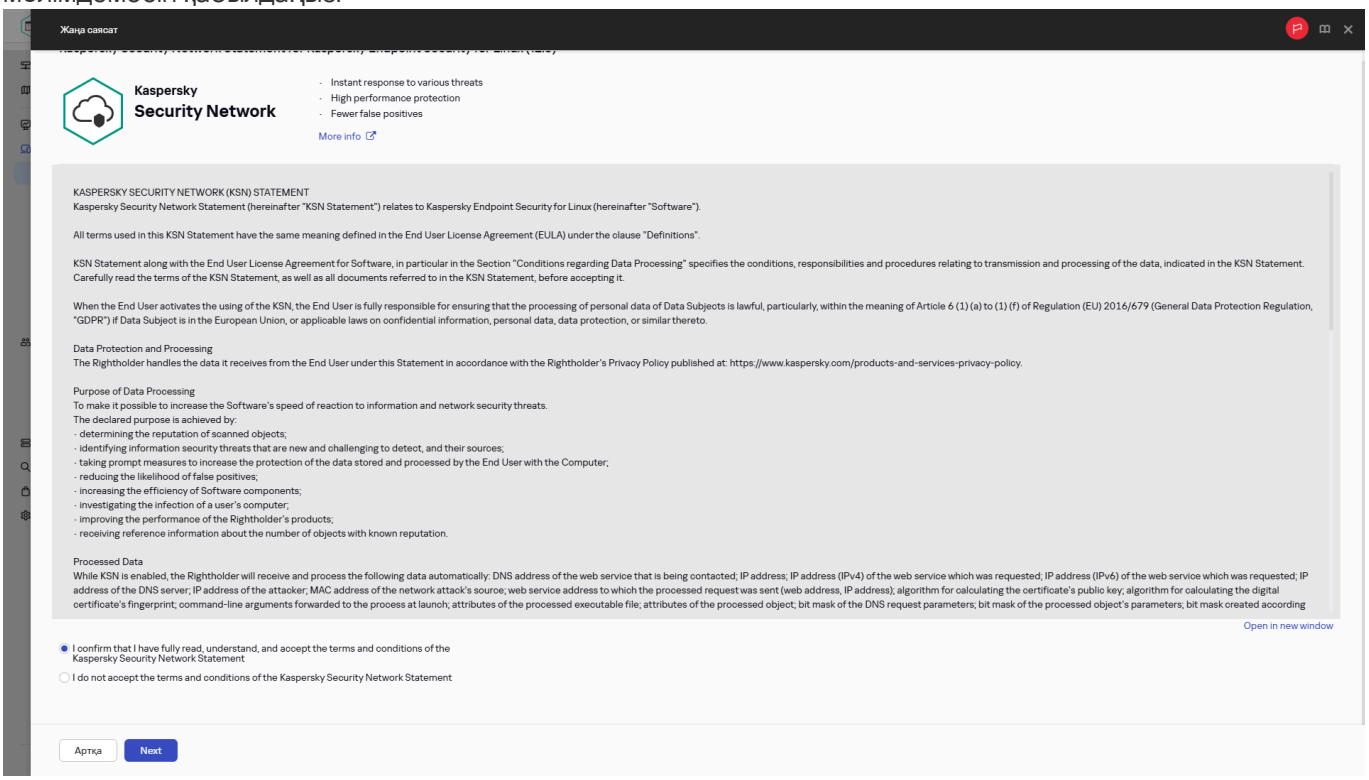
   Бағдарламаны таңдаңыз терезесі ашылады.



Жаңа саясат жасау

4. Саясат жасауды қажет ететін бағдарламаны таңдаңыз.

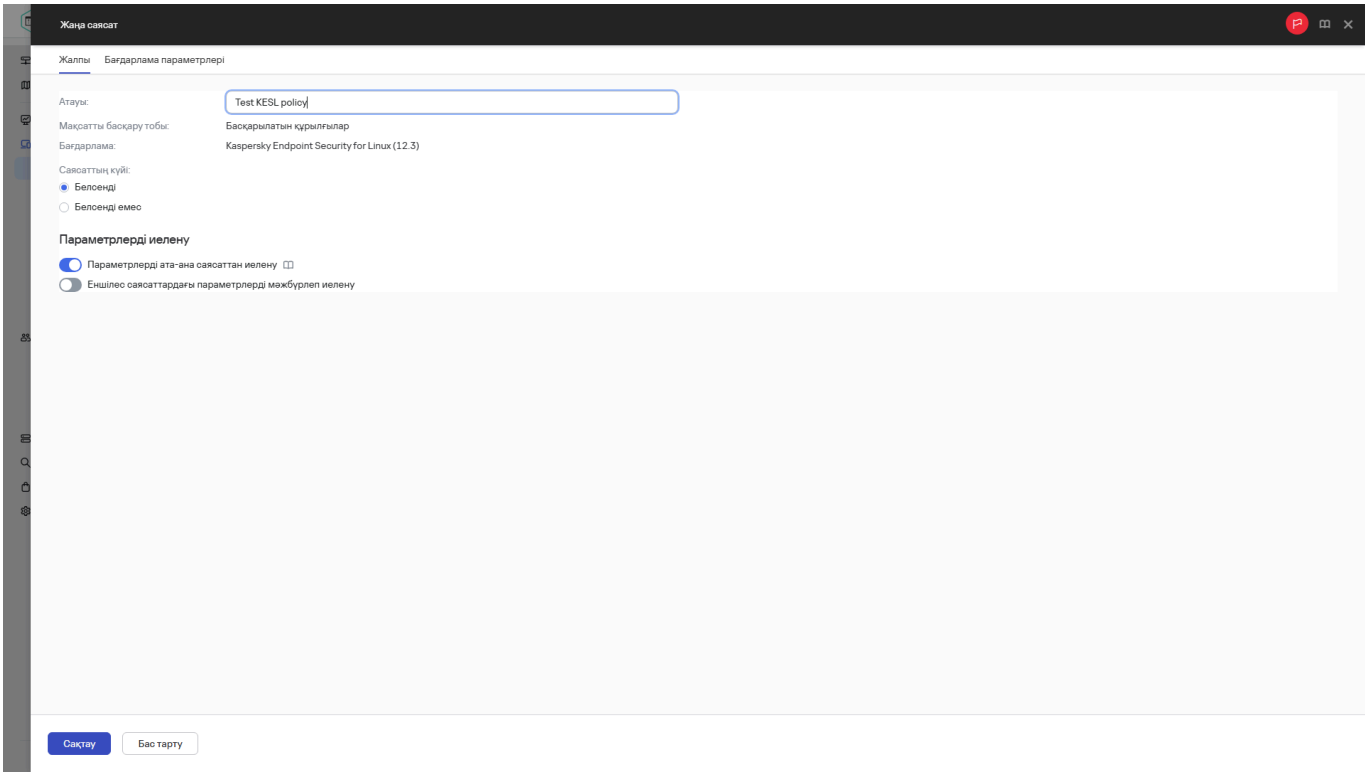
5. Kaspersky Security Network жүйесіне сіз саясат жасап жатқан Kaspersky қолданбасы қолдау көрсетсе, сізден KSN мәлімдемесін қабылдау сұралады. Kaspersky Security Network пайдаланғыңыз келсе, KSN мәлімдемесін қабылдаңыз.



KSN мәлімдемесін қабылдау

6. **Келесі** түймесін басыңыз.

Жалпы қойыншасында жаңа саясат параметрлері терезесі ашылады. Қаласаңыз, әдепкі бойынша белгіленген келесі саясат параметрерін өзгерте аласыз: атауы, күйі және иелену.



Жаңа саясат параметрлері терезесі

7. **Бағдарлама параметрлері** қойыншасын таңдаңыз.

Не болмаса, шығу үшін **Сақтау** түймесін басыңыз. Саясат саясаттар тізіміне пайда болып, сіз оның сипаттарын кейінірек өзгерте аласыз.

8. **Бағдарлама параметрлері** қойыншасының сол жағында, сізге қажетті бөлімді таңдап, нәтижелер тақтасында саясат параметрлерін өзгертіңіз. Сіз әрбір бөлімдегі саясат параметрлерін өзгерте аласыз.

   Параметрлер жиынтығы, сіз саясат жасап жатқан бағдарламаға байланысты. Толығырақ ақпарат келесі дереккөздерде келтірілген:

   - Басқару серверін конфигурациялау
   - Желілік агент саясатының параметрлері
   - Kaspersky Endpoint Security for Linux онлайн-анықтамасы
   - Kaspersky Endpoint Security for Windows онлайн-анықтамасы

   Басқа қауіпсіздік бағдарламаларының параметрлері туралы толығырақ білу үшін тиісті бағдарламаның құжаттамасын қараңыз.

   Өзгерістерді болдырмау үшін **Бас тарту** түймесін басуға болады.

9. Саясат өзгерістерін сақтау үшін **Сақтау** түймесін басыңыз.

   Келесі хабарламамен хабарландыру көрсетіледі: **Саясат сақталып жатыр және басқару серверлерінің иерархиясы арқылы таратылып жатыр**.

   Егер саясат валидациядан өтсе, келесі хабарландыру көрсетіледі: **Саясат сақталды**.

   Егер саясат тексеруден өтпей қалса, келесі хабарлама көрсетіледі: **Басқару серверінің иерархиясы арқылы саясатын сақтау және тарату сәтсіз аяқталды. Техникалық қолдау қызметіне хабарласыңыз**. Саясат параметрлерін қарап шығып, қайталап көріңіз. Егер мәселе шешілмесе, Техникалық қолдау қызметіне хабарласыңыз.

Нәтижесінде, қосылған саясат саясаттар тізімінде көрсетіледі. Саясат жасалғаннан кейін, егер бұл опция қосылған болса, саясатты өзгерту оқиғалары SIEM жүйесіне экспортталады.

Саясаттардың жалпы параметрлері

Жалпы

Жалпы қойыншасында саясаттың күйін өзгертуге және саясат параметрлерін иеленуді конфигурациялауға болады:

- **Саясаттың күйі** блогында саясаттың әрекет ету ауқымы нұсқаларының біреуін таңдауға болады:
  - **Белсенді**

    Осы нұсқа таңдалған болса, саясат белсенді болады.

    Әдепкі бойынша, осы нұсқа таңдалған.
  - **Кеңседен тыс**

    Егер бұл нұсқа таңдалса, құрылғы ұйым желісінен шыққан кезде саясат күшіне енеді.

- **Белсенді емес**

  Егер бұл нұсқа таңдалса, саясат белсенді болмайды, бірақ **Саясат** қалтасында сақталады. Қажет болса, оны белсенді етуге болады.

- **Параметрлерді иелену** блогында саясатты иелену параметрлерін конфигурациялауға болады:

  - **Параметрлерді ата-ана саясаттан иелену**

    Параметр қосулы болса, саясат параметрлері мәндері иерархияның жоғарғы деңгейіндегі топқа арналған саясаттан иеленеді және өзгерту үшін қолжетімді емес.

    Әдепкі бойынша, параметр қосулы.

  - **Еншілес саясаттардағы параметрлерді мәжбүрлеп иелену**

    Егер параметр қосылса, саясатқа өзгертулер қолданылғаннан кейін келесі қадамдар орындалады:

    - саясат параметрлерінің мәндері салынған басқару топтарының саясаты – еншілес саясаттарға қатысты қолданылады;

    - Әрбір еншілес саясат сипаттары терезесінің **Жалпы** бөлімінің **Параметрлерді иелену** блогында **Параметрлерді негізгі саясаттан иелену** параметрі автоматты түрде қосылады.

    Параметр қосулы болған кезде, еншілес саясат параметрлерінің мәндерін өзгерту қолжетімді емес.

    Әдепкі бойынша, параметр өшірулі.

Оқиғаларды конфигурациялау

Оқиғаларды конфигурациялау қойыншасында оқиғаларды тіркеуді және оқиғалар туралы хабарлауды конфигурациялауға болады. Оқиғалар қойыншалардағы маңыздылық деңгейлері бойынша бөлінген:

- **Маңызды**

  Маңызды бөлімі Желілік агент саясатының сипаттарында көрсетілмейді.

- **Функционалдық ақау**

- **Ескерту**

- **Ақпараттық**

Оқиғалар тізіміндегі әрбір бөлімде оқиғалардың атаулары және әдепкі бойынша Басқару серверінде оқиғаларды сақтау уақыты (күндерде) көрсетіледі. Оқиға түрін басу арқылы сіз келесі параметрлерді көрсете аласыз:

- **Оқиғаларды тіркеу**

  Сіз оқиғаларды сақтау күндерінің санын көрсете аласыз және оқиғаларды қайда сақтау керектігін таңдай аласыз:

  - **Syslog протоколы арқылы SIEM жүйесіне экспорттау**

  - **Құрылғыдағы ОЖ оқиғалар журналында сақтау**

  - **Басқару серверіндегі ОЖ оқиғалар журналында сақтау**

- **Оқиға хабарландырулары**

  Оқиға хабарландырулары тәсілін таңдауға болады:

  - **Электрондық пошта арқылы хабарлау**
  - **SMS арқылы хабарлау**
  - **Орындалатын файлды немесе сценарийді іске қосып хабарлау**
  - **SNMP арқылы хабарлау**

  Әдепкі бойынша, Басқару сервері сипаттарының қойыншасында көрсетілген хабарландыру параметрлері қолданылады (мысалы, алушының мекенжайы). Қаласаңыз, бұл параметрлерді **Электрондық пошта**, **SMS** және **Іске қосылатын орындалатын файл** қойыншаларында өзгертіңіз.

Сондай-ақ **Оқиғаларды конфигурациялау** қойындысы жаңа оқиға түрлері қосылғанда (мысалы, өнімнің жаңа нұсқасында) хабарландыруды көрсетеді және **Сақтау** немесе **Сақтау және жабу** түймесін басу арқылы жаңа параметрлерді қолдануға мүмкіндік береді.

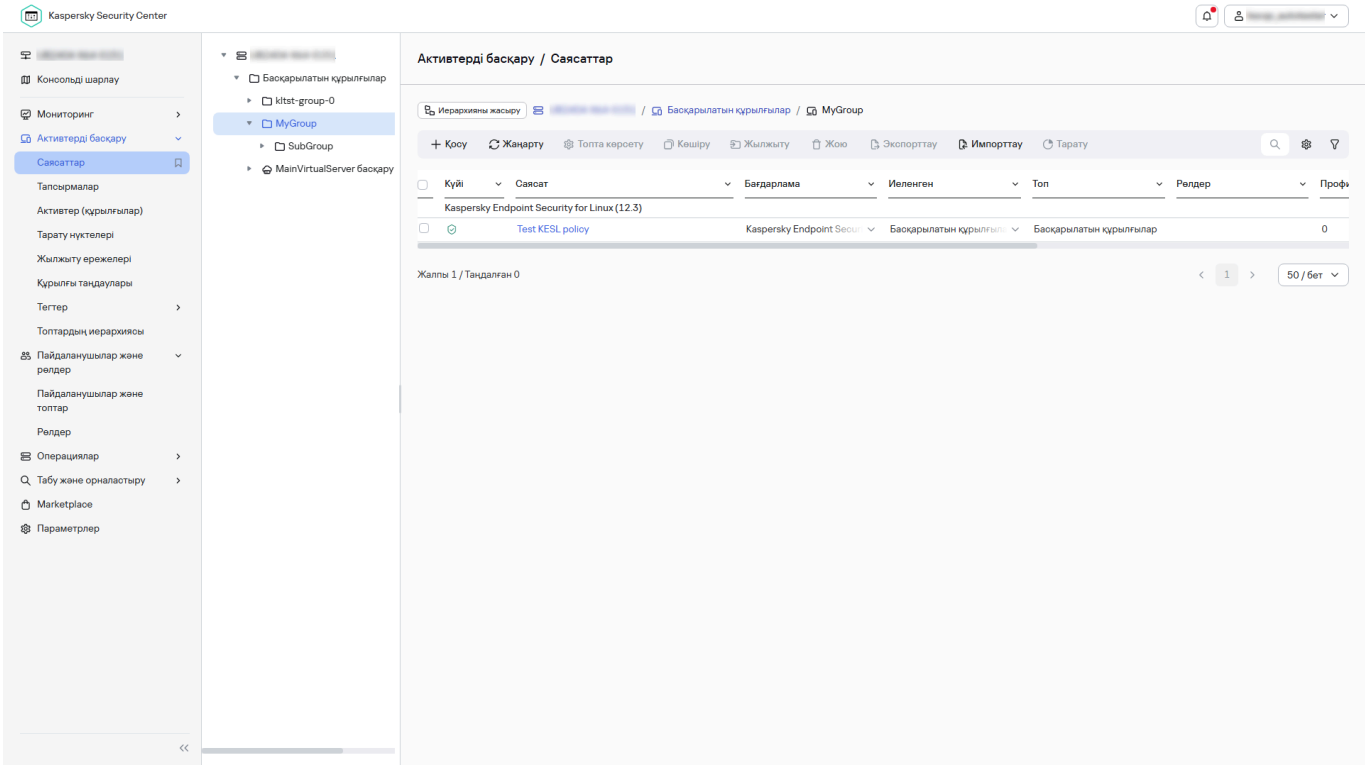
Тексерістер журналы

Тексерістер журналы қойыншасы саясат нұсқаларының тізімін көруге, саясат нұсқаларын салыстыруға және қажет болған жағдайда саясатқа енгізілген өзгерістерді кері қайтаруға мүмкіндік береді.

Саясатты өзгерту

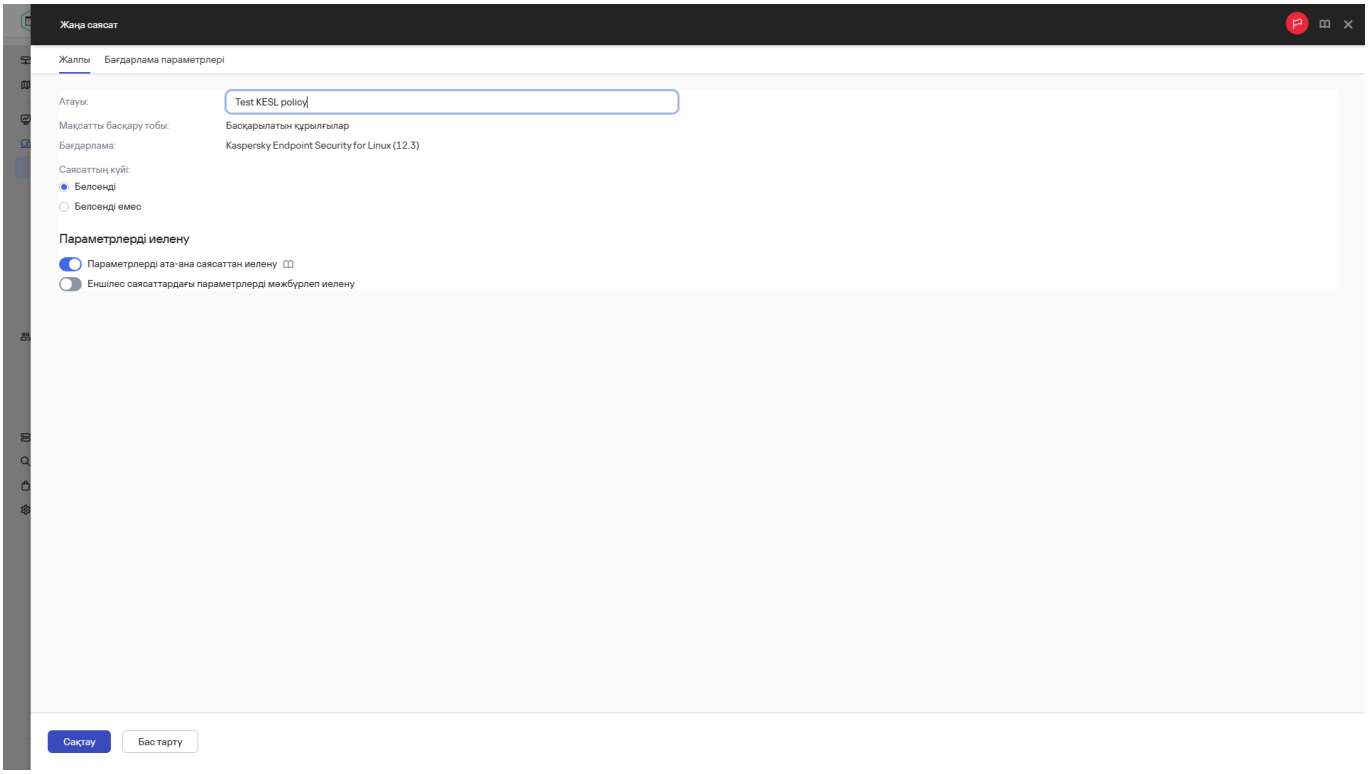
Саясатты өзгерту үшін:

1. Бағдарламаның негізгі терезесінде **Активтерді басқару** → **Саясаттар** бөліміне өтіңіз.



2. Өзгертуді қажет ететін саясатты таңдаңыз.

   Саясат сипаттары терезесі ашылады.



3. Сіз саясатты жасайтын жалпы параметрлер мен бағдарлама параметрлерін көрсетіңіз. Толығырақ ақпарат келесі дереккөздерде келтірілген:

   - Басқару серверін конфигурациялау
   - Желілік агент саясатының параметрлері
   - Kaspersky Endpoint Security for Linux онлайн-анықтамасы
   - Kaspersky Endpoint Security for Windows онлайн-анықтамасы

   Басқа қауіпсіздік бағдарламаларының параметрлері туралы толығырақ білу үшін осы бағдарламалардың құжаттамасын қараңыз.

4. **Сақтау** түймесін басыңыз.

   Келесі хабарламамен хабарландыру көрсетіледі: **Саясат сақталып жатыр және басқару серверлерінің иерархиясы арқылы таратылып жатыр**.

   Егер саясат валидациядан өтсе, келесі хабарландыру көрсетіледі: **Саясат сақталды**.

   Егер саясат тексеруден өтпей қалса, келесі хабарлама көрсетіледі: **Басқару серверінің иерархиясы арқылы саясатын сақтау және тарату сәтсіз аяқталды. Техникалық қолдау қызметіне хабарласыңыз**. Саясат параметрлерін қарап шығып, қайталап көріңіз. Егер мәселе шешілмесе, Техникалық қолдау қызметіне хабарласыңыз.

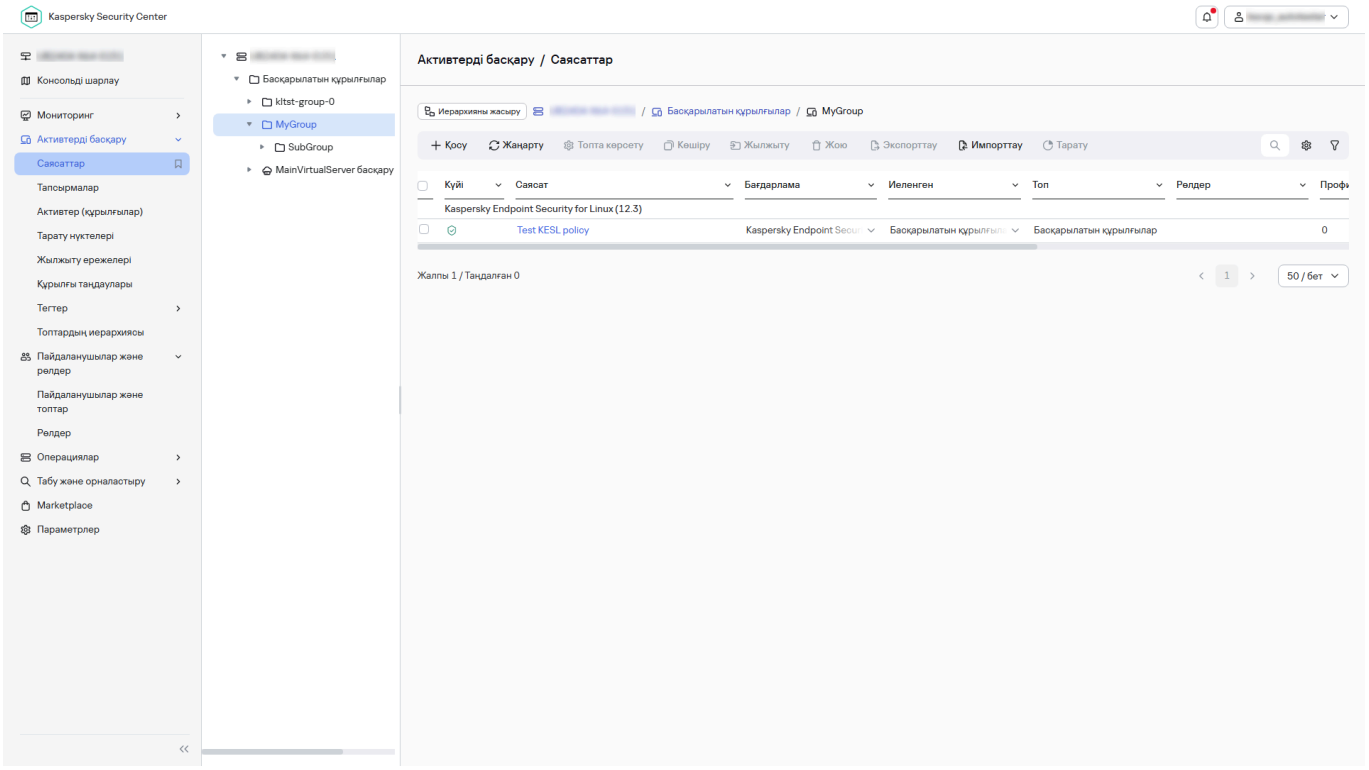
Саясат өзгерістері саясаттың сипаттарында сақталып, **Тексерістер журналы** бөлімінде көрсетіледі. Саясат өзгертілгеннен кейін, егер бұл опция қосылған болса, саясатты өзгерту оқиғалары SIEM жүйесіне экспортталады.

Қажет болса, саясат түзетулерін салыстыра аласыз. Бұл опция Басқару сервері, Желілік агент, Kaspersky Endpoint Security for Windows (14.0 веб-плагин нұсқасынан бастап) және Kaspersky Endpoint Security for Mac (12.2.1 Patch A веб-плагин нұсқасынан бастап) саясаттары үшін қолжетімді.

Саясатты иелену параметрін қосу және өшіру

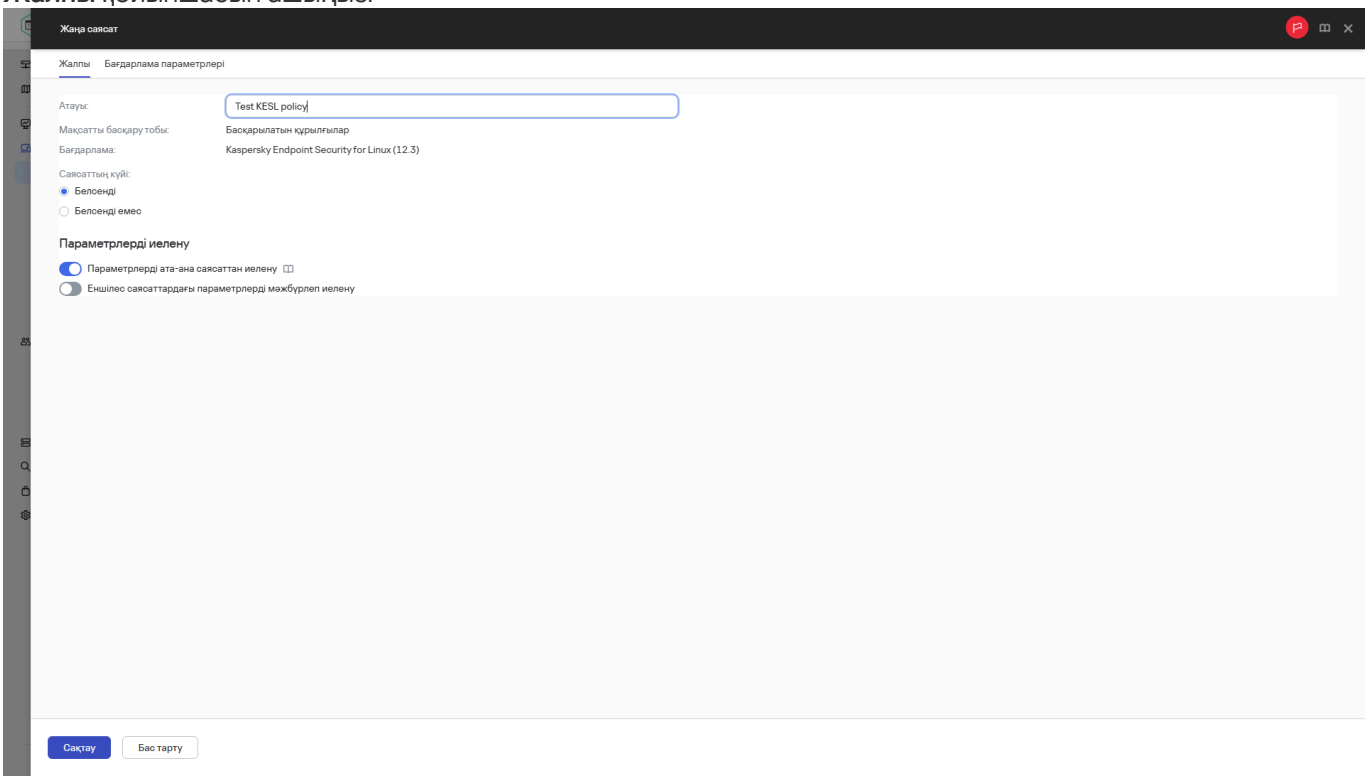
Саясатта иелену параметрін қосу немесе өшіру үшін:

1. Қажетті саясатты ашыңыз.



Саясаттар тізімі

2. **Жалпы** қойыншасын ашыңыз.



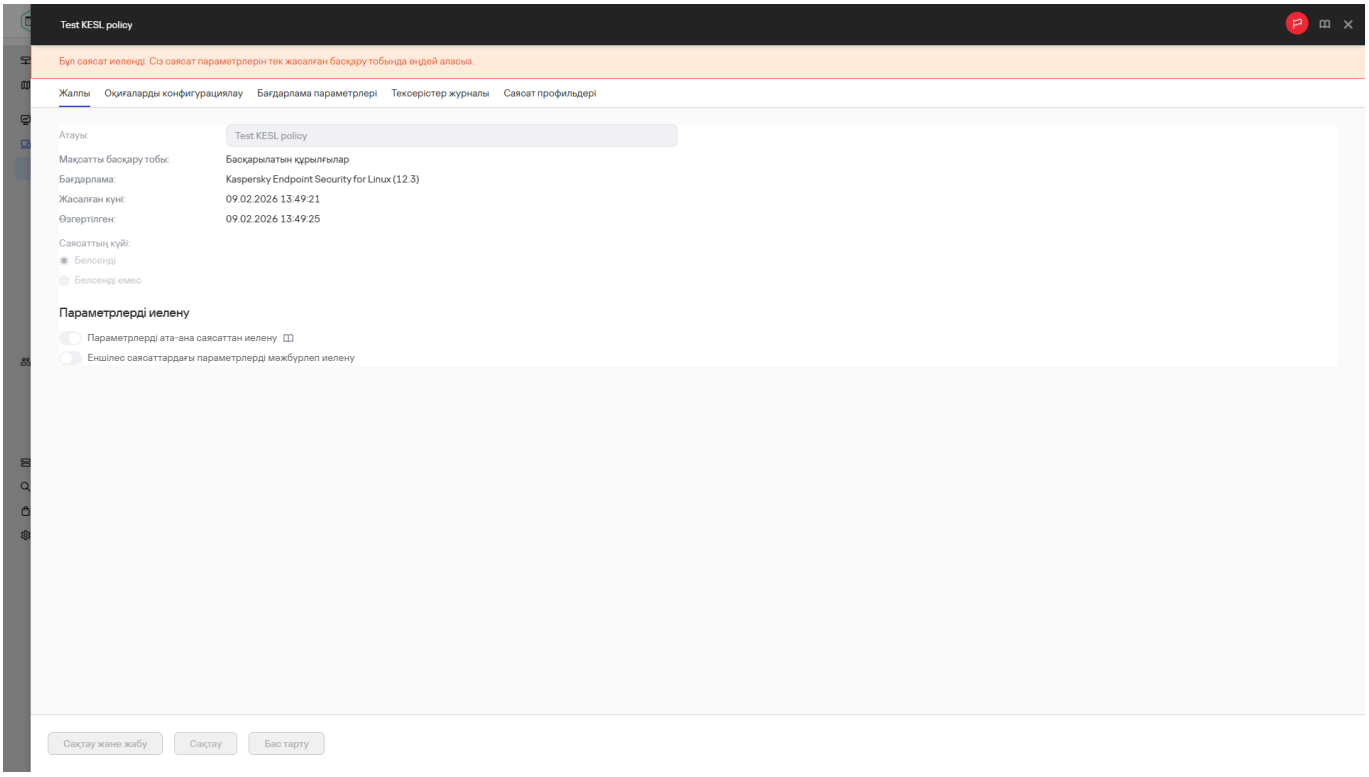
Жаңа саясат жасау

3. Саясатты иеленуді қосыңыз немесе өшіріңіз:

   - Егер еншілес топта **Параметрлерді ата-ана саясаттан иелену** параметрі қосылған болса және тектік саясаттағы кейбір параметрлер бұғатталса, онда сіз осы саясат параметрлерін еншілес топ үшін өзгерте алмайсыз.

   - Егер еншілес саясатта **Параметрлерді ата-ана саясаттан иелену** параметрі өшірулі болса, онда сіз тектік саясатта кейбір параметрлер "бұғатталған" болса да, еншілес саясаттағы барлық параметрлерді өзгерте аласыз.

   - Тектік топта **Еншілес саясаттардағы параметрлерді мәжбүрлеп иелену** параметрі қосулы болса, әрбір еншілес саясат үшін **Параметрлерді ата-ана саясаттан иелену** параметрі де қосылады. Бұл жағдайда, сіз осы параметрді еншілес саясат үшін өшіре алмайсыз. Негізгі саясатта бұғатталған барлық параметрлер еншілес топтарда мәжбүрлеп иеленеді және сіз бұл параметрлерді еншілес топтарда өзгерте алмайсыз.



Құлыпталған саясат параметрлері

4. Өзгерістерді сақтау үшін **Сақтау** түймесін басыңыз немесе өзгерістерді қабылдамау үшін **Бас тарту** түймесін басыңыз.

Әдепкі бойынша, **Параметрлерді ата-ана саясаттан иелену** параметрі жаңа саясат үшін қосулы.

Егер саясатта профильдер болса, барлық еншілес саясаттар осы профильдерді иеленеді.

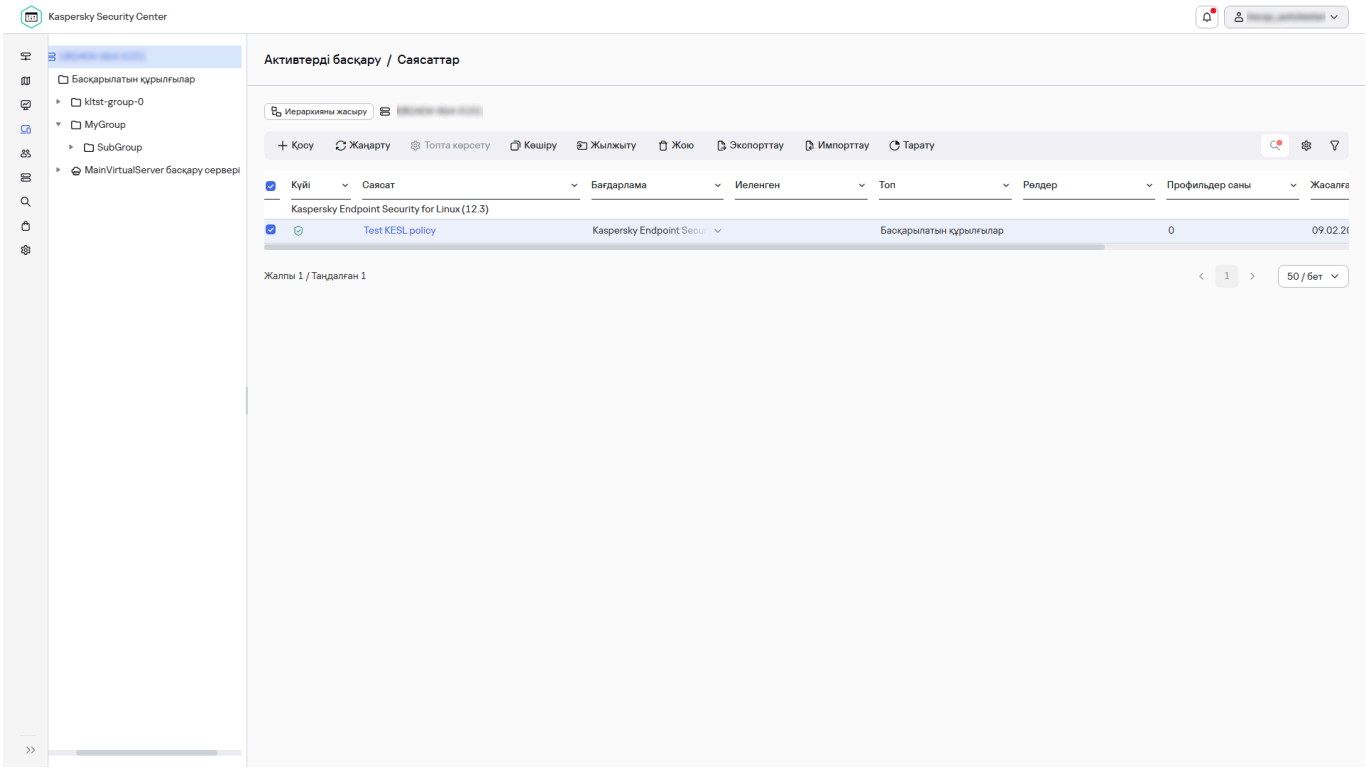
Саясатты көшіру

Сіз саясатты бір басқару тобынан екіншісіне көшіре аласыз.

Саясаты басқа басқару тобына көшіру үшін:

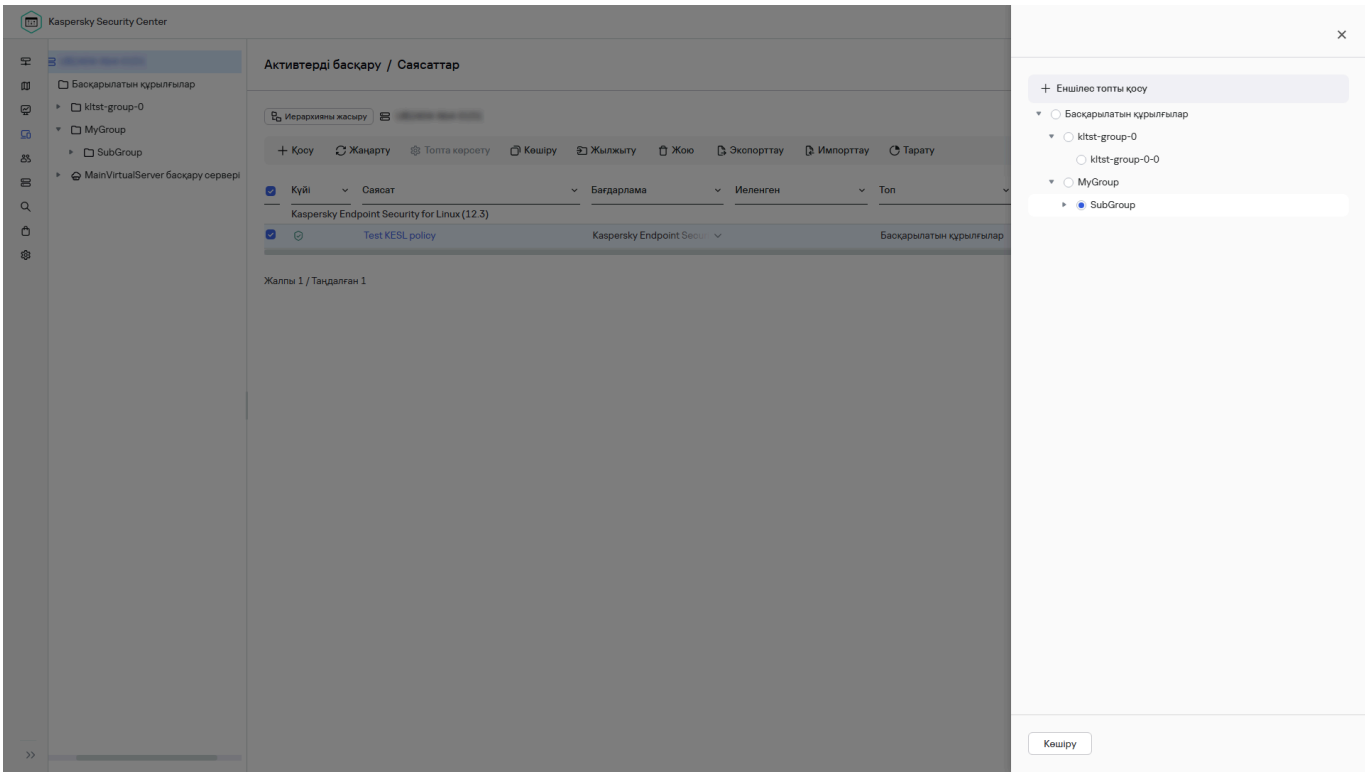
1. Бағдарламаның негізгі терезесінде **Активтерді басқару** → **Саясаттар** бөліміне өтіңіз.

2. Жалаушаны, көшірілетін саясатқа (немесе саясаттарға) қарама-қарсы қойыңыз.



3. **Көшіру** түймесін басыңыз.

   Экранның оң жағында басқару топтарының ағашы көрсетіледі.



4. Ағаштағы мақсатты топты, яғни саясатты (немесе саясаттарды) көшіргіңіз келетін топты таңдаңыз.

5. Экранның астындағы **Көшіру** түймесін басыңыз.

6. Операцияны растау үшін **ОК** түймесін басыңыз.

Саясат (саясаттар) және оның барлық профильдері мақсатты басқару тобына көшіріледі. Мақсатты топтағы әрбір көшірілген саясат **Белсенді емес** күйін қабылдайды. Саясаттың күйін кез келген уақытта **Белсенді** деп өзгерте аласыз.

Егер саясаттың мақсатты тобында көшірілетін саясаттың атына сәйкес келетін саясат болса, көшірілген саясаттың атына түрдің жалғауы қосылады (<келесі реттік нөмір>), мысалы: (1).

Саясатты жылжыту

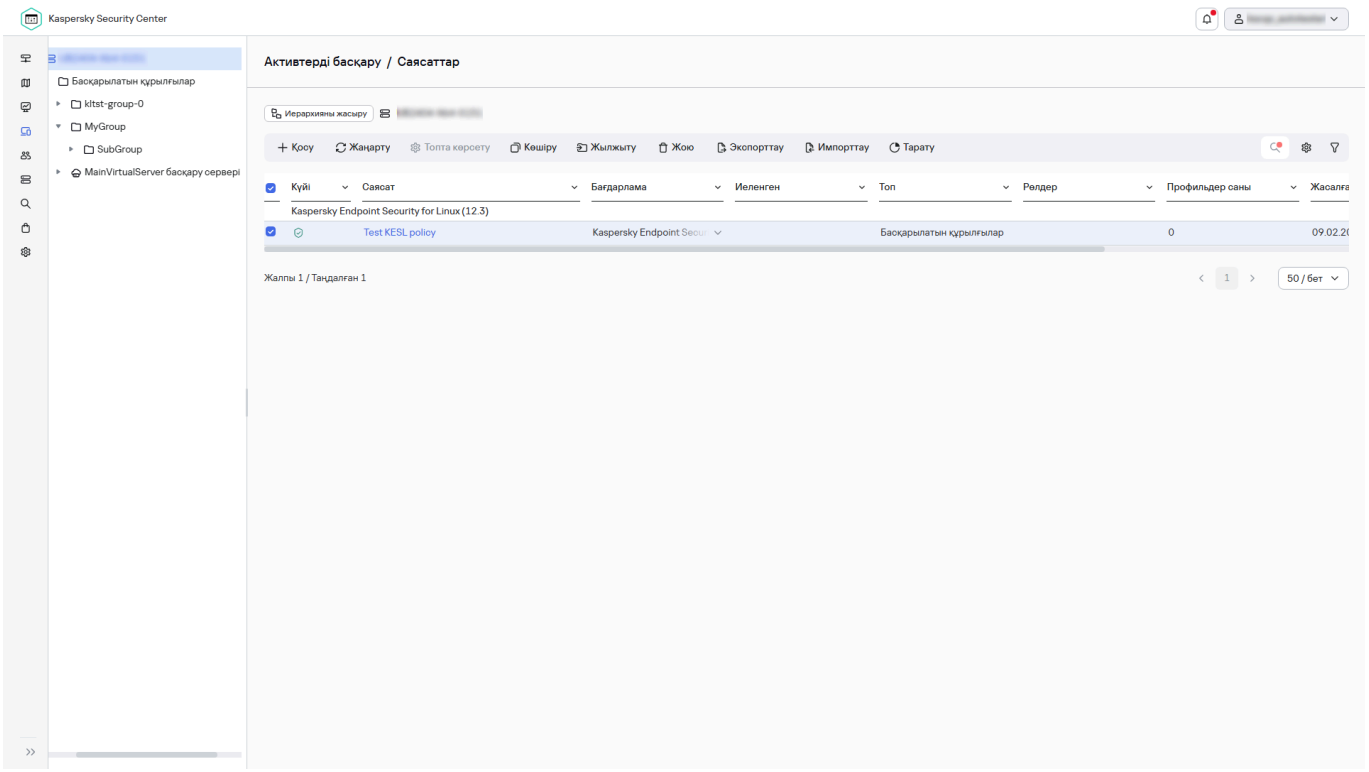
Сіз саясаттарды бір басқару тобынан екіншісіне жылжыта аласыз. Мысалы, сіз бір басқару тобын жойғыңыз келеді, бірақ оның саясаттарын басқа басқару тобы үшін қолданғыңыз келеді. Бұл жағдайда, ескі басқару тобын жою алдында саясатты ескі басқару тобынан жаңасына жылжыту қажет болуы мүмкін.

> Саясатты басқа басқару тобына ауыстырған кезде, саясаттың түзету тарихы жойылады. **Тексерістер журналы** қойындысында тек соңғы өзгеріс туралы ақпарат көрсетіледі.

Саясатты басқа басқару тобына жылжыту үшін:

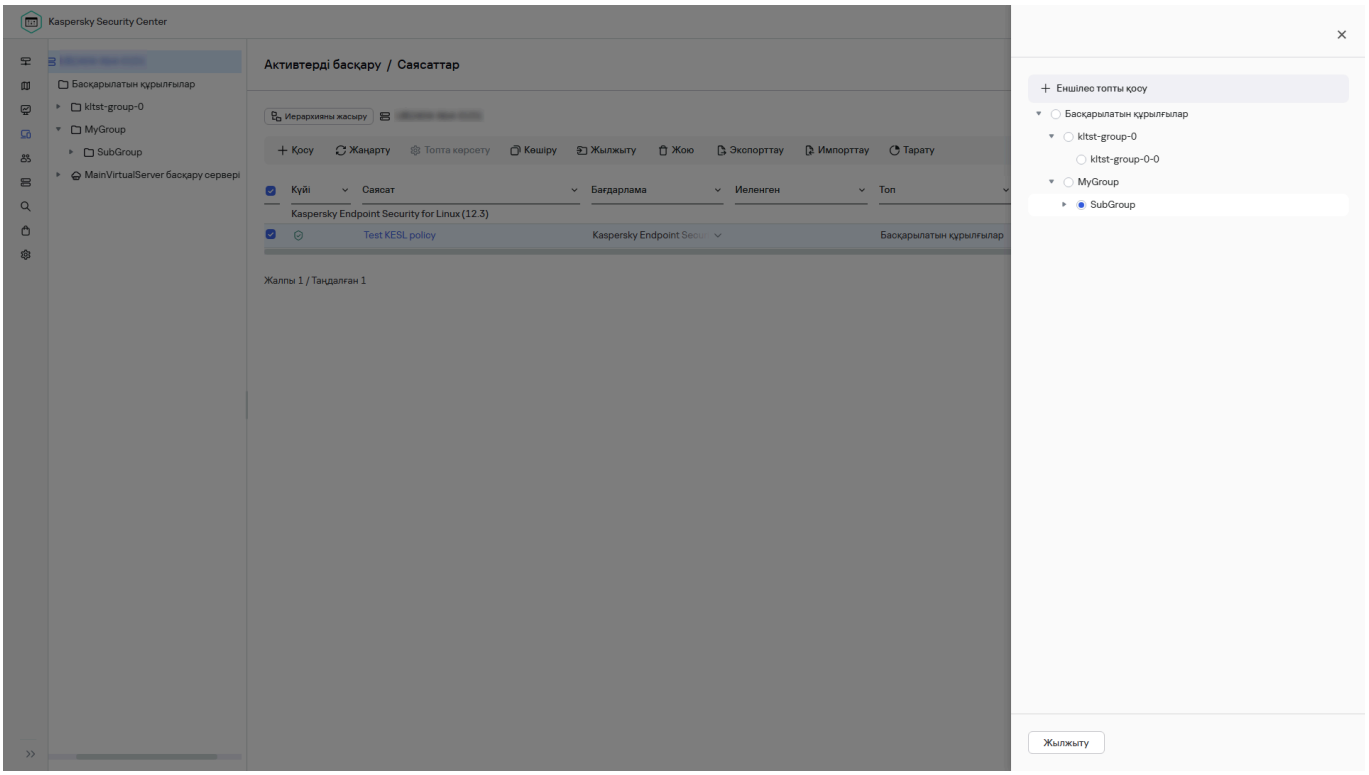
1. Бағдарламаның негізгі терезесінде **Активтерді басқару** → **Саясаттар** бөліміне өтіңіз.

2. Жалаушаны, жылжытылатын саясатқа (немесе саясаттарға) қарама-қарсы қойыңыз.



3. **Жылжыту** түймесін басыңыз.

   Экранның оң жағында басқару топтарының ағашы көрсетіледі.



4. Ағашта мақсатты басқару тобын, яғни саясатты (немесе саясаттарды) жылжытқыңыз келетін топты таңдаңыз.

5. Экранның астындағы **Жылжыту** түймесін басыңыз.

6. Операцияны растау үшін **OK** түймесін басыңыз.

Егер саясат дереккөз тобынан иеленген болмаса, ол барлық саясат профильдері бар мақсатты топқа жылжытылады. Мақсатты басқару тобындағы саясаттың күйі **Белсенді емес** болады. Саясаттың күйін кез келген уақытта **Белсенді** деп өзгерте аласыз.

Саясат дереккөз тобынан иеленген болса, ол дереккөз тобында қала береді. Саясат мақсатты топқа барлық профильдерімен бірге көшірілген. Мақсатты басқару тобындағы саясаттың күйі **Белсенді емес** болады. Саясаттың күйін кез келген уақытта **Белсенді** деп өзгерте аласыз.

Егер саясаттың мақсатты тобында көшірілетін саясаттың атына сәйкес келетін саясат болса, көшірілген саясаттың атына түрдің жалғауы қосылады (<келесі реттік нөмір>), мысалы: (1).

Саясатты экспорттау

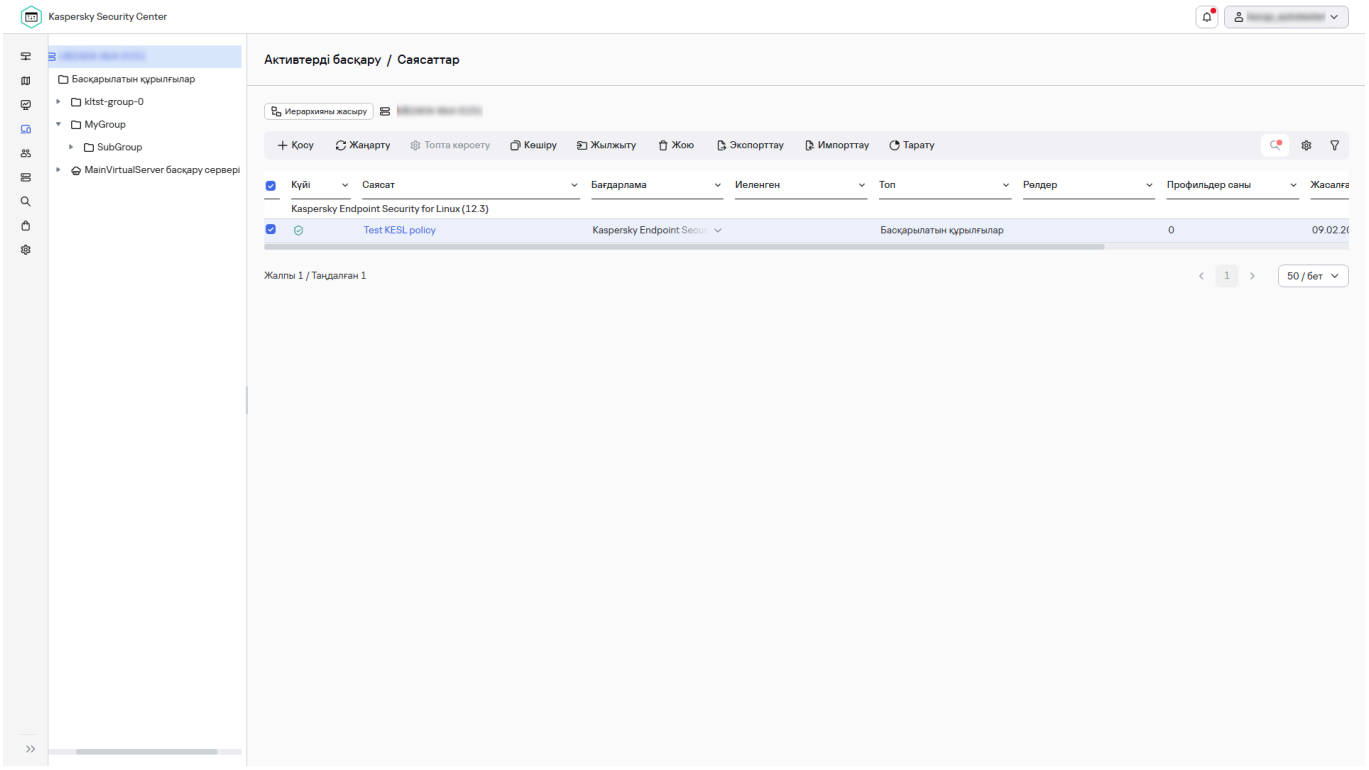
Kaspersky Security Center Linux бағдарламасы саясатты, оның параметрлерін және саясат профильдерін KLP файлына сақтауға мүмкіндік береді. Сақталған саясатты Kaspersky Security Center Windows, сондай-ақ Kaspersky Security Center Linux жүйелерінде импорттау үшін KLP файлын пайдалануға болады.

Саясатты экспорттау үшін:

1. Бағдарламаның негізгі терезесінде **Активтерді басқару** → **Саясаттар** бөліміне өтіңіз.

2. Экспорттағыңыз келетін саясаттың жанына жалаушаны қойыңыз.

Бір уақытта бірнеше саясатты экспорттауға болмайды. Егер сіз бірден артық саясатты таңдасаңыз, **Экспорттау** түймесі белсенді емес болмайды.



Экспорттау үшін саясатты таңдау

3. **Экспорттау** түймесін басыңыз.

4. Ашылған **Басқаша сақтау** терезесінде саясат файлының атауы мен жолын көрсетіңіз. **Сақтау** түймесін басыңыз.

   Басқаша сақтау терезесі Google Chrome, Microsoft Edge немесе Opera қолдансаңыз ғана көрсетіледі. Басқа браузерді қолданып жатсаңыз, саясат файлы автоматты түрде **Жүктеп алулар** қалтасына сақталады.

Саясатты импорттау

Kaspersky Security Center Linux бағдарламасы саясатты KLP файлынан импорттауға мүмкіндік береді. KLP файлында экспортталған саясат, оның параметрлері және саясат профильдері бар.

Саясатты импорттау үшін:

1. Бағдарламаның негізгі терезесінде **Активтерді басқару** → **Саясаттар** бөліміне өтіңіз.

2. **Импорттау** түймесін басыңыз.

3. Импорттағыңыз келетін саясат файлын таңдау үшін **Шолу** түймесін басыңыз.

4. Ашылған терезеде KLP саясаты файлына апаратын жолды көрсетіңіз және **Ашу** түймесін басыңыз. Назар аударыңыз, сіз тек бір саясатын файлын ғана таңдай аласыз.

   Саясатты өңдеу басталады.

5. Саясатты өңдеу сәтті аяқталғаннан кейін, саясатты қолданғыңыз келетін басқару тобын таңдаңыз.

6. Саясатты импорттауды аяқтау үшін **Аяқтау** түймесін басыңыз.

Импорт нәтижелері бар хабарландыру пайда болады. Саясатты импорттау сәтті орындалса, сіз саясат сипаттарын қарап шығу үшін **Мәліметтер** сілтемесінен өте аласыз.

Импорт сәтті орындалғаннан кейін, саясат саясаттар тізімінде көрсетіледі. Сондай-ақ, саясат параметрлері мен профильдері импортталады. Экспортта таңдалған саясаттың күйіне қарамастан, импортталатын саясат белсенді емес. Саясат сипаттарындағы саясаттың күйін өзгертуге болады.

Импортталған жаңа саясаттың атауы бұрыннан бар саясаттың атауымен бірдей болса, импортталған саясаттың атауы түр **(<реттік нөмір>)**, мысалы: **(1)**, **(2)** жалғауы көмегімен кеңейтіледі.

Мәжбүрлеп синхрондау

Kaspersky Security Center Linux бағдарламасы басқарылатын құрылғылар үшін күйді, параметрлерді, тапсырмаларды және саясаттарды автоматты түрде синхрондайтынына қарамастан, кейбір жағдайларда әкімші белгілі бір құрылғы үшін ағымдағы уақытта синхрондау орындалғанын нақты білуі керек.

Бір құрылғыны синхрондау

Басқару сервері мен басқарылатын құрылғы арасында мәжбүрлеп синхрондауды жүзеге асыру:

1. Бағдарламаның негізгі терезесінде **Активтерді басқару** → **Активтер (құрылғылар)** бөліміне өтіңіз.
2. Басқару серверімен синхрондау қажет құрылғының атауын таңдаңыз.

   Ашылған сипаттар терезесінде **Жалпы** бөлімін таңдаңыз.
3. **Мәжбүрлеп синхрондау** түймесін басыңыз.

Бағдарлама таңдалған құрылғыны Басқару серверімен синхрондауды орындайды.

Бірнеше құрылғыны синхрондау

Басқару сервері мен бірнеше басқарылатын құрылғылар арасында мәжбүрлеп синхрондауды жүзеге асыру:

1. Басқару тобы құрылғылары тізімін немесе құрылғы таңдауларын ашыңыз:
   - Құрылғылар тізімін қарау үшін құрылғы таңдауларын іске қосыңыз.
   - Негізгі мәзірде **Активтерді басқару** → **Активтер (құрылғылар)** тармағына өтіп, синхрондалатын құрылғылары бар басқару тобын таңдаңыз:
     - Түбірлік топ үшін келесі қадамға өтуге болады.
     - Ішкі топ үшін беттің жоғарғы жағындағы **Иерархияны көрсету** түймесін басыңыз, содан кейін ашылатын терезеде ішкі топтың атауын басыңыз.

       Таңдалған топ жолы беттің жоғарғы жағында көрсетіледі. Қажет болса, топқа өту үшін басқару тобының атауы бар сілтемені басуға болады. Әдепкісінше жолдағы соңғы сілтеме белсенді емес. Сондай-ақ **Иерархияны жасыру** түймесін басу арқылы иерархия терезесін жабуға болады.

2. Басқару серверімен синхрондауды қажет ететін құрылғылардың жанында жалауша қойыңыз.

3. Басқарылатын құрылғылар тізімі үстінде көп нүктелі (...) түймесін басып, **Мәжбүрлеп синхрондау** түймесін басыңыз.

   Бағдарлама таңдалған құрылғыларды Басқару серверімен синхрондауды орындайды.

4. Құрылғылар тізімінде таңдалған құрылғылар үшін соңғы Басқару серверіне қосылу уақыты ағымдағы уақытқа өзгергенін тексеріңіз. Егер уақыт өзгермесе, **Жаңарту** түймесін басу арқылы беттің мазмұнын жаңартыңыз.

Таңдалған құрылғылар Басқару серверімен синхрондалады.

Саясатты жеткізу уақытын қарау

Басқару серверіндегі Kaspersky бағдарламасының саясатын өзгерткеннен кейін, әкімші өзгертілген саясаттың белгілі бір басқарылатын құрылғыларға жеткізілгенін не жеткізілмегенін тексере алады. Саясат тұрақты немесе мәжбүрлеп синхрондау кезінде жеткізілуі мүмкін.

Басқарылатын құрылғыларға бағдарлама саясатын жеткізу күні мен уақытын көру үшін:

1. Бағдарламаның негізгі терезесінде **Активтерді басқару** → **Активтер (құрылғылар)** бөліміне өтіңіз.

2. Басқару серверімен синхрондау қажет құрылғының атауын таңдаңыз.

   Ашылған сипаттар терезесінде **Жалпы** бөлімін таңдаңыз.

3. **Бағдарламалар** қойыншасын таңдаңыз.

4. Саясатты синхрондау күнін көру қажет бағдарламаны таңдаңыз.

   Бағдарлама саясаты терезесі **Жалпы** таңдалған бөлімімен бірге ашылады және саясаттың жеткізілу күні мен уақыты көрсетіледі.

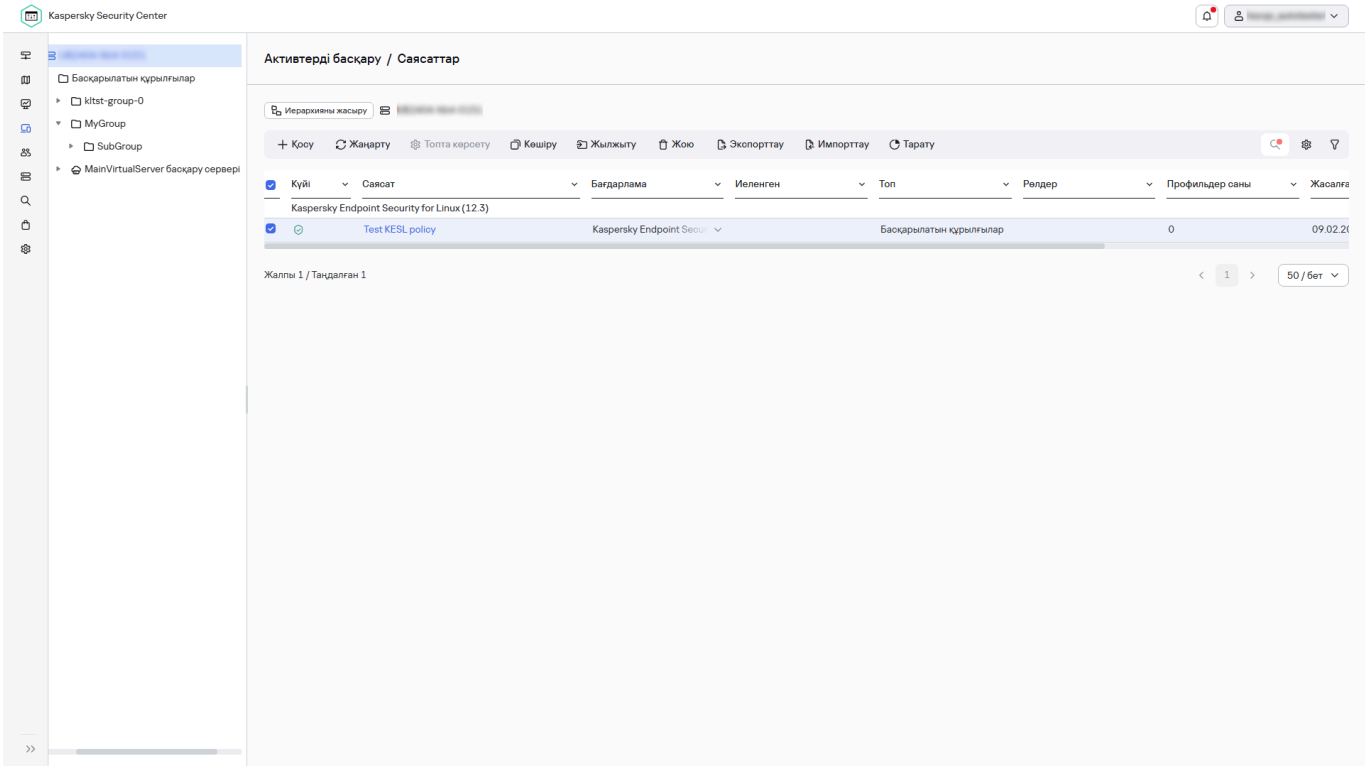
Саясатты қолдану күйінің диаграммасын қарау

Kaspersky Security Center Linux бағдарламасында диаграммадағы әрбір құрылғыда саясатты қолдану күйін көруге болады.

Әр құрылғыда саясатты қолдану күйін көру үшін:

1. Бағдарламаның негізгі терезесінде **Активтерді басқару** → **Саясаттар** бөліміне өтіңіз.

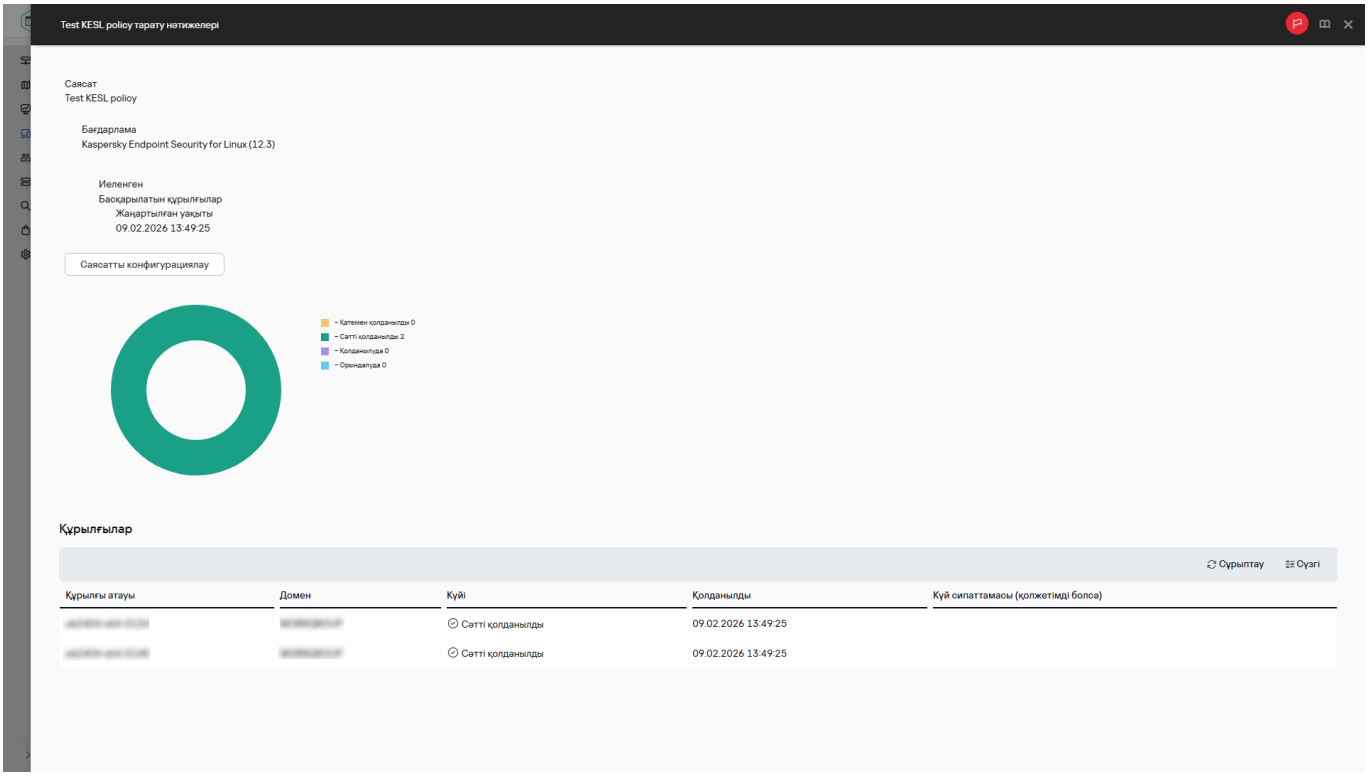
2. Құрылғыдағы қолдану күйін көргіңіз келетін саясат атауының жанына жалаушаны қойыңыз.



Саясаттар тізімі

3. Пайда болған мәзірден **Тарату** тармағын таңдаңыз.

   <саясат атауы> тарату нәтижесі терезесі ашылады.



Саясаттың тарату нәтижелері

4. Ашылған **<саясат атауы> тарату нәтижесі** терезесінде **Күйдің сипаттамасы** көрсетіледі.

Саясатты қолдану нәтижелері тізімінде көрсетілген нәтижелер санын өзгертуге болады. Құрылғылардың ең көп саны: 100,000.

Саясатты қолдану нәтижелерімен бірге тізімде көрсетілген құрылғылардың санын өзгерту үшін:

1. Негізгі мәзірдегі **Параметрлер** → **Интерфейс опциялары** бөліміне өтіңіз.
2. **Саясаттың тарату нәтижелерінде көрсетілетін құрылғылардың шегінде** құрылғылардың санын (100 000-ға дейін) енгізіңіз.

   Құрылғылардың әдепкі бойынша саны: 5000.
3. **Сақтау** түймесін басыңыз.

   Параметрлер сақталған және қолданылған.

"Вирустық шабуыл" оқиғасы бойынша саясатты автоматты түрде белсендіру

"Вирустық шабуыл" оқиғасы басталған кезде саясат автоматты түрде белсендірілді:

1. Негізгі мәзірдегі басқару серверінің атауын басыңыз.

   Жалпы қойыншасында Басқару сервері сипаттары терезесі ашылады.
2. **Вирустың тарауы** бөлімін таңдаңыз.
3. Оң жақ тақтада **Вирустық шабуыл оқиғасы орын алған кезде белсендірілетін саясаттарды конфигурациялау** сілтемесін басыңыз.

   Саясаттарды белсендіру терезесі ашылады.
4. Вирустық шабуылды анықтаған құрамдас (жұмыс станциялары мен файлдық серверлерге арналған вирусқа қарсы, пошталық серверлерге арналған вирусқа қарсы, периметрлік қорғанысқа арналған вирусқа қарсы бағдарламалар) қатысты болып келетін бөлімде өзіңізге қажетті жазбаны таңдап, **Қосу** түймесін басыңыз.

   Басқарылатын құрылғылар басқару тобы бар терезе ашылады.
5. **Басқарылатын құрылғылар** жанындағы шеврон (>) белгішесін басыңыз.

   Басқару топтары мен олардың саясаттары иерархиясы көрсетіледі.
6. Басқару топтары мен олардың саясаттарының иерархиясында вирустық шабуыл туындаған кезде іске қосылатын саясаттың (немесе саясаттардың) атын басыңыз.

   Тізімдегі немесе топтағы барлық саясаттарды таңдау үшін қажетті атаудың жанындағы жалаушаны қойыңыз.

7. **Сақтау** түймесін басыңыз.

   Басқару топтары мен олардың саясатының иерархиясы бар терезе жабылды.

Таңдалған саясаттар вирустық шабуыл туындаған кезде іске қосылатын саясаттар тізіміне қосылады. Таңдалған саясаттар вирустық шабуыл кезінде белсенді немесе белсенді емес екендігіне қарамастан іске қосылады.

Вирустық шабуыл оқиғасы бойынша саясат белсендірілген жағдайда, алдыңғы саясатқа тек қолмен оралуға болады.

Саясатты жою

Саясатты қажет болмаған кезде жоя аласыз. Таңдалған басқару тобында иеленбеген саясатты ғана жоюға болады. Егер саясат иеленген болса, оны тек ол жасалған басқару тобында жоюға болады.

Саясатты жою үшін:

1. Бағдарламаның негізгі терезесінде **Активтерді басқару** → **Саясаттар** бөліміне өтіңіз.
2. Жалаушаны, жойғыңыз келетін саясат атының жанына қойып, **Жою** түймесін басыңыз.

   Иеленген саясатты таңдаған болсаңыз, **Жою** түймесі белсенді емес (сұр) болады.
3. Операцияны растау үшін **OK** түймесін басыңыз.

Саясат және оның саясат профильдерінің барлығы жойылған. Саясат жойылғаннан кейін, егер бұл опция қосылған болса, саясатты өзгерту оқиғалары SIEM жүйесіне экспортталады.

Саясат профильдерін басқару

Бұл бөлім саясат профильдерін басқаруды сипаттайды және саясат профильдерін қарау, саясат профилінің басымдылығын өзгерту, саясат профилін жасау, саясат профилін көшіру, саясат профилін белсендіру ережесін жасау, саясат профилін жою, экспорттау және импорттау туралы ақпарат береді.

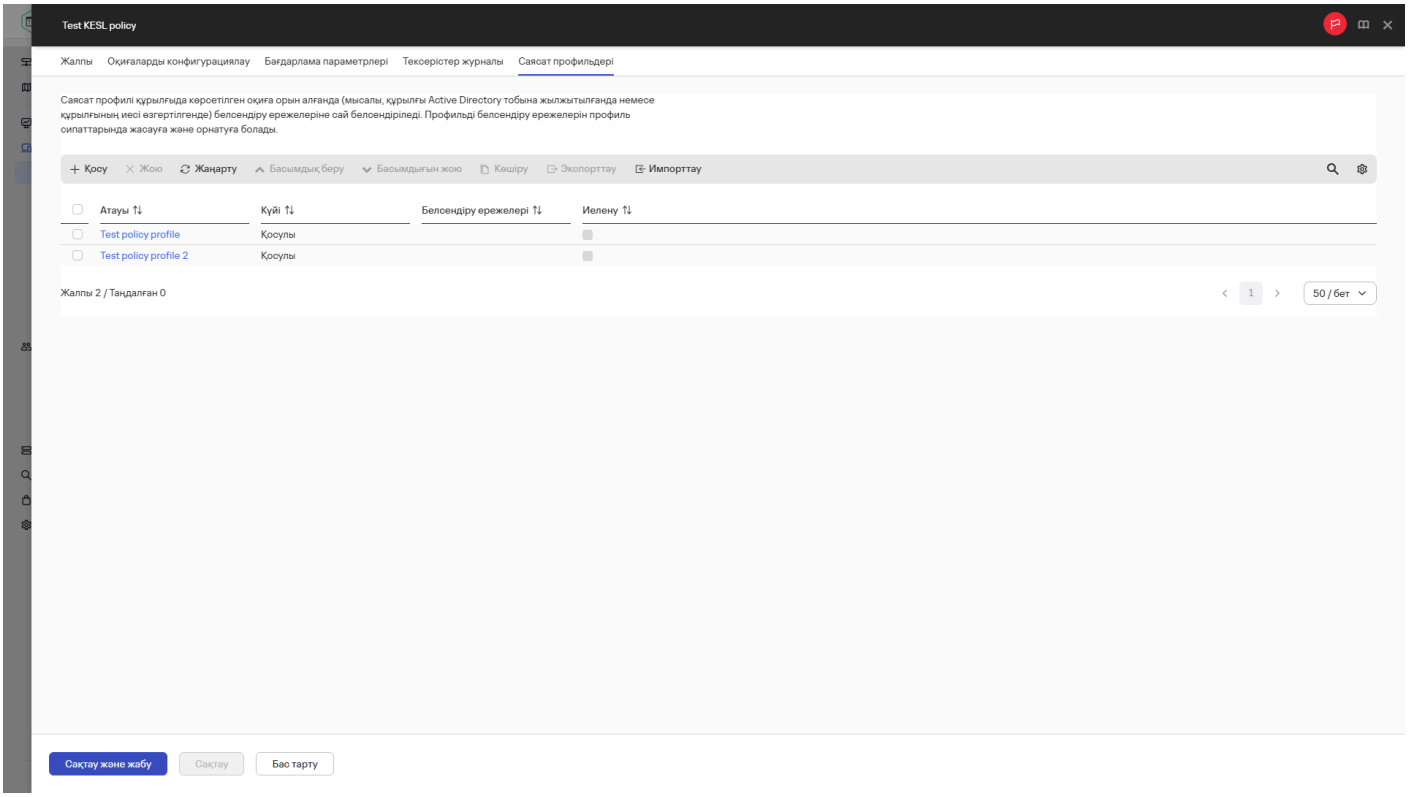
Саясат профильдерін қарау

Саясат профильдерін қарау үшін:

1. Бағдарламаның негізгі терезесінде **Активтерді басқару** → **Саясаттар** бөліміне өтіңіз.
2. Профильдерін қарау қажет саясатты таңдаңыз.

   Жалпы қойыншасында саясат сипаттары терезесі ашылады.
3. **Саясат профильдері** қойыншасын ашыңыз.

Саясат профильдері кесте түрінде көрсетіледі. Саясатта саясат профильдері болмаса, бос кесте көрсетіледі.



Саясат профильдері тізімі

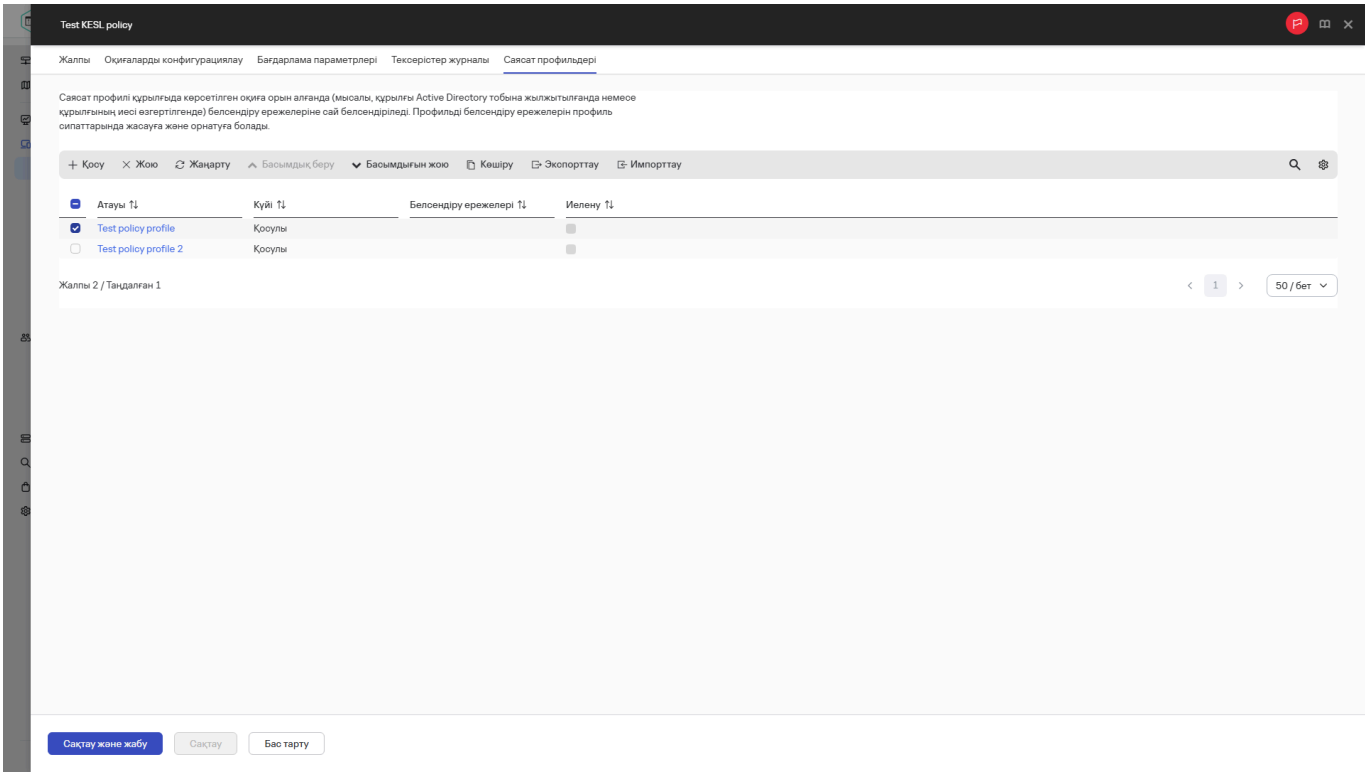
Саясат профилі басымдығын өзгерту

Саясат профилі басымдығын өзгерту үшін:

1. Таңдалған саясат профильдері тізіміне өтіңіз.

   Саясат профильдері тізімі ашылады.
2. **Саясат профильдері** қойыншасында, басымдығын өзгерту керек болған саясат профилінің жанында жалаушаны қойыңыз.
3. Саясат профилін **Басымдық беру** немесе **Басымдығын жою** түймелерінің көмегімен тізімдегі жаңа жайғасымға қойыңыз.

Тізімдегі саясат профилі неғұрлым жоғары болса, оның басымдығы да соғұрлым жоғары болады.



4. **Сақтау** түймесін басыңыз.

Таңдалған саясат профилі басымдығы өзгертілген және қолданылған.

Саясат профилін жасау

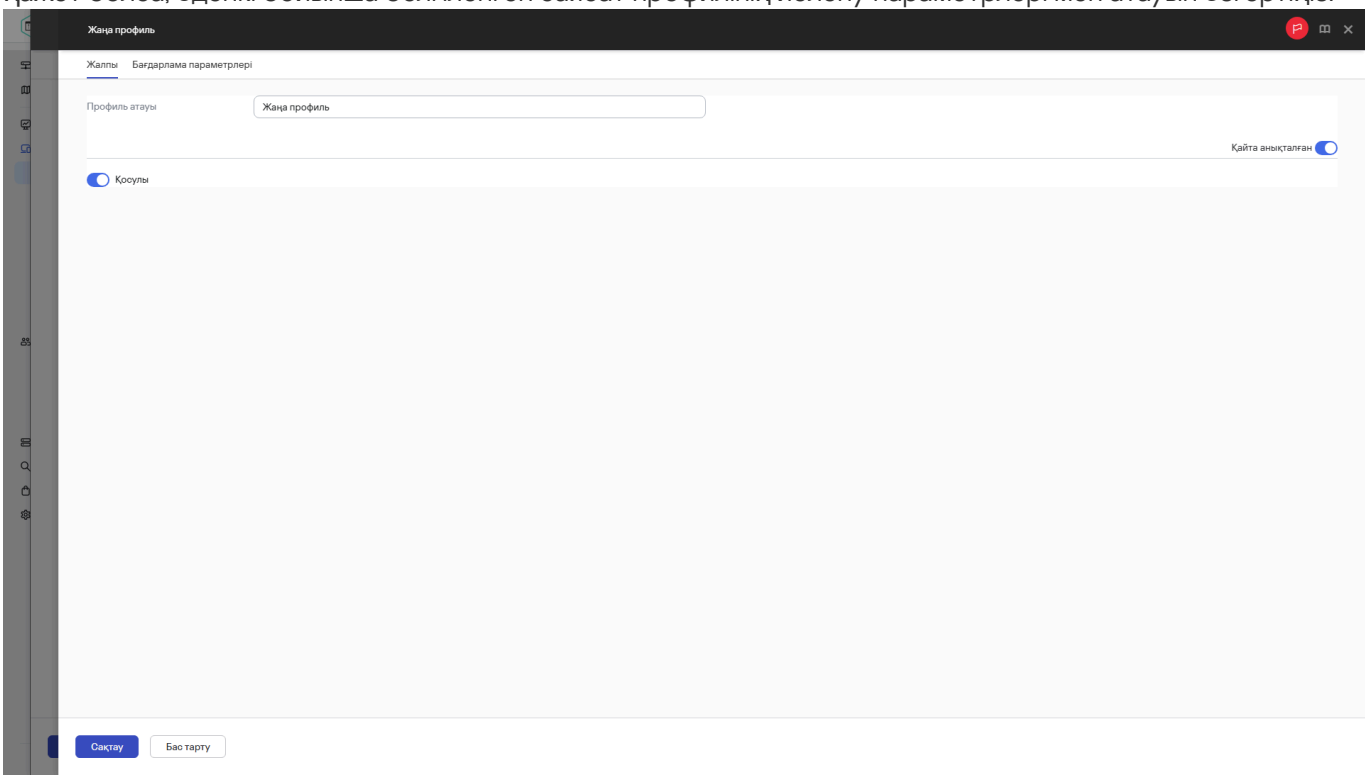
Саясат профилін жасау үшін:

1. Таңдалған саясат профильдері тізіміне өтіңіз.

Саясат профильдері тізімі ашылады. Саясатта саясат профильдері болмаса, бос кесте көрсетіледі.

2. **Қосу** түймесін басыңыз.

3. Қажет болса, әдепкі бойынша белгіленген саясат профилінің иелену параметрлері мен атауын өзгертіңіз.



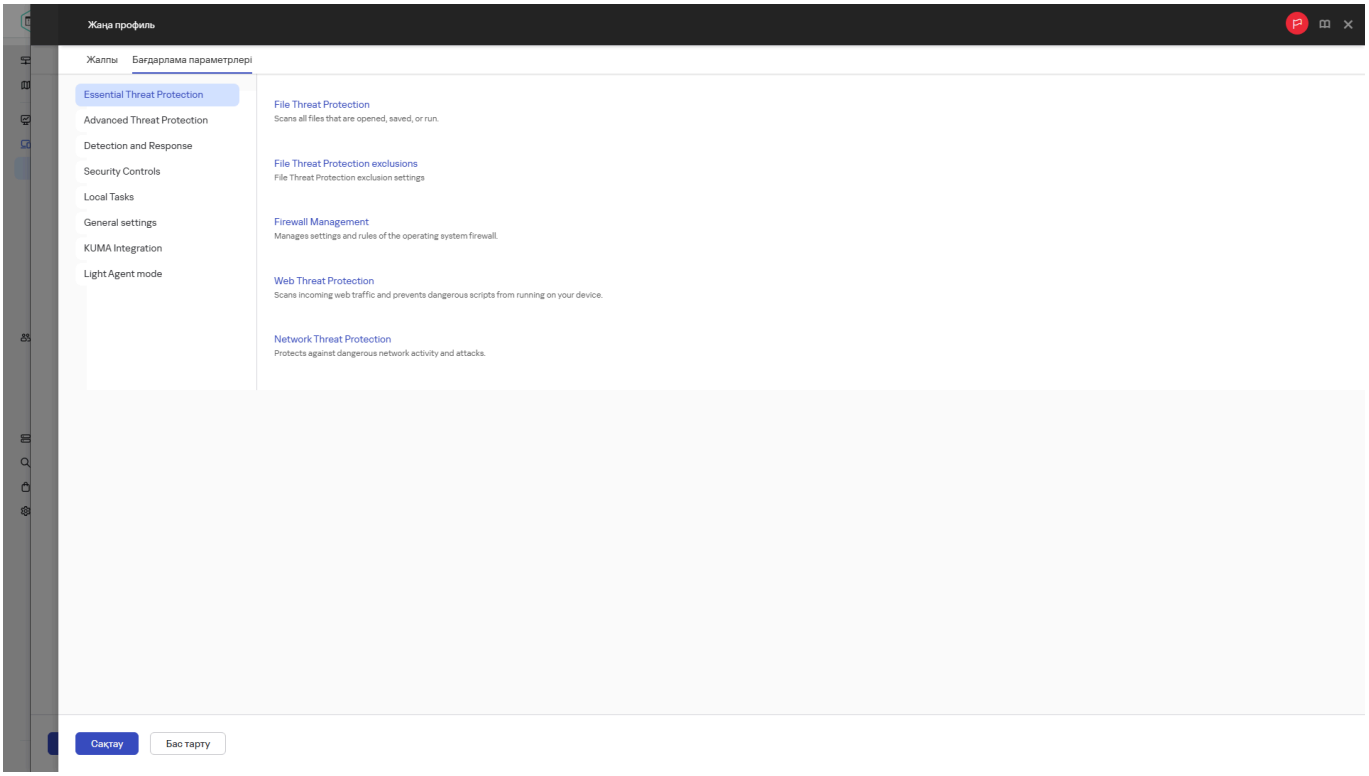
Жаңа саясат профилін жасау

4. **Бағдарлама параметрлері** қойыншасын таңдаңыз.

   Шығу үшін **Сақтау** түймесін басуға да болады. Құрылған саясат профилі саясат профильдерінің тізімінде көрсетіліп, сіз оның сипаттарын кейінірек өзгерте аласыз.

5. **Бағдарлама параметрлері** қойыншасының сол жағында, сізге қажетті бөлімді таңдап, нәтижелер тақтасында саясат профилі параметрлерін өзгертіңіз. Сіз әрбір бөлімдегі саясат профилі параметрлерін өзгерте аласыз.

Өзгерістерді болдырмау үшін **Бас тарту** түймесін басуға болады.



Саясат профилі параметрлерін анықтау

6. Профиль өзгерістерін сақтау үшін **Сақтау** түймесін басыңыз.

Саясат профилі саясат профильдері тізімінде көрсетіледі.

Саясат профилін көшіру

Саясат профилін ағымдағы саясатқа немесе басқа саясатқа көшіруге болады, мысалы, әртүрлі саясаттар үшін бірдей саясат профильдеріне ие болғыңыз келсе. Сондай-ақ, егер сіз параметрлердің аз санымен ерекшеленетін екі немесе одан да көп саясат профиліне ие болғыңыз келсе, көшіруді пайдалана аласыз.

Саясат профилін көшіру үшін:

1. Таңдалған саясат профильдері тізіміне өтіңіз.

   Саясат профильдері тізімі ашылады. Саясатта саясат профильдері болмаса, бос кесте көрсетіледі.

2. **Саясат профильдері** қойыншасында көшіру қажет болған профильді таңдаңыз.

3. **Көшіру** түймесін басыңыз.

4. Ашылған терезеде саясат профилін көшіру қажет болған саясатты таңдаңыз.

   Саясат профилін сол саясатқа немесе сіз таңдаған саясатқа көшіруге болады.

5. **Көшіру** түймесін басыңыз.

Саясат профилі сіз таңдаған саясатқа көшірілді. Жаңа көшірілген саясат профилі ең төменгі басымдыққа ие. Сіз саясат профилін сол саясатқа көшірген болсаңыз, осындай профильдің атауына түрдің жалғауы (<реттік нөмір>) қосылады, мысалы: (1), (2).

Кейінірек профиль параметрлерін, соның ішінде оның атауын және басымдығын өзгертуге болады; бұл жағдайда бастапқы саясат профилі өзгертілмейді.

Саясатын профилін белсендіру ережесін жасау

Саясатын профилін белсендіру ережесін жасау үшін:

1. Таңдалған саясат профильдері тізіміне өтіңіз.

   Саясат профильдері тізімі ашылады.

2. **Саясат профильдері** қойыншасында белсендіру ережесін жасауды қажет ететін саясат профилін басыңыз.

   Саясат профильдері тізімі бос болса, саясат профилін жасай аласыз.

3. **Белсендіру ережелері** қойыншасында **Қосу** түймесін басыңыз.

   Саясат профилін белсендіру ережелері бар терезе ашылады.

4. Белсендіру ережесінің атын көрсетіңіз.

5. Жасалғалы жатқан саясат профилін белсендіруге әсер етуі тиісті шарттарға қарама-қарсы жалаушалар қойыңыз:

   - **Саясат профилін белсендірудің жалпы ережелері**

     Құрылғының автономды режимі күйіне, құрылғыны Басқару серверіне қосу ережелеріне және құрылғыға тағайындалған тегтерге байланысты құрылғыдағы саясат профилін белсендіру ережелерін конфигурациялау үшін жалаушаны қойыңыз.

     Бұл параметр үшін келесі қадамда мынаны көрсетіңіз:

     - **Құрылғының күйі**

       Құрылғының желіде болу шартын анықтайды:

       - **Онлайн** – құрылғы желіде орналасқан, Басқару сервері қолжетімді.
       - **Офлайн** – құрылғы сыртқы желіде орналасқан, яғни Басқару сервері қолжетімді емес.
       - **Қолданылмайды** – өлшемшарт қолданылмайды.

     - **Құрылғының желідегі орны**

       Саясат профилін белсендіру үшін шартты таңдаңыз (бұл ереже орындалса да, орындалмаса да) және ереже атауын таңдаңыз.

       Ереже, шарттарын орындау немесе орындамау кезінде саясат профилі белсендірілетін Басқару серверіне қосылуға арналған құрылғының желілік орнымен анықталады.

       Басқару серверіне қосылу үшін құрылғылардың желілік орнының сипаттамасын Желілік агентті ауыстырып қосу ережесінде жасауға немесе конфигурациялауға болады.

   - **Арнайы құрылғы иесіне арналған ережелер**

Бұл параметр үшін келесі қадамда мынаны көрсетіңіз:

- **Құрылғының иесі**

  Құрылғының иесі бойынша құрылғыдағы профильді белсендіру ережесін конфигурациялау және қосу үшін параметрді қосыңыз. Жалауша астындағы ашылмалы тізімнен профильді белсендіру өлшемшартын таңдауға болады:

  - құрылғы көрсетілген иеленушіге тисілі ("=" белгісі);
  - құрылғы көрсетілген иеленушіге тисілі емес ("#" белгісі).

    Параметр қосулы болса, құрылғыдағы профильді белсендіру конфигурацияланған өлшемшартқа сәйкес орындалады. Параметр қосылған кезде, құрылғы иесін көрсетуіңізге болады. Бұл параметр өшірулі болса, профильді белсендіру өлшемшарты қолданылмайды. Әдепкі бойынша, параметр өшірулі.

- **Құрылғы иесі ішкі қауіпсіздік тобына кіреді**

  Kaspersky Security Center Linux ішкі қауіпсіздік тобындағы құрылғы иесінің мүшелігі бойынша құрылғыдағы профильді белсендіру ережесін конфигурациялау және қосу үшін параметрді қосыңыз. Жалауша астындағы ашылмалы тізімнен профильді белсендіру өлшемшартын таңдауға болады:

  - құрылғының иесі көрсетілген қауіпсіздік тобының мүшесі ("=" белгісі);
  - құрылғының иесі көрсетілген қауіпсіздік тобының мүшесі емес ("#" белгісі).

    Параметр қосулы болса, құрылғыдағы профильді белсендіру конфигурацияланған өлшемшартқа сәйкес орындалады. Сіз Kaspersky Security Center Linux қауіпсіздік тобын көрсете аласыз. Бұл параметр өшірулі болса, профильді белсендіру өлшемшарты қолданылмайды. Әдепкі бойынша, параметр өшірулі.

- **Жабдық сипаттамалары ережелері**

  Жадтың көлеміне және құрылғының логикалық процессорларының санына байланысты құрылғыдағы саясатты белсендіру шартын конфигурациялау үшін жалаушаны қойыңыз.

  Бұл параметр үшін келесі қадамда мынаны көрсетіңіз:

  - **ЖЖҚ-тың көлемі, МБ түрінде**

    Құрылғының жедел жад көлемі бойынша құрылғыдағы профильді белсендіру ережесін конфигурациялау және қосу үшін параметрді қосыңыз. Жалауша астындағы ашылмалы тізімнен профильді белсендіру өлшемшартын таңдауға болады:

    - құрылғының жедел жады көлемі көрсетілген мәннен аз ("<" белгісі);
    - құрылғының жедел жады көлемі көрсетілген мәннен артық (">" белгісі).

    Параметр қосулы болса, құрылғыдағы профильді белсендіру конфигурацияланған өлшемшартқа сәйкес орындалады. Құрылғының жедел жадының көлемін көрсетуге болады. Бұл параметр өшірулі болса, профильді белсендіру өлшемшарты қолданылмайды. Әдепкі бойынша, параметр өшірулі.

- **Логикалық процессорлардың саны**

  Құрылғының логикалық процессорлардың саны бойынша құрылғыдағы профильді белсендіру ережесін конфигурациялау және қосу үшін параметрді қосыңыз. Жалауша астындағы ашылмалы тізімнен профильді белсендіру өлшемшартын таңдауға болады:

  - құрылғының логикалық процессорларының саны көрсетілген мәннен аз немесе оған тең ("<" белгісі);
  - құрылғының логикалық процессорларының саны көрсетілген мәннен артық немесе оған тең (">" белгісі).

  Параметр қосулы болса, құрылғыдағы профильді белсендіру конфигурацияланған өлшемшартқа сәйкес орындалады. Құрылғының логикалық процессорларының санын көрсетуіңізге болады. Бұл параметр өшірулі болса, профильді белсендіру өлшемшарты қолданылмайды. Әдепкі бойынша, параметр өшірулі.

- **Рөлді тағайындау ережелері**

  Бұл параметр үшін келесі қадамда мынаны көрсетіңіз:

  - **Құрылғы иесінің арнайы рөлі бойынша саясат профилін белсендіру**

    Құрылғы иесінің белгілі бір рөлінің болуына байланысты, құрылғыда саясат профилін белсендіру ережесін конфигурациялау және қосу үшін осы параметрді қосыңыз. Қолданыстағы рөлдер тізімінен рөлді қолмен қосыңыз.

    Параметр қосулы болса, құрылғыдағы профильді белсендіру конфигурацияланған өлшемшартқа сәйкес орындалады.

- **Тегті қолдану ережелері**

  Құрылғыға тағайындалған тегтерге байланысты құрылғыдағы саясат профилін белсендіру ережелерін конфигурациялау үшін жалаушаны қойыңыз. Саясат профилін таңдалған тегтері бар немесе жоқ құрылғыларда белсендіруге болады.

  Бұл параметр үшін келесі қадамда мынаны көрсетіңіз:

  - **Тегтер тізімі**

    Тегтер тізімінде қажетті тегтерге жалаушалар қою арқылы құрылғыларды саясат профиліне қосу ережесін белгілеңіз.

    Тізімге жаңа тегтерді қосу үшін оларды тізімнің үстіндегі өріске енгізіп, **Қосу** түймесін басуыңызға болады.

    Саясат профиліне, сипаттамасында барлық таңдалған тегтері бар құрылғылар қосылады. Жалаушалар алынып тасталса, өлшемшарт қолданылмайды. Әдепкі бойынша, жалаушалар алынып тасталған.

  - **Көрсетілген тегтерсіз құрылғыларға қолдану**

    Тег таңдауын терістету қажет болса, параметрді қосыңыз.

    Параметр қосулы болса, онда саясат профиліне, сипаттамасында таңдалған тегтері жоқ құрылғылар қосылады. Бұл параметр өшірулі болса, өлшемшарт қолданылмайды.

    Әдепкі бойынша, параметр өшірулі.

- **Active Directory қызметін пайдалану ережелері**

  Құрылғының Active Directory бөлімшесінде орналасуына немесе құрылғының не оның иесінің Active Directory қауіпсіздік тобына мүше болуына байланысты құрылғыдағы саясат профилін белсендіру ережелерін конфигурациялау үшін жалаушаны қойыңыз.

  Бұл параметр үшін келесі қадамда мынаны көрсетіңіз:

  - **Құрылғы иесінің Active Directory қауіпсіздік тобындағы мүшелігі**

    Параметр қосулы болса, онда саясат профилі, иесі аталған қауіпсіздік тобының мүшесі болып табылатын құрылғыда іске қосылады. Бұл параметр өшірулі болса, профильді белсендіру өлшемшарты қолданылмайды. Әдепкі бойынша, параметр өшірулі.

  - **Құрылғының Active Directory қауіпсіздік тобындағы мүшелігі**

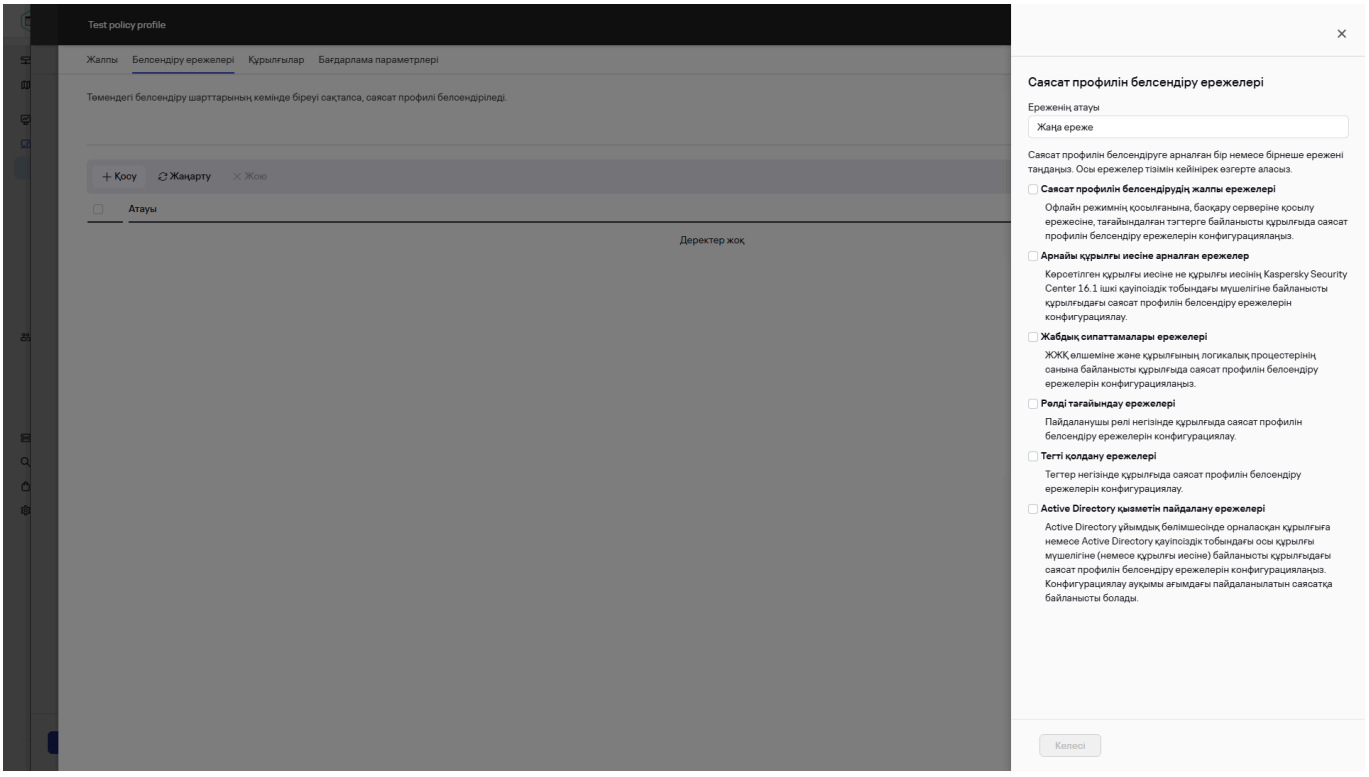
    Параметр қосулы болса, құрылғыда саясат профилі белсендіріледі. Бұл параметр өшірулі болса, профильді белсендіру өлшемшарты қолданылмайды. Әдепкі бойынша, параметр өшірулі.

  - **Active Directory бөлімшесіне құрылғыны орналастыру**

    Параметр қосулы болса, саясат профилі көрсетілген Active Directory бөлімшесіне кіретін құрылғыда белсендіріледі. Бұл параметр өшірулі болса, профильді белсендіру өлшемшарты қолданылмайды.

    Әдепкі бойынша, параметр өшірулі.

Шебер терезелерінің кейінгі саны осы қадамдағы параметрлерді таңдауға байланысты. Саясат профилін белсендіру ережелерін кейінірек өзгертуге болады.



Саясатын профилін белсендіру ережесін жасау

6. Конфигурацияланған параметрлер тізімін тексеріңіз. Тізімі дұрыс болса, **Жасау** түймесін басыңыз.

Нәтижесінде, профиль сақталады. Белсендіру ережелері орындалған кезде профиль құрылғыда белсендіріледі.

Профиль үшін жасалған саясат профилін белсендіру ережелері **Белсендіру ережелері** қойыншасындағы саясат профилінің сипаттарында көрсетіледі. Саясат профилін белсендіру ережесін өзгертуге немесе жоюға болады.

Бірнеше белсендіру ережесі бір уақытта орындалуы мүмкін.

Саясат профилін жою

Саясат профилін жою үшін:

1. Таңдалған саясат профильдері тізіміне өтіңіз.

   Саясат профильдері тізімі ашылады.

2. **Саясат профильдері** бетінде, жойғыңыз келетін саясат профилінің жанында жалауша қойып, **Жою** түймесін басыңыз.

3. Пайда болған терезеде **Жою** түймесін тағы да басыңыз.

Саясат профилі жойылды. Егер саясатты аса төменгі деңгейдегі топ иеленсе, саясат профилі осы топта қала береді, бірақ осы топтың саясат профиліне айналады. Бұл, төменгі деңгейдегі топтардың құрылғыларына орнатылған басқарылатын бағдарламалардың параметрлерінде өзгерістерді азайтуға мүмкіндік береді.

Саясат профилін экспорттау және импорттау

Саясат профилін саясатты экспорттамастан KLPROF файлына сақтауға болады, содан кейін сақталған профильді саясатқа импорттау үшін осы KLPROF файлын пайдалануға болады.

Бұл профиль саясаты параметрлерін қайта конфигурациялаудың орнына жылдам қалпына келтіруге мүмкіндік береді.

Саясат профилі профильді экспорттаған қолданбаның бірдей нұсқасының саясатына импортталады. Саясаттардың кері үйлесімділігін қолдайтын қолданбалар үшін (мысалы, Kaspersky Endpoint Security for Windows), саясат профильдерін саясаттың әртүрлі нұсқаларына импорттай аласыз.

Саясатты экспорттау үшін:

1. Таңдалған саясат профильдері тізіміне өтіңіз.

   Саясат профильдері тізімі ашылады.

2. **Саясат профильдері** қойыншасында өзгерткіңіз келетін саясат профилін нұқыңыз.

3. Құралдар тақтасындағы **Экспорттау** түймесін басыңыз.

4. Ашылған терезеде саясат профилі бар файлды сақтағыңыз келетін каталогты көрсетіңіз.

   Қажет болса, файл атауын өзгертуге болады.

5. **Сақтау** түймесін басыңыз.

Егер оператор сәтті аяқталса, экранда тиісті хабарлама көрсетіледі. Әйтпесе, қате туралы хабар көрсетіледі.

Саясатты импорттау үшін:

1. Таңдалған саясат профильдері тізіміне өтіңіз.

   Саясат профильдері тізімі ашылады.

2. Құралдар тақтасындағы **Импорттау** түймесін басыңыз.

3. Ашылған терезеде қажетті саясат профилі бар KLPROF файлын таңдап, **Ашу** түймесін басыңыз.

   Импортталған файлдың максималды өлшемі 4 МБ.

Егер оператор сәтті аяқталса, экранда тиісті хабарлама көрсетіледі. Әйтпесе, қате туралы хабар көрсетіледі.

Саясат профилі KLPROF файлының атауымен емес, экспорттаған кездегі атауымен импортталады. Файл экспорттауға дейін саясат профилінде қандай басымдық болғанына қарамастан, **Өшірулі** мәртебесімен және ең төменгі басымдықпен импортталады.

Импорттауды келесі жағдайларда орындай алмайсыз:

- Саясаттың аты бірдей профиль бар болса.
- Саясаттағы профильдер саны 100 болса.

Желілік агент саясатының параметрлері

Желілік агент саясаты параметрлерін конфигурациялау үшін:

1. Қолданбаның негізгі терезесінде **Активтерді басқару** → **Саясаттар** бөліміне өтіңіз.

2. Желілік агент саясатының атауын басыңыз.

   Желілік агент саясатының сипаттары терезесі ашылады. Сипаттар терезесі төменде сипатталған қойындылар мен параметрлерді қамтиды.

Пайдаланылатын операциялық жүйе түріне байланысты төмендегі параметрлердің қалай қолданылатынын егжей-тегжейлі сипаттайтын салыстыру кестесін қараңыз.

Жалпы

Бұл қойыншада саясаттың атауын, саясаттың күйін өзгертуге және саясат параметрлерін иеленуді конфигурациялауға болады:

- **Атауы** өрісінде саясаттың атауын өзгертуге болады.
- **Саясаттың күйі** блогында саясаттың әрекет ету ауқымы нұсқаларының біреуін таңдауға болады:
  - **Белсенді**

    Осы нұсқа таңдалған болса, саясат белсенді болады.

    Әдепкі бойынша, осы нұсқа таңдалған.
  - **Белсенді емес**

    Егер бұл нұсқа таңдалса, саясат белсенді болмайды, бірақ **Саясат** қалтасында сақталады. Қажет болса, оны белсенді етуге болады.
- **Параметрлерді иелену** блогында саясатты иелену параметрлерін конфигурациялауға болады:
  - **Параметрлерді ата-ана саясаттан иелену**

    Параметр қосулы болса, саясат параметрлері мәндері иерархияның жоғарғы деңгейіндегі топқа арналған саясаттан иеленеді және өзгерту үшін қолжетімді емес.

    Әдепкі бойынша, параметр қосулы.
  - **Еншілес саясаттардағы параметрлерді мәжбүрлеп иелену**

    Егер параметр қосылса, саясатқа өзгертулер қолданылғаннан кейін келесі қадамдар орындалады:
    - саясат параметрлерінің мәндері салынған басқару топтарының саясаты – еншілес саясаттарға қатысты қолданылады;
    - Әрбір еншілес саясат сипаттары терезесінің **Жалпы** бөлімінің **Параметрлерді иелену** блогында **Параметрлерді негізгі саясаттан иелену** параметрі автоматты түрде қосылады.

    Параметр қосулы болған кезде, еншілес саясат параметрлерінің мәндерін өзгерту қолжетімді емес.

    Әдепкі бойынша, параметр өшірулі.

Оқиғаларды конфигурациялау

Бұл қойыншада оқиғаларды тіркеуді және оқиғалар туралы хабарлауды конфигурациялауға болады. Оқиғалар маңыздылық деңгейі бойынша келесі бөлімдерде бөлінеді:

- **Функционалдық ақау**
- **Ескерту**
- **Ақпараттық**

Оқиғалар тізіміндегі әрбір бөлімде оқиғалардың атаулары және әдепкі бойынша Басқару серверінде оқиғаларды сақтау мерзімі (күндерде) көрсетіледі. Оқиға түрін басқаннан кейін тізімде таңдалған оқиғаларды тіркеу және хабарландыру параметрлерін конфигурациялауға болады. Әдепкі бойынша, барлық Басқару сервері үшін көрсетілген жалпы хабарландыру конфигурациясы оқиғалардың барлық түрлері үшін қолданылады. Дегенмен, белгіленген оқиға түрлері үшін белгілі бір параметрлерді өзгертуге болады.

Мысалы, **Ескерту** бөлімінде **Қауіпсіздік мәселесі пайда болды** оқиға түрін конфигурациялауға болады. Мұндай оқиғалар, мысалы, тарату нүктесінің дискісіндегі бос орын 2 ГБ-тан аз болған кезде туындауы мүмкін (бағдарламаларды орнату және жаңартуларды қашықтан жүктеу үшін кемінде 4 ГБ қажет). **Қауіпсіздік мәселесі пайда болды** оқиғасын конфигурациялау үшін оған басып, орын алған оқиғаларды қайда сақтау керектігін және олар туралы қалай хабарлау керектігін көрсетіңіз.

Желілік агент қауіпсіздік мәселесін анықтаса, сіз бұл қауіпсіздік мәселесін басқарылатын құрылғы параметрлері арқылы басқара аласыз.

Бағдарлама параметрлері

Параметрлер

Параметрлер бөлімінде Желілік агент саясатының параметрлерін конфигурациялауға болады:

- **Файлдарды тек тарату нүктелері арқылы тарату**

  Егер бұл параметр қосылса, басқарылатын құрылғылардағы Желілік агенттер жаңартуларды тек тарату нүктелерінен алады.

  Егер бұл параметр өшірулі болса, басқарылатын құрылғылардағы Желілік агенттер тарату нүктелерінен немесе Басқару серверінен жаңартулар алады.

  Басқарылатын құрылғылардағы қауіпсіздік бағдарламалары әрбір қауіпсіздік бағдарламасы үшін жаңарту тапсырмасында белгіленген көзден жаңартуларды алатынын ескеріңіз. Егер **Файлдарды тек тарату нүктелері арқылы тарату** параметрін қоссаңыз, Kaspersky Security Center Linux жаңарту тапсырмаларында жаңарту көзі ретінде орнатылғанына көз жеткізіңіз.

  Әдепкі бойынша, параметр өшірулі.

- **Оқиғалар кезегінің максималды өлшемі, МБ**

  Өрісте оқиғалар кезегі болуы мүмкін дискідегі максималды орынды көрсетуге болады.

  Әдепкі бойынша, 2 МБ мәні көрсетілген.

- **Бағдарламаға құрылғыда саясаттың кеңейтілген деректерін шығарып алуға рұқсат берілген**

  Басқарылатын құрылғыға орнатылған Желілік агент, қолданылатын саясат туралы ақпаратты қауіпсіздік бағдарламасына жібереді (мысалы, Kaspersky Endpoint Security for Linux). Берілетін ақпарат қауіпсіздік бағдарламасының интерфейсінде көрсетіледі.

Желілік агент келесі ақпаратты береді:

- Саясатты басқарылатын құрылғыға жеткізу уақыты.
- Саясатты басқарылатын құрылғыға жеткізу кезінде белсенді саясат атауы.
- Басқарылатын құрылғыға саясатты жеткізу сәтіндегі кеңседен тыс саясаттың атауы (Linux жүйесіне арналған желілік агент үшін қолжетімді емес).
- Саясатты басқарылатын құрылғыға жеткізу кезінде басқарылатын құрылғыға тиесілі басқару тобының атауы және толық жолы.
- Басқарылатын құрылғыға саясатты жеткізу сәтіндегі атаулары мен басымдықтары бар белсенді саясат профильдерінің тізімі.

Бұл ақпаратты, құрылғыға дұрыс саясатты қолдануды қамтамасыз ету үшін және ақауларды жою мақсатында пайдалана аласыз. Әдепкі бойынша, параметр өшірулі.

- **Желілік агент қызметін рұқсатсыз өшіруден немесе тоқтатудан қорғау және параметрлердегі өзгерістердің алдын алу**

  Желілік агент басқарылатын құрылғыға орнатылғаннан кейін, құрамдасты қажетті құқықтарсыз жою немесе өзгерту мүмкін емес. Желілік агенттің жұмысын тоқтату мүмкін емес. Бұл параметр домен контроллерлеріне әсер етпейді.

  Жергілікті әкімші құқықтарымен басқарылатын жұмыс станцияларында Желілік агентті қорғау үшін осы параметрді қосыңыз.

  Әдепкі бойынша, параметр өшірулі.

- **Жою құпиясөзін пайдалану**

  Бұл опция қосулы болса, **Өзгерту** түймесін басқан кезде, желілік агентті Windows негізіндегі құрылғылардан қашықтан жою тапсырмасы үшін klmover утилитасына арналған құпиясөзді көрсетуге болады.

  Әдепкі бойынша, параметр өшірулі.

Қоймалар

Қоймалар бөлімінде желілік агенттен басқару серверіне жіберілетін нысандардың түрлерін таңдауға болады.

- **Орнатылған бағдарламалардың мәліметтері**

  Егер бұл параметр қосылса, клиент құрылғыларында орнатылған бағдарламалар туралы ақпарат Басқару серверге жіберіледі.

  Әдепкі бойынша, параметр қосулы.

- **Патчтар туралы ақпаратты қамту**

  Клиент құрылғыларында орнатылған бағдарлама патчтары туралы ақпарат Басқару серверіне жіберіледі. Бұл параметрді қосу, Басқару сервері мен ДҚБЖ-не түсетін жүктемені арттырып, дерекқор көлемінің ұлғаюына әкелуі мүмкін.

  Әдепкі бойынша, параметр қосулы. Тек Windows үшін қолжетімді.

- **Windows Update жаңартулар мәліметтері**

  Опция қосылса, клиент құрылғыларына орнатылуы керек Microsoft Windows Update міндетті жаңартулары туралы ақпарат басқару серверіне жіберіледі.

  Әдепкі бойынша, параметр қосулы. Тек Windows үшін қолжетімді.

  Қосымша Microsoft Windows жаңартулары туралы ақпарат басқару серверіне жіберілмейді.

- **Бағдарламалық жасақтама осалдықтары мен сәйкес жаңартулар туралы мәліметтер**

  Егер бұл параметр қосылса, басқарылатын құрылғыларда табылған үшінші тарап бағдарламаларындағы (Microsoft бағдарламалық жасақтамасын қоса) осалдықтар туралы ақпарат және осалдықтарды түзету бағдарламалық жасақтамасының жаңартулары (Microsoft бағдарламалық жасақтамасын қоспағанда) Басқару серверіне жіберіледі.

  Осы параметрді таңдау (**Бағдарламалық жасақтама осалдықтары мен сәйкес жаңартулар туралы мәліметтер**) желі жүктемесін, Басқару сервері дискісінің жүктемесін және Желілік агент ресурстарын тұтынуды арттырады.

  Әдепкі бойынша, параметр қосулы. Тек Windows үшін қолжетімді.

  Microsoft бағдарламаларының жаңартуларын басқару үшін **Windows Update жаңартулар мәліметтері** параметрін пайдаланыңыз

- **Жабдық тізімдемесі туралы ақпарат**

  Құрылғыға орнатылған Желілік агент құрылғының жабдықтары туралы ақпаратты Басқару серверіне жібереді. Жабдық туралы ақпаратты құрылғының сипаттарынан көруге болады.

  lshw утилитасы, жабдық туралы ақпарат алғыңыз келетін Linux құрылғыларында орнатылғанын тексеріңіз. Виртуалды машиналардан алынған жабдық туралы мәлімет пайдаланылатын гипервизорға байланысты толық болмауы мүмкін

Желілік агент саясатында, осы бөлімде көрсетілген параметрлерді өзгертуге тыйым салынса, бұл параметрлерді өзгерту мүмкін емес.

Бағдарламалық жасақтаманың жаңартулары мен осалдықтары

Бағдарламалық жасақтаманың жаңартулары мен осалдықтары бөлімінде орындалатын файлдарда осалдықтар бар-жоғын сканерлеуге болады.

- **Іске қосу кезінде орындалатын файлдарда осалдықтар бар-жоғын сканерлеу**

  Параметр қосулы болса, орындалатын файлдарды іске қосу кезінде олардың осалдығын тексеру жүргізіледі.

  Әдепкі бойынша, параметр қосулы.

Өшіріп қайта іске қосуды басқару

Қолданбаны дұрыс пайдалану, орнату не жою үшін басқарылатын құрылғының операциялық жүйесін өшіріп қосу қажет болса, **Өшіріп қайта іске қосуды басқару** бөлімінде орындалатын әрекетті көрсетуге болады.

- **Операциялық жүйені қайта жүктемеу**

  Операция аяқталғаннан кейін, клиент құрылғылары автоматты түрде қайта жүктелмейді. Операцияны аяқтау үшін құрылғыны қайта қосу қажет (мысалы, қолмен немесе құрылғыны басқару тапсырмасы арқылы). Қайта жүктеу қажеттілігі туралы ақпарат тапсырманы орындау нәтижелерінде және құрылғы күйінде сақталады. Бұл нұсқа, үздіксіз жұмыс өте маңызды болып саналатын серверлердегі және басқа құрылғылардағы тапсырмалар үшін жарамды.

- **Қажет болса, операциялық жүйені автоматты түрде қайта іске қосыңыз**

  Бұл жағдайда, операцияны аяқтау үшін қайта жүктеу қажет болса, қайта жүктеу әрқашан автоматты түрде орындалады. Бұл нұсқа, мезгіл-мезгіл үзілістерге (өшіру, қайта жүктеу) рұқсат етілген құрылғылардағы тапсырмалар үшін жарамды.

- **Пайдаланушыдан әрекетті орындауды сұрау**

  Клиент құрылғысының экранында құрылғыны қолмен қайта жүктеу керек деген хабар пайда болады. Бұл нұсқа үшін қосымша параметрлерді конфигурациялауға болады: пайдаланушыға арналған хабар мәтіні, хабардың жиілігі, сондай-ақ қайта жүктеу мәжбүрлі түрде орындалатын уақыт (пайдаланушының растауынсыз). Бұл нұсқа жұмыс станциялары үшін оңтайлы болып табылады, сондықтан пайдаланушылар қайта жүктеудің ең қолайлы уақытын таңдай алады.

  Әдепкі бойынша, осы нұсқа таңдалған.

  - **Сұрауды қайталау жиілігі (мин)**

    Егер бұл нұсқа таңдалса, белгілі бір жиіліктегі бағдарлама пайдаланушыға операциялық жүйені қайта жүктеуді ұсынады.

    Әдепкі бойынша, параметр қосулы. Әдепкі бойынша аралық 5 минутты құрайды. Рұқсат етілген мәндер: 1-ден 1440 минутқа дейін.

    Егер параметр өшірулі болса, қайта жүктеу ұсынысы тек бір рет көрсетіледі.

  - **Осы уақыттан кейін мәжбүрлеп қайта іске қосу (мин)**

    Пайдаланушыға операциялық жүйені қайта жүктеуді ұсынғаннан кейін, бағдарлама көрсетілген уақыттан кейін мәжбүрлеп қайта жүктеуді орындайды.

    Әдепкі бойынша, параметр қосулы. Әдепкі бойынша уақыт аралығы 30 минутты құрайды. Рұқсат етілген мәндер: 1-ден 1440 минутқа дейін.

  - **Бұғатталған сеанстардағы бағдарламалардың мәжбүрлі жабылуы**

    Іске қосылған қолданбалар клиент құрылғысын қайта жүктеуге мүмкіндік бермеуі мүмкін. Мысалы, егер мәтіндік редакторда құжатпен жұмыс жасалса және өзгертулер сақталмаса, бағдарлама құрылғыны қайта жүктеуге мүмкіндік бермейді.

    Егер бұл параметр қосулы болса, құрылғыны қайта іске қоспас бұрын бұғатталған құрылғылардағы мұндай бағдарламалар мәжбүрлі түрде жабылады. Нәтижесінде, пайдаланушылар сақталмаған жұмысын жоғалтуы мүмкін.

Егер бұл параметр өшірулі болса, бұғатталған құрылғы қайта жүктелмейді. Бұл құрылғыдағы тапсырманың күйі құрылғыны қайта іске қосу қажеттілігін көрсетеді. Пайдаланушылар бұғатталған құрылғыларда жұмыс істейтін барлық бағдарламаларды қолмен жауып, сол құрылғыларды қайта іске қосуы керек.

Әдепкі бойынша, параметр өшірулі.

Патчтарды және жаңартуларды басқару

Патчтарды және жаңартуларды басқару бөлімінде жаңартуларды алу мен таратуды және патчтарды басқарылатын құрылғыларға орнатуды конфигурациялауға болады:

- **Белгісіз күйге ие компоненттер үшін қолданылатын жаңартулар мен патчтарды автоматты түрде орнату**

  Егер жалауша қойылса, *Анықталмаған* мақұлдау мәртебесі бар Kaspersky патчтары жаңарту серверлерінен жүктелгеннен кейін автоматты түрде басқарылатын құрылғыларға орнатылады.

  Егер жалауша алынып тасталса, *Анықталмаған* мәртебесі бар Kaspersky жүктелген патчтары, әкімші олардың мәртебесін *Расталды* деп өзгерткеннен кейін орнатылады.

  Әдепкі бойынша, параметр қосулы.

- **Басқару серверінен жаңартулар мен антивирустық дерекқорларды алдын ала жүктеп алу (ұсынылған)**

  Параметр қосулы болса, жаңартуларды алуға арналған офлайн-модель қолданылады. Басқару сервері жаңартуларды алған кезде, ол Желілік агентті (ол орнатылған құрылғыларда) басқарылатын бағдарламалар үшін қажет етілетін жаңартулар туралы хабардар етеді. Желілік агенттер жаңартулар туралы ақпаратты алған кезде, олар Басқару серверінен қажетті файлдарды ертерек жүктеп алады. Бірінші рет қосылған кезде, Сервер осы Агенттің жаңартуларды жүктеуіне түрткі болады. Желілік агент клиент құрылғысында барлық жаңартуларды жүктегеннен кейін, жаңартулар құрылғыдағы бағдарламалар үшін қолжетімді болады.

  Клиент құрылғысындағы басқарылатын бағдарлама жаңартуларды алу үшін Желілік агентке жүгінген кезде, Агент өзінде қажетті жаңартулардың бар ма екенін тексереді. Жаңартулар басқарылатын бағдарлама сұрау салған сәттен бастап 25 сағаттан ерте болмайтын мерзімнің ішінде Басқару серверінен алынған болса, онда Желілік агент Басқару серверіне қосылмайды және басқарылатын бағдарламаға жергілікті кэштегі жаңартуларды ұсынады. Желілік агент бағдарламаларға арналған жаңартуларды клиент құрылғыларында ұсынса, бірақ жаңарту үшін қосылым талап етілмесе, Басқару серверімен қосылым орындалмауы мүмкін.

  Параметр өшірулі болса, жаңартуларды жүктеп алудың офлайн үлгісі пайдаланылмайды. Жаңартулар, жаңартуларды жүктеу тапсырмасының кестесіне сәйкес таратылады.

  Әдепкі бойынша, параметр қосулы.

Қосылым мүмкіндігі

Қосылым мүмкіндігі бөлімі үш ішкі бөлімді қамтиды:

- **Желі**
- **Байланыс профильдері**
- **Байланыс кестесі**

Желі бөлімінде Басқару серверіне қосылым параметрлерін конфигурациялауға, UDP портын пайдалану мүмкіндігін қосуға және оның нөмірін көрсетуге болады.

- **Басқару серверіне қосылу** блогында Басқару серверіне қосылу параметрлерін конфигурациялауға және клиент құрылғыларының Басқару серверімен синхрондау кезеңін көрсетуге болады:

  - **Синхрондау аралығы (мин)**

    Желілік агент басқарылатын құрылғыларды Басқару серверімен синхрондайды. Синхрондау кезеңін (мерзімді сигнал) 10 000 басқарылатын құрылғыға 15 минутқа тең етіп белгілеу ұсынылады.

  - **Желілік трафикті қысу**

    Егер параметр өшірулі болса, Желілік агент деректерін беру жылдамдығы арттырылады, берілетін ақпарат көлемі азайтылады және Басқару серверіне түсетін жүктемені азайтады.

    > Клиент компьютерінің орталық процессорына түсетін жүктеме артуы мүмкін.

    Әдепкі бойынша, жалауша қойылған.

  - **Microsoft Windows желілік экранында Желілік агенттің порттарын ашу**

    Параметр қосылса, Желілік агенттің жұмысына қажетті порттар Microsoft Windows брандмауэрінің ерекшеліктер тізіміне қосылады.

    Әдепкі бойынша, параметр қосулы.

  - **SSL байланысын пайдалану**

    Бұл параметр қосулы болса, Басқару серверіне қосылу SSL протоколының көмегімен, қорғалған порт арқылы орындалатын болады.

    Әдепкі бойынша, параметр қосулы.

  - **Әдепкі байланыс параметрлері астындағы тарату нүктесіндегі (қолжетімді болса) қосылу шлюзін пайдаланыңыз**

    Егер параметр қосулы болса, онда параметрлері басқару тобының сипаттарында белгіленген тарату нүктесінің қосылым шлюзі қолданылады.

    Әдепкі бойынша, параметр қосулы.

- **UDP портын пайдалану**

  Желілік агент басқару серверіне UDP порты арқылы қосылуы үшін, **UDP портын пайдалану** жалаушасын қойып, **UDP порт нөмірі** өрісінде порт нөмірін көрсетіңіз. Әдепкі бойынша, параметр қосулы. Әдепкі бойынша басқару серверіне қосылу 15000 UDP порты арқылы жүзеге асырылады.

- **UDP портының нөмірі**

  Өрісте UDP портының нөмірін енгізуге болады. Әдепкі бойынша 15000-порт орнатылған.

  Ондық жазба нысаны қолданылады.

- **Басқару серверіне мәжбүрлі қосылу үшін тарату нүктесін пайдаланыңыз**

  Егер сіз тарату нүктесі опциялары терезесінде **Осы тарату нүктесін push сервері ретінде пайдалану** параметрін таңдасаңыз, осы параметрді таңдаңыз. Әйтпесе, тарату нүктесі push серверінің рөлін атқармайды.

Байланыс профильдері ішкі бөлімінде желі орнының параметрлерін көрсетуге және басқару сервері қолжетімді болмаған кезде, автономды пайдаланушы режимін қосуға болады.

- **Желілік орналасудың параметрлері**

  Желілік орналасудың параметрлері клиент құрылғысы қосылған желінің сипаттамаларын анықтайды және желі сипаттамалары өзгерген кезде Желілік агентті бір Басқару сервері қосылымы профилінен екіншісіне ауыстыру ережелерін белгілейді.

- **Басқару серверіне байланыс профильдері**

  Желілік агенттің Басқару серверіне қосылу профильдерін қарауға және қосуға болады. Бұл бөлімде келесі оқиғалар орын алған кезде Желілік агентті басқа Басқару серверіне ауыстыру ережелерін құрастыруға болады:

  - клиент құрылғысын басқа жергілікті желіге қосу;
  - құрылғыны ұйымның жергілікті желісінен ажырату;
  - қосылым шлюзінің мекенжайын өзгерту немесе DNS серверінің мекенжайын өзгерту.

- **Басқару сервері қолжетімсіз болғанда автономды пайдаланушы режиміне ауысу**

  Параметр қосулы болса, осы профиль арқылы қосылу кезінде, клиент құрылғысында орнатылған бағдарламалар автономды режимдегі құрылғыларға арналған саясат профильдерін және автономды пайдаланушыларға арналған саясаттарды қолданатын болады. Бағдарлама үшін автономды пайдаланушыларға арналған саясат анықталмаған болса, бағдарлама белсенді саясатты қолданатын болады.

  Параметр өшірулі болса, бағдарламалар белсенді саясаттарды қолданатын болады.

  Әдепкі бойынша, параметр өшірулі.

Байланыс кестесі бөлімінде Желілік агент деректерді Басқару серверіне жіберетін уақыт аралықтарын белгілеуге болады:

- **Қажет болғанда қосылу**

  Егер бұл нұсқа таңдалса, байланыс Желілік агент деректерді Басқару серверіне жіберуі қажет болған кезде орнатылады.

  Әдепкі бойынша, осы нұсқа таңдалған.

- **Көрсетілген кезеңдерде қосылу**

  Егер бұл нұсқа таңдалса, Желілік агентті Басқару серверіне қосу белгілі бір уақыт аралығында жүзеге асырылады. Бірнеше қосылу кезеңдерін қосуға болады.

Тарату нүктелері бойынша желіні сұрау

Тарату нүктелері бойынша желіні сұрау бөлімінде автоматты желі сауалнамаларын конфигурациялауға болады. Сауалнаманы қосу және оның кестесін конфигурациялау үшін келесі параметрлерді пайдалануға болады:

- **Windows желісі**

  Бұл опция тек Windows негізіндегі тарату нүктелері үшін қолжетімді.

Егер бұл параметр қосылса, Басқару сервері **Жылдам сауалнама жүргізу кестесін орнату** және **Толық сауалнама жүргізу кестесін орнату** сілтемелері бойынша конфигурацияланған кестеге сәйкес желіге автоматты түрде сауалнама жүргізеді.

Бұл параметр өшірілсе, Басқару сервері **Желі сұрауларының жиілігі (мин)** өрісінде көрсетілген кезеңмен желіде сауалнама өткізеді.

Басқару серверіне арналған құрылғыларды анықтау уақытын **Windows домендерінен сұраулар жиілігі (мин)** (Windows желісінде жылдам сұрау жүргізу үшін) және **Желі сұрауларының жиілігі (мин)** (Windows желісінде толық сұрау жүргізу үшін) өрістерінде реттеуге болады.

Әдепкі бойынша, параметр өшірулі.

- **IP ауқымдары**

  Егер бұл параметр қосылса, тарату нүктесі **Сауалнама кестесін орнату** түймесі бойынша конфигурацияланған кестеге сәйкес IP ауқымына автоматты түрде сауалнама жүргізеді.

  Егер параметр өшірулі болса, тарату нүктесі IP ауқымдарының сауалнамасын өткізеді.

  10.2-ден төмен нұсқаны Желілік агент нұсқалары үшін IP ауқымдарының сауалнамасын өткізу мерзімділігін **Сұрау аралығы (мин)** өрісінде конфигурациялауға болады. Егер параметр қосулы болса, өріс қолжетімді.

  Әдепкі бойынша, параметр өшірулі.

- **Zeroconf**

  Егер бұл параметр қосулы болса, тарату нүктесі автоматты түрде нөлдік конфигурациясы бар желіні (бұдан әрі *Zeroconf*) пайдалану арқылы IPv6 құрылғылары бар желіде автоматты түрде сауалнама өткізеді. Бұл жағдайда, IP ауқымдарының сауалнамасы еленбейді, өйткені тарату нүктесі бүкіл желіге сауалнама жүргізеді.

  Zeroconf пайдалануды бастау үшін келесі шарттар орындалуы керек:

  - Тарату нүктесі Linux басқаруымен жұмыс істеуі керек.
  - Тарату нүктесіне avahi-browse утилитасын орнату қажет.

  Егер бұл параметр өшірілген болса, тарату нүктесі IPv6 құрылғылары бар желілерде сауалнама жүргізбейді.

  Әдепкі бойынша, параметр өшірулі.

- **Домен контроллерлері**

  Опция қосылса, тарату нүктесі **Сауалнама кестесін орнату** түймесін басу арқылы конфигурацияланған кестеге сәйкес домен контроллерлеріне автоматты түрде сауалнама жүргізеді.

  Егер бұл параметр өшірулі болса, тарату нүктесі домен контроллерлеріне сауалнама жүргізбейді.

  10.2-ден төмен желілік агент нұсқалары үшін домен контроллерлері сауалнамасын өткізу мерзімділігін **Сұрау аралығы (мин)** өрісінде орнатуға болады. Егер осы параметр қосулы болса, өріс қолжетімді.

  Әдепкі бойынша, параметр өшірулі.

Тарату нүктелерінің желі параметрлері

Тарату нүктелерінің желі параметрлері бөлімінде интернетке кіру параметрлерін көрсетуге болады:

- **Прокси-серверді пайдалану**
- **Мекенжай**
- **Порт нөмірі**
- **Жергілікті мекенжайларға арналған прокси-серверді айналып өту**

  Егер параметр қосулы болса, жергілікті желідегі құрылғыларға қосылған кезде прокси сервері пайдаланылмайды.

  Әдепкі бойынша, параметр өшірулі.

- **Прокси-сервердегі аутентификация**

  Жалауша қойылған болса, енгізу өрістерінде прокси-сервердегі түпнұсқалық растама үшін есептік деректерді көрсетуге болады.

  Әдепкі бойынша, жалауша алынып тасталған.

KSN прокси (тарату нүктелері)

KSN прокси (тарату нүктелері) бөлімінде бағдарламаны тарату нүктесі басқарылатын құрылғылардан Kaspersky Security Network (KSN) сұрауларын жіберу үшін пайдаланылатындай етіп орнатуға болады:

- **Тарату нүктесі тарапынан KSN проксиін қосу**

  KSN прокси-сервері қызметі тарату нүктесі ретінде әрекет ететін құрылғыда орындалады. Бұл параметрді желі трафигін қайта тарату және оңтайландыру үшін пайдаланыңыз.

  Тарату нүктесі Kaspersky Security Network мәлімдемесінде көрсетілген KSN статистикасын Kaspersky ұйымына жібереді.

  Әдепкі бойынша, параметр өшірулі. Осы параметрді қосу, **Басқару серверін прокси-сервер ретінде пайдалану** және **Kaspersky Security Network бағдарламасын пайдалану шарттарын қабылдаймын** параметрлері Басқару серверінің сипаттары терезесінде қосылған жағдайда ғана күшіне енеді.

  Суық резерві бар істен шығуға төзімді кластер түйініне (белсенді / пассивті) тарату нүктесін тағайындауға және сол түйінде KSN прокси-серверін қосуға болады.

- **KSN сұрауын Басқару серверіне қайта жіберу**

  Тарату нүктесі басқарылатын құрылғылардан KSN сұрауларын Басқару серверіне жібереді.

  Әдепкі бойынша, параметр қосулы.

- **KSN бұлтына/KPSN бағдарламасына интернет арқылы тікелей кіру**

  Тарату нүктесі KSN-ге басқарылатын құрылғылардан KSN немесе KPSN бұлттық қызметіне сұраулар жібереді. Тарату нүктесінде жасалған KSN сұраулары да тікелей KSN Cloud немесе KPSN-ге жіберіледі.

- **TCP порты**

  Басқарылатын құрылғылар KSN прокси-серверіне қосылу үшін қолдана алатын TCP портының нөмірі. Әдепкі бойынша 13111-порт орнатылған.

- **UDP порты**

  Желілік агент басқару серверіне UDP порты арқылы қосылуы үшін, **UDP портын пайдалану** жалаушасын қойып, **UDP порт нөмірі** өрісінде порт нөмірін көрсетіңіз. Әдепкі бойынша, параметр қосулы. Әдепкі бойынша басқару серверіне қосылу 15000 UDP порты арқылы жүзеге асырылады.

- **HTTPS порты**

  Басқарылатын құрылғылардың KSN прокси-серверіне HTTPS порты арқылы қосылуын қаласаңыз, **HTTPS пайдалану** параметрін қосыңыз және **HTTPS порты** өрісінде порт нөмірін көрсетіңіз. Әдепкі бойынша, параметр өшірулі. Әдепкі бойынша, KSN прокси-серверіне қосылу 17111 HTTPS порты арқылы жүзеге асырылады.

Жаңартулар (тарату нүктелері)

Жаңартулар (тарату нүктелері) бөлімінде айырмашылық файлдарын жүктеу функциясын қосуыңызға болады, себебі тарату нүктелері жаңартуларды Kaspersky жаңартулар серверлерінен айырмашылық файлдары түрінде алып тұрады.

Жергілікті есептік жазбаны басқару (тек Linux)

Жергілікті есептік жазбаны басқару (тек Linux) бөлімі үш бөлікшеден тұрады:

- **Пайдаланушы сертификаттарын басқару**
- **Қолданылатын жергілікті әкімші топтарын қосу не өңдеу**
- **Пайдаланушы құрылғысындағы sudoer файлдарын өзгерістерден қорғау үшін сілтемелік файл жүктеп салу**

Пайдаланушы сертификаттарын басқару бөлікшесінде қай түбірлік сертификаттарды орнату керектігін көрсетуге болады. Бұл сертификаттарды, мысалы, веб-сайттардың немесе веб-серверлердің түпнұсқалығын тексеру үшін пайдалануға болады.

- **Түбірлік сертификаттарды орнату**

  Бұл параметр қосылса, кестеге қосылған сертификаттар көрсетілген құрылғыларда орнатылады.

  Бұл параметр өшірілсе, сертификаттар көрсетілген құрылғыларда орнатылмайды.

  Әдепкі бойынша, параметр өшірулі.

- **Қосу**

  Бұл түймені басқан соң, сертификатты қосуға болатын терезе ашылады.

  Сертификат өлшемі 10 МБ-тан аз болуы керек.

Kaspersky Security Center қолданбасы CER, CRT, CERT, PEM және KEY кеңейтімдері бар сертификаттарды қолдайды.

Қолданылатын жергілікті әкімші топтарын қосу не өңдеу бөлімінде жергілікті әкімші топтарын басқаруға болады. Бұл топтар, мысалы, жергілікті әкімші құқықтарын кері қайтарып алу кезінде пайдаланылады. Сондай-ақ, артықшылықты пайдаланушы есептік жазбаларының тізімін **Артықшылықтары бар құрылғы пайдаланушылары туралы есеп (тек Linux)** арқылы тексеруге болады.

- **Қосу**

  Жергілікті әкімшілер тобын қосу үшін осы түймені басыңыз.

- **Өзгерту**

  Жергілікті әкімшілер тобын өзгерту үшін осы түймені басыңыз.

  Бұл түйме жергілікті әкімшілер тобының жанында құсбелгі қойылған жағдайда қолжетімді болады.

- **Жою**

  Таңдалған жергілікті әкімшілер тобын кестеден жою үшін осы түймені басыңыз.

  Бұл түйме жергілікті әкімшілер тобының жанында құсбелгі қойылған жағдайда қолжетімді болады.

Пайдаланушы құрылғысындағы sudoer файлдарын өзгерістерден қорғау үшін сілтемелік файл жүктеп салу бөлікшесінде sudoers файлын басқаруды конфигурациялауға болады. Артықшылықтары бар топтар мен құрылғы пайдаланушылары құрылғыдағы sudoers файлы арқылы анықталады. sudoers файлы `/etc/sudoers` қалтасында орналасқан. Sudoers файлын өзгерістерден қорғау үшін sudoers анықтамалық файлын жүктеп салуға болады. Бұл sudoers файлын қажетсіз өзгертудің алдын алады.

Жарамсыз sudoers анықтамалық файлы пайдаланушы құрылғысының дұрыс жұмыс істемеуіне әкелуі мүмкін.

- **Басқаруға арналған sudoers файлы**

  Бұл параметр қосылса, sudoers файлы ағымдағы sudoers анықтамалық файлымен ауыстырылады.

  Бұл параметр өшірілсе, sudoers файлы өзгеріссіз қалады.

  Әдепкі бойынша, параметр өшірулі.

- **Сілтемелік sudoer файлы**

  Бұл өріс жүктелген sudoers анықтамалық файлының атауын көрсетеді.

- **Жүктеп салу**

  sudoers анықтамалық файлын жүктеп салу үшін осы түймені басыңыз.

- **Ағымдағы сілтемелік sudoer файлы**

  Ағымдағы sudoers файлын көру үшін осы түймені басыңыз.

Тексерістер журналы

Тексерістер журналы қойындысында мына әрекеттерді орындай аласыз:

- Саясат өзгерістерінің тарихын қарау және сақтау.
- Саясатты тексеруге қайта шегіну.
- Саясатты тексеру сипаттамасын қосу және өзгерту.
- Саясат түзетулерін салыстыру.

Желілік агентті Windows, Linux және macOS үшін қолдану: салыстыру

Желілік агентті пайдалану құрылғының операциялық жүйесіне байланысты. Желілік агент саясатының және орнату пакетінің сипаттары операциялық жүйеге байланысты. Төмендегі кестеде Windows, Linux және macOS операциялық жүйелері үшін қолжетімді Желілік агентінің мүмкіндіктері мен пайдалану сценарийлері салыстырылады.

Желілік агент функцияларын салыстыру

Желілік агент функциясы	Windows	Linux	macOS
Орнату			
Операциялық жүйесі мен Желілік агенті бар әкімші қатты дискісі кескінін үшінші тарап құралдарымен клондау әдісімен орнату	✓ Шектеу: Arm жүйесіндегі Microsoft Windows жүйесіне арналған Желілік агент қолдамайды.	✓	✓
Бағдарламаларды қашықтан орнатудың үшінші тарап құралдары арқылы бағдарламалар орнату	✓	✓	✓
Құрылғыларда бағдарлама инсталляторларын іске қосу арқылы қолмен орнату	✓	✓	✓
Желілік агентті тыныш режимде орнату	✓	✓	✓
Клиент құрылғысын Басқару серверіне қолмен қосу	✓	✓	✓
Kaspersky Security Center құрамдастарына арналған жаңартулар мен патчтарды автоматты түрде орнату	✓	✓	–
Кілтті автоматты түрде тарату	✓	✓	✓
Мәжбүрлеп синхрондау	✓	✓	✓ Push серверінен басқа

Желілік агент функциясы	Windows	Linux	macOS
Тарату нүктесі			
Тарату нүктесін қолдану	✓ Шектеу: Arm жүйесіндегі Microsoft Windows жүйесіне арналған Желілік агент қолдамайды.	✓	✓
Тарату нүктелерінің саны мен конфигурациясын есептеу	✓ Шектеу: Arm жүйесіндегі Microsoft Windows жүйесіне арналған Желілік агент қолдамайды.	✓ Network Location Awareness (NLA) қолданбай.	✓ Network Location Awareness (NLA) қолданбай.
Жаңартуларды алудың офлайн-моделі	✓ Шектеу: Arm жүйесіндегі Microsoft Windows жүйесіне арналған Желілік агент қолдамайды.	✓	✓
Желіде сауалнама өткізу	✓ • IP ауқымдарының сауалнамасы • Домен контроллерлеріне сауалнама жүргізу (Microsoft Active Directory) Шектеу: Arm жүйесіндегі Microsoft Windows жүйесіне арналған Желілік агент қолдамайды.	✓ IP ауқымдарының сауалнамасы Zeroconf сауалнамасы Домен контроллерінің сауалнамасы (Microsoft Active Directory, Samba 4 Active Directory, FreeIPA, ALD Pro)	—
KSN прокси-сервері қызметін тарату нүктесінің жағында іске қосу	✓ Шектеу: Arm жүйесіндегі Microsoft Windows жүйесіне арналған Желілік агент қолдамайды.	✓	—
Жаңартуларды басқарылатын құрылғыларға тарататын тарату нүктесі қоймаларына Kaspersky жаңарту серверлері арқылы жүктеп алу	✓ Шектеу: Arm жүйесіндегі Microsoft Windows жүйесіне арналған Желілік агент қолдамайды.	✓	— Linux немесе macOS операциялық жүйесі бар құрылғылар Жаңартуларды тарату орындарының қоймаларына жүктеп алу тапсырмасының әрекет ету ауқымында болса, онда тапсырма Windows операциялық жүйесі бар құрылғылардың барлығында сәтті аяқталса да, Сәтсіз аяқталды мәртебесімен аяқталады.
Бағдарламаларды күшпен орнату	✓ Шектеу: Arm жүйесіндегі Microsoft Windows жүйесіне арналған Желілік агент қолдамайды.	Шектеумен: Linux операциялық жүйесі бар тарату нүктелерін қолдана отырып, Windows операциялық жүйесі басқаратын құрылғыларда күшпен орнату мүмкін емес.	Шектеумен: macOS операциялық жүйесі бар тарату нүктелерін қолдана отырып, Windows операциялық жүйесі басқаратын құрылғыларда күшпен орнату мүмкін емес.
Push-сервер ретінде қолдану	✓ Шектеу: Arm жүйесіндегі Microsoft Windows жүйесіне арналған Желілік агент қолдамайды.	✓	—
Үшінші тарап бағдарламаларымен жұмыс істеу			
Бағдарламаларды құрылғыларға қашықтан орнату	✓	✓	✓ Мәліметтер алу үшін келесі мақаланы қараңыз: Қолданбаларды macOS құрылғыларына қашықтан орнату.
Желілік агент саясатында операциялық жүйенің жаңартуларын конфигурациялау	✓ Шектеу: Arm жүйесіндегі Microsoft Windows жүйесіне арналған Желілік агент қолдамайды.	—	—

Желілік агент функциясы	Windows	Linux	macOS
Бағдарламалық жасақтама осалдықтары туралы ақпаратты қарау	✓ Шектеу: Arm жүйесіндегі Microsoft Windows жүйесіне арналған Желілік агент қолдамайды.	—	—
Бағдарламалық жасақтама осалдықтарын іздеу	✓ Шектеу: Arm жүйесіндегі Microsoft Windows жүйесіне арналған Желілік агент қолдамайды.	—	—
Бағдарламалық жасақтама жаңартуы	✓ Шектеу: Arm жүйесіндегі Microsoft Windows жүйесіне арналған Желілік агент қолдамайды.	—	—
Құрылғыларда орнатылған бағдарламалық жасақтаманы түгендеу	✓	✓	—
Виртуалды машиналар			
Виртуалды машиналарға Желілік агент орнату	✓	✓	✓
VDI үшін параметрлерді оңтайландыру	✓ Шектеу: Arm жүйесіндегі Microsoft Windows жүйесіне арналған Желілік агент қолдамайды.	✓	✓
Динамикалық виртуалды машиналарды қолдау	✓ Шектеу: Arm жүйесіндегі Microsoft Windows жүйесіне арналған Желілік агент қолдамайды.	✓	✓
Басқа			
Windows компьютерлік бөлісу қызметі арқылы қашықтағы клиент құрылғысындағы әрекеттер аудиті	✓	—	—
Антивирустық қорғаныс күйі мониторингі	✓	✓	✓
Құрылғыларды қайта іске қосуды басқару	✓	—	—
Файлдық жүйені шегіндіруді қолдау	✓	✓	✓
Желілік агентті қосылым шлюзі ретінде пайдалану	✓	✓	✓
Байланыс менеджері	✓	✓	✓
Кеңседе жоқ пайдаланушыларға арналған қосылым профильдері	✓	✓	✓
Желілік агентті бір Басқару серверінен екіншісіне ауыстырып қосу (автоматты түрде желілік орналасуы бойынша)	✓	✓	✓
Клиент құрылғысы мен басқару сервері арасындағы қосылымды тексеру. klnagchk утилитасы	✓	✓	✓

Желілік агент функциясы	Windows	Linux	macOS
Клиент құрылғысының жұмыс үстеліне қашықтан қосылу	✓	✓	✓ Virtual Network Computing (VNC) жүйесін пайдалану.
Деректерді тасымалдау шебері арқылы жеке орнату пакетін жүктеу	✓	✓	✓
Клиент құрылғыларының аппараттық жасақтамасы туралы ақпаратты қарау	✓	✓ Осы құрылғыларда орнатылған желілік агент арқылы басқару серверіне жіберілген Linux құрылғыларының аппараттық жасақтамасы туралы ақпарат басқарылатын құрылғылар параметрлерінің сипаттамасында көрсетілген ақпаратпен шектеледі.	✓ Осы құрылғыларда орнатылған желілік агент арқылы басқару серверіне жіберілген macOS құрылғыларының аппараттық жасақтамасы туралы ақпарат басқарылатын құрылғы параметрлерінің сипаттамасында көрсетілген ақпаратпен шектеледі.

Желілік агенттің параметрлерін операциялық жүйелер бойынша салыстыру

Төмендегі кестеде желілік агент орнатылған басқарылатын құрылғының операциялық жүйесіне байланысты қандай Желілік агент саясатының параметрлері қолжетімді екені көрсетілген.

Желілік агенттің параметрлері: операциялық жүйелер бойынша салыстыру

Параметрлер бөлімі	Windows	Linux	macOS
Жалпы	✓	✓	✓
Оқиғаларды конфигурациялау	✓	✓	✓
Параметрлер	✓	✓ Келесі параметрлер қолжетімді: • **Файлдарды тек тарату нүктелері арқылы тарату** • **Оқиғалар кезегінің максималды өлшемі, МБ** • **Бағдарламаға құрылғыда саясаттың кеңейтілген деректерін шығарып алуға рұқсат берілген**	✓
Қоймалар	✓	✓ Келесі параметрлер қолжетімді: • **Орнатылған бағдарламалардың мәліметтері** • **Жабдық тізімдемесі туралы ақпарат**	✓ **Жабдық тізімдемесі туралы ақпарат** параметрі қолжетімді.
Қосылым мүмкіндігі → Желі	✓	✓ **Microsoft Windows желілік экранында Желілік агенттің порттарын ашу** параметрлерінен басқа.	✓
Қосылым мүмкіндігі → Байланыс профильдері	✓	✓	✓
Қосылым мүмкіндігі → Байланыс кестесі	✓	✓	✓

Параметрлер бөлімі	Windows	Linux	macOS
Тарату нүктелері бойынша желіні сұрау	✓ Келесі параметрлер қолжетімді: • **Windows желісі** • **IP ауқымдары** • **Домен контроллерлері**	✓ Келесі параметрлер қолжетімді: • **Zeroconf** • **IP ауқымдары** • **Домен контроллерлері**	—
Тарату нүктелерінің желі параметрлері	✓	✓	✓
KSN прокси (тарату нүктелері)	✓	✓	—
Жаңартулар (тарату нүктелері)	✓	✓	—
Тексерістер журналы	✓	✓	✓

Желілік агент үшін ресурстарды аз тұтыну режимін қосу немесе өшіру

Ресурстарды аз тұтыну режимі клиент құрылғысында орнатылған Желілік агент жедел жадын пайдалануды шектеуге мүмкіндік береді. Әдепкі бойынша, ресурстарды аз тұтыну режимі өшірілген.

Төмендегі функциялар ресурстарды аз тұтыну режимінде орындалмайды:

- Желілік агентті тарату нүктесі ретінде белгілеу мүмкін емес (қолмен немесе автоматты түрде).
- Желілік агент Желілік агенттің күйі туралы ақпаратты бөлек мәтіндік файлға жазбайды.
- Желілік агент жаңартуларды алудың офлайн-үлгісін қолдамайды.
- Келесі құрамдастар мен процестер өшірілген:
  - Үшінші тарап жаңартулары мен осалдықтары туралы ақпаратты алу.
  - KSN прокси-серверін тарату нүктесінің жағында іске қосу.
  - Тарату нүктелерінің қоймасында жаңартуларды жүктеп алу.
  - DNS серверін бұғаттауды қолданбау.
  - Дискідегі бос орын туралы ақпарат алу.

Құрамдастар мен процестер ресурстарды аз тұтыну режимі өшірілгеннен кейін өз жұмысын жалғастырады.

Ресурстарды аз тұтыну режимін қосу үшін:

1. Клиент құрылғысындағы пәрмен желісінде келесі пәрменді орындаңыз:

   ```
   sudo /opt/kaspersky/klnagent64/sbin/klscflag -fset -pv klnagent -n
   KLNAG_FLAG_TEST_VM_PERF -t d -v 1
   ```

2. Келесі пәрменді пайдаланып, Желілік агентті қайта іске қосыңыз:

   ```
   sudo service klnagent64 restart
   ```

3. Операциялық жүйе журналында **Kaspersky Security Center Желілік агенті ресурсты аз тұтынатын режимде жұмыс істеп жатыр** енгізілімінің көрсетілгенін тексеріңіз.

Ресурстарды аз тұтыну режимі қосулы.

Ресурстарды аз тұтыну режимін сөндіру үшін:

1. Клиент құрылғысындағы пәрмен желісінде келесі пәрменді орындаңыз:

   ```
   sudo /opt/kaspersky/klnagent64/sbin/klscflag -fset -pv klnagent -n
   KLNAG_FLAG_TEST_VM_PERF -t d -v 0
   ```

2. Келесі пәрменді пайдаланып, Желілік агентті қайта іске қосыңыз:

   ```
   sudo service klnagent64 restart
   ```

Ресурстарды аз тұтыну режимі өшірулі.

Сондай-ақ *Скриптілерді қашықтан орындау* тапсырмасының көмегімен ресурстарды аз тұтыну режимін қашықтан қосуға болады.

Басқарылатын қолданбалардың қорғаныс параметрлерін конфигурациялау

Басқарылатын Kaspersky қолданбаларының қорғаныс параметрлерін конфигурациялау үшін саясаттарды пайдалануға болады.

Kaspersky Endpoint Security саясаттарын конфигурациялау туралы қосымша ақпарат алу үшін тиісті анықтаманы қараңыз:

- Kaspersky Endpoint Security for Windows онлайн-анықтамасы
- Kaspersky Endpoint Security for Linux онлайн-анықтамасы
- Kaspersky Endpoint Security for Mac анықтамасы

Kaspersky Endpoint Security жаңарту топтық тапсырмасын қолмен конфигурациялау

Қоймаға жаңартуларды жүктеу кезінде жалаушасы қойылған кезде Kaspersky Endpoint Security **Тапсырманы бастау үшін автоматты түрде араластырылған кідірісті пайдалану** үшін кестенің оңтайлы және ұсынылатын нұсқасы.

Kaspersky Endpoint Security құрылғысын тексеру топтық тапсырмасын қолмен конфигурациялау

Бағдарламаны жылдам іске қосу шебері құрылғыны тексерудің топтық тапсырмасын жасайды. Топтық тексеру тапсырмасының автоматты түрде орнатылған кестесі ұйымыңызға сәйкес келмесе, ұйымда қабылданған жұмыс процесі ережелеріне негізделген бұл тапсырма үшін ең қолайлы кестені қолмен орнату қажет.

Мысалы, тапсырма үшін автоматты рандомизациясы бар **Жұма күні 19:00-де іске қосу** кестесі таңдалған және **Өткізіп алынған тапсырмаларды іске қосу** жалаушасы алынған. Демек, егер ұйымның құрылғылары жұма күндері сағат 18:30-да сөндірілсе, онда құрылғыны сканерлеу тапсырмасы ешқашан іске қосылмайды. Бұл жағдайда топтық тексеру тапсырмасын қолмен орнату қажет.

Kaspersky Security Network (KSN)

Бұл бөлімде Kaspersky Security Network (KSN) онлайн-қызметтері инфрақұрылымын қолдану тәсілі сипатталған. KSN туралы ақпарат, сондай-ақ KSN қосу, KSN бағдарламасына қатынасуды конфигурациялау, KSN прокси-серверін пайдалану статистикасын қарау бойынша нұсқаулар берілген.

Жаңарту функционалдығы (антивирустық қолтаңба жаңартуларын және код дерекқоры жаңартуларын қоса) және KSN функционалдығы АҚШ аймағындағы бағдарламада қолжетімді болмауы мүмкін.

KSN туралы

Kaspersky Security Network (KSN) – файлдардың, веб-ресурстардың және бағдарламалық жасақтаманың беделі туралы Kaspersky жедел білім базасына қатынасуды ұсынатын онлайн-қызметтер инфрақұрылымы. Kaspersky Security Network деректерін пайдалану Kaspersky бағдарламаларының қауіптерге реакциясының жоғары жылдамдығын қамтамасыз етеді, кейбір қорғаныс құрамдастарының тиімділігін арттырады, сондай-ақ жалған іске қосылудың ықтималдығын азайтады. KSN бағдарламасы Kaspersky беделдік дерекқорларынан басқарылатын құрылғыларға орнатылған бағдарламалар туралы ақпаратты алуға мүмкіндік береді.

KSN бағдарламасына қатыса отырып, сіз автоматты режимде Kaspersky ұйымына Kaspersky Security Center Linux басқаратын клиент құрылғыларына орнатылған Kaspersky бағдарламаларының жұмысы туралы ақпарат беруге келісесіз. Ақпаратты беру, конфигурацияланған KSN бағдарламасына қатынасу параметрлеріне сәйкес орындалады.

Kaspersky Security Center Linux бағдарламасы келесі KSN инфрақұрылымдық шешімдерін қолдайды:

- *Глобалды KSN* – Kaspersky Security Network бағдарламасымен ақпарат алмасуға мүмкіндік беретін шешім. KSN бағдарламасына қатыса отырып, сіз автоматты режимде Kaspersky ұйымына Kaspersky Security Center Linux басқаратын клиент құрылғыларына орнатылған Kaspersky бағдарламаларының жұмысы туралы ақпарат беруге келісесіз. Ақпаратты беру, конфигурацияланған KSN бағдарламасына қатынасу параметрлеріне сәйкес орындалады. Kaspersky мамандары алынған ақпаратты қосымша талдап, оны Kaspersky Security Network беделдік және статистикалық дерекқорларына қосады. Kaspersky Security Center Linux бағдарламасы осы шешімді әдепкі бойынша қолданады.

- *Kaspersky Private Security Network (KPSN)* – бұл Kaspersky қолданбалары орнатылған құрылғыларды пайдаланушыларға өз құрылғыларынан жаһандық KSN қолданбасына деректерді жібермей, Kaspersky Security Network дерекқорларына және басқа да статистикалық деректерге қол жеткізуді қамтамасыз ететін шешім. KPSN келесі себептердің бірі бойынша Kaspersky Security Network бағдарламасына қатыса алмайтын ұйымдарға арналған:

  - Пайдаланушы құрылғылары интернетке қосылмаған.

  - Кез келген деректерді елден немесе корпоративтік желіден (LAN) тыс жерге жіберуге заңмен немесе корпоративті қауіпсіздік саясаттарымен тыйым салынады.

  Басқару сервері терезесінің **KSN проксиі** бөлімінде Kaspersky Private Security Network қатынасу параметрлерін конфигурациялай аласыз.

Қолданба, қолданбаны бастапқы орнату шеберінің жұмысы барысында KSN қолданбасына қосылуға ұсынады. Сіз KSN қолдана бастай аласыз немесе бағдарламамен жұмыс істеген кез келген сәтте KSN қолданудан бас тарта аласыз.

Сіз KSN бағдарламасын KSN қосу кезінде оқитын және қабылдайтын KSN мәлімдемесіне сай қолданасыз. KSN мәлімдемесі жаңартылған болса, ол басқару серверін алдыңғы нұсқасынан жаңарту кезінде көрсетіледі. Сіз жаңартылған KSN мәлімдемесін қабылдауға немесе қабылдамауға болады. Оны қабылдамасаңыз, сіз бұған дейін қабылдаған KSN мәлімдемесінің алдыңғы нұсқасына сәйкес KSN бағдарламасын қолдануды жалғастырасыз.

KSN қосылған кезде, басқарылатын құрылғылардың қауіпсіздік деңгейінің сақталуына көз жеткізу үшін Kaspersky Security Center Linux KSN серверлерінің қолжетімділігін тексереді. Жүйелік DNS арқылы серверлерге қатынасу мүмкін болмаса, бағдарлама жалпыға ортақ DNS серверлерін пайдаланады.

Басқару сервері басқаратын клиент құрылғылары KSN бағдарламасымен KSN прокси-серверінің көмегімен өзара әрекеттеседі. KSN прокси-сервері қызметі келесі мүмкіндіктерді ұсынады:

- Клиент құрылғылары, тіпті интернетке тікелей қатынасу мүмкіндігі болмаса да, KSN бағдарламасына сұраулар жасай алады, KSN бағдарламасынан ақпарат ала алады және KSN бағдарламасына ақпаратты жібере алады.

- KSN прокси-сервері өңделген деректерді кэштей отырып сыртқы желіге арнаға түсетін жүктемені азайтады және клиент құрылғысының сұралған ақпаратты алуын тездетеді.

Сіз KSN прокси-сервері параметрлерін Басқару сервері сипаттары терезесінің **KSN проксиі** бөлімінде конфигурациялай аласыз.

KSN бағдарламасына қатынасуды конфигурациялау

Kaspersky Security Network (KSN) бағдарламасына Басқару серверінен және тарату нүктесінен қатынасуды белгілеуге болады.

Басқару серверінің KSN бағдарламасына қатынасуын конфигурациялау үшін:

1. Негізгі мәзірдегі басқару серверінің атауын басыңыз.

   Басқару серверінің сипаттары терезесі ашылады.

2. **Жалпы** қойыншасында **KSN проксиі** бөлімін таңдаңыз.

3. Қосқышты **Басқару серверіндегі KSN проксиді қосу Қосулы** күйіне ауыстырыңыз.

   Бұл параметр қосылса, KSN прокси-сервері Kaspersky Security Center компоненттері мен Kaspersky қолданбаларының жұмыс тиімділігін арттыру үшін деректерді KSN-ге жібереді. KSN-де клиент құрылғыларынан деректерді беру клиент құрылғыларында жұмыс істейтін Kaspersky Endpoint Security саясатымен реттеледі. Қосқыш өшірілсе, басқару серверінен және клиенттік құрылғылардан Kaspersky Security Center Linux арқылы KSN қолданбасына деректер берілмейді. Бұл ретте, клиент құрылғылары өздерінің параметрлеріне сәйкес деректерді KSN бағдарламасына тікелей (Kaspersky Security Center Linux арқылы емес) жібере алады. Клиент құрылғыларында жұмыс істейтін Kaspersky Endpoint Security саясаты осы құрылғылардың қандай деректерін тікелей (Kaspersky Security Center Linux арқылы емес) KSN бағдарламасына жіберетінін анықтайды.

4. KSN инфрақұрылымдық шешімін таңдаңыз.

   KSN мәлімдемесіне қатысу бөлімінде келесі әрекеттердің бірін орындаңыз:

   - Глобалды KSN қолдансаңыз, қосқышты **Kaspersky Security Network пайдалану Қосулы** күйіне ауыстырыңыз.

     Бұл параметрді қосқан кезде KSN мәлімдемесі шарттарын оқып, қабылдағаныңызға көз жеткізіңіз.

   - KPSN пайдаланасаңыз, қосқышты **Kaspersky Private Security Network пайдалану Қосулы** күйіне жылжытыңыз және KPSN параметрлерін (pkcs7 және pem кеңейтімдері бар файлдар) жүктеп алу үшін **KSN прокси параметрлері бар файлды таңдау** түймесін басыңыз. Параметрлер жүктелгеннен кейін, интерфейсте провайдердің атауы, провайдердің контактілері және KPSN параметрлері бар файл жасалған күн көрсетіледі.

   Қосқышты **Kaspersky Private Security Network пайдалану Қосулы** күйіне жылжытқанда, KPSN туралы толық ақпарат бар хабар пайда болады.

   KPSN келесі Kaspersky қолданбаларына қолдау көрсетеді:

   - Kaspersky Security Center Linux
   - Kaspersky Endpoint Security for Linux
   - Kaspersky Endpoint Security for Windows

   KPSN қолданбасын Kaspersky Security Center Linux жүйесіне қоссаңыз, бұл қолданбалар KPSN қолдауы туралы ақпарат алады. Қолданба сипаттары терезесіндегі **Кеңейтілген қорғаныс** бөлімінің **Kaspersky Security Network** бөлімшесінде KSN: KSN немесе KPSN жеткізушісі көрсетіледі.

   > **KSN проксиі** бөліміндегі Басқару сервер сипаттары терезесінде KSN орнатылмаған болса, Kaspersky Security Center Linux жүйесі Kaspersky Security Network статистикасын жібермейді.

5. Прокси-сервер параметрлері басқару сервері сипаттарында орнатылса, бірақ желі архитектурасы KPSN-ді тікелей пайдалануды талап ететін болса, **KPSN желісіне қосылған кезде прокси-сервер параметрлерін елемеу** жалаушасын қойыңыз. Әйтпесе, басқарылатын қолданбадан сұрау KPSN қолданбасына берілмейді.

6. Басқару серверін KSN прокси-сервері қызметіне қосу параметрлерін конфигурациялаңыз:

   - **Қосылым параметрлері** блогында, **TCP порты** енгізу өрісінде, KSN прокси-серверіне қосылу орындалатын TCP порты нөмірін көрсетіңіз. Әдепкі бойынша, KSN прокси-серверіне қосылу 13111-порт арқылы жүзеге асырылады.

   - Басқару серверін UDP порты арқылы KSN прокси-серверіне қосу үшін **UDP портын пайдалану** параметрін таңдап, **UDP порты** өрісінде порт нөмірін көрсетіңіз. Әдепкі бойынша, параметр өшірулі, TCP порты қолданылады. Егер параметр қосулы болса, әдепкі бойынша KSN прокси-серверіне қосылу 15111 санды UDP порты арқылы жүзеге асырылады.

   - Басқару серверін HTTPS порты арқылы KSN прокси-серверіне қосу үшін **HTTPS пайдалану** параметрін таңдап, **HTTPS порты** өрісінде порт нөмірін көрсетіңіз. Әдепкі бойынша, параметр өшірулі, TCP порты қолданылады. Егер параметр қосулы болса, әдепкі бойынша KSN прокси-серверіне қосылу 17111 санды HTTPS порты арқылы жүзеге асырылады.

7. Қосқышты **Қосалқы Басқару серверлерін KSN желісіне негізгі Басқару сервері арқылы қосу Қосулы** күйіне ауыстырыңыз.

   Егер бұл параметр қосулы болса, қосалқы Басқару серверлері негізгі Басқару серверін KSN прокси-сервері ретінде пайдаланады. Егер бұл параметр өшірулі болса, қосалқы Басқару серверлері KSN бағдарламасына өздігінен қосылады. Бұл жағдайда, басқарылатын құрылғылар қосалқы Басқару серверлерін KSN прокси-серверлері ретінде пайдаланады.

   > Егер **KSN проксиі** бөліміндегі қосалқы Басқару серверлерінің сипаттарында қосқыш дәл солай **Басқару серверіндегі KSN проксиді қосу Қосулы** күйіне ауыстырылса, қосалқы Басқару серверлері негізгі Басқару серверін прокси-сервер ретінде пайдаланады.

8. **Сақтау** түймесін басыңыз.

Нәтижесінде, KSN бағдарламасына қатынасу параметрлері сақталады.

Сондай-ақ, KSN бағдарламасына тарату нүктесі жағынан қатынасуды конфигурациялауға болады, мысалы, Басқару серверіне жүктемені азайту қажет болса. KSN прокси-серверінің рөлін атқаратын тарату нүктесі, Басқару серверін айналып өтіп, басқарылатын құрылғылардан келетін KSN сұрауларын тікелей Kaspersky бағдарламасына жібереді.

Тарату нүктесінің Kaspersky Security Network (KSN) бағдарламасына қатынасуын конфигурациялау үшін:

1. Тарату нүктесі қолмен тағайындалғанына көз жеткізіңіз.

2. Негізгі мәзірдегі басқару серверінің атауын басыңыз.

   Басқару серверінің сипаттары терезесі ашылады.

3. **Жалпы** қойыншасында **Тарату нүктелері** бөлімін таңдаңыз.

4. Оның сипаттары терезесін ашу үшін тарату нүктесінің атын басыңыз.

5. Тарату нүктесі сипаттары терезесінде, **KSN проксиі** бөлімінде **Тарату нүктесі тарапынан KSN проксиін қосу** параметрі мен **KSN бұлтына/KPSN бағдарламасына интернет арқылы тікелей кіру** параметрін қосыңыз.

6. **ОК** түймесін басыңыз.

Тарату нүктесі KSN прокси-серверінің рөлін атқарады.

Тарату нүктесі басқарылатын құрылғының NTLM протоколы арқылы түпнұсқалығын тексеруге қолдау көрсетпейтінін ескеріңіз.

KSN қолданысын қосу және өшіру

KSN қолданысын қосу үшін:

1. Негізгі мәзірдегі басқару серверінің атауын басыңыз.

   Басқару серверінің сипаттары терезесі ашылады.

2. **Жалпы** қойыншасында **KSN проксиі** бөлімін таңдаңыз.

3. Қосқышты **Басқару серверіндегі KSN проксиді қосу Қосулы** күйіне ауыстырыңыз.

KSN прокси-сервері қосылды және Kaspersky Security Center компоненттері мен Kaspersky қолданбаларының жұмыс тиімділігін арттыру үшін деректерді KSN-ге жібереді.

1. Қолданылатын KSN инфрақұрылымының шешіміне байланысты сәйкес қосқыштарды қосыңыз.

   - Глобалды KSN қолдансаңыз, қосқышты **Kaspersky Security Network пайдалану Қосулы** күйіне ауыстырыңыз.

     Енді KSN-ге деректер жіберу қолжетімді. Бұл параметрді қоссаңыз, KSN мәлімдемесін оқып, оның шарттарын қабылдауыңыз қажет.

   - KPSN пайдалансаңыз, қосқышты **Kaspersky Private Security Network пайдалану Қосулы** күйіне жылжытыңыз және KPSN параметрлерін (pkcs7 және pem кеңейтімдері бар файлдар) жүктеп алу үшін **KSN прокси параметрлері бар файлды таңдау** түймесін басыңыз. Параметрлер жүктелгеннен кейін, интерфейсте провайдердің атауы, провайдердің контактілері және KPSN параметрлері бар файл жасалған күн көрсетіледі.

     Қосқышты **Kaspersky Private Security Network пайдалану Қосулы** күйіне жылжытқанда, KPSN туралы толық ақпараты бар хабар пайда болады.

2. **Сақтау** түймесін басыңыз.

KSN қолданысын өшіру үшін:

1. Негізгі мәзірдегі басқару серверінің атауын басыңыз.

   Басқару серверінің сипаттары терезесі ашылады.

2. **Жалпы** қойыншасында **KSN проксиі** бөлімін таңдаңыз.

3. KSN прокси-сервері қызметін өшіру үшін қосқышты **Басқару серверіндегі KSN Проксиді қосу Өшірулі** күйіне ауыстырыңыз.

4. **Сақтау** түймесін басыңыз.

Қабылданған KSN мәлімдемесін қарау

Kaspersky Security Network (KSN) қосқан кезде сіз KSN мәлімдемесін оқып, қабылдауыңыз керек. Сіз қабылданған KSN мәлімдемесін кез келген уақытта көре аласыз.

Қабылданған KSN мәлімдемесін қарап шығу үшін:

1. Негізгі мәзірдегі басқару серверінің атауын басыңыз.

   Басқару серверінің сипаттары терезесі ашылады.

2. **Жалпы** қойыншасында **KSN проксиі** бөлімін таңдаңыз.

3. **Kaspersky Security Network мәлімдемесін қарау** сілтемесінен өтіңіз.

Ашылған терезеде сіз қабылданған KSN мәлімдемесінің мәтінін көре аласыз.

Жаңартылған KSN мәлімдемесін қабылдау

Сіз KSN бағдарламасын KSN қосу кезінде оқитын және қабылдайтын KSN мәлімдемесіне сай қолданасыз. KSN мәлімдемесі жаңартылған болса, ол басқару серверін алдыңғы нұсқасынан жаңарту кезінде көрсетіледі. Сіз жаңартылған KSN мәлімдемесін қабылдауға немесе қабылдамауға болады. Оны қабылдамасаңыз, сіз бұған дейін қабылдаған KSN мәлімдемесінің нұсқасына сәйкес KSN бағдарламасын қолдануды жалғастырасыз.

Басқару серверін алдыңғы нұсқасынан жаңартқаннан кейін, жаңартылған KSN мәлімдемесі автоматты түрде көрсетіледі. Жаңартылған KSN мәлімдемесін қабылдамасаңыз, оны бәрібір кейінірек қарап шыға аласыз және қабылдай аласыз.

Жаңартылған KSN мәлімдемесін қарап шығу және қабылдау немесе қабылдамау үшін:

1. Бағдарламаның басты терезесінің жоғарғы оң жақ бұрышындағы **Хабарландыруларды қарау** белгішесін басыңыз.

   Хабарландырулар терезесі ашылады.

2. **Жаңартылған KSN мәлімдемесін қарау** сілтемесінен өтіңіз.

   Kaspersky Security Network мәлімдемесін жаңарту терезесі ашылады.

3. KSN мәлімдемесін оқып шығыңыз, содан соң келесі түймелердің бірін басып, шешім қабылдаңыз:

   - **Мен жаңартылған KSN мәлімдемесінің шарттарын қабылдаймын**
   - **Ескі KSN мәлімдемесі бар KSN қолдану**

Сіздің таңдауыңызға байланысты KSN ағымдағы немесе жаңартылған KSN мәлімдемесінің шарттарына сәйкес жұмысын жалғастырады. Сіз кез келген уақытта қабылданған KSN мәлімдемесі мәтінін Басқару сервері сипаттарынан көре аласыз.

Тарату нүктесі KSN прокси-сервері ретінде жұмыс істейтінін тексеру

Тарату нүктесі рөлін атқаратын басқарылатын құрылғыда Kaspersky Security Network (KSN) прокси-серверін қосуға болады. Басқарылатын құрылғыда ksnproxy қызметі іске қосылған болса, ол KSN прокси-сервері ретінде жұмыс істейді. Бұл қызметті құрылғыда жергілікті түрде қосуға немесе өшіруге болады.

Windows немесе Linux операциялық жүйесі бар құрылғыны тарату нүктесі ретінде тағайындауға болады. Тарату нүктесі қалай тексерілетіні осы тарату нүктесінің операциялық жүйесіне байланысты.

Тарату нүктесі Linux операциялық жүйесімен KSN прокси-сервері ретінде жұмыс істейтінін тексеру үшін:

1. Тарату нүктесі құрылғысында, іске қосылған процестердің тізімін көрсету үшін `ps aux` пәрменін орындаңыз.

2. Іске қосылған процестер тізімінде `/opt/kaspersky/klnagent64/sbin/ksnproxy` процесінің іске қосылғанын тексеріңіз.

Егер `/opt/kaspersky/klnagent64/sbin/ksnproxy` процесі іске қосылып тұрса, онда құрылғыдағы Желілік агент Kaspersky Security Network бағдарламасына қатысады және тарату нүктесінің әрекет ету ауқымына кіретін басқарылатын құрылғылар үшін KSN прокси-сервері ретінде жұмыс істейді.

Тарату нүктесі Windows операциялық жүйесімен KSN прокси-сервері ретінде жұмыс істейтінін тексеру үшін:

1. Тарату нүктесі рөлін атқаратын құрылғыда Windows операциялық жүйесінде **Қызметтер** терезесін ашыңыз (**Барлық бағдарламалар** → **Басқару** → **Қызметтер**).

2. Қызметтер тізімінде KSN – ksnproxy прокси-сервері қызметі жұмыс істеп тұрғанын тексеріңіз.

   Егер ksnproxy қызметі жұмыс істеп тұрса, онда құрылғыдағы Желілік агент Kaspersky Security Network бағдарламасына қатысады және тарату нүктесінің әрекет ету ауқымына кіретін басқарылатын құрылғылар үшін KSN Proxy прокси-сервері ретінде жұмыс істейді.

Қажет болса, ksnproxy қызметін өшіруге болады. Бұл жағдайда, тарату нүктесінде Желілік агент бұдан былай Kaspersky Security Network бағдарламасына қатыспайды. Бұл үшін, жергілікті әкімші құқықтары керек.

KSN прокси-серверінің статистикасын көру

Kaspersky Security Center Web Console жүйесі KSN прокси-серверінің қолданыс статистикасын көруге мүмкіндік береді.

Статистика келесі параметрлерді қамтиды:

- KSN-ге қосылу күйі
- Кэш жазбаларының саны
- Кэште өңделген пакеттер саны
- Алынған пакеттер саны

KPSN-ді инфрақұрылым шешімі ретінде пайдалансаңыз, KPSN қолданыс статистикасы көрсетіледі.

Статистиканы көру үшін:

1. Негізгі мәзірдегі басқару серверінің атауын басыңыз.

   Басқару серверінің сипаттары терезесі ашылады.

2. **Жалпы** қойындысында **KSN проксиі** бөлімін таңдап, **Статистика** қойындысын ашыңыз.

   Бұл қойынды KSN прокси-серверін пайдаланудың нақты статистикасын көрсетеді. Статистика 15 секунд сайын жаңарады.

Аралық сақтағышқа көшіру түймесін басып, статистиканы көшіруге болады.

Тапсырмаларды басқару

Бұл бөлімде, Kaspersky Security Center Linux-те қолданылатын тапсырмалар сипатталған.

Тапсырмалар туралы

Kaspersky Security Center Linux *тапсырмаларды* құру және іске қосу арқылы құрылғыларда орнатылған Kaspersky қауіпсіздік бағдарламаларының жұмысын басқарады. Тапсырмалардың көмегімен бағдарламаларды орнату, іске қосу және тоқтату, файлдарды сканерлеу, бағдарламалардың дерекқорлары мен модульдерін жаңарту, бағдарламалармен басқа әрекеттер орындалады.

Kaspersky Security Center Web Console серверінде осы бағдарлама үшін басқару плагині орнатылған жағдайда ғана Kaspersky Security Center Web Console серверінде осы бағдарлама үшін тапсырма жасай аласыз.

Тапсырмалар Басқару серверінде және құрылғыларда орындалуы мүмкін.

Басқару серверінде орындалатын тапсырмаларға мыналар жатады:

- Есептерді автоматты түрде жеткізу
- Жаңартуларды сақтау орнына жүктеу
- Басқару сервері деректерінің сақтық көшірмесін жасау
- Дерекқорларға қызмет көрсету

Құрылғыларда тапсырмалардың келесі түрлері орындалады:

- *Жергілікті тапсырмалар* – нақты құрылғыда орындалатын тапсырмалар.

  Жергілікті тапсырмаларды Kaspersky Security Center Web Console көмегімен тек әкімші ғана емес, қашықтағы құрылғының пайдаланушысы да өзгерте алады (мысалы, қауіпсіздік бағдарламасының интерфейсінде). Егер жергілікті тапсырманы басқарылатын құрылғыда әкімші де, пайдаланушы да бір уақытта өзгерткен болса, онда әкімші енгізген өзгерістер басым болып күшіне енеді.

- *Топтық тапсырмалар* – бұл аталған топтың барлық құрылғыларында орындалатын тапсырмалар.

  Егер тапсырманың сипаттарында басқаша көрсетілмесе, топтық тапсырма аталған топтың ішкі топтарына да таралады. Топтық тапсырмалар (міндетті емес) осы топқа және ішкі топтарға орналастырылған қосалқы және виртуалды Басқару серверлеріне қосылған құрылғыларда да жұмыс істейді.

- *Глобалдық тапсырмалар* – бұл басқару топтарына кіретіндігіне қарамастан, таңдалған құрылғыларда орындалатын тапсырмалар.

Әр бағдарлама үшін сіз топтық тапсырмалардың, глобалдық тапсырмалардың және жергілікті тапсырмалардың кез келген санын жасай аласыз.

Тапсырма параметрлеріне өзгертулер енгізуге, тапсырмалардың орындалуын бақылауға, тапсырмаларды көшіруге, экспорттауға және импорттауға, сондай-ақ жоюға болады.

Құрылғыдағы тапсырмаларды іске қосу тек осы тапсырмалар жасалған бағдарлама іске қосылған жағдайда ғана орындалады.

Тапсырма нәтижелері әр құрылғыдағы операциялық жүйенің оқиғалар журналында, Басқару серверіндегі оқиғалар журналында және Басқару серверінің дерекқорында сақталады.

Тапсырмалар параметрлерінде құпия деректерді пайдаланбаңыз. Мысалы, домен әкімшісінің құпиясөзін көрсетпеуге тырысыңыз.

Тапсырма аймағы

Тапсырма ауқымы — тапсырма орындалатын құрылғылар жинағы. Тапсырма ауқымының келесі түрлері бар:

- *Жергілікті тапсырма* ауқымы – құрылғының өзі.
- *Басқару серверінің тапсырмасы* ауқымы – Басқару сервері.
- *Топтық тапсырма* ауқымы – топқа кіретін құрылғылардың тізбесі.

Глобалдық тапсырма жасаған кезде оның ауқымын анықтаудың келесі әдістерін қолдануға болады:

- Қажетті құрылғыларды қолмен көрсету.

  Құрылғының мекенжайы ретінде сіз IP мекенжайын (немесе IP аралығын) немесе DNS атауын пайдалана аласыз. Басқару серверімен анықталған желілік құрылғыларды таңдауға да болады.

- Құрылғылар тізімін қосылатын құрылғылар мекенжайлары тізбесін қамтитын TXT пішіміндегі файлдан құрылғылар тізімін импорттау (әр мекенжай бөлек жолда орналасуы тиіс).

  Егер құрылғылар тізімі файлдан импортталса немесе қолмен қалыптастырылса, ал құрылғылар атауы бойынша анықталса, онда тізімге ақпараты Басқару серверінің дерекқорына әлдеқашан қосылған құрылғылар ғана қосылуы мүмкін. Деректер, осы құрылғыларды қосу кезінде немесе құрылғыларды анықтау нәтижесінде дерекқорға енгізілуі тиіс.

- Құрылғы таңдауларын көрсету.

Уақыт өте келе, тапсырманың әрекет ету ауқымы, таңдауға кіретін құрылғылардың жиынтығы қалай өзгеретіндігіне байланысты өзгеріп отырады. Құрылғыны таңдауы құрылғы атрибуттары негізінде, соның ішінде құрылғыда орнатылған бағдарламалық жасақтама негізінде, сондай-ақ құрылғыға белгіленген тегтер негізінде құрылуы мүмкін. Құрылғыны таңдауы тапсырманың әрекет ету ауқымын белгілеудің ең икемді тәсілі болып саналады.

Құрылғы таңдаулары үшін тапсырмаларды кесте бойынша іске қосуды әрқашан Басқару сервері орындайды. Мұндай тапсырмалар Басқару серверімен байланысы жоқ құрылғыларда іске қосылмайды. Әрекет ету ауқымы басқа тәсілмен белгіленетін тапсырмалар құрылғыларда тікелей іске қосылады және құрылғы мен Басқару сервері арасындағы байланыстың болуына тәуелді емес.

Құрылғылар таңдауына арналған тапсырмалар құрылғының жергілікті уақыты бойынша емес, Басқару серверінің жергілікті уақыты бойынша іске қосылады. Әрекет ету ауқымы басқа тәсілмен белгіленетін тапсырмалар құрылғының жергілікті уақыты бойынша іске қосылады.

Тапсырманы жасау

Тапсырма жасау үшін:

1. Бағдарламаның негізгі терезесінде **Тапсырмалар** бөліміне өтіңіз.

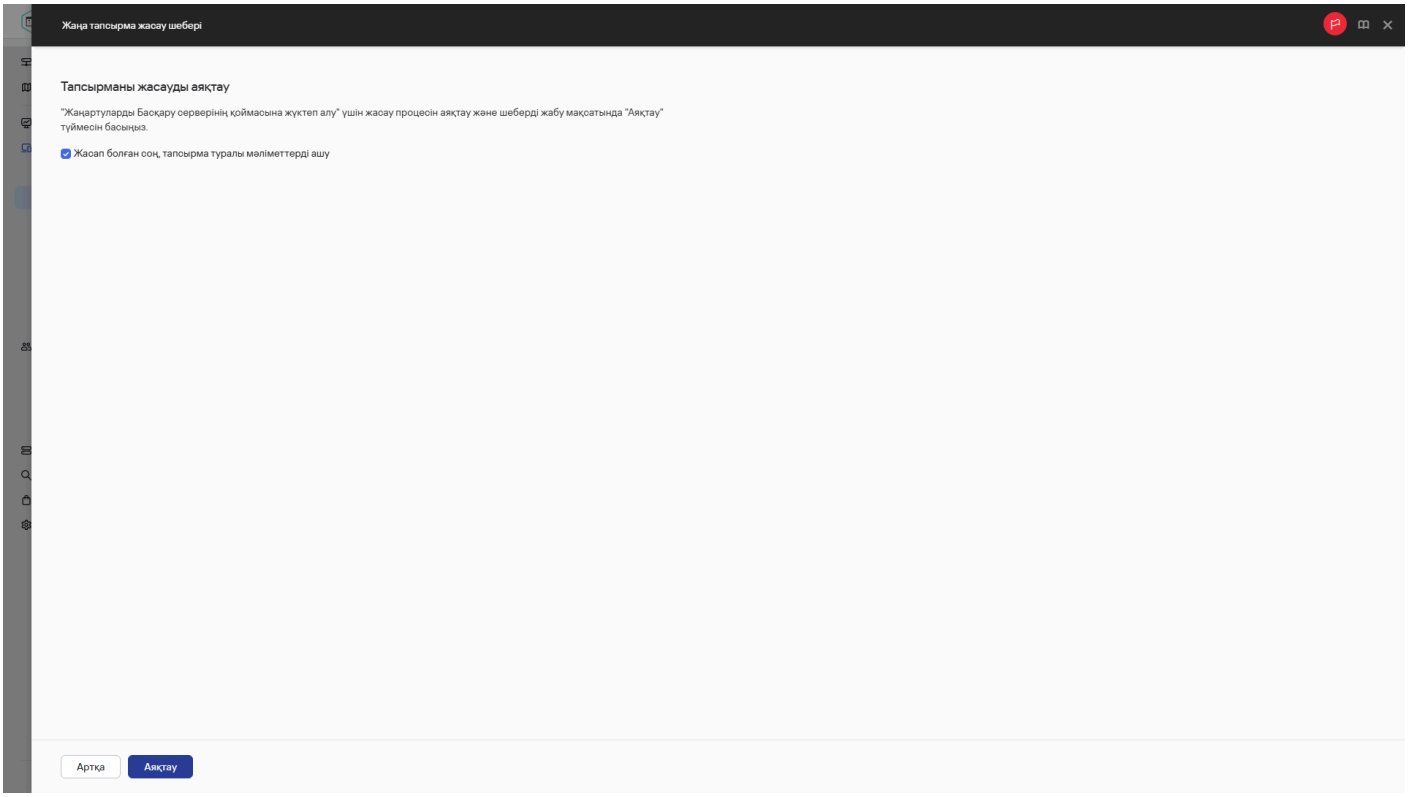
2. **Қосу** түймесін басыңыз.

   Жаңа тапсырма жасау шебері іске қосылады. Шебердің қадамдарын орындаңыз.

3. **Жасап болған соң, тапсырма туралы мәліметтерді ашу** бетінде **Тапсырманы жасауды аяқтау** параметрін қоссаңыз, әдепкі бойынша белгіленген тапсырма параметрлері мәндерін өзгерте аласыз. Егер сіз бұл параметрді қоспасаңыз, тапсырма әдепкі бойынша белгіленген параметр мәндерімен жасалады. Әдепкі бойынша параметр мәндерін кейінірек кез келген уақытта өзгертуге болады.

4. **Аяқтау** түймесін басыңыз.

Тапсырма жасалып, тапсырмалар тізімінде көрсетіледі.



Тапсырманы жасауды аяқтау

Таңдалған құрылғыларға тағайындалған тапсырманы жасау үшін:

1. Бағдарламаның негізгі терезесінде **Активтерді басқару** → **Активтер (құрылғылар)** бөліміне өтіңіз.

   Басқарылатын құрылғылардың тізімі көрсетіледі.

2. Басқарылатын құрылғылар тізімінде тапсырманы іске қосу қажет құрылғылардың жанына құсбелгілерді қойыңыз. Қажетті құрылғыларды табу үшін іздеу және сүзгі функцияларын пайдалана аласыз.

3. **Тапсырманы іске қосу** түймесін басып, **Жаңа тапсырма қосу** тармағын таңдаңыз.

   Жаңа тапсырма жасау шебері іске қосылады.

   Шебердің бірінші қадамында тапсырманың әрекет ету ауқымына қосу үшін таңдалған құрылғыларды жоюға болады. Шебердің нұсқауларын орындаңыз.

4. **Аяқтау** түймесін басыңыз.

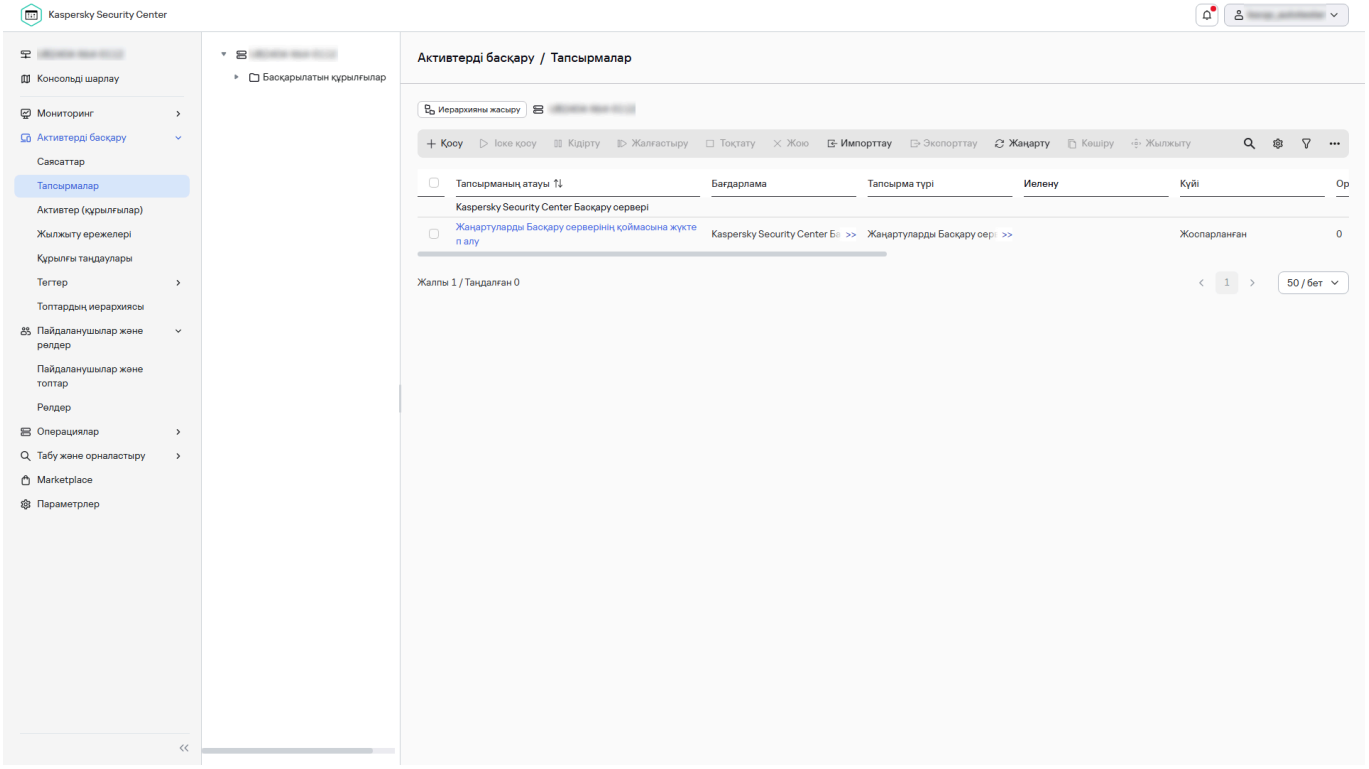
Таңдалған құрылғылар үшін тапсырма жасалды.

Тапсырманы қолмен іске қосу

Бағдарлама әр тапсырманың сипаттарында белгіленген кестеге сәйкес тапсырмаларды орындайды. Тапсырманы кез келген уақытта тапсырмалар тізімінен қолмен іске қосуға болады. Сондай-ақ, **Активтер (құрылғылар)** тізімінен құрылғыларды таңдап, олар үшін бар тапсырманы орындауға болады.

Тапсырманы қолмен іске қосу үшін:

1. Бағдарламаның негізгі терезесінде **Тапсырмалар** бөліміне өтіңіз.
2. Көрсетілген тапсырмалар тізімінде іске қосқыңыз келетін тапсырманың жанына жалауша қойыңыз.
3. **Іске қосу** түймесін басыңыз.



Тапсырмалар тізімінен тапсырманы іске қосу

Тапсырма іске қосылды. Тапсырма күйін **Күйі** бағанында немесе **Нәтиже** түймесін басу арқылы тексере аласыз.

Таңдалған құрылғылар үшін тапсырманы іске қосу.

Құрылғылар тізімінен бір немесе бірнеше клиент құрылғыларын таңдап, олар үшін бұрын жасалған тапсырманы орындауға болады. Бұл белгіленген құрылғылар жинағы үшін бұрын жасалған тапсырмаларды орындауға мүмкіндік береді.

Бұл әрекет осы тапсырма қолданылатын тапсырмадағы құрылғылардың тізімін өзгертеді.

Таңдалған құрылғыларға арналған тапсырманы орындау үшін:

1. Бағдарламаның негізгі терезесінде **Активтерді басқару → Активтер (құрылғылар)** бөліміне өтіңіз. Басқарылатын құрылғылардың тізімі көрсетіледі.

2. Басқарылатын құрылғылар тізімінде тапсырма орындалатын құрылғыларды таңдау үшін жалаушаларды пайдаланыңыз. Қажетті құрылғыларды табу үшін іздеу және сүзгі функцияларын пайдалана аласыз.

3. **Тапсырманы іске қосу** түймесін басып, **Бар тапсырманы қолдану** тармағын таңдаңыз.

   Бар тапсырмалар тізімі көрсетіледі.

4. Таңдалған құрылғылар тапсырмалар тізімінің үстінде пайда болады. Қажет болса, құрылғыны осы тізімнен жоюға болады. Біреуден басқа барлық құрылғыларды жоюға болады.

5. Тізімнен қажетті тапсырманы таңдаңыз. Тапсырманы аты бойынша іздеу үшін тізімнің үстіндегі іздеу өрісін пайдалануға болады. Тек бір құрылғыны ғана таңдауға болады.

6. **Тапсырманы сақтау және бастау** түймесін басыңыз.

Таңдалған тапсырма таңдалған құрылғылар үшін бірден іске қосылады. Тапсырмадағы Кесте бойынша іске қосу параметрлері өзгермейді.

Тапсырмалар тізімін қарап шығу

Сіз Kaspersky Security Center Linux бағдарламасында жасалған тапсырмалар тізімін көре аласыз.

Тапсырмалар тізімін көру үшін,

Бағдарламаның негізгі терезесінде **Тапсырмалар** бөліміне өтіңіз.

Тапсырмалар тізімі көрсетіледі. Тапсырмалар, өздері қатысты болып табылатын бағдарламалардың атауы бойынша топтастырылған. Мысалы, *Бағдарламаны қашықтан орнату* тапсырмасы Басқару серверіне, ал *Жаңарту* тапсырмасы Kaspersky Endpoint Security-ге қатысты болып келеді.

Тапсырма сипаттарын көру үшін,

тапсырманың атауын басыңыз.

Тапсырма сипаттары терезесі бірнеше атаулы қойындылармен бірге көрсетіледі. Мысалы, **Тапсырма түрі** тармағы **Жалпы** қойындысында, ал тапсырма кестесі **Кесте** қойындысында көрсетіледі.

Тапсырмалардың жалпы параметрлері

Бұл бөлім көптеген тапсырмаларыңыз үшін көруге және конфигурациялауға болатын параметрлердің сипаттамасын қамтиды. Қолжетімді параметрлердің тізімі конфигурацияланатын тапсырмаға байланысты.

Тапсырманы жасау кезінде белгіленген параметрлер

Тапсырманы жасау кезінде кейбір параметрлерді белгілеуге болады. Осы параметрлердің кейбірін жасалған тапсырманың сипаттарында да өзгертуге болады.

- Операциялық жүйені қайта жүктеу параметрлері:
  - **Құрылғыны қайта іске қоспау**

    Операция аяқталғаннан кейін, клиент құрылғылары автоматты түрде қайта жүктелмейді. Операцияны аяқтау үшін құрылғыны қайта қосу қажет (мысалы, қолмен немесе құрылғыны басқару тапсырмасы арқылы). Қайта жүктеу қажеттілігі туралы ақпарат тапсырманы орындау нәтижелерінде және құрылғы күйінде сақталады. Бұл нұсқа, үздіксіз жұмыс өте маңызды болып саналатын серверлердегі және басқа құрылғылардағы тапсырмалар үшін жарамды.

  - **Құрылғыны қайта іске қосу**

    Бұл жағдайда, операцияны аяқтау үшін қайта жүктеу қажет болса, қайта жүктеу әрқашан автоматты түрде орындалады. Бұл нұсқа, мезгіл-мезгіл үзілістерге (өшіру, қайта жүктеу) рұқсат етілген құрылғылардағы тапсырмалар үшін жарамды.

  - **Бұғатталған сеанстардағы бағдарламалардың мәжбүрлі жабылуы**

    Іске қосылған қолданбалар клиент құрылғысын қайта жүктеуге мүмкіндік бермеуі мүмкін. Мысалы, егер мәтіндік редакторда құжатпен жұмыс жасалса және өзгертулер сақталмаса, бағдарлама құрылғыны қайта жүктеуге мүмкіндік бермейді.

    Егер бұл параметр қосулы болса, құрылғыны қайта іске қоспас бұрын бұғатталған құрылғылардағы мұндай бағдарламалар мәжбүрлі түрде жабылады. Нәтижесінде, пайдаланушылар сақталмаған жұмысын жоғалтуы мүмкін.

    Егер бұл параметр өшірулі болса, бұғатталған құрылғы қайта жүктелмейді. Бұл құрылғыдағы тапсырманың күйі құрылғыны қайта іске қосу қажеттілігін көрсетеді. Пайдаланушылар бұғатталған құрылғыларда жұмыс істейтін барлық бағдарламаларды қолмен жауып, сол құрылғыларды қайта іске қосуы керек.

    Әдепкі бойынша, параметр өшірулі.

- Тапсырма кестесі параметрлері:

  Тапсырмаға байланысты кесте түрлері әртүрлі болуы мүмкін.

  Кестенің кейбір түрлері басқа Kaspersky қолданбалары үшін қолжетімсіз болуы мүмкін.

  - **Тапсырманы бастау параметрлері:**
    - **N сағат сайын**

      Тапсырма көрсетілген күн мен уақыттан бастап, сағат түрінде белгіленген аралықпен жүйелі түрде орындалады.

      Әдепкі бойынша, тапсырма ағымдағы жүйелік күн мен уақыттан бастап 6 сағат сайын іске қосылып тұрады.

- **N күн сайын**

  Тапсырма, күндер түрінде белгіленген аралықпен жүйелі түрде орындалады. Сондай-ақ, сіз тапсырманы бірінші рет іске қосу күні мен уақытын да көрсете аласыз. Бұл қосымша параметрлерге сіз тапсырма жасап жатқан бағдарлама қолдау көрсетсе, олар қолжетімді болады.

  Әдепкі бойынша, тапсырма ағымдағы жүйелік күн мен уақыттан бастап күн сайын іске қосылады.

- **N минут сайын**

  Тапсырма жүйелі түрде, тапсырма жасалған күні көрсетілген уақыттан бастап, минуттар түрінде белгіленген аралықпен орындалады.

  Әдепкі бойынша, тапсырма ағымдағы жүйелік уақыттан бастап 30 минут сайын іске қосылады.

- **Апта күндері бойынша**

  Тапсырма жүйелі түрде, аптаның көрсетілген күндерінде, көрсетілген уақытта орындалады.

  Әдепкі бойынша, тапсырма жұма сайын, сағат 18:00:00-де іске қосылады.

- **Ай сайын**

  Тапсырма жүйелі түрде, айдың көрсетілген күнінде, көрсетілген уақытта орындалады.

  Көрсетілген күні жоқ айларда тапсырма соңғы күні орындалады.

  Әдепкі бойынша, тапсырма әр айдың бірінші күнінде, ағымдағы жүйелік уақытта орындалады.

- **Қолмен**

  Тапсырма автоматты түрде іске қосылмайды. Тапсырманы тек қолмен іске қосуға болады.

  Әдепкі бойынша, осы нұсқа таңдалған.

- **Бір рет**

  Тапсырма көрсетілген күн мен уақытта тек бір рет орындалады (тапсырманың жасалған күніне сәйкес).

- **Дереу**

  Тапсырма параметрлері сақталғаннан кейін бірден орындалады.

- **Таңдалған апта күні ай сайын**

  Тапсырма жүйелі түрде, әр айдың көрсетілген күндерінде, көрсетілген уақытта орындалады.

  Әдепкі бойынша, басталу уақыты 18:00 және айдың күндері таңдалмайды.

  > Айдағы нақты күнді де, апта нөмірін де (айдың бірінші, екінші аптасын) емес, ай ішіндегі апта күнінің реттік нөмірін таңдайтыныңызды ескеріңіз. Мысалы, егер сіз курсорды **Сс** жолдың **Бірінші** ұяшығына орнатсаңыз, бұл тапсырма әр жаңа айдың бірінші сейсенбісінде орындалатынын білдіреді.

  Аптаның бірнеше күнін таңдай аласыз.

- **Қоймаға жаңартуларды жүктеу кезінде**

  Бұл тапсырма жаңартуларды қоймаға жүктегеннен кейін іске қосылады. Мысалы, сізге *Жаңарту* тапсырмасы үшін осы кесте қажет болуы мүмкін.

- **Басқа тапсырманы аяқтағанда**

  Ағымдағы тапсырма басқа тапсырма аяқталғаннан кейін іске қосылады. Екі тапсырма да бір құрылғы арқылы тағайындалса ғана, осы параметр жұмыс істейді. Мысалы, *Құрылғыларды басқару* тапсырмасын **Құрылғыны қосу** параметрінің көмегімен іске қоса аласыз және ол аяқталғаннан кейін *Вирустарды іздеу* тапсырмасын іске қоса аласыз.

  Кестеден іске қосу тапсырмасын және осы тапсырма орындалатын күйді таңдау керек (**Сәтті аяқталды** немесе **Сәтсіз аяқталды**).

  Қажет болса, кестедегі тапсырмаларды төмендегідей іздеуге, сұрыптауға және сүзуге болады:

  - Тапсырманы атауы бойынша іздеу үшін іздеу өрісіне тапсырма атауын енгізіңіз.
  - Тапсырмаларды атауы бойынша сұрыптау үшін сұрыптау белгішесін басыңыз.

    Әдепкі бойынша, тапсырмалар өсу ретімен әліпбилік ретпен сұрыпталады.
  - Сүзгі белгішесін басыңыз және ашылатын терезеде тапсырмаларды топтар бойынша сүзіңіз, содан кейін **Қолдану** түймесін басыңыз.

- **Өткізіп алынған тапсырмаларды іске қосу**

  Бұл параметр, тапсырма басталғалы тұрған кезде клиент құрылғысы желіде көрсетілмесе, тапсырманың жүріс-тұрысын анықтайды.

  Параметр қосулы болса, клиент құрылғысында Kaspersky бағдарламасын кезекті рет іске қосу кезінде тапсырманы іске қосу әрекеті жасалады. Тапсырманың кестесінде **Қолмен**, **Бір рет** немесе **Дереу** іске қосу көрсетілсе, онда тапсырма желіде құрылғы көзге көрінетін болғаннан кейін немесе құрылғы тапсырманың әрекет ету ауқымына қосылғаннан кейін бірден іске қосылады.

  Егер параметр өшірулі болса, клиент құрылғыларында тапсырманы іске қосу тек кесте бойынша орындалатын болады. **Қолмен**, **Бір рет** және **Дереу** кестесі үшін тапсырмалар желіде көрінетін клиенттік құрылғыларда ғана орындалады. Мысалы, сіз бұл параметрді тек жұмыс уақытынан тыс уақытта іске қосқыңыз келетін ресурстарды қажетсінетін тапсырма үшін өшіре аласыз.

  Әдепкі бойынша, параметр өшірулі.

- **Тапсырманы бастау үшін автоматты түрде араластырылған кідірісті пайдалану**

  Параметр қосулы болса, тапсырма клиент құрылғыларында белгілі бір уақыт аралығында кездейсоқ іске қосылады, яғни *тапсырманың таратылған іске қосылуы* орын алады. Тапсырманың таратылған іске қосылуы, тапсырманы кесте бойынша іске қосу кезінде көптеген клиент құрылғыларының Басқару серверіне бір уақытта жүгінуіне жол бермейді.

  Таратылған іске қосылу кезеңі, тапсырма тағайындалған клиент құрылғыларының санына байланысты тапсырманы жасау кезінде автоматты түрде есептеледі. Кейінірек, тапсырма әрқашан есептелген іске қосу уақытында іске қосылады. Алайда, тапсырма параметрлеріне түзетулер енгізілгенде немесе тапсырма қолмен іске қосылғанда, тапсырманы іске қосу уақытының есептелген мәні өзгереді.

  Егер параметр өшірулі болса, клиент құрылғыларында тапсырманы іске қосу кесте бойынша орындалады.

- **Тапсырманы бастауға арналған келесі аралықтағы автоматты кездейсоқ кідірісті пайдалану**

  Параметр қосулы болса, тапсырма клиент құрылғыларында белгілі бір уақыт аралығында кездейсоқ іске қосылады. Тапсырманың таратылған іске қосылуы, тапсырманы кесте бойынша іске қосу кезінде көптеген клиент құрылғыларының Басқару серверіне бір уақытта жүгінуіне жол бермейді.

  Егер параметр өшірулі болса, клиент құрылғыларында тапсырманы іске қосу кесте бойынша орындалады.

  Әдепкі бойынша, параметр өшірулі. Әдепкі бойынша, уақыт аралығы бір минутқа тең.

- Тапсырма белгіленетін құрылғыларды таңдау терезесі:

  - **Басқару серверімен анықталған желілік құрылғыларды таңдау**

    Бұл жағдайда, тапсырма арнайы құрылғыларға тағайындалады. Арнайы құрылғыларға сіз басқару топтарындағы құрылғыларды да, тағайындалмаған құрылғыларды да қоса аласыз.

    Мысалы, сіз бұл параметрді Желілік агентті тағайындалмаған құрылғыларға орнату тапсырмасында пайдалана аласыз.

  - **Құрылғының мекенжайларын қолмен белгілеу немесе тізімнен импорттау.**

    Сіз DNS атауларын, IP мекенжайларын, сондай-ақ тапсырманы тағайындауды қажет ететін құрылғылардың IP мекенжайы ауқымдарын белгілей аласыз.

    Бұл параметрді белгіленген ішкі желі үшін тапсырманы орындау үшін пайдалануға болады. Мысалы, сіз бухгалтерлердің құрылғыларына белгілі бір бағдарламаны орната аласыз немесе вирус жұқтыруы мүмкін ішкі желідегі құрылғыларды тексере аласыз.

  - **Құрылғы таңдауына тапсырманы белгілеу**

    Тапсырма құрылғы таңдауларына кіретін құрылғыларға тағайындалады. Қолданыстағы таңдаулардың бірін көрсетуге болады.

    Мысалы, операциялық жүйенің белгілі бір нұсқасы бар құрылғыларда тапсырманы іске қосу үшін осы параметрді пайдалануға болады.

  - **Басқару тобына тапсырманы белгілеу**

    Тапсырма бұрын жасалған басқару тобына кіретін құрылғыларға тағайындалады. Бар топтардың бірін көрсетуге немесе жаңа топ құруға болады.

    Мысалы, хабар белгілі бір басқару тобындағы құрылғыларға арналған болса, пайдаланушыларға хабар жіберу тапсырмасын іске қосу үшін осы параметрді пайдалануға болады.

    Тапсырма Басқару тобына тағайындалса, **Қауіпсіздік** қойындысы тапсырма сипаттары терезесінде көрсетілмейді, себебі топтық тапсырмалар олар тиесілі болып саналатын қауіпсіздік топтарының параметрлеріне бағынады.

- Есептік жазба параметрлері:

  - **Әдепкі бойынша есептік жазба**

    Тапсырма, сол тапсырманы орындайтын бағдарлама орнатылған және іске қосылған сол есептік жазбамен іске қосылады.

    Әдепкі бойынша, осы нұсқа таңдалған.

  - **Есептік жазбаны көрсету**

    Есептік жазба және **Құпиясөз** өрістерінде тапсырма іске қосылуы тиісті есептік жазба деректерін көрсетіңіз. Есептік жазбада тапсырманы орындау үшін қажетті құқықтар болуы керек.

- **Есептік жазба**

  Тапсырманы іске қосатын есептік жазба.

- **Құпиясөз**

  Тапсырманы іске қосатын есептік жазбаның құпиясөзі.

Тапсырма жасалғаннан кейін белгіленген параметрлер

Тапсырманы жасағаннан кейін ғана келесі параметрлерді белгілеуге болады.

- Топтық тапсырма параметрлері:

  - **Ішкі топтарға тарату**

    Бұл параметр тек топтық тапсырмалардың сипаттарында қолжетімді.

    Бұл параметр қосылған кезде, тапсырманың әрекет ету ауқымы мыналарды қамтиды:

    - тапсырманы жасау кезінде сіз таңдаған басқару тобы;
    - топтар иерархиясы бойынша кез келген деңгейде таңдалған басқару тобына бағынатын басқару топтары.

    Егер бұл параметр өшірулі болса, тапсырманың құрамына тапсырманы жасау кезінде таңдаған басқару тобы ғана кіреді.

    Әдепкі бойынша, параметр қосулы.

  - **Қосалқы және виртуалды Басқару серверлеріне тарату**

    Бұл параметрді қосқан кезде, негізгі Басқару серверінде жұмыс істейтін тапсырма қосалқы (соның ішінде виртуалды) Басқару серверлерінде қолданылады. Егер Қосалқы Басқару серверінде бірдей типтегі тапсырма бұрыннан бар болса, онда қосалқы Басқару серверінде екі тапсырма да қолданылады — қолданыстағы және негізгі Басқару серверінен қабыл алынған.

    Ішкі топтарға тарату параметрі қосулы болса, бұл параметр қолжетімді болады.

    Әдепкі бойынша, параметр өшірулі.

- Кестенің қосымша параметрлері:

  - **Тапсырманы бастамас бұрын, Wake-on-LAN функциясы көмегімен құрылғыларды іске қосыңыз**

    Егер жалауша қойылса, құрылғыдағы операциялық жүйе тапсырма басталғанға дейін көрсетілген уақытта жүктеледі. Әдепкі бойынша белгіленген уақыт – 5 минут.

    Тапсырманы тапсырмалар аймағындағы барлық клиент құрылғыларында, соның ішінде тапсырма басталғалы тұрған кезде өшірілген құрылғыларда орындағыңыз келсе, осы параметрді қосыңыз.

    Тапсырманы орындағаннан кейін құрылғыны автоматты түрде өшіру қажет болса, **Тапсырманы орындағаннан кейін құрылғыларды өшіру** опциясын қосыңыз. Параметр сол терезеде орналасқан.

    Әдепкі бойынша, параметр өшірулі.

- **Тапсырманы орындағаннан кейін құрылғыларды өшіру**

  Мысалы, жұмыс уақытынан кейін жұма сайын клиент құрылғыларына жаңартуларды орнататын, содан кейін демалыс күндері сол құрылғыларды өшіретін жаңартуларды орнату тапсырмасы үшін осы параметрді қосуға болады.

  Әдепкі бойынша, параметр өшірулі.

- **Тапсырма мынанша уақыттан көбірек орындалып жатса, оны тоқтату**

  Белгіленген уақыттан кейін, тапсырма аяқталғанына немесе аяқталмағанына қарамастан автоматты түрде тоқтатылады.

  Егер сіз тым ұзақ орындалатын тапсырмаларды үзгіңіз келсе (немесе тоқтатқыңыз келсе), осы параметрді қосыңыз.

  Әдепкі бойынша, параметр өшірулі. Әдепкі бойынша тапсырманы орындау уақыты – 120 минут.

- Хабарландыру параметрлері:

  - **Тапсырмалар журналын сақтау** блогы:

    - **Басқару серверінің дерекқорында сақтау мерзімі (күндер)**

      Тапсырма аймағындағы барлық клиент құрылғыларында тапсырманы орындаумен байланысты бағдарлама оқиғалары көрсетілген күндер ішінде Басқару серверінде сақталады. Осы кезеңнен кейін ақпарат Басқару серверінен жойылады.

      Әдепкі бойынша, параметр қосулы.

    - **Құрылғыдағы ОЖ оқиғалар журналында сақтау**

      Тапсырманы орындауға байланысты, бағдарлама оқиғалары әрбір клиент құрылғысының жүйелік оқиғалар журналында жергілікті түрде сақталады.

      Әдепкі бойынша, параметр өшірулі.

    - **Басқару серверіндегі ОЖ оқиғалар журналында сақтау**

      Тапсырма аймағындағы барлық клиент құрылғыларында тапсырманы орындаумен байланысты бағдарлама оқиғалары Басқару серверінің операциялық жүйесінің жүйелік оқиғалар журналында орталықтандырылған түрде сақталады.

      Әдепкі бойынша, параметр өшірулі.

    - **Барлық оқиғаларды сақтау**

      Егер бұл параметр таңдалса, тапсырмаға қатысты оқиғалардың барлығы оқиғалар журналына жазылады.

    - **Тапсырманы орындау барысына қатысты оқиғаларды сақтау**

      Егер бұл параметр таңдалса, оқиғалар журналына тек тапсырманы орындаумен байланысты оқиғалар жазылады.

    - **Тек тапсырманы орындау нәтижелерін сақтау**

      Егер бұл параметр таңдалса, оқиғалар журналына тек тапсырманы орындау нәтижелерімен байланысты оқиғалар жазылады.

- **Әкімшіге тапсырманы орындау нәтижелері туралы хабарлау**

  Сіз әкімшілердің тапсырманы орындау нәтижелері туралы хабар алу жолдарын таңдай аласыз: электрондық пошта, SMS арқылы және орындалатын файлды іске қосу кезінде. Хабарландыру параметрлерін конфигурациялау үшін **Параметрлер** сілтемесі арқылы өтіңіз.

  Барлық хабарландыру тәсілдері әдепкі бойынша өшірілген.

- **Тек қателер туралы хабарлау**

  Егер бұл параметр қосылса, әкімшілер тапсырма қате аяқталған жағдайда ғана хабарландыру алады.

  Егер бұл параметр өшірулі болса, әкімшілер тапсырма аяқталғаннан кейін хабарландыру алады.

  Әдепкі бойынша, параметр қосулы.

- Қауіпсіздік параметрлері.

- Тапсырманың әрекет ету ауқымының параметрлері.

  Тапсырманың әрекет ету ауқымы қалай анықталатынына байланысты келесі параметрлер бар:

  - **Devices**

    Егер тапсырманың әрекет ету ауқымы басқару топтарымен анықталса, сіз сол топты қарай аласыз. Мұнда ешқандай өзгерістер қолжетімді емес. Алайда, сіз **Тапсырма ауқымынан шығарып тастау** конфигурациялай аласыз.

    Егер тапсырманың әрекет ету ауқымы құрылғылар тізімімен анықталса, бұл тізім құрылғыларды қосу және жою арқылы өзгертілуі мүмкін.

  - **Құрылғыны таңдау**

    Тапсырма қолданылатын құрылғылар таңдауын өзгертуге болады.

  - **Тапсырма ауқымынан шығарып тастау**

    Тапсырма қолданылмайтын құрылғылар тобын көрсетуге болады. Шығарылатын топтар тек тапсырма қолданылатын басқару тобының ішкі топтары бола алады.

- **Тексерістер журналы**.

Тапсырманы экспорттау

Kaspersky Security Center Linux бағдарламасы тапсырманы және оның параметрлерін KLT файлына сақтауға мүмкіндік береді. Сақталған тапсырманы Kaspersky Security Center Windows, сондай-ақ Kaspersky Security Center Linux жүйелерінде импорттау үшін KLT файлын пайдалануға болады.

Тапсырманы экспорттау үшін:

1. Бағдарламаның негізгі терезесінде **Тапсырмалар** бөліміне өтіңіз.

2. Экспорттағыңыз келетін тапсырманың жанына жалаушаны қойыңыз.

   Бір уақытта бірнеше тапсырманы экспорттауға болмайды. Бірнеше тапсырманы таңдайтын болсаңыз, **Экспорттау** түймесі белсенді емес болады. Басқару серверінің тапсырмалары да экспорттау үшін қолжетімді емес.

3. **Экспорттау** түймесін басыңыз.

4. Ашылған **Басқаша сақтау** терезесінде тапсырма файлының атауы мен жолын көрсетіңіз. **Сақтау** түймесін басыңыз.

   Басқаша сақтау терезесі Google Chrome, Microsoft Edge немесе Opera қолдансаңыз ғана көрсетіледі. Басқа браузерді қолданып жатсаңыз, тапсырма файлға автоматты түрде **Жүктеп алулар** қалтасына сақталады.

Тапсырманы импорттау

Kaspersky Security Center Linux бағдарламасы тапсырманы KLT файлынан импорттауға мүмкіндік береді. KLT файлдында экспортталған тапсырма мен оның параметрлері бар.

Kaspersky қолданбасының тапсырмасын дұрыс импорттау үшін сізге сәйкес басқару плагинін орнату қажет.

Тапсырманы импорттау үшін:

1. Бағдарламаның негізгі терезесінде **Тапсырмалар** бөліміне өтіңіз.

2. **Импорттау** түймесін басыңыз.

3. Импорттағыңыз келетін тапсырма файлын таңдау үшін **Шолу** түймесін басыңыз.

4. Ашылған терезеде тапсырманың KLT файлына апаратын жолды көрсетіңіз және **Ашу** түймесін басыңыз. Назар аударыңыз, сіз тек бір тапсырма файлын ғана таңдай аласыз.

   Тапсырманы өңдеу басталады.

5. Тапсырма сәтті аяқталғаннан кейін, тапсырманы тағайындағыңыз келетін құрылғыларды таңдаңыз. Бұл үшін, келесі параметрлердің бірін таңдаңыз:

   - **Басқару тобына тапсырманы белгілеу**

     Тапсырма бұрын жасалған басқару тобына кіретін құрылғыларға тағайындалады. Бар топтардың бірін көрсетуге немесе жаңа топ құруға болады.

     Мысалы, хабар белгілі бір басқару тобындағы құрылғыларға арналған болса, пайдаланушыларға хабар жіберу тапсырмасын іске қосу үшін осы параметрді пайдалануға болады.

     Тапсырма Басқару тобына тағайындалса, **Қауіпсіздік** қойындысы тапсырма сипаттары терезесінде көрсетілмейді, себебі топтық тапсырмалар олар тиесілі болып саналатын қауіпсіздік топтарының параметрлеріне бағынады.

   - **Құрылғының мекенжайларын қолмен белгілеу немесе тізімнен импорттау**

     Сіз DNS атауларын, IP мекенжайларын, сондай-ақ тапсырманы тағайындауды қажет ететін құрылғылардың IP мекенжайы ауқымдарын белгілей аласыз.

     Бұл параметрді белгіленген ішкі желі үшін тапсырманы орындау үшін пайдалануға болады. Мысалы, сіз бухгалтерлердің құрылғыларына белгілі бір бағдарламаны орната аласыз немесе вирус жұқтыруы мүмкін ішкі желідегі құрылғыларды тексере аласыз.

- **Құрылғы таңдауына тапсырманы белгілеу**

  Тапсырма құрылғы таңдауларына кіретін құрылғыларға тағайындалады. Қолданыстағы таңдаулардың бірін көрсетуге болады.

  Мысалы, операциялық жүйенің белгілі бір нұсқасы бар құрылғыларда тапсырманы іске қосу үшін осы параметрді пайдалануға болады.

6. Тапсырманың әрекет ету ауқымын көрсетіңіз.

7. Импорттау тапсырмасын аяқтау үшін **Аяқтау** түймесін басыңыз.

Импорт нәтижелері бар хабарландыру пайда болады. Тапсырманы импорттау сәтті орындалса, сіз тапсырмасипаттарын қарап шығу үшін **Мәліметтер** сілтемесінен өте аласыз.

Импорт сәтті орындалғаннан кейін, тапсырма тапсырмалар тізімінде көрсетіледі. Тапсырма параметрлері мен кесте де импортталады. Тапсырма кестеге сәйкес іске қосылады.

Импортталған жаңа тапсырманың атауы бұрыннан бар тапсырманың атауымен бірдей болса, импортталған тапсырманың атауы түр **(<реттік нөмір>)**, мысалы: **(1)**, **(2)** жалғауы көмегімен кеңейтіледі.

Тапсырмалардың құпиясөзін өзгерту шеберін іске қосу

Жергілікті емес тапсырма үшін, сіз тапсырманы іске қосуға құқық беретін есептік жазбаны көрсете аласыз. Есептік жазбаны, тапсырманы жасау кезінде немесе қолданыстағы тапсырманың сипаттарында көрсетуге болады. Егер аталған есептік жазба ұйымда белгіленген қауіпсіздік ережелеріне сәйкес пайдаланылса, бұл ережелер есептік жазбаның құпиясөзін мезгіл-мезгіл өзгертуді талап етуі мүмкін. Есептік жазба құпиясөзінің мерзімі аяқталғаннан кейін және жаңа құпиясөзді орнатқаннан кейін, тапсырма сипаттарында жаңа жарамды құпиясөзді көрсеткенге дейін тапсырма іске қосылмайды.

Тапсырмалардың құпиясөзін өзгерту шебері, есептік жазба көрсетілген барлық тапсырмаларда ескі құпиясөзді жаңасына автоматты түрде тапсыруға мүмкіндік береді. Сондай-ақ, құпиясөзді әр тапсырманың сипаттарында қолмен өзгертуге болады.

Тапсырмалардың құпиясөзін өзгерту шеберін іске қосу үшін:

1. Бағдарламаның негізгі терезесінде **Тапсырмалар** бөліміне өтіңіз.

2. **Тапсырмаларды іске қосу үшін есептік жазбалардың тіркелгі деректерін басқару** түймесін басыңыз.

Содан кейін, шебердің нұсқауларын орындаңыз.

1-қадам. Есептік деректерді таңдау

Жүйеңізде қазіргі уақытта жарамды жаңа есептік деректерді көрсетіңіз. Шебердің келесі қадамына өткен кезде, Kaspersky Security Center Linux бағдарламасы аталған есептік жазбаның атауы әрбір жергілікті емес тапсырманың сипаттарындағы есептік жазбаның атауына сәйкес келетінін тексереді. Егер есептік жазба атаулары сәйкес келсе, тапсырма сипаттарындағы құпиясөз автоматты түрде жаңасына ауысады.

Жаңа есептік жазбаны көрсету үшін келесі нұсқалардың бірін таңдаңыз:

- **Қолданыстағы есептік жазбаны пайдалану**

  Шебер, қазір Kaspersky Security Center Web Console веб-консоліне кірген есептік жазбаның атын пайдаланады. **Тапсырмаларда пайдаланылатын ағымдағы құпиясөз** өрісінде есептік жазба құпия сөзін қолмен енгізіңіз.

- **Басқа есептік жазбаны анықтау**

  Тапсырмалар іске қосылуы тиісті есептік жазбаның атын көрсетіңіз. Есептік жазбаның құпиясөзін **Тапсырмаларда пайдаланылатын ағымдағы құпиясөз** өрісінде көрсетіңіз.

Алдыңғы құпиясөз (міндетті емес; егер оны ағымдағы құпиясөзбен ауыстырғыңыз келсе) өрісін толтырған кезде, Kaspersky Security Center Linux бағдарламасы құпиясөзді тек атауы мен ескі құпиясөз мәндері сәйкес келетін тапсырмалар үшін ауыстырады. Ауыстыру автоматты түрде орындалады. Барлық басқа жағдайларда, шебердің келесі қадамында орындалатын әрекетті таңдау керек.

2-қадам. Орындалып жатқан әрекетті таңдау

Егер шебердің бірінші қадамында сіз алдыңғы құпиясөзді көрсетпеген болсаңыз немесе көрсетілген ескі құпиясөз тапсырмалардың сипаттарында көрсетілген құпиясөздерге сәйкес келмесе, онда сіз осы тапсырмалармен орындалатын әрекетті таңдауыңыз керек.

Тапсырмамен жасалатын әрекетті таңдау үшін:

1. Әрекетті орындағыңыз келетін тапсырманың жанына жалаушаны қойыңыз.

2. Келесі әрекеттердің бірін орындаңыз:

   - Тапсырманың сипаттарында құпиясөзді жою үшін **Тіркелгі деректерін жою** түймесін басыңыз.

     Тапсырма әдепкі бойынша есептік жазбамен іске қосуға ауыстырып қосылған.

   - Құпиясөзді жаңасына ауыстыру үшін **Тіпті ескі құпиясөз дұрыс емес немесе берілмесе де, құпиясөзді мәжбүрлеп өзгерту** түймесін басыңыз.

   - Құпиясөзді өзгертуді болдырмау үшін **Әрекет таңдалмады** түймесін басыңыз.

Таңдалған әрекеттер шебердің келесі қадамына өткеннен кейін қолданылады.

3-қадам. Нәтижелерді қарап шығу

Шебердің соңғы қадамында анықталған тапсырмалардың әрқайсысының нәтижелерін қараңыз. Шебердің жұмысын аяқтау үшін **Аяқтау** түймесін басыңыз.

Басқару серверінде сақталатын тапсырмаларды орындау нәтижелерін қарап шығу

Kaspersky Security Center Linux сізге топтық тапсырмалардың нәтижелерін, арнайы құрылғыларға арналған тапсырмаларды және Басқару сервері тапсырмаларын көруге мүмкіндік береді.

Тапсырманы орындау нәтижелерін көру үшін келесі әрекеттерді орындаңыз:

1. Тапсырма сипаттары терезесінде **Жалпы** бөлімін таңдаңыз.
2. **Нәтижелер** сілтемесі арқылы **Тапсырма нәтижелері** терезесін ашыңыз.

Қосалқы Басқару серверіне арналған тапсырманың нәтижелерін көру үшін:

1. Тапсырма сипаттары терезесінде **Жалпы** бөлімін таңдаңыз.
2. **Нәтижелер** сілтемесі арқылы **Тапсырма нәтижелері** терезесін ашыңыз.
3. **Қосалқы серверлердің статистикасы** түймесін басыңыз.
4. **Тапсырма нәтижелері** терезесін көрсеткіңіз келетін қосалқы Серверді таңдаңыз.

Бағдарлама тегтері

Бұл бөлімде бағдарлама тегтері сипатталған, оларды жасау және өзгерту, сондай-ақ үшінші тарап бағдарламаларына тегтерді тағайындау бойынша нұсқаулар берілген.

Бағдарлама тегтері

Kaspersky Security Center Linux бағдарламасы бағдарламалар тізілімінен қолданбаларға тегтерді тағайындауға мүмкіндік береді. Тег, бағдарламаларды топтастыру және іздеу үшін пайдалануға болатын бағдарлама белгісі болып саналады. Бағдарламаға тағайындалған тегті құрылғыларды таңдауға арналған шарттарда қолдануға болады.

Мысалы, `[Шолғыштар]` тегін жасап, оны Microsoft Internet Explorer, Google Chrome, Mozilla Firefox сияқты барлық шолғыштарға тағайындауға болады.

Бағдарлама тегтерін жасау

Бағдарлама тегін жасау үшін:

1. Бағдарламаның негізгі терезесінде **Бағдарламалық жасақтаманы басқару → Үшінші тарап бағдарламалары → Бағдарлама тегтері** бөліміне өтіңіз.
2. **Қосу** түймесін басыңыз.

   Тег жасау терезесі көрсетіледі.
3. Тегті көрсетіңіз.
4. Өзгерістерін сақтау үшін **OK** түймесін басыңыз.

Жаңа жасалған тег бағдарлама тегтерінің тізімінде пайда болады.

Бағдарлама тегтерін өзгерту

Бағдарлама тегін қайта атау үшін:

1. Бағдарламаның негізгі терезесінде **Бағдарламалық жасақтаманы басқару → Үшінші тарап бағдарламалары → Бағдарлама тегтері** бөліміне өтіңіз.
2. Атын өзгерткіңіз келетін тегтің жанындағы жалаушаны қойып, **Өңдеу** түймесін басыңыз.

   Тегтің сипаттары терезесі ашылады.
3. Тег атауын өзгертіңіз.
4. Өзгерістерін сақтау үшін **OK** түймесін басыңыз.

Жаңартылған тег бағдарлама тегтері тізімінде пайда болады.

Бағдарламаларға тегтер тағайындау

Бағдарламаға тегтер тағайындау үшін:

1. Бағдарламаның негізгі терезесінде **Бағдарламалық жасақтаманы басқару → Үшінші тарап бағдарламалары → Бағдарламалар тізімдемесі** бөліміне өтіңіз.
2. Тегтерді белгілеу қажет бағдарламаны таңдаңыз.
3. **Тегтер** қойыншасын таңдаңыз.

   Қойыншада Басқару серверінде бар барлық бағдарлама тегтері пайда болады. Таңдалған бағдарламаға тағайындалған тегтер **Тег белгіленді** бағанындағы жалаушалармен белгіленеді.

4. Тағайындау қажет тегтер үшін **Тег белгіленді** бағанындағы жалаушаларды қойыңыз.

5. Өзгерістерін сақтау үшін **Сақтау** түймесін басыңыз.

Бағдарламаға тегтер белгіленді.

Бағдарламаларға тағайындалған тегтерді алып тастау

Бағдарламадан тегтерді алып тастау үшін:

1. Бағдарламаның негізгі терезесінде **Бағдарламалық жасақтаманы басқару** → **Үшінші тарап бағдарламалары** → **Бағдарламалар тізімдемесі** бөліміне өтіңіз.

2. Тегтерді алып тастау қажет бағдарламаны таңдаңыз.

3. **Тегтер** қойыншасын таңдаңыз.

   Қойыншада Басқару серверінде бар барлық бағдарлама тегтері пайда болады. Таңдалған бағдарламаға тағайындалған тегтер **Тег белгіленді** бағанындағы жалаушалармен белгіленеді.

4. Алып тастау қажет тегтер үшін **Тег белгіленді** бағанындағы жалаушаларды алып тастаңыз.

5. Өзгерістерін сақтау үшін **Сақтау** түймесін басыңыз.

Тегтер бағдарламадан алынады.

Бағдарламалардан алынған тегтер жойылмайды. Қажет болса, оларды қолмен жоюға болады.

Бағдарлама тегтерін жою

Бағдарлама тегін жою үшін:

1. Бағдарламаның негізгі терезесінде **Бағдарламалық жасақтаманы басқару** → **Үшінші тарап бағдарламалары** → **Бағдарлама тегтері** бөліміне өтіңіз.

2. Тізімнен жойғыңыз келетін бағдарлама тегтерін таңдаңыз.

3. **Жою** түймесін басыңыз.

4. Пайда болған терезеде **OK** түймесін басыңыз.

Таңдалған бағдарлама тегі жойылды. Жойылған тег, ол тағайындалған барлық бағдарламалардан автоматты түрде алынып тасталады.

13291-портты ашу үшін klscflag утилитасын пайдалану

Kaspersky Security Center Linux жұмысын klakaut утилитасының көмегімен автоматтандыра аласыз. klakaut утилитасы және оған арналған анықтамалық жүйе Kaspersky Security Center Linux орнату қалтасында орналасқан. Егер klakaut утилитасын пайдаланғыңыз келсе, klscflag утилитасы арқылы 13291 портын ашыңыз.

Утилита KLSRV_SP_SERVER_SSL_PORT_GUI_OPEN параметрінің мәнін өзгертеді.

13291-портты ашу үшін:

1. Пәрмен жолында келесі пәрменді орындаңыз:
   ```
   /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. Келесі пәрменді орындау арқылы Kaspersky Security Center басқару серверінің қызметін қайта іске қосыңыз:
   ```
   sudo systemctl restart kladminserver_srv
   ```

13291-порт ашық.

13291-порттың сәтті ашылғанын тексеру үшін:

Пәрмен жолында келесі пәрменді орындаңыз:

```
/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\";"
```

Бұл пәрмен келесі нәтижені қайтарады:

```
+--- (PARAMS_T)
+---KLSRV_SP_SERVER_SSL_PORT_GUI_OPEN = (BOOL_T)true
```

`true` мәні порттың ашық екенін білдіреді. Әйтпесе, `false` мәні көрсетіледі.

Kaspersky Security Center Web Console веб-консолінде Kaspersky Industrial CyberSecurity for Networks бағдарламаларын тіркеу

Kaspersky Industrial CyberSecurity for Networks қолданбасымен Kaspersky Security Center Web Console арқылы жұмысты бастау үшін оны алдын ала Kaspersky Security Center Web Console веб-консолінде тіркеу керек.

Kaspersky Industrial CyberSecurity for Networks қолданбасын тіркеу үшін:

1. Келесі әрекеттердің орындалғанына көз жеткізіңіз:

   - Kaspersky Industrial CyberSecurity for Networks веб-плагинін жүктеп алып, орнаттыңыз.

     Мұны кейінірек, Kaspersky Industrial CyberSecurity for Networks серверінің Басқару сервермен синхрондалуын күте отырып орындауға болады. Плагинді жүктеп алып, орнатқаннан кейін **KICS for Networks** бөлімі Kaspersky Security Center Web Console негізгі мәзірінде көрсетіледі.

   - Kaspersky Industrial CyberSecurity for Networks веб-интерфейсінде Kaspersky Security Center Linux-пен өзара әрекеттесу орнатылады және қосылады. Толық ақпарат Kaspersky Industrial CyberSecurity for Networks онлайн анықтамасында келтірілген.

2. Kaspersky Industrial CyberSecurity for Networks сервері орнатылған құрылғыны Тағайындалмаған құрылғылар тобынан Басқарылатын құрылғылар тобына жылжытыңыз:

   a. Бағдарламаның негізгі терезесінде **Активтерді басқару** → **Тағайындалмаған құрылғылар** бөліміне өтіңіз.

   b. Kaspersky Industrial CyberSecurity for Networks Server орнатылған құрылғының жанына жалауша қойыңыз.

   c. **Топқа жылжыту** түймесін басыңыз.

   d. Басқару топтарының иерархиясында **Басқарылатын құрылғылар** тобының жанына жалауша қойыңыз.

   e. **Жылжыту** түймесін басыңыз.

3. Kaspersky Industrial CyberSecurity for Networks сервері орнатылған құрылғының сипаттары терезесін ашыңыз.

4. Құрылғы сипаттары терезесінде, **Жалпы** бөлімінде **Басқару серверімен байланысты үзбеу** параметрін таңдаңыз, содан соң **Сақтау** түймесін басыңыз.

5. Құрылғы сипаттары терезесінде **Қолданбалар** бөлімін таңдаңыз.

6. **Қолданбалар** бөлімінде Kaspersky Security Center Network Желілік агентін таңдаңыз.

7. Бағдарламаның ағымдағы күйі *Тоқтатылды* болса, ол *Орындалуда* күйіне өзгергенше күтіңіз.

   Бұл 15 минутқа дейін созылуы мүмкін. Kaspersky Industrial CyberSecurity for Networks веб-плагинін әлі орнатпаған болсаңыз, оны дәл қазір жасай аласыз.

8. Kaspersky Industrial CyberSecurity for Networks туралы статистиканы көргіңіз келсе, басқару тақтасына веб-виджеттерді қосуға болады. Веб-виджеттерді қосу үшін келесі әрекеттерді орындаңыз:

   a. Бағдарламаның негізгі терезесінде **Мониторинг** → **Бақылау тақтасы** бөліміне өтіңіз.

   b. Басқару тақтасында **Веб-виджетті қосу немесе қалпына келтіру** түймесін басыңыз.

   c. Пайда болған веб-виджетте **Басқа** түймесін басыңыз.

d. Қосқыңыз келетін веб-виджетті таңдаңыз.

- KICS for Networks орналастыру картасы
- KICS for Networks серверлері туралы ақпарат
- KICS for Networks ағымдағы оқиғалары
- KICS for Networks ішінде назар аударуды қажет ететін құрылғылар
- KICS for Networks маңызды оқиғалары
- KICS for Networks күйлері

9. Kaspersky Industrial CyberSecurity for Networks веб-интерфейсіне өту үшін мына қадамдарды орындаңыз:

a. Қолданбаның негізгі терезесінде **KICS for Networks** → **Іздеу** бөліміне өтіңіз.

b. **Оқиғаларды немесе құрылғыларды табу** түймесін басыңыз.

c. Ашылған **Сауалнама параметрлері** терезесінде **Сервер** өрісін басыңыз.

d. Kaspersky Security Center Linux-пен біріктірілген серверлердің ашылмалы тізімінде Kaspersky Industrial CyberSecurity for Networks серверін таңдап, **Табу** түймесін басыңыз.

e. Kaspersky Industrial CyberSecurity for Networks сервер атауының жанындағы **Серверге өту** сілтемесіне өтіңіз.

Kaspersky Industrial CyberSecurity for Networks кіру беті ашылады.

> Kaspersky Industrial CyberSecurity for Networks веб-интерфейсіне кіру үшін қолданба пайдаланушысының есептік жазба деректерін енгізу керек.

Пайдаланушылар мен пайдаланушы рөлдерді басқару

Бұл бөлімде пайдаланушылармен және пайдаланушы рөлдерімен жасалатын жұмыс сипатталған, сондай-ақ оларды құру және өзгерту, пайдаланушыларға рөлдер мен топтарды тағайындау және саясат профильдерін рөлдермен байланыстыру бойынша нұсқаулар келтірілген.

Пайдаланушылардың есептік жазбалары туралы

Kaspersky Security Center Linux пайдаланушы есептік жазбалары мен қауіпсіздік топтарын басқаруға мүмкіндік береді. Қолданба есептік жазбалардың үш түрін қолдайды:

- Ұйым қызметкерлерінің есептік жазбалары. Басқару сервері ұйымның домен контроллерінде сауалнама жүргізу кезінде осы домен пайдаланушыларының есептік жазбалары туралы деректерді алады.
- Жергілікті пайдаланушылардың есептік жазбалары. Басқарылатын құрылғылардың жергілікті есептік жазбалары, сондай-ақ басқару сервері орнатылған құрылғының жергілікті есептік жазбалары.
- Kaspersky Security Center Linux ішкі пайдаланушы есептік жазбалары. Ішкі пайдаланушылардың есептік жазбаларын жасай аласыз. Бұл есептік жазбалар тек Kaspersky Security Center Linux жүйесінде пайдаланылады.

kladmins тобын Kaspersky Security Center Linux жүйесіндегі Kaspersky Security Center Web Console веб-консоліне кіру үшін пайдалану мүмкін емес. kladmins тобында тек Kaspersky Security Center Linux қызметтерін іске қосу үшін пайдаланылатын есептік жазбалар болуы мүмкін.

Пайдаланушы есептік жазбаларының және қауіпсіздік тобының кестелерін көру үшін:

1. Қолданбаның негізгі терезесінде **Пайдаланушылар және рөлдер** → **Пайдаланушылар және топтар** бөліміне өтіңіз.
2. **Пайдаланушылар** немесе **Топтар** қойындысына өтіңіз.

Пайдаланушылардың немесе қауіпсіздік топтарының тізімі ашылады. Кестені тек ішкі пайдаланушылар немесе топ есептік жазбаларымен көргіңіз келсе, **Есептік жазба түрі** сүзгісін **Ішкі** немесе **Жергілікті** өлшемшартына орнатыңыз.

Егер пайдаланушылар кестесінде 50 000-нан астам пайдаланушы болса, тек алғашқы 50 000 пайдаланушы көрсетіледі, ал қалған пайдаланушылар көрсетілмейді.

Пайдаланушы рөлдері туралы

Пайдаланушы рөлі (бұдан әрі *рөл* деп те аталады) – бұл құқықтар мен рұқсаттар жиынтығын қамтитын нысан. Рөл, пайдаланушының құрылғысында орнатылған Kaspersky бағдарламаларының параметрлерімен байланысты болуы мүмкін. Сіз рөлді пайдаланушылар жиынтығына немесе қауіпсіздік топтарының жиынтығына басқару топтары иерархиясының, Басқару серверлерінің кез келген деңгейінде немесе нақты нысандар деңгейінде тағайындай аласыз.

Егер сіз құрылғыларды виртуалды Басқару серверлерін қамтитын Басқару сервері иерархиясы арқылы басқарсаңыз, пайдаланушы рөлдерін тек физикалық Басқару серверінде жасауға, өзгертуге және жоюға болатынын ескеріңіз. Содан кейін, сіз қосалқы Басқару серверлеріне, соның ішінде виртуалды Серверлерге пайдаланушы рөлдерін тарата аласыз.

Сіз рөлдерді саясат профильдерімен байланыстыра аласыз. Егер пайдаланушыға рөл тағайындалған болса, пайдаланушы қызметтік міндеттерді орындауға қажетті қауіпсіздік параметрлерін алады.

Пайдаланушы рөлі белгіленген басқару тобы пайдаланушыларының құрылғыларымен байланысты болуы мүмкін.

Пайдаланушы рөлі ауқымы

Пайдаланушы рөлі ауқымы – бұл пайдаланушылар мен басқару топтарының тіркесімі. Пайдаланушы рөліне қатысты параметрлер тек осы рөл тағайындалған пайдаланушыларға тиесілі құрылғыларға қолданылады және бұл құрылғылар осы рөл тағайындалған топтарға, соның ішінде еншілес топтарға жататын болса ғана қолданылады.

Рөлдерді пайдаланудың артықшылығы

Рөлдерді пайдаланудың артықшылығы, әрбір басқарылатын құрылғы үшін немесе әрбір пайдаланушы үшін қауіпсіздік параметрлерін бөлек көрсетудің қажеті жоқ. Компаниядағы пайдаланушылар мен құрылғылардың саны көп болуы мүмкін, бірақ әртүрлі қауіпсіздік конфигурацияларын қажет ететін әртүрлі жұмыс функцияларының саны айтарлықтай аз.

Саясат профильдерін қолданудан ерекшеліктері

Саясат профильдері – бұл Kaspersky әр бағдарламасы үшін бөлек құрылған саясаттың сипаттары. Рөл әртүрлі бағдарламалар үшін жасалған көптеген саясат профильдерімен байланысты. Осылайша, рөл – белгілі бір пайдаланушы түріне арналған параметрлерді біріктіру әдісі болып табылады.

Бағдарлама функцияларына қатынасу құқықтарын конфигурациялау. Рөлге негізделген қатынасуды басқару

Kaspersky Security Center Linux бағдарламасы рөлдер негізінде Kaspersky Security Center Linux функцияларына және Kaspersky басқарылатын бағдарламаларының функцияларына қатынасуды қамтамасыз етеді.

Сіз Kaspersky Security Center Linux пайдаланушылары үшін бағдарлама функцияларына қатынасу құқығын келесі тәсілдердің бірімен конфигурациялай аласыз:

- әр пайдаланушының немесе пайдаланушылар тобының құқықтарын жеке-жеке конфигурациялау;
- алдын ала конфигурацияланған құқықтар жиынтығы бар типтік пайдаланушы рөлдерін жасау және пайдаланушыларға олардың қызметтік міндеттеріне қарай рөлдер тағайындау.

Пайдаланушы рөлдерін қолдану пайдаланушының бағдарламаға қатынасу құқығын конфигурациялаудың күнделікті әрекеттерін жеңілдетеді және азайтады. Рөлдегі қатынасу құқықтары пайдаланушылардың типтік тапсырмалары мен қызметтік міндеттеріне сәйкес конфигурацияланады.

Пайдаланушы рөлдеріне олардың мақсатына сәйкес атаулар берілуі мүмкін. Бағдарламада рөлдердің шексіз санын жасай аласыз.

Сіз алдын ала анықталған пайдаланушы рөлдерін бұрыннан конфигурацияланған құқықтар жиынтығымен бірге пайдалана аласыз немесе рөлдер жасай аласыз және қажетті құқықтарды өзіңіз конфигурациялай аласыз.

Бағдарлама функцияларына қатынасу құқықтары

Төмендегі кестеде тапсырмаларды, есептерді, параметрлерді басқаруға және пайдаланушы әрекеттерін орындауға құқық беретін Kaspersky Security Center Linux функциялары берілген.

Кестеде көрсетілген пайдаланушы әрекеттерін орындау үшін пайдаланушының әрекеттің жанында көрсетілген құқығы болуы керек.

Оқу, **Жазу** және **Орындау** құқығы кез келген тапсырмаға, есепке немесе параметрлерге қолданылуы мүмкін. Осы құқықтардан басқа, пайдаланушы тапсырмаларды, есептерді басқару немесе құрылғылар таңдауы параметрлерін өзгерту үшін пайдаланушыда **Құрылғылардың таңдауларында әрекеттерді орындау** құқығы болуы керек.

Кестеде жоқ барлық тапсырмалар, есептер, параметрлер және орнату пакеттері **Жалпы функционал: Базалық функционалдылық** аймағы аймағына жатады.

Функционалдық аймақ	Құқық	Пайдаланушының әрекеті: әрекетті орындауға қажетті құқық	Тапсырма	Есеп	Ба
Жалпы функциялар: **Басқару топтарын басқару**	**Жазу**	• Басқару тобына құрылғыны қосу: **Жазу** • Басқару тобы құрамынан құрылғыны жою: **Жазу** • Басқару тобын басқа басқару тобына қосу: **Жазу** • Басқару тобын басқа басқару тобынан жою: **Жазу**	Жоқ	Жоқ	Жоқ

Функционалдық аймақ	Құқық	Пайдаланушының әрекеті: әрекетті орындауға қажетті құқық	Тапсырма	Есеп	Ба
Жалпы функциялар: ACL тізімдеріне қарамастан, нысандарға қатынасу	**Оқу**	Барлық нысандарға қатысты оқуға қатынас алу: **Оқу**	Жоқ	Жоқ	**Жалпы функцион тізіміне қарамаст нысандар қатынасу** мақсатта арналған. Пайдалан осы функ аймақта құқықтары берілгенд барлық ны толық **Оқ** алады жә жергілікті құқықтары жүйесіне түбір) жел арқылы ба серверіне құрылғыл таңдау бо келген жа тапсырма орындай құқықтард қызметтік міндеттер үшін қаже пайдалан шектеулі мұқият бе ұсынылад Қолжетім құқықтарғ қарамаст олар белг нысандар рұқсат бе беріледі.
Жалпы функционал: **Базалық функционал**	• **Оқу** • **Жазу** • **Орындау** • **Құрылғы таңдаулары бойынша әрекеттерді орындау**	• Виртуалды сервер үшін құрылғыны жылжыту ережелері (жасау, өзгерту немесе жою): **Жазу**, **Құрылғы таңдаулары бойынша әрекеттерді орындау** • Мобильдік (LWNGT) протоколдың арнаулы сертификатын алу: **Оқу** • Пайдаланушы сертификатының мобильді протоколын (LWNGT) орнату: **Жазу** • NLA анықтаған желілер тізімін алу: **Оқу** • NLA анықтаған желілер тізімін қосу, өзгерту немесе жою: **Жазу**	• "Жаңартуларды Басқару серверінің қоймасына жүктеп алу" • "Есептерді жеткізу" • "Орнату пакеттерін тарату" • "Қосалқы Басқару серверлеріне бағдарламаларды орнату"	• "Қорғаныс жағдайы туралы есеп" • "Қауіп-қатер туралы есеп" • "Ең көп зақымдалған құрылғылар туралы есеп" • "Антивирустық дерекқордың күйі туралы есеп" • "Қателер туралы есеп" • "Желілік шабуылдар туралы есеп" • "Пошталық жүйелерді қорғауға арналған бағдарламалар туралы жиынтық есеп"	Жоқ

Функционалдық аймақ	Құқық	Пайдаланушының әрекеті: әрекетті орындауға қажетті құқық	Тапсырма	Есеп	Ба
		• Топтардың қатынасын бақылау тізімін қарау: **Оқу** • Операциялық жүйе журналын көру: **Оқу** • BitLocker арқылы шифрланған қатқыл дискіге кіруді қалпына келтіру үшін қалпына келтіру кілтін қараңыз: **Орындау**		• "Жұмыс станцияларын және Windows серверлерін қорғау бағдарламалары туралы жиынтық есеп" • "Периметрді қорғайтын бағдарламалар туралы жиынтық есеп" • "Орнатылған бағдарлама түрлері туралы жиынтық есеп" • "Вирус жұққан құрылғылардың пайдаланушылары туралы есеп" • "Қауіпсіздік мәселелері туралы есеп" • "Оқиғалар туралы есеп" • "Тарату нүктелерінің әрекетіндегі есеп" • "Қосалқы Басқару серверлері туралы есеп" • "Құрылғыларды басқару оқиғалары туралы есеп" • "Осалдықтар туралы есеп" • "Рұқсат берілмеген бағдарламалар бойынша есеп" • "Веб-бақылау туралы есеп" • "Басқарылатын құрылғыларды шифрлаудың күйі туралы есеп" • "Жаппай сақтау құрылғыларының шифрлау күйлері туралы есеп беру" • "Шифрланған құрылғыға қатынасу құқықтары туралы есеп" • "Файлдарды шифрлау қателері туралы есеп" • "Шифрланған файлдарға қатынасты бұғаттау туралы есеп" • "Пайдаланушының тиімді құқықтары туралы есеп" • "Құқықтар туралы есеп"	

Функционалдық аймақ	Құқық	Пайдаланушының әрекеті: әрекетті орындауға қажетті құқық	Тапсырма	Есеп	Ба
Жалпы функциялар: **Жойылған нысандар**	• **Оқу** • **Жазу**	• Себетте жойылған нысандарды қарау: **Оқу** • Себеттен нысандарды жою: **Жазу**	Жоқ	Жоқ	Жоқ
Жалпы функциялар: **Оқиғаларды өңдеу**	• **Оқиғаларды жою** • **Оқиғалар туралы хабарландыру параметрлерін өзгерту** • **Оқиғалар журналына оқиғаларды жазу параметрлерін өзгерту** • **Жазу**	• Оқиғаларды тіркеу параметрлерін өзгерту: **Оқиғалар журналына оқиғаларды жазу параметрлерін өзгерту** • Оқиғалар туралы хабарландыру параметрлерін өзгерту: **Оқиғалар туралы хабарландыру параметрлерін өзгерту** • Оқиғаларды жою: **Оқиғаларды жою**	Жоқ	Жоқ	Параметр • Дере сақта оқиға макси саны • Қашы құры оқиға сақта
Жалпы функциялар: **Басқару серверімен жасалатын операциялар**	• **Оқу** • **Жазу** • **Орындау** • **Нысанның ACL тізімдерін өзгерту** • **Құрылғы таңдаулары бойынша әрекеттерді орындау**	• Желілік агентті қосу үшін Басқару сервері порттарын өзгерту: **Жазу** • Басқару серверінде іске қосылған белсендіру прокси-серверінің порттарын өзгерту: **Жазу** • Басқару серверінде жұмыс істейтін ұялы құрылғылар үшін белсендіру прокси-серверінің порттарын өзгерту: **Жазу** • Автономды пакеттерді тарату үшін Веб-сервер порттарын өзгерту: **Жазу** • iOS MDM профильдерін тарату үшін Веб-сервер порттарын өзгерту: **Жазу** • Kaspersky Security Center Web Console көмегімен қосылу үшін Басқару серверінің SSL порттарын өзгерту: **Жазу** • Ұялы құрылғыларды қосу үшін Басқару сервері порттарын өзгерту: **Жазу** • Басқару серверінің дерекқорында сақталатын оқиғалардың максималды санын көрсетіңіз: **Жазу**	• "Басқару сервері деректерінің сақтық көшірмесін жасау" • "Дерекқорларға қызмет көрсету"	Жоқ	Жоқ

Функционалдық аймақ	Құқық	Пайдаланушының әрекеті: әрекетті орындауға қажетті құқық	Тапсырма	Есеп	Ба
		• Басқару сервері жібере алатын оқиғалардың максималды санын көрсетіңіз: **Жазу** • Басқару сервері оқиғаларды жібере алатын кезеңді өзгерту: **Жазу**			
Жалпы функционал: **Kaspersky бағдарламаларын орналастыру**	• **Kaspersky патчтарын басқару** • **Оқу** • **Жазу** • **Орындау** • **Құрылғы таңдаулары бойынша әрекеттерді орындау**	Патчты орнатуды растау немесе қабылдамау: **Kaspersky патчтарын басқару**	Жоқ	• "Виртуалды Басқару серверінің лицензиялық кілтін пайдалануы туралы есеп" • "Kaspersky бағдарламалық жасақтамасының нұсқалары туралы есеп" • "Үйлесімсіз қосымшалар туралы есеп" • "Kaspersky бағдарламалық жасақтама модулі жаңартуларының нұсқалары туралы есеп" • "Қорғаныс орналастыру туралы есеп"	Орнату па "Kaspersk
Жалпы функциялар: **Лицензиялық кілттерді басқару**	• **Кілт файлын экспорттау** • **Жазу**	• Кілт файлын экспорттау: **Кілт файлын экспорттау** • Басқару серверінің лицензиялық кілтінің параметрлерін өзгерту: **Жазу**	Жоқ	Жоқ	Жоқ
Жалпы функциялар: **Есептерді басқару**	• **Оқу** • **Жазу**	• ACL тізімдеріне қарамастан, нысандар үшін есептер жасау: **Жазу** • ACL тізімдеріне қарамастан, есептерді орындау: **Оқу**	Жоқ	Жоқ	Жоқ
Жалпы функционал: **Басқару серверлері иерархиясы**	**Басқару серверлерінің иерархиясын конфигурациялау**	• Қосалқы Басқару серверлерін қосу, жаңарту немесе жою: **Басқару серверлерінің иерархиясын конфигурациялау**	Жоқ	Жоқ	Жоқ
Жалпы функциялар: **Пайдаланушы құқықтары**	**Нысанның ACL тізімдерін өзгерту**	• Кез келген нысанның Қауіпсіздігі сипаттарын өзгерту: **Нысанның ACL тізімдерін өзгерту** • Пайдаланушы рөлдерін басқару: **Нысанның ACL тізімдерін өзгерту**	Жоқ	Жоқ	Жоқ

Функционалдық аймақ	Құқық	Пайдаланушының әрекеті: әрекетті орындауға қажетті құқық	Тапсырма	Есеп	Ба
		• Ішкі пайдаланушыларды басқару: **Нысанның ACL тізімдерін өзгерту** • Қауіпсіздік топтарын басқару: **Нысанның ACL тізімдерін өзгерту** • Лақап аттарды басқару: **Нысанның ACL тізімдерін өзгерту**			
Жалпы функциялар: **Виртуалды Басқару серверлері**	• **Виртуалды Басқару серверлерін басқару** • **Оқу** • **Жазу** • **Орындау** • **Құрылғы таңдаулары бойынша әрекеттерді орындау**	• Виртуалды Басқару серверлері тізімін алу: **Оқу** • Виртуалды Басқару сервері туралы ақпаратты алу: **Оқу** • Виртуалды Басқару серверін жасау, жаңарту немесе жою: **Виртуалды Басқару серверлерін басқару** • Виртуалды Басқару серверін басқа топқа жылжыту: **Виртуалды Басқару серверлерін басқару** • Виртуалды Басқару серверіне қатынасу құқықтарын белгілеу: **Виртуалды Басқару серверлерін басқару**	Жоқ	Жоқ	Жоқ

Функционалдық аймақ	Құқық	Пайдаланушының әрекеті: әрекетті орындауға қажетті құқық	Тапсырма	Есеп	Ба
Жалпы функционал: **Шифрлау кілттерін басқару**	**Жазу**	Шифрлау кілттерін импорттау: **Жазу**	Жоқ	Жоқ	Жоқ
Ұялы құрылғыларды басқару: **Жалпы**	• **Жаңа құрылғыларды қосу** • **Ұялы құрылғыларға ақпараттық пәрмендерді ғана жіберу** • **Ұялы құрылғыларға пәрмендер жіберу** • **Сертификаттарды басқару** • **Оқу** • **Жазу**	• Кілттерді басқару қызметінің қалпына келтірілген деректерін алу: **Оқу** • Пайдаланушы сертификаттарын жою: **Сертификаттарды басқару** • Пайдаланушы сертификатының жария бөлігін алу: **Оқу** • Жалпыға ортақ кілттердің инфрақұрылымы қосулы ма екенін тексеру: **Оқу** • Жалпыға ортақ кілттердің инфрақұрылымының есептік жазбасын тексеру: **Оқу** • Жалпыға ортақ кілттер инфрақұрылымы үлгілерін алу: **Оқу** • Сертификат кілтін кеңейтілген қолдану (EKU) арқылы жалпыға ортақ кілттер инфрақұрылымы үлгілерін алу: **Оқу** • Жалпыға ортақ кілттер инфрақұрылымы сертификатының қайтарып алынбағанын тексеру: **Оқу** • Пайдаланушы сертификаттарын шығару параметрлерін жаңарту: **Сертификаттарды басқару** • Пайдаланушы сертификаттарын шығару параметрлерін алу: **Оқу** • Бағдарламалардың атауы және нұсқалары бойынша пакеттер алу: **Оқу** • Пайдаланушы сертификаттарын орнату немесе олардан бас тарту: **Сертификаттарды басқару** • Пайдаланушы сертификатын жаңарту: **Сертификаттарды басқару**	Жоқ	Жоқ	Жоқ

Функционалдық аймақ	Құқық	Пайдаланушының әрекеті: әрекетті орындауға қажетті құқық	Тапсырма	Есеп	Ба
		• Пайдаланушы сертификаты үшін тег белгілеу: **Сертификаттарды басқару** • iOS MDM профилін қамтитын орнату пакетін жасауды іске қосу; iOS MDM профилін қамтитын орнату пакетін жасаудан бас тарту: **Жаңа құрылғыларды қосу**			
Жүйені басқару: **Қосылымдар**	• **RDP сеанстарын бастау** • **Бұрыннан бар RDP сеанстарына қосылу** • **Туннельдеу** • **Құрылғылардағы файлдарды әкімшінің жұмыс үстелінде сақтау** • **Оқу** • **Жазу** • **Орындау** • **Құрылғы таңдаулары бойынша әрекеттерді орындау**	• Жұмыс үстеліне бірлесіп қатынасу сеансын жасау: **Жұмыс үстеліне бірлесіп қатынасу сеансын жасау құқығы** • RDP сеансын жасау: **Бұрыннан бар RDP сеанстарына қосылу** • Туннель жасау: **Туннельдеу** • Желілер тізімін сақтау: **Құрылғылардағы файлдарды әкімшінің жұмыс үстелінде сақтау**	Жоқ	"Құрылғы пайдаланушылары туралы есеп"	Жоқ
Жүйені басқару: **Осалдықтар мен патчтарды басқару**	• **Оқу** • **Жазу** • **Орындау** • **Құрылғы таңдаулары бойынша әрекеттерді орындау**	• Үшінші тарап патчтарының сипаттарын көру: **Оқу** • Үшінші тарап патчтарының сипаттарын өзгерту: **Жазу**	• "Осалдықтарды түзету" • "Қажетті жаңартуларды орнату және осалдықтарды түзету"	"Бағдарламалық жасақтаманың жаңартулары туралы есеп"	Жоқ
Жүйені басқару: **Скрипттерді қашықтан орындау**	• **Оқу** • **Жазу** • **Орындау** • **Құрылғы таңдаулары бойынша әрекеттерді орындау**	Пайдаланушы **Оқу** арқылы тапсырмасының сипаттарын көре алады Пайдаланушы **Жазу** арқылы орнату пакетін жасай, жоя немесе өзгерте алады. Пайдаланушы тапсырманы орындай алады: **Жазу**. Linux операциялық жүйесімен жұмыс істейтін клиенттік құрылғыларда скриптілер root құқықтарымен орындалады. Пайдаланушы **Іске қосу** арқылы тапсырманы іске қоса алады немесе оны іске қосу үшін жоспарлауы мүмкін	"Скрипттерді қашықтан орындау"	Жоқ	Жоқ

Функционалдық аймақ	Құқық	Пайдаланушының әрекеті: әрекетті орындауға қажетті құқық	Тапсырма	Есеп	Ба
		Пайдаланушы **Таңдалған құрылғыларда әрекеттерді орындау** арқылы таңдалған құрылғыларда тапсырманы іске қоса алады			

Алдын ала анықталған пайдаланушы рөлдері

Kaspersky Security Center Linux пайдаланушыларына тағайындалған пайдаланушы рөлдері оларға бағдарламаның функцияларын пайдалану құқықтарының жиынтығын береді.

Виртуалды серверде жасалған пайдаланушыларға басқару серверінде рөлдерді тағайындау мүмкін емес.

Конфигурацияланған құқықтар жинағы бар алдын ала анықталған пайдаланушы рөлдерін пайдалануға немесе жаңа рөлдер жасауға болады. Жаңа рөл жасаған кезде, рөл ауқымын өзіңіз орнатуыңыз және пайдалану құқықтарын Kaspersky Security Center Linux мүмкіндіктеріне тағайындауыңыз керек. Kaspersky Security Center Linux жүйесінде қолжетімді кейбір алдын ала анықталған пайдаланушы рөлдері, мысалы, **Аудитор**, **Қауіпсіздік маманы**, **Супервайзер** нақты лауазымдармен байланыстырылы мүмкін. Бұл рөлдерге қатынасу құқықтары тиісті лауазымдардың стандартты тапсырмалары мен міндеттеріне сәйкес алдын ала конфигурацияланады. Төмендегі кестеде рөлдердің белгілі бір лауазымдармен қалай байланысты болуы мүмкін екендігі көрсетілген.

Белгілі бір лауазымдарға арналған рөлдердің мысалдары

Рөл	Пікір
Аудитор	Басқару серверіне жергілікті әкімші құқықтары (Linux жүйесіне арналған түбір) бар желілік агент арқылы қосылған құрылғылар жинағында барлық көру операциясына және жасалған тапсырмаларды орындауға рұқсат береді. Бұл қызметтік міндеттерді орындау үшін осы рөлді пайдаланушылардың шектеулі жинағына мұқият тағайындауға кеңес береміз.
Супервайзер	Барлық операцияларды қарауға рұқсат етіледі, басқа операцияларға рұқсат етілмейді. Сіз бұл рөлді қауіпсіздік қызметінің офицеріне және ұйымыңыздағы IT қауіпсіздігіне жауап беретін басқа менеджерлерге тағайындай аласыз.
Қауіпсіздік қызметінің офицері	Барлық қарау операцияларына рұқсат етіледі, есептерді басқаруға рұқсат етіледі; **Жүйені басқару**: **Қосылым мүмкіндігі** аймағындағы шектулі құқықтар ұсынған. Сіз бұл рөлді ұйымыңыздағы IT қауіпсіздігіне жауапты қызметкерге тағайындай аласыз.

Төмендегі кестеде пайдаланушының әрбір алдын ала анықталған рөліне арналған құқықтар келтірілген.

Рөл	Сипаттамасы
Басқару серверінің әкімшісі	Келесі функционалдық аймақтардағы барлық операцияларға рұқсат береді: • **Жалпы функциялар**: • **Базалық функционалдылық** • **Шифрлау кілтін басқару** • **Оқиғаларды өңдеу** • **Басқару серверлерінің иерархиясы** • **Виртуалды Басқару серверлері** • **Жүйені басқару**: • **Қосылымдар** • **Жабдықты түгендеу** • **Бағдарламалық жасақтамаларды түгендеу**
Басқару серверінің операторы	Барлық келесі функционалдық аймақтарда **Оқу** және **Орындау** (қолданылса) құқықтарын ұсынады: • **Жалпы функциялар**: • **Базалық функционалдылық** • **Шифрлау кілтін басқару** • **Виртуалды Басқару серверлері** • **Жүйені басқару**: • **Қосылымдар** • **Жабдықты түгендеу** • **Бағдарламалық жасақтамаларды түгендеу**
Аудитор	Келесі функционалдық аймақтарда барлық операцияларға рұқсат береді: **Жалпы функционал**: • **ACL тізіміне қарамастан, нысандарға қатынасу** • **Жойылған нысандар** • **Есептерді басқару** Сіз бұл рөлді ұйымыңыздың аудитін жүргізетін қызметкерге тағайындай аласыз.
Бағдарламаларды орнату әкімшісі	Келесі функционалдық аймақтардағы барлық операцияларға рұқсат береді: • **Жалпы функциялар:** • **Базалық функционалдылық** • **Kaspersky қолданбасын орналастыру** • **Лицензиялық кілттерді басқару** • **Жүйені басқару:** • **Операциялық жүйені орналастыру** • **Осалдықтар мен патчтарды басқару** • **Қашықтан орнату** • **Бағдарламалық жасақтамаларды түгендеу** **Жалпы функционал: Виртуалды Басқару серверлері** аймағында **Оқу** және **Орындау** құқықтарын ұсынады.

Рөл	Сипаттамасы
Бағдарламаларды орнату операторы	Барлық келесі функционалдық аймақтарда **Оқу** және **Орындау** (қолданылса) құқықтарын ұсынады: • **Жалпы функциялар:** • **Базалық функционалдылық** • **Kaspersky қолданбасын орналастыру** (сондай-ақ осы аймақта **Kaspersky патчтарын басқару** құқығын береді) • **Виртуалды Басқару серверлері** • **Жүйені басқару:** • **Операциялық жүйені орналастыру** • **Осалдықтар мен патчтарды басқару** • **Қашықтан орнату** • **Бағдарламалық жасақтамаларды түгендеу**
Kaspersky Endpoint Security әкімшісі	Келесі функционалдық аймақтардағы барлық операцияларға рұқсат береді: • **Жалпы функционал: Базалық функционал** • **Жалпы функциялар: шифрлау кілттерін басқару** • Барлық функцияны қоса алғанда, **Kaspersky Endpoint Security** аймағы
Kaspersky Endpoint Security операторы	Барлық келесі функционалдық аймақтарда **Оқу** және **Орындау** (қолданылса) құқықтарын ұсынады: • **Жалпы функционал: Базалық функционал** • **Жалпы функциялар: шифрлау кілттерін басқару** • Барлық функцияны қоса алғанда, **Kaspersky Endpoint Security** аймағы
Бас әкімші	Келесі аймақтарды *қоспағанда*, функционалдық аймақтардағы барлық операцияларға рұқсат береді: **Жалпы функционал**: • **ACL тізіміне қарамастан, нысандарға қатынасу** • **Есептерді басқару**
Бас оператор	Барлық келесі функционалдық аймақтарда **Оқу** және **Орындау** (қолданылса) құқықтарын ұсынады: • **Жалпы функциялар**: • **Базалық функционалдылық** • **Жойылған нысандар** • **Шифрлау кілтін басқару** • **Басқару серверіне қатысты әрекеттер** • **Құрылғы тегтері** • **Kaspersky қолданбасын орналастыру** • **Бағдарламаларды біріктіру** • **Виртуалды Басқару серверлері** • Барлық функцияны қоса алғанда, **Мобильдік құрылғыларды басқару** аймағы • Барлық функцияны қосқанда, **Жүйені басқару** аймағы • Барлық функцияны қоса алғанда, **Kaspersky Endpoint Security** аймағы
Ұялы құрылғыларды басқару әкімшісі	Келесі функционалдық аймақтардағы барлық операцияларға рұқсат береді: • **Жалпы функционал: Базалық функционал** • Барлық функцияны қоса алғанда, **Мобильдік құрылғыларды басқару** аймағы **Жалпы функциялар: лицензия кілтін басқару** аймағында **Кілт файлын экспорттау** құқығын береді. **Жүйені басқару: осалдықтар мен патчтарды басқару** аймағында **Оқу** құқығын береді.
Ұялы құрылғыларды басқару операторы	**Жалпы функциялар: негізгі функционалдық** аймағында **Оқу** және **Орындау** құқықтарын береді. **Мобильдік құрылғыларды басқару** бөлімінде **Оқу** және **Мобильдік құрылғыларға ақпарат пәрмендерін ғана жіберу** құқықтарын береді: • **Жалпы** • **Self Service Portal**

Рөл	Сипаттамасы
Қауіпсіздік қызметінің офицері	Келесі функционалдық аймақтарда барлық операцияларға рұқсат береді: **Жалпы функционал**: • **ACL тізіміне қарамастан, нысандарға қатынасу** • **Есептерді басқару** **Жүйені басқару: қосылу мүмкіндігі** функционалдық аймағында келесі құқықтарды береді: **Оқу**, **Жазу**, **Орындау**, **Құрылғылардағы файлдарды әкімшінің жұмыс орнында сақтау** және **Құрылғылардың таңдауларында әрекеттерді орындау**. Сіз бұл рөлді ұйымыңыздағы IT қауіпсіздігіне жауапты қызметкерге тағайындай аласыз.
Self Service Portal пайдаланушысы	**Ұялы құрылғыларды басқару: Self Service Portal** аймағында барлық операцияларға рұқсат береді.
Супервайзер	**Жалпы функционал**: **ACL тізіміне қарамастан, нысандарға қатынасу** және **Жалпы функционал**: **Есептерді басқару** функционалдық аймағының аймағында **Оқу** құқықтарын ұсынады. Сіз бұл рөлді қауіпсіздік қызметінің офицеріне және ұйымыңыздағы IT қауіпсіздігіне жауап беретін басқа менеджерлерге тағайындай аласыз.
Осалдықтар мен патчтарды басқару әкімшісі	**Жалпы функциялар**: **негізгі функционалдық** және **Жүйені басқару** функционалды аймақтарында барлық операцияға рұқсат береді (**Скриптілерді қашықтан орындау** мүмкіндігін *қоспағанда* барлық мүмкіндік).
Осалдықтар мен патчтарды басқару операторы	**Жалпы функциялар**: **негізгі функционалдық** және **Жүйені басқару** функционалды аймақтарында **Оқу** және **Орындау** құқықтарын береді (**Скриптілерді қашықтан орындау** мүмкіндігін *қоспағанда* барлық мүмкіндік).

Нысандар жиынтығына қатынасу құқықтарын тағайындау

Сервер деңгейінде қатынасу құқықтарын тағайындауға қосымша ретінде, сіз нақты нысандарға, мысалы, қажетті тапсырмаға қатынасу мүмкіндігін тағайындай аласыз. Бағдарлама келесі нысан түрлеріне қатынасу құқықтарын көрсетуге мүмкіндік береді:

- Басқару топтары
- Тапсырмалар
- Есептер
- Құрылғыны таңдаулары
- Оқиғалар таңдау

Нақты нысанға қатынасу құқықтарын тағайындау үшін:

1. Нысанның түріне байланысты, басты мәзірде тиісті бөлімге өтіңіз:
   - **Активтерді басқару → Топтардың иерархиясы**.
   - **Тапсырмалар**
   - **Мониторинг → Есептер**.
   - **Активтерді басқару → Құрылғы таңдаулары**.
   - **Мониторинг → Оқиғаларды таңдау**.
2. Қатынасу құқықтарын тағайындағыңыз келетін нысанның сипаттарын ашыңыз.

   Басқару тобының немесе тапсырманың сипаттары терезесін ашу үшін, нысанның атауын басыңыз. Басқа нысандардың сипаттарын құралдар тақтасындағы түйменің көмегімен ашуға болады.

3. Сипаттар терезесінде **Қатынасу құқықтары** бөлімін ашыңыз.

   Пайдаланушылар тізімі ашылады. Атап көрсетілген пайдаланушылар мен қауіпсіздік топтарының нысанға қатынасу құқықтары бар. Басқару топтарының немесе Серверлердің иерархиясын қолданып жатсаыз, әдепкі бойынша тізім мен қатынасу құқықтары тектік басқару тобынан немесе басты Серверден иеленеді.

4. Тізімді өзгерту мүмкіндігіне ие болу үшін **Реттелетін рұқсаттарды пайдалану** параметрін қосыңыз.

5. Қатынасу құқықтарын конфигурациялаңыз:

   - Тізімді өзгерту үшін **Қосу** және **Жою** түймелерін қолданыңыз.
   - Пайдаланушы немесе басқару топтары үшін қатынасу құқықтарын көрсетіңіз. Келесі әрекеттердің бірін орындаңыз:
     - Егер сіз қатынасу құқықтарын қолмен көрсеткіңіз келсе, пайдаланушыны немесе қауіпсіздік тобын таңдап, **Қатынасу құқықтары** түймесін басып, қатынасу құқықтарын көрсетіңіз.
     - Пайдаланушыға немесе қауіпсіздік тобына пайдаланушы рөлін тағайындағыңыз келсе, пайдаланушыны немесе қауіпсіздік тобын таңдап, **Рөлдер** түймесін басыңыз және тағайындалатын рөлді таңдаңыз.

6. **Сақтау** түймесін басыңыз.

Нысанға қатынасу құқықтары конфигурацияланған.

Пайдаланушыларға немесе қауіпсіздік топтарына құқықтарды тағайындау

Басқару серверінің әртүрлі мүмкіндіктерін пайдалану үшін пайдаланушыларға немесе қауіпсіздік топтарына кіру құқықтарын тағайындауға болады, мысалы, Kaspersky Endpoint Security for Linux.

Пайдаланушыға немесе қауіпсіздік тобына құқықтарды тағайындау үшін:

1. Негізгі мәзірдегі басқару серверінің атауын басыңыз.

   Басқару серверінің сипаттары терезесі ашылады.

2. **Қатынасу құқықтары** қойындысында құқық тағайындағыңыз келетін пайдаланушы немесе қауіпсіздік тобы атының жанындағы жалаушаны белгілеп, **Қатынасу құқықтары** түймесін басыңыз.

   Бір уақытта бірнеше пайдаланушыны немесе қауіпсіздік тобын таңдау мүмкін емес. Бірнеше нысанды таңдасаңыз, **Қатынасу құқықтары** түймесі өшірулі болады.

3. Пайдаланушы немесе топ үшін құқықтар жинағын орнатыңыз:

   a. Түйінді Басқару сервер немесе басқа Kaspersky бағдарламасының функцияларымен кеңейтіңіз.

   b. Қажетті функцияның немесе қол жеткізу құқығының жанындағы **Рұқсат** немесе **Қабылдамау** жалаушасын белгілеңіз.

      1-мысал: пайдаланушыға немесе топқа бағдарламаны біріктіру функциясына (**Оқу**, **Жазу** және **Орындау**) барлық қолжетімді қол жеткізу құқықтарын беру үшін **Бағдарлама интеграциялары** түйінінің жанындағы **Рұқсат ету** жалаушасын белгілеңіз.

2-мысал. **Шифрлау кілттерін басқару** түйінін кеңейтіңіз және пайдаланушыға немесе топқа шифрлау кілттерін басқару функциясына **жазу** құқығын беру үшін **Жазу** рұқсатының жанындағы **Рұқсат ету** жалаушасын белгілеңіз.

4. Қол жеткізу құқықтарының жинағын орнатқаннан кейін **OK** түймесін басыңыз.

Пайдаланушы немесе пайдаланушылар тобы үшін құқықтар жиынтығы конфигурацияланған.

Басқару серверінің (немесе басқару тобының) құқықтары келесі аймақтарға бөлінеді:

- Жалпы функционал:
  - Басқару топтарын басқару
  - ACL тізіміне қарамастан, нысандарға қатынасу
  - Базалық функционалдылық
  - Жойылған нысандар
  - Шифрлау кілтін басқару
  - Оқиғаларды өңдеу
  - Басқару серверіне қатысты әрекеттер (тек Басқару сервері сипаттары терезесінде)
  - Құрылғы тегтері
  - Kaspersky бағдарламасын орналастыру
  - Лицензиялық кілттерді басқару
  - Бағдарламаны біріктіру
  - Есеп файлын мәжбүрлеп басқару
  - Басқару серверлерінің иерархиясы
  - Пайдаланушы рұқсаттары
  - Виртуалды Басқару серверлері
- Мобильді құрылғыларды басқару:
  - Жалпы
  - Self Service Portal
- Жүйені басқару:
  - Қосылым мүмкіндігі
  - Скрипттерді қашықтан орындау
  - Жабдықты түгендеу

- Желіге қол жеткізуді басқару
- ОЖ орналастыру
- Осалдықтар мен патчтарды басқару
- Қашықтан орнату
- Бағдарламалық жасақтамаларды түгендеу

Құқық үшін не **Рұқсат**, не **Қабылдамау** таңдалмаса, ол *анықталмаған* болып саналады: құқық пайдаланушы үшін айқын түрде қабылданбайынша немесе рұқсат етілмейінше қабылданбайды.

Пайдаланушылардың құқықтары келесінің жиынтығы болып саналады:

- Пайдаланушының өзіндік құқықтары
- Пайдаланушыға тағайындалған барлық рөлдердің құқықтары
- Пайдаланушы кіретін барлық қауіпсіздік топтарының құқықтары
- Пайдаланушы кіретін топтарға тағайындалған барлық рөлдердің құқықтары

Ең болмаса бір құқықтар жиынтығында тыйым салынған құқық болса (құқық үшін **Қабылдамау** жалаушасы қойылған), онда бұл құқық басқа құқықтар жиынтығында рұқсат етілген немесе анықталмаған болса да, пайдаланушы үшін тыйым салынған болып саналады.

Сондай-ақ, Басқару серверінің әртүрлі мүмкіндіктерін пайдалану үшін пайдаланушы рөлі аймағына пайдаланушылар мен қауіпсіздік топтарын қосуға болады. Пайдаланушы рөліне қатысты параметрлер тек осы рөл тағайындалған пайдаланушыларға тиесілі құрылғыларға қолданылады және бұл құрылғылар осы рөл тағайындалған топтарға, соның ішінде еншілес топтарға жататын болса ғана қолданылады.

Ішкі пайдаланушының есептік жазбасын қосу

Пайдаланушының есептік жазбасын қосқыңыз келсе, есептік жазбаңызда "Жалпы функционал: Пайдаланушылардың құқықтары" функционалдық аймағында Нысандарға қол жеткізуді басқару тізімдерін өзгерту құқығы бар екенін тексеріңіз.

Kaspersky Security Center Linux жаңа пайдаланушы есептік жазбасын қосу үшін:

1. Қолданбаның негізгі терезесінде **Пайдаланушылар және рөлдер** → **Пайдаланушылар және топтар** бөліміне өтіп, **Пайдаланушылар** қойындысын таңдаңыз.
2. **Қосу** түймесін басыңыз.
3. Ашылған **Пайдаланушыны қосу** терезесінде жаңа пайдаланушы параметрлерін көрсетіңіз:
   - **Атауы**.
   - **Құпиясөз** пайдаланушыны Kaspersky Security Center Linux-ке қосу үшін.

Құпиясөз келесі ережелерге сәйкес келуі керек:

- Құпиясөздің ұзындығы 8-ден 256 таңбаға дейін болуы керек.
- Құпиясөзде төмендегі тізімдегі кемінде үш топтың таңбалары болуы керек:
  - Бас әріптер (A-Z)
  - Кіші әріптер (a-z)
  - Сандар (0-9)
  - Арнайы таңбалар (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)
- Құпиясөзде бос орындар, Юникод таңбалары немесе "." таңбасы "@" алдында тұрған кезде "." және "@" тіркесімі болмауы тиіс.

Енгізілген құпиясөзді көру үшін түймесін басыңыз.

Пайдаланушының бірінші аутентификациясында құпиясөзді өзгертуге мәжбүрлеу үшін **Пайдаланушы бірінші кірген кезде құпиясөзді өзгертуі керек** параметрін қосуға болады.

4. Пайдаланушы есептік жазбасын жасауды аяқтау үшін өзгерістерді сақтаңыз.

Пайдаланушының есептік жазбасы пайдаланушылар тізіміне қосылды.

Kaspersky Security Center Web Console веб-консолінде жасалған ішкі пайдаланушы есептік жазбасымен кіру үшін есептік жазбаға рөл тағайындауыңыз керек. Кірмес бұрын, ішкі пайдаланушы есептік жазбасында рөл бар екеніне көз жеткізіңіз. Әйтпесе, кіру қатесі орын алады.

Пайдаланушылар тобын жасау

Қауіпсіздік тобын жасау үшін:

1. Қолданбаның негізгі терезесінде **Пайдаланушылар және рөлдер** → **Пайдаланушылар және топтар** бөліміне өтіп, **Топтар** қойындысын таңдаңыз.
2. **Қосу** түймесін басыңыз.
3. Ашылатын **Қауіпсіздік тобын жасау** терезесінде жаңа қауіпсіздік тобы үшін келесі параметрлерді көрсетіңіз:
   - **Топ атауы**
   - **Сипаттама**
4. Өзгерістерін сақтау үшін **Сақтау** түймесін басыңыз.

Қауіпсіздік тобы топтар тізіміне қосылды.

Ішкі пайдаланушының есептік жазбасын өзгерту

Пайдаланушының есептік жазбасын өзгерткіңіз келсе, есептік жазбаңызда "Жалпы функционал: Пайдаланушылардың құқықтары" функционалдық аймағында Нысандарға қол жеткізуді басқару тізімдерін өзгерту құқығы бар екенін тексеріңіз.

Kaspersky Security Center Linux ішкі пайдаланушы есептік жазбасын өзгерту үшін:

1. Қолданбаның негізгі терезесінде **Пайдаланушылар және рөлдер** → **Пайдаланушылар және топтар** бөліміне өтіп, **Пайдаланушылар** қойындысын таңдаңыз.
2. Өзгерту қажет болған реттелетін есептік жазбасын таңдаңыз.
3. Ашылған терезедегі **Жалпы** қойыншасында пайдаланушы есептік жазбасының параметрлерін өзгертіңіз:
   - **Пайдаланушы есептік жазбасы**

     Қажет болса, пайдаланушының бағдарламаға қосылуына тыйым салу үшін қосқышты **Белсенді емес** күйіне ауыстырыңыз. Мысалы, қызметкер компаниядан жұмыстан шыққаннан кейін, есептік жазбаны өшіруге болады.
   - Сипаттама
   - **Толық атауы**
   - **Электрондық пошта мекенжайы**
   - **Негізгі телефон нөмірі**
   - **Құпиясөз**

     Қажет болса, пайдаланушыны Kaspersky Security Center Linux орталығына қосу үшін келесі әдіспен жаңа құпиясөз орнатуға болады:

     a. **Құпиясөзді өзгерту** түймесін басып, пайдаланушы есептік жазбасы үшін жаңа құпиясөз орнатыңыз.

     Құпиясөз келесі ережелерге сәйкес келуі керек:

     - Құпиясөздің ұзындығы 8-ден 256 таңбаға дейін болуы керек.
     - Құпиясөзде төмендегі тізімдегі кемінде үш топтың таңбалары болуы керек:
       - Бас әріптер (A-Z)
       - Кіші әріптер (a-z)
       - Сандар (0-9)
       - Арнайы таңбалар (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)
     - Құпиясөзде бос орындар, Юникод таңбалары немесе "." таңбасы "@" алдында тұрған кезде "." және "@" тіркесімі болмауы тиіс.

Енгізілген құпиясөзді көру үшін түймесін басыңыз.

b. Қажет болса, пайдаланушының келесі аутентификациясында құпиясөзді өзгертуге мәжбүрлеу үшін **Пайдаланушы бірінші кірген кезде құпиясөзді өзгертуі керек** параметрін қосыңыз.

c. Егер пайдаланушы есептік жазбасы рұқсатсыз өзгертуден қорғалған болса, осы есептік жазбаны өзгертуге рұқсатыңыз бар екенін растауыңыз қажет. **Есептік жазба қорғанысы** терезесінде "Жалпы функционал: Пайдаланушылар құқықтары" функционалдық аймағында Нысандарға қол жеткізуді басқару тізімдерін өзгерту құқығы бар есептік жазба деректерін көрсетіңіз.

4. **Екі факторлы аутентификация** қойыншасында осы есептік жазбаға арналған қауіпсіздік параметрлерін көрсете аласыз.

5. **Топтар** қойыншасында пайдаланушыны немесе қауіпсіздік тобын қосуға болады.

6. **Құрылғылар** қойыншасында пайдаланушыға құрылғыларды тағайындауға болады.

7. **Рөлдер** қойыншасында пайдаланушыға рөлді тағайындауға болады.

8. Пайдаланушы есептік жазбасын өзгертуді аяқтау үшін өзгерістерді сақтаңыз.

Өзгертілген пайдаланушы есептік жазбасы пайдаланушылар тізімінде көрсетіледі.

Пайдаланушылар тобын өзгерту

Қауіпсіздік тобын өзгерту үшін:

1. Қолданбаның негізгі терезесінде **Пайдаланушылар және рөлдер** → **Пайдаланушылар және топтар** бөліміне өтіп, **Топтар** қойындысын таңдаңыз.

2. Өзгерту қажет қауіпсіздік тобын таңдаңыз.

3. Ашылған терезеде қауіпсіздік тобының параметрлерін өзгертіңіз:

   - **Жалпы** қойындысында **Атауы** және **Сипаттама** параметрлерін өзгертуге болады. Бұл параметрлер тек ішкі қауіпсіздік топтары үшін қолжетімді.
   - **Пайдаланушылар** қойындысында пайдаланушыларды қауіпсіздік тобына қосуға болады. Бұл параметрлер тек ішкі пайдаланушыларға және ішкі қауіпсіздік топтарына қолжетімді.
   - **Рөлдер** қойындысында қауіпсіздік тобына рөл тағайындай аласыз.

4. Өзгерістерін сақтау үшін **Сақтау** түймесін басыңыз.

Өзгерістер қауіпсіздік тобына қолданылды.

Пайдаланушыға немесе қауіпсіздік тобына рөл тағайындау

Пайдаланушыға немесе қауіпсіздік тобына рөл тағайындау үшін:

1. Қолданбаның негізгі терезесінде **Пайдаланушылар және рөлдер** → **Пайдаланушылар және топтар** бөліміне өтіп, **Пайдаланушылар** немесе **Топтар** қойындысын таңдаңыз.
2. Рөл тағайындағыңыз келетін пайдаланушының немесе қауіпсіздік тобының атын таңдаңыз.

   Бірнеше ат таңдауға болады.
3. Мәзірде **Рөлді тағайындау** түймесін басыңыз.

   Рөлді тағайындау шебері іске қосылады.
4. Шебер нұсқауларын орындаңыз: таңдалған пайдаланушыларға немесе қауіпсіздік топтарына тағайындағыңыз келетін рөлді таңдаңыз және рөлдің әрекет ету ауқымын таңдаңыз.

   Пайдаланушы рөлі ауқымы – бұл пайдаланушылар мен басқару топтарының тіркесімі. Пайдаланушы рөліне қатысты параметрлер тек осы рөл тағайындалған пайдаланушыларға тиесілі құрылғыларға қолданылады және бұл құрылғылар осы рөл тағайындалған топтарға, соның ішінде еншілес топтарға жататын болса ғана қолданылады.

Нәтижесінде Басқару сервермен жұмыс істеу құқықтарының жиынтығы бар рөл пайдаланушыға (немесе пайдаланушылар тобына не қауіпсіздік тобына) тағайындалады. Пайдаланушылар немесе қауіпсіздік топтарының тізімінде **Тағайындалған рөлдері бар** бағанында жалауша көрсетіледі.

Пайдаланушылардың есептік жазбаларын ішкі қауіпсіздік топқа қосу

Ішкі пайдаланушылар есептік жазбаларын тек ішкі қауіпсіздік тобына қосуға болады.

Пайдаланушылардың есептік жазбаларын қауіпсіздік тобына қосу үшін:

1. Бағдарламаның негізгі терезесінде **Пайдаланушылар және рөлдер** → **Пайдаланушылар және топтар** бөліміне өтіп, **Пайдаланушылар** қойындысын таңдаңыз.
2. Қауіпсіздік тобына қосқыңыз келетін пайдаланушылардың есептік жазбаларына қарама-қарсы жалаушаларды белгілеңіз.
3. **Топты тағайындау** түймесін басыңыз.
4. **Топты тағайындау** ашылған терезесінде пайдаланушылардың есептік жазбаларын қосу қажет қауіпсіздік тобын таңдаңыз.
5. **Сақтау** түймесін басыңыз.

Пайдаланушылардың есептік жазбалары қауіпсіздік тобына қосылған. Ішкі пайдаланушыларды қауіпсіздік тобына топ параметрлері арқылы да қосуға болады.

Пайдаланушыны құрылғының иесі етіп тағайындау

Пайдаланушыны мобильдік құрылғының иесі етіп тағайындау туралы ақпаратты Kaspersky Secure Mobility Management анықтамасынан қараңыз.

Пайдаланушыны ұялы құрылғының иесі етіп тағайындау үшін:

1. Егер сіз виртуалды Басқару серверіне қосылған құрылғының иесін тағайындағыңыз келсе, алдымен виртуалды Басқару серверіне ауысыңыз:

   a. Басты мәзірде, Басқару серверінің ағымдағы атауының оң жағындағы шеврон (›) белгішесін басыңыз.

   b. Қажетті Басқару серверін таңдаңыз.

2. Бағдарламаның негізгі терезесінде **Пайдаланушылар және рөлдер** → **Пайдаланушылар және топтар** бөліміне өтіп, **Пайдаланушылар** қойындысын таңдаңыз.

   Пайдаланушылар тізімі ашылады. Егер сіз қазір виртуалды Басқару серверіне қосылған болсаңыз, тізімге ағымдағы виртуалды Басқару сервері мен негізгі Басқару серверінің пайдаланушылары кіреді.

3. Құрылғының иесі ретінде тағайындалуы қажет пайдаланушы есептік жазбасын түртіңіз.

4. Ашылған пайдаланушы сипаттары терезесінде **Құрылғылар** қойыншасын таңдаңыз.

5. **Қосу** түймесін басыңыз.

6. Құрылғылар тізімінен пайдаланушыға тағайындағыңыз келетін құрылғыны таңдаңыз.

7. **ОК** түймесін басыңыз.

Таңдалған құрылғы пайдаланушыға тағайындалған құрылғылар тізіміне қосылады.

Сондай-ақ, тағайындағыңыз келетін құрылғы атауын таңдау және **Құрылғы иесін басқару** сілтемесінен өту арқылы, бұл операцияны **Активтерді басқару** → **Активтер (құрылғылар)** тобында орындауға болады.

Желілік агентті орнату кезінде пайдаланушыны құрылғы иесі ретінде тағайындау

Орнату пакетін пайдаланып Желілік агентті орнату кезінде пайдаланушыны құрылғы иесі ретінде тағайындау үшін төмендегі кестеде тізімделген айнымалы мәндерді Желілік агенттің орнату пакетінің параметрлеріне қосыңыз.

Айнымалының атауы	Міндетті	Сипаттамасы	Ықтимал мәндер
KLNAGENT_DEVICEOWNER_REGISTRATION_START	Жоқ	Желілік агентті орнатқаннан кейін пайдаланушыны құрылғы иесі ретінде тіркеу үшін утилитаны іске қосуға мүмкіндік береді. Өшірілген болса, құрылғы иесі ретінде тіркелу пайдаланушыға қолжетімді емес.	1 – пайдаланушыны құрылғы иесі ретінде тіркеуге арналған утилита Желілік агентті орнатқаннан кейін іске қосылады. Басқа – утилита қолжетімді емес.
KLNAGENT_DEVICEOWNER_LOGIN	Жоқ Иә, құпиясөзді енгізсеңіз	Құрамында құрылғы иесі ретінде тіркелетін пайдаланушы есептік жазбасы бар.	Kaspersky Security Center Linux жүйесіндегі пайдаланушылар тізімінде тізімделген пайдаланушы есептік жазбасы.
KLNAGENT_DEVICEOWNER_PASSWORD	Жоқ Иә, егер сіз есептік жазбаны енгізсеңіз	Құрылғының иесі ретінде тіркелетін пайдаланушының шифрланған құпиясөзін қамтиды.	Пайдаланушы құпиясөзі.

Желілік агент Kaspersky Security Center Linux орнату кезінде көрсетілген есептік жазба мен құпиясөздің шифрын шешеді және пайдаланушы құрылғының иесі ретінде тіркеледі.

Сондай-ақ, Желілік агентті жауап файлымен тыныш режимде орнатқан кезде пайдаланушыны құрылғы иесі ретінде тағайындауға болады.

Жауап файлымен тыныш режимде Желілік агентті орнату кезінде пайдаланушыны құрылғы иесі ретінде тағайындау үшін:

1. Жауап файлына KLNAGENT_DEVICEOWNER_REGISTRATION_START параметрін қосыңыз және оның мәнін 1-ге орнатыңыз.

   Пайдаланушыны құрылғы иесі ретінде тіркеуге арналған утилита Желілік агентті орнатқаннан кейін іске қосылады.

2. Клиент құрылғысындағы пәрмен желісінде есептік жазба мен құпиясөзді енгізіңіз.

   Пайдаланушы құрылғы иесі ретінде тағайындалған.

Пайдаланушы ішкі қауіпсіздік тобының мүшесі болса, есептік жазбада пайдаланушы аты болуы керек.

Пайдаланушы Active Directory қауіпсіздік тобының мүшесі болса, есептік жазбада пайдаланушы аты мен домен атауы болуы керек.

Екі факторлы аутентификация үшін қолданбадан уақытқа негізделген бір реттік құпия сөзді (TOTP) енгізу керек.

Желілік агентті орнатқаннан кейін пайдаланушыны Linux құрылғысының иесі ретінде тағайындау

Пайдаланушыға Linux құрылғысының иесі ретінде тіркелуге рұқсат беру үшін:

1. Kaspersky Security Center Web Console веб-консолінде **Бағдарламалық жасақтаманы басқару → Орнату пакеттері** бөліміне өтіңіз.

   Орнату пакеттерінің тізімі ашылады.

2. Желілік агенттің орнату пакетін басыңыз.

   Орнату пакеті сипаттары терезесі көрсетіледі.

3. Ашылатын орнату пакетінің сипаттары терезесінде **Параметрлер** → **Кеңейтілген** қойындысына өтіңіз.

4. **Пайдаланушыны құрылғы иесі ретінде тіркеу (тек Linux)** бөлімінде **Желілік агентті орнатқаннан кейін пайдаланушыны тіркеу утилитасын іске қосуға рұқсат беру** параметрін қосып, **Сақтау** түймесін басыңыз.

Пайдаланушыны құрылғы иесі ретінде тіркеуге арналған утилитаны клиент құрылғысындағы пәрмен желісінен іске қосуға болады.

Пайдаланушыны клиент құрылғысында Linux құрылғысының иесі ретінде тіркеу үшін:

1. Клиент құрылғысындағы пәрмен желісінде келесі пәрменді іске қосыңыз:
   ```
   $ /opt/kaspersky/klnagent64/bin/nagregister -set_owner
   ```

2. Сұралған жағдайда, есептік жазба мен құпиясөзді енгізіңіз.

   Есептік жазба мен құпиясөз жауап файлында немесе Желілік агенттің орнату пакетінде болса, клиент құрылғысындағы пәрмен жолында келесі пәрменді іске қосыңыз:
   ```
   $ /opt/kaspersky/klnagent64/bin/nagregister -set_owner -unattended
   ```

Пайдаланушы ішкі қауіпсіздік тобының мүшесі болса, есептік жазбада пайдаланушы аты болуы керек.

Пайдаланушы Active Directory қауіпсіздік тобының мүшесі болса, есептік жазбада пайдаланушы аты мен домен атауы болуы керек.

Екі факторлы аутентификация үшін қолданбадан уақытқа негізделген бір реттік құпия сөзді (TOTP) енгізу керек.

Пайдаланушы құрылғы иесі ретінде тіркеледі.

Пайдаланушыны құрылғының иесі етіп тағайындаудың күшін жою

Пайдаланушыны клиент құрылғысында құрылғы иесі ретінде тағайындаудан шығару үшін:

1. Клиент құрылғысындағы пәрмен желісінде келесі пәрменді орындаңыз:
   ```
   $ /opt/kaspersky/klnagent64/bin/nagregister -remove_owner
   ```

2. Пайдаланушының аты мен құпиясөзін енгізіңіз.

Пайдаланушы ішкі қауіпсіздік тобының мүшесі болса, есептік жазбада пайдаланушы аты болуы керек.

Пайдаланушы Active Directory қауіпсіздік тобының мүшесі болса, есептік жазбада пайдаланушы аты мен домен атауы болуы керек.

Екі факторлы аутентификация үшін қолданбадан уақытқа негізделген бір реттік құпия сөзді (TOTP) енгізу керек.

Пайдаланушыны құрылғының иесі етіп тағайындаудың күші жойылды.

Есептік жазбаны рұқсатсыз өзгертуден қорғауды қосу

Сондай-ақ, сіз пайдаланушының есептік жазбасын рұқсатсыз өзгертуден қорғауды да қоса аласыз. Бұл параметр қосулы болса, пайдаланушының есептік жазбасының параметрлерін өзгерту үшін, өзгерту құқықтары бар пайдаланушы авторизациядан өтуі қажет.

Есептік жазбаны рұқсатсыз өзгертуден қорғауды қосу немесе өшіру үшін:

1. Бағдарламаның негізгі терезесінде **Пайдаланушылар және рөлдер → Пайдаланушылар және топтар** бөліміне өтіп, **Пайдаланушылар** қойындысын таңдаңыз.

2. Есептік жазбаны рұқсатсыз өзгертуден қорғауды конфигурациялағыңыз келетін ішкі пайдаланушы есептік жазбасын басыңыз.

3. Ашылған пайдаланушы сипаттары терезесінде **Екі факторлы аутентификация** қойыншасын таңдаңыз.

4. Есептік жазба параметрлерін өзгерткен кезде есептік деректерді әрбір рет сұрағыңыз келсе, **Екі факторлы аутентификация** қойыншасында **Пайдаланушының есептік жазбаларын өзгерту рұқсатын тексеру үшін аутентификацияны сұраңыз** параметрін және екі факторлы аутентификация үшін бір реттік қауіпсіздік кодын таңдаңыз. Не болмаса **Пайдаланушыларға осы есептік жазбаны қосымша аутентификациясыз өзгертуге рұқсат беріңіз** нұсқасын таңдаңыз.

5. Өзгерістерді сақтаңыз.

Екі факторлы аутентификацияны конфигурациялау

Басқару серверінің 16.1 нұсқасынан бастап, екі факторлы аутентификация автоматты түрде қосылады. Екі факторлы аутентификацияны өшірудің жаһандық опциясына қолдау көрсетілмейді. Бұл сценарий бірінші кіру кезінде екі сатылы аутентификацияны конфигурациялау және Басқару серверінде екі факторлы аутентификация параметрлерін конфигурациялау қадамдарын ұсынады.

Кезеңдер

Екі факторлы аутентификацияны конфигурациялау кезең-кезеңмен жүзеге асырылады:

1. **Құрылғыда аутентификация қолданбасы орнатылуда**

   Уақытқа негізделген бір реттік құпиясөз (TOTP) алгоритмін қолдайтын кез келген түпнұсқалықты тексеру қолданбасын орнатуға болады.

   Ресейде қолжетімді:

   - Kaspersky Password Manager for Business (ұсынылады)
   - Bitrix24 OTP
   - Яндекс ID

- Avanpost Authenticator
- Aladdin 2FA
- Rutoken OTP

Дүние жүзінде қолжетімді (Ресейді қоса алғанда):

- Google Authenticator
- Microsoft Authenticator

Kaspersky Security Center Linux өзіңіз пайдаланғыңыз келетін аутентификация қолданбасын қолдайтынын тексеру үшін, барлық пайдаланушылар немесе белгілі бір пайдаланушы үшін екі факторлы аутентификацияны қосыңыз.

Қадамдардың бірі аутентификация қолданбасы жасаған қауіпсіздік кодын беруді болжайды. Бәрі сәтті болса, Kaspersky Security Center Linux таңдалған түпнұсқалықты тексеру қолданбасын қолдайды.

> Басқару серверіне қосылатын сол құрылғыда аутентификация қолданбасын орнату мүлдем ұсынылмайды.

2. **Құрылғыдағы уақытты "authenticator" қолданбасымен Басқару сервері орнатылған құрылғының уақытымен синхрондау**

   Аутентификация қолданбасы бар құрылғыдағы уақыт пен Басқару сервері бар құрылғыдағы уақыт UTC-пен синхрондалғанына көз жеткізіңіз. Дәлдікті арттыру үшін бүкіл инфрақұрылымыңызда бірдей NTP серверлерін пайдалануды ұсынамыз. Әйтпесе, екі факторлы аутентификацияны конфигурациялау кезінде қателер орын алуы мүмкін.

3. **Web Console веб-консоліне кіру кезінде пайдаланушы есептік жазбалары үшін екі факторлы аутентификацияны конфигурациялау**

   Web Console веб-консоліне кіру және екі факторлы аутентификацияны конфигурациялау.

   Егер екі факторлы аутентификация конфигурациясы сізге қолжетімді болмаса, Жалпы функционалдық: Пайдаланушы рұқсаттары функционалдық аймағының **нысан ACL өзгерту** құқығы бар және есептік жазбаңызды екі факторлы аутентификацияға рұқсат тізіміне қосу үшін екі факторлы аутентификацияны конфигурациялаған пайдаланушыға контакт жасаңыз.

4. **Басқару серверінде екі факторлы аутентификация параметрлерін конфигурациялау**

   Егер сіз екі факторлы аутентификацияны және **Жалпы функционал**: **Пайдаланушы рұқсаттары** функционалдық аймағының оң жағындағы Нысанның ACL мәндерін өзгертуді конфигурациялаған болсаңыз, Басқару серверінде екі факторлы аутентификация параметрлерін келесідей конфигурациялай аласыз:

   1. Жүйеге кіру кезінде екі сатылы аутентификацияны конфигурациялай алатын пайдаланушылар тізімін қарап шығу:

      - Басқару сервері 16.1 нұсқасын нөлден орнату үшін: Қажетті пайдаланушыларды екі факторлы аутентификацияға рұқсат тізіміне қосыңыз, бұл оларға алғашқы кіру кезінде екі факторлы аутентификацияны конфигурациялауға мүмкіндік береді.
      - Басқару сервері 16.1 нұсқасын жаңарту немесе қалпына келтіру үшін: Екі факторлы аутентификация рұқсаттарының тізімін қарап шығыңыз және Басқару серверіне кіру мүмкіндігі болмауы керек тіркелгілерді жойыңыз.

2. екі факторлы аутентификацияны қосуды қажет етпейтін пайдаланушы есептік жазбаларын алып тастау

   Қажет болса, екі факторлы аутентификацияны конфигурацияламаған болса да, пайдаланушы есептік жазбаларын екі қадамдық тексеруден шығарыңыз, бұл оларға Басқару серверіне кіруге мүмкіндік береді. Екі факторлы аутентификациядан есептік жазбаларды шығару аутентификация кезінде қауіпсіздік кодын бере алмайтын интеграция есептік жазбалары үшін қажет болуы мүмкін. Интеграция есептік жазбалары OpenAPI арқылы сценарийлерді іске қосу үшін пайдаланылады.

3. Екі факторлы аутентификация құпия кілтін қалпына келтіру немесе жою (міндетті емес)

   Пайдаланушы екі факторлы аутентификация құрылғысына кіру мүмкіндігін жоғалтқанда немесе жаңа құрылғыда екі факторлы аутентификацияны орнату қажет болғанда екі факторлы аутентификация құпия кілтін қалпына келтіруге болады. Сондай-ақ, өз есептік жазбаңыз үшін құпия кілтті қалпына келтіруге болады.

   Пайдаланушының Web Console веб-консоліне кіруіне толығымен тыйым салу және пайдаланушының Басқару серверіне кіруіне жол бермеу үшін құпия кілтті жоюға болады.

4. Қауіпсіздік кодын шығарушының атын өзгерту (міндетті емес)

   Аттары ұқсас бірнеше Басқару серверіңіз болса, бәлкім, әртүрлі серверлерді оңайырақ ажырату үшін қауіпсіздік коды эмитенттерінің атауларын өзгертуіңіз қажет болуы мүмкін.

Нәтижелер

Бұл сценарийді орындағаннан кейін:

- Екі факторлы аутентификация сіздің жеке пайдаланушы есептік жазбаңыз үшін және Басқару серверіне кіруі қажет басқа пайдаланушы есептік жазбасы үшін конфигурацияланған.
- Тұтастық есептік жазбалары екі факторлы аутентификациядан шығарылады.

Есептік жазбаның екі факторлы аутентификациясы туралы

Kaspersky Security Center Linux бағдарламасы Kaspersky Security Center Web Console пайдаланушылары туралы екі факторлы аутентификацины ұсынады. Екі факторлы аутентификация RFC 6238 стандартына негізделген (TOTP: Уақытқа негізделген бір реттік құпиясөз алгоритмі).

Kaspersky Security Center Web Console веб-консоліне кірген сайын пайдаланушы атыңызды, құпиясөзіңізді және қосымша бір реттік қауіпсіздік кодын енгізесіз. Бір реттік қауіпсіздік кодын алу үшін, сіз өзіңіздің компьютерге немесе ұялы құрылғыға аутентификация қолданбасын орнатуыңыз керек.

Уақытқа негізделген бір реттік құпиясөз алгоритмін (TOTP) қолдайтын кез келген аутентификация бағдарламалық жасақтамасын "authenticator" қолданбасы (мысалы, Google Authenticator) ретінде пайдалануға болады. Бір реттік қауіпсіздік кодын жасау үшін құрылғыда орнатылған уақытты аутентификация қолданбасымен Басқару сервері құрылғысында орнатылған уақытпен синхрондау керек. Дәлдікті арттыру үшін бүкіл инфрақұрылымыңызда бірдей NTP серверлерін пайдалануды ұсынамыз.

Kaspersky Security Center Linux пайдаланғыңыз келетін аутентификация қолданбасын қолдайтынын тексеру үшін осы аутентификация қолданбасымен екі факторлы аутентификацияны конфигурациялап көріңіз.

Қадамдардың бірі аутентификация қолданбасы жасаған бір реттік қауіпсіздік кодын беруді болжайды. Бәрі сәтті болса, Kaspersky Security Center Linux таңдалған түпнұсқалықты тексеру қолданбасын қолдайды.

Аутентификация қолданбасын пайдаланып құпия кодты жасау

Аутентификация қолданбасы құпия кодты келесідей жасайды:

1. Басқару сервері арнайы құпия кілт пен QR кодын жасайды.

2. Сіз жасалған құпия кілтті немесе QR кодын аутентификация бағдарламасына жібересіз.

3. Аутентификация қолданбасы Басқару серверінің түпнұсқалық растама терезесіне жіберетін бір реттік қауіпсіздік кодын жасайды.

Қауіпсіздік кодында *шығарушы аты* деп те аталатын идентификатор бар. Қауіпсіздік кодын шығарушының аты аутентификация қолданбасында Басқару сервері идентификаторы ретінде пайдаланылады. Қауіпсіздік кодын шығарушының атын өзгерте аласыз. Қауіпсіздік кодын шығарушының аты Басқару серверінің атауы сияқты әдепкі бойынша мәнге ие. Келесі кіруден кейін Басқару серверіне жаңа қауіпсіздік коды эмитентінің атауы тағайындалады. Қауіпсіздік коды бір реттік болып табылады және 30 секундқа дейін жарамды (нақты уақыты әртүрлі болуы мүмкін).

Құпия кілтті (немесе QR кодын) сақтап қою және оны қауіпсіз жерде сақтау қатаң ұсынылады. Бұл аутентификация қолданбасы орнатылған құрылғыға қол жеткізе алмай қалған жағдайда, Kaspersky Security Center Web Console веб-консоліне кіру мүмкіндігін қалпына келтіруге көмектеседі.

Екі факторлы аутентификацияның келесі мүмкіндіктері бар:

- Басқару серверінің 16.1 нұсқасынан бастап, екі факторлы аутентификация автоматты түрде қосылады және кіру кезінде екі факторлы аутентификацияны конфигурациялау опциясы әдепкі бойынша өшірілген. Кіру кезінде екі факторлы аутентификацияны конфигурациялау тек екі факторлы аутентификацияға рұқсат тізіміне енгізілген пайдаланушылар үшін қолжетімді.

- Пайдаланушы екі факторлы аутентификацияны тек өзінің есептік жазбасы үшін ғана конфигурациялай алады.

- Пайдаланушы екі факторлы аутентификациядан аккаунттарды шығара алады. Бұл аутентификация үшін бір реттік қауіпсіздік кодын ала алмайтын интеграция аккаунттары үшін қажет болуы мүмкін. Интеграция есептік жазбалары OpenAPI арқылы сценарийлерді іске қосу үшін пайдаланылады.

- Екі факторлы аутентификация құпия кілтін қайта жасау үшін пайдаланушы өз аккаунтының құпия кілтін қалпына келтіруі керек.

- Басқа пайдаланушының аккаунты үшін екі факторлы аутентификация құпия кілтін қалпына келтіру немесе жою үшін пайдаланушыда екі факторлы аутентификация конфигурацияланған және **Жалпы функционал**: **Пайдаланушы рұқсаттары** функционалдық аймағында Нысан ACL-ін өзгерту бар аккаунт болуы керек.

- Басқа пайдаланушылардың аккаунттарын екі факторлы аутентификациядан шығару немесе екі факторлы аутентификацияға рұқсат тізімін өзгерту үшін пайдаланушыда екі факторлы аутентификация конфигурацияланған және **Жалпы функционал**: **Пайдаланушы рұқсаттары** функционалдық аймағында Нысан ACL-ін өзгерту бар аккаунт болуы керек.

- Әрқашан кем дегенде бір пайдаланушы екі факторлы аутентификацияны конфигурациялаған болуы керек, сонда бұл пайдаланушы екі факторлы аутентификацияның рұқсат етілген тізімін және алып тастау тізімін басқара алады.

- Екі факторлы аутентификация тек Басқару серверінің 16.1 нұсқасы үшін автоматты түрде қосылады. Егер басқа негізгі немесе қосымша Басқару серверлері 16 немесе одан бұрынғы нұсқаны іске қосса, олардың екі факторлы аутентификация параметрлері өзгеріссіз қалады.

- Виртуалды Басқару сервері екі факторлы аутентификация параметрлерін физикалық Басқару серверінен мұра етеді, сондықтан егер екі факторлы аутентификация физикалық Басқару серверінде қосылған болса, ол виртуалды Басқару серверінде де қосылады. Виртуалды Басқару серверінде екі факторлы аутентификация параметрлерін конфигурациялау мүмкін емес.

- Екі факторлы аутентификация дұрыс жұмыс істеуі үшін Басқару сервері мен Web Console веб-консолін 16.1 немесе одан кейінгі нұсқасына жаңарту қажет.

Екі факторлы аутентификацияны пайдалану арқылы кешенді қорғауды қамтамасыз ету үшін тек Басқару серверін ғана емес, сонымен қатар ол орнатылған құрылғыны да қорғау қажет. Ол үшін Қауіпсіздікті күшейту жөніндегі нұсқаулық ұсыныстарын ескеріңіз.

Kaspersky Security Center Web Console веб-консоліне кіру кезінде екі факторлы аутентификация құпия кілтін баптау

Kaspersky Security Center Linux 16.1 немесе одан кейінгі нұсқасына алғаш рет кірген кезде, екі факторлы аутентификацияны конфигурациялау терезесі ашылады.

Есептік жазба үшін екі факторлы аутентификацияны конфигурациялау үшін:

1. Ұялы құрылғыда немесе компьютерде уақытқа негізделген бір реттік құпиясөз алгоритмін (TOTP) қолдайтын кез келген қолданбаны орнатыңыз, мысалы:

   - Google Authenticator
   - Microsoft Authenticator
   - Bitrix24 OTP
   - Яндекс ID
   - Avanpost Authenticator
   - Aladdin 2FA
   - Rutoken OTP

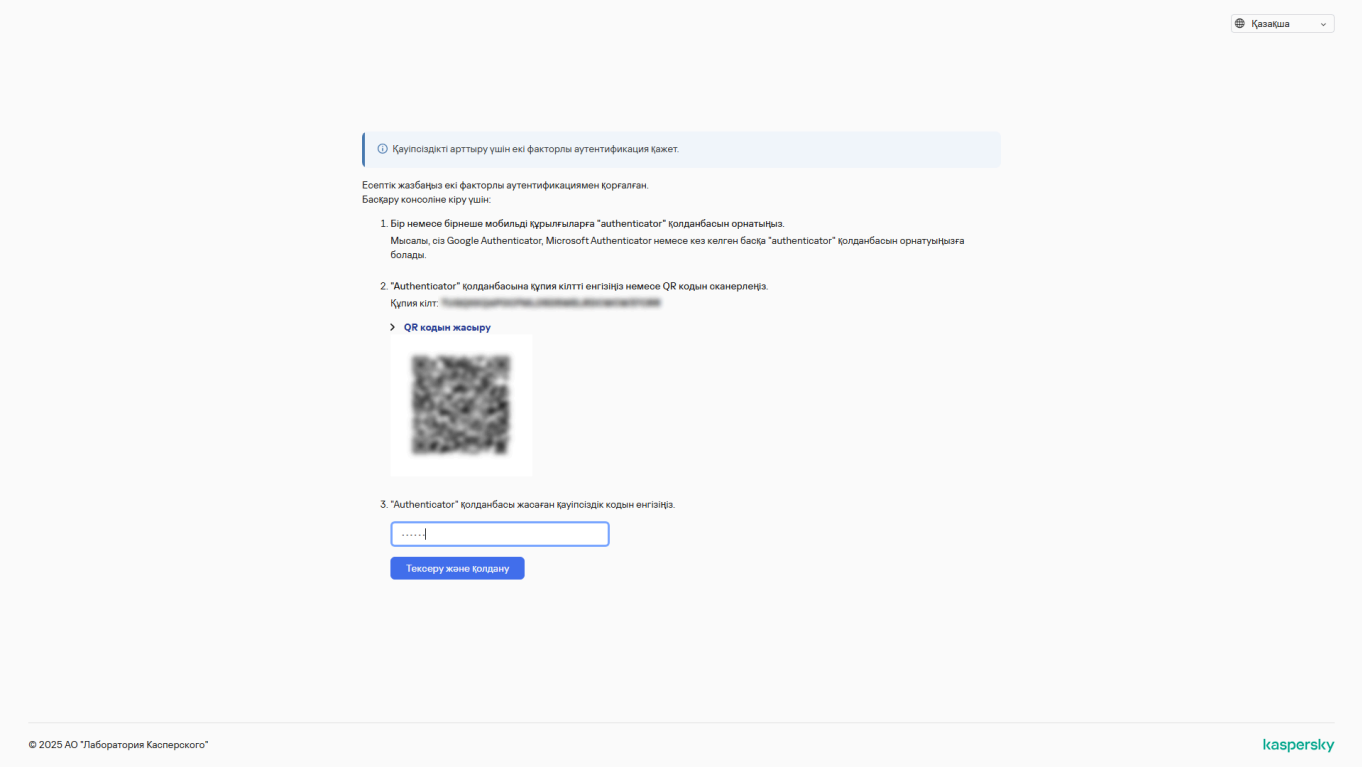
   Басқару серверіне қосылатын сол құрылғыда аутентификация қолданбасын орнату мүлдем ұсынылмайды.

2. Аутентификация қолданбасы бар құрылғыдағы уақыт пен Басқару сервері бар құрылғыдағы уақыт UTC-пен синхрондалғанына көз жеткізіңіз. Дәлдікті арттыру үшін бүкіл инфрақұрылымыңызда бірдей NTP серверлерін пайдалануды ұсынамыз.

3. Ұялы құрылғыдағы немесе компьютердегі аутентификация қолданбасын пайдаланып бір реттік қауіпсіздік кодын жасаңыз. Ол үшін келесі әрекеттердің бірін орындаңыз:

   - Екі факторлы аутентификация құпия кілтін аутентификация қолданбасына қолмен енгізіңіз.
   - **QR кодын қарау** түймесін басып, QR кодын аутентификация қолданбасымен сканерлеңіз.

Ұялы құрылғыда 6 таңбалы бір реттік қауіпсіздік коды көрсетіледі.



Kaspersky Security Center Web Console веб-консолінe кіру кезінде екі факторлы аутентификация құпия кілтін баптау

4. **Екі факторлы аутентификация** терезесінде аутентификация қолданбасы жасаған бір реттік қауіпсіздік кодын көрсетіп, **Тексеру және қолдану** түймесін басыңыз.

   Rutoken OTP конфигурациясы

   Егер сіз Rutoken OTP пайдалансаңыз, сізге Rutoken OTP қолданбасы орнатылған Android мобильді құрылғысы қажет. Android мобильді құрылғысы келесі талаптарға сай болуы керек:

   - Операциялық жүйе – Android 7 немесе одан жаңа.
   - NFC модулі – қолжетімді және қосылған.

   Rutoken OTP қолданбасында келесі параметрлерді конфигурациялау керек:

   - Екі сатылы конфигурация шеберінде көрсетілген QR кодын сканерлеу.
   - Уақыт аралығын 30 секундқа орнатыңыз.
   - Алгоритм ретінде SHA1 таңдаңыз.

   Rutoken OTP конфигурациялау үшін:

   1. Rutoken OTP құрылғысын NFC модулі бар мобильдік құрылғының жанына қойыңыз.
   2. Rutoken OTP қолданбасында **Қосылу токенін** басыңыз.
   3. Rutoken OTP қолданбасында **Параметрлерді конфигурациялау** түймесін басып, **Құпия кілтті сақтау** түймесін басыңыз.

Токен мобильдік құрылғыға сәтті қосылған болса, Rutoken OTP қолданбасы келесі күй хабарларын көрсетеді:

- **Токен қосылды.**
- **Параметрлер конфигурацияланды.**
- **Құпия кілт сақталды.**

4. Rutoken OTP құрылғысында түймені басыңыз.

   Құрылғыда қауіпсіздік коды көрсетіледі.

5. Kaspersky Security Center Web Console веб-консолінде екі қадамдық тексеру терезесінде қауіпсіздік кодын енгізіңіз.

Есептік жазбаңыз үшін екі факторлы аутентификация конфигурацияланған. Сіздің құқықтарыңызға сәйкес Басқару серверіне қатынасу мүмкіндігі бар.

Егер екі факторлы аутентификация конфигурациясы сізге қолжетімді болмаса, **Жалпы мүмкіндіктер**: **Жалпы функционал** функционалдық аймағында Пайдаланушы рұқсаттары бар және аккаунтыңызды екі факторлы аутентификацияға рұқсат тізіміне қосу үшін екі факторлы аутентификацияны конфигурациялаған пайдаланушыға хабарласыңыз.

Пайдаланушыларға екі факторлы аутентификацияны конфигурациялауға мүмкіндік беру

Екі факторлы аутентификацияға рұқсат беру тізімі – Web Console жүйесіне кірген кезде екі факторлы аутентификацияны бастапқыда конфигурациялауға рұқсат етілген пайдаланушылардың тізімі. Бұл тізімде екі факторлы аутентификациясы конфигурацияланбаған пайдаланушы есептік жазбалары бар. Әдепкі бойынша, жаңа пайдаланушы есептік жазбалары екі факторлы аутентификацияға рұқсат беру тізіміне кірмейді және оларды әкімші тізімге қосуы керек. Егер жаңа есептік жазба OpenAPI скрипттерін іске қосу үшін пайдаланылатын интеграция есептік жазбасы болса, оны екі факторлы аутентификациядан шығару керек.

Пайдаланушы есептік жазбасы екі факторлы аутентификацияны конфигурациялаған немесе екі факторлы аутентификациядан шығарылған кезде екі факторлы аутентификацияға рұқсат беру тізімінен автоматты түрде жойылады.

Екі факторлы аутентификацияға рұқсат беру тізімін қолмен өзгерту екі факторлы аутентификацияны конфигурациялаған және **Жалпы мүмкіндіктер**: **Жалпы функционал** функционалдық аймағында Пайдаланушы рұқсаттары жазбалар үшін қолжетімді.

Пайдаланушы есептік жазбаларын екі факторлы аутентификацияға рұқсат тізімінен қолмен жою үшін:

1. Негізгі мәзірдегі басқару серверінің атауын басыңыз.

   Басқару серверінің сипаттары терезесі ашылады.

2. Сипаттар терезесінің **Екі факторлы аутентификация** қойындысында, **Құпия кілттер жасауға рұқсаты бар пайдаланушылар** кестесінде **Қосу** түймесін басыңыз.

3. Ашылған терезеде:

   a. Жойғыңыз келетін пайдаланушы есептік жазбасын таңдаңыз.

      Екі факторлы аутентификация рұқсат ету тізіміне тек екі факторлы аутентификациядан шығарылмаған және екі факторлы аутентификацияның құпия кілті жоқ пайдаланушылар ғана қосыла алады.

   b. Пайдаланушы есептік жазбасы рұқсатсыз өзгертуден қорғалған болса, осы есептік жазбаны өзгертуге рұқсатыңыз бар екенін растауыңыз қажет. **Есептік жазба қорғанысы** терезесінде өз тіркелгіңіздің есептік жазбаның деректерін және екі факторлы аутентификация үшін бір реттік қауіпсіздік кодын көрсетіңіз.

   c. Өзгерістерді сақтаңыз.

Таңдалған пайдаланушы есептік жазбасы екі факторлы аутентификацияға рұқсат тізіміне қосылады. Келесі кіру кезінде пайдаланушы құпия кілт жасай алады.

Пайдаланушы есептік жазбасын екі факторлы аутентификация сол есептік жазба үшін конфигурацияланғанға дейін екі факторлы аутентификацияға рұқсат тізімінен жоюға болады.

Пайдаланушы тіркелгілерін екі факторлы аутентификацияға рұқсат тізімінен қолмен жою үшін:

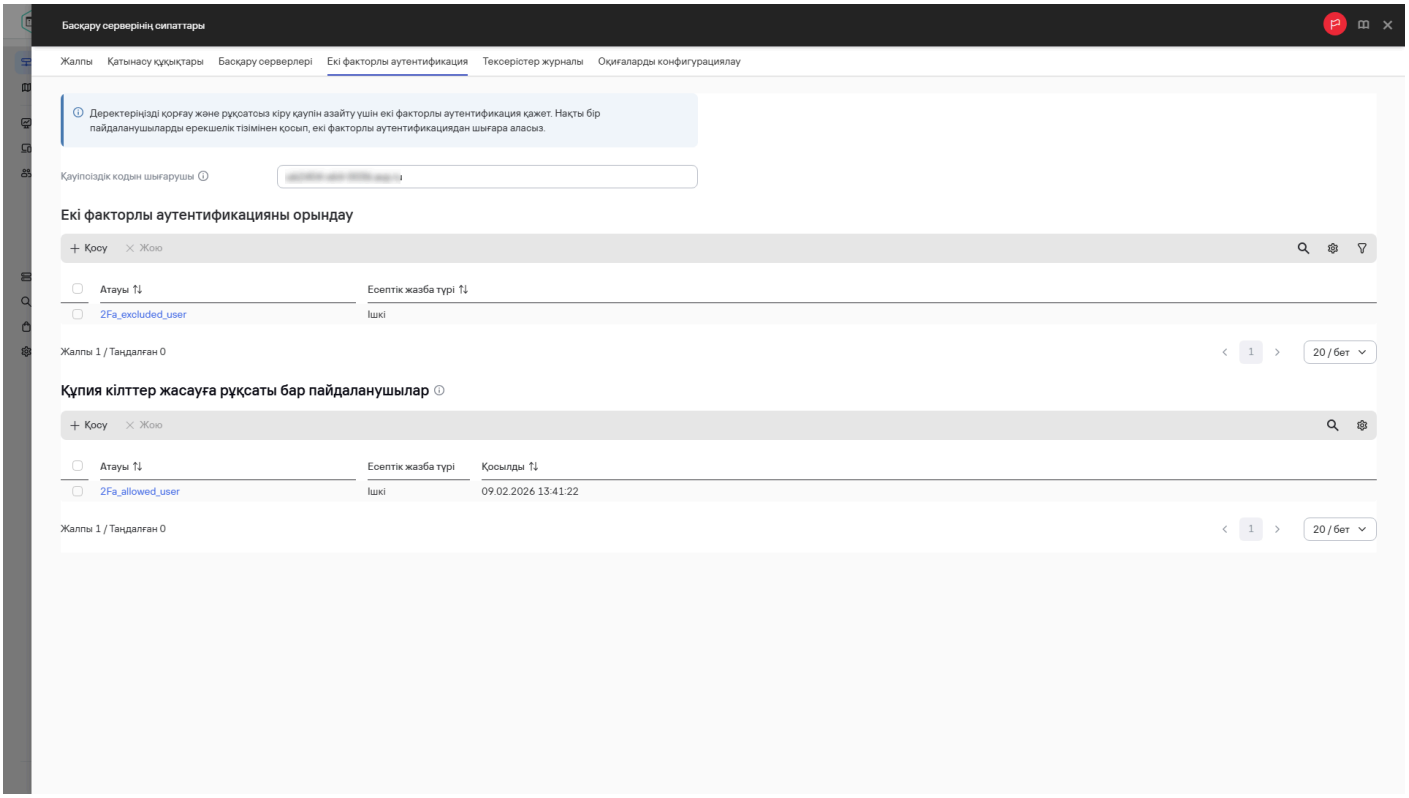
1. Негізгі мәзірдегі басқару серверінің атауын басыңыз.

   Басқару серверінің сипаттары терезесі ашылады.

2. Сипаттар терезесінің **Екі факторлы аутентификация** қойындысында, **Құпия кілттер жасауға рұқсаты бар пайдаланушылар** кестесінде жойғыңыз келетін пайдаланушы есептік жазбаларын таңдап, **Жою** түймесін басыңыз.

3. Пайдаланушы есептік жазбасы рұқсатсыз өзгертуден қорғалған болса, осы есептік жазбаны өзгертуге рұқсатыңыз бар екенін растауыңыз қажет. **Есептік жазба қорғанысы** терезесінде өз тіркелгіңіздің есептік жазбаның деректерін және екі факторлы аутентификация үшін бір реттік қауіпсіздік кодын көрсетіңіз.

Таңдалған пайдаланушы есептік жазбалары екі факторлы аутентификацияның рұқсат ету тізімінен жойылды.



Екі факторлы аутентификацияны алып тастау тізімін конфигурациялау

Егер Басқару серверіндегі белсенді сеанс кезінде сіздің екі факторлы аутентификация құпия кілтіңізді басқа пайдаланушы жойса немесе сіз кілтті өзіңіз қалпына келтірсеңіз, бірақ жаңасын жасамасаңыз, екі факторлы аутентификация рұқсат тізімін өзгерту мүмкіндігі бұғатталады.

Пайдаланушы есептік жазбаларын екі факторлы аутентификация рұқсат тізімінен автоматты түрде қосуға және жоюға болады.

Басқа есептік жазбалар үшін екі факторлы аутентификация құпия кілтін қалпына келтірген кезде, олардың есептік жазбалары жаңа құпия кілт жасай алуы үшін автоматты түрде екі факторлы аутентификацияға рұқсат тізіміне қосылады.

Басқару серверін 16 немесе одан бұрынғы нұсқасынан 16.1 немесе одан кейінгі нұсқасына жаңартқан кезде, сондай-ақ Басқару сервері 16 немесе одан бұрынғы нұсқасында деректердің сақтық көшірмесін жасап, оны Басқару сервері 16.1 немесе одан кейінгі нұсқасында қалпына келтірген кезде, келесі шарттардың барлығы орындалған жағдайда пайдаланушы есептік жазбалары автоматты түрде екі факторлы аутентификацияға рұқсат тізіміне қосылады:

- Пайдаланушының функционалдық аймағында Оқу рұқсаты бар *Жалпы функционал: Базалық функционалдылық* пайдаланушыға тікелей тағайындалады (қауіпсіздік тобы арқылы емес). Бұл рұқсаты бар пайдаланушы рөлінің ауқымы барлық басқарылатын және Тағайындалмаған құрылғыларды қамтуы керек және Басқару сервері деңгейінде орнатылуы керек.
- Пайдаланушы екі факторлы аутентификациядан шығарылмаған.
- Пайдаланушыда екі факторлы аутентификация құпия кілті жоқ.
- Алдыңғы нұсқадағы Басқару серверіндегі барлық пайдаланушылар үшін екі факторлы аутентификация қосылмаған.

Бір шартты орындамау пайдаланушының екі факторлы аутентификацияға рұқсат тізіміне қосылмауына әкеледі.

> Жаңартудан немесе қалпына келтіруден кейін, екі факторлы аутентификация рұқсат тізімінде тек Басқару серверіне кіруі керек пайдаланушы есептік жазбалары ғана бар екеніне көз жеткізуді ұсынамыз. Екі факторлы аутентификацияға рұқсат тізімін қарап шығыңыз және одан басқа аутентификация есептік жазбаларын алып тастаңыз. Сценарийлердің істен шығуын болдырмау үшін OpenAPI арқылы сценарийлерді іске қосу үшін пайдаланылатын тұтастық есептік жазбаларын ерекшеліктер тізіміне қосыңыз.

Пайдаланушылардың тіркелгілері келесі шарттардың барлығы орындалған жағдайда жаңартудан немесе қалпына келтіруден кейін Басқару серверге кіру мүмкіндігін жоғалтады:

- Пайдаланушының функционалдық аймағында Оқу рұқсаты бар *Жалпы функционал: Қауіпсіздік тобы арқылы тағайындалған Базалық функционалдылық* (тікелей пайдаланушыға емес) немесе бұл рұқсат мүлдем жоқ.
- Пайдаланушы екі факторлы аутентификациядан шығарылмаған.
- Пайдаланушыда екі факторлы аутентификация құпия кілті жоқ.
- Екі факторлы аутентификация барлық пайдаланушылар үшін қосылған. алдыңғы нұсқаның әкімшілік серверінде.

Қажет болған жағдайда, бұл есептік жазбаларды екі факторлы аутентификацияның рұқсат етілген тізіміне қолмен қосуға болады.

Екі факторлы аутентификация құпия кілтін қалпына келтіру және жою

Пайдаланушы құрылғысына кіру мүмкіндігін жоғалтқанда немесе жаңа құрылғыда екі факторлы аутентификацияны орнату қажет болғанда екі факторлы аутентификация құпия кілтін қалпына келтіруге болады. Құпия кілтті қалпына келтіру пайдаланушыға Web Console жүйесіне қайта кіріп, жаңа құпия кілт жасауға мүмкіндік береді.

Басқа пайдаланушылардың есептік жазбалары үшін екі факторлы аутентификацияның құпия кілтін қалпына келтіруге немесе жоюға болады, егер сіз екі факторлы аутентификацияны конфигурациялаған болсаңыз және **Жалпы функционал**: **Пайдаланушы рұқсаттары** функционалдық аймағында нысанның ACL өзгерту мүмкіндігіңіз болса ғана. Сондай-ақ, өзіңіздің құпия кілтіңізді қалпына келтіре аласыз.

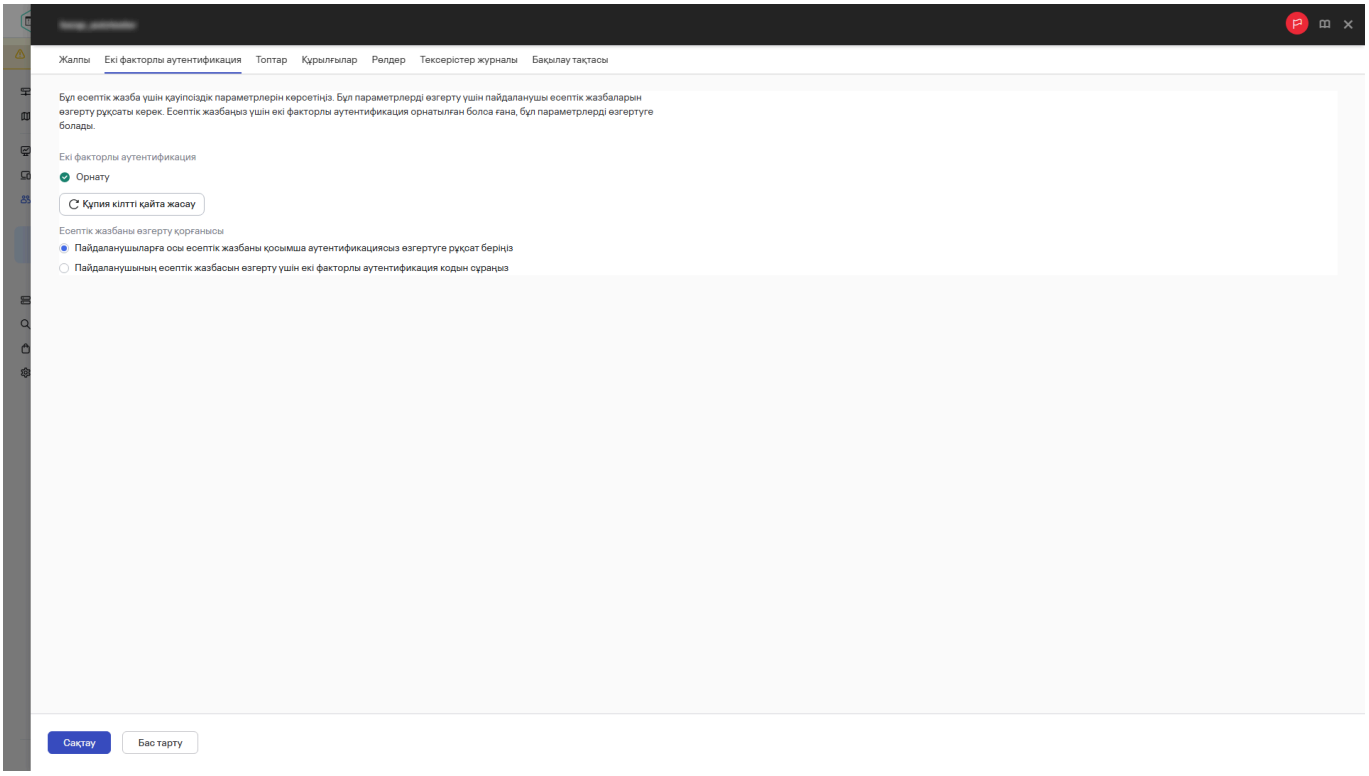
Есептік жазба үшін құпия кілтті қалпына келтіру үшін:

1. Бағдарламаның негізгі терезесінде **Пайдаланушылар және рөлдер** → **Пайдаланушылар және топтар** бөліміне өтіп, **Пайдаланушылар** қойындысын таңдаңыз.

2. Құпия кілтті қалпына келтіргіңіз келетін пайдаланушы есептік жазбасының атын басыңыз.

3. Егер сіз есептік жазбаңыз үшін құпия кілтті қалпына келтіргіңіз келсе:

a. **Екі факторлы аутентификация** қойындысында **Құпия кілтті қайта жасау** түймесін басыңыз.

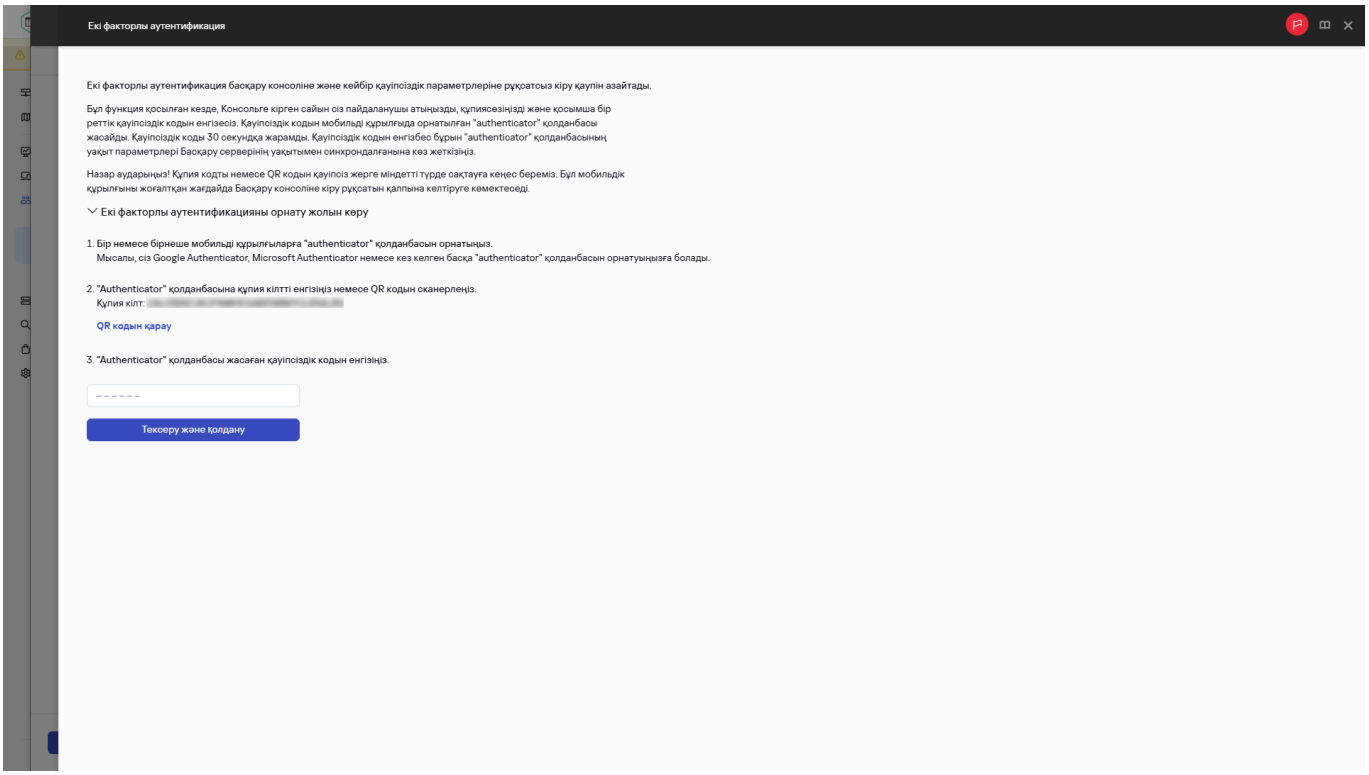


Ағымдағы пайдаланушы есептік жазбасы үшін екі факторлы аутентификация құпия кілтін қайта жасау

a. Пайдаланушы есептік жазбасы рұқсатсыз өзгертуден қорғалған болса, осы есептік жазбаны өзгертуге рұқсатыңыз бар екенін растауыңыз қажет. **Есептік жазба қорғанысы** терезесінде өз есептік жазбаңыздың деректерін және екі факторлы аутентификация кодын көрсетіңіз.

b. **Екі факторлы аутентификация** терезесінде **Екі факторлы аутентификацияны орнату жолын көру** түймесін, содан кейін **QR кодын қарау** түймесін басыңыз.

c. QR кодын сканерлеу және бір реттік қауіпсіздік кодын алу үшін мобильді құрылғыдағы аутентификация қолданбасын пайдаланыңыз.



Ағымдағы пайдаланушы есептік жазбасы үшін жаңа екі факторлы аутентификация құпия кілтін конфигурациялау

a. **Екі факторлы аутентификация** терезесінде аутентификация қолданбасы жасаған қауіпсіздік кодын көрсетіп, **Тексеру және қолдану** түймесін басыңыз.

Rutoken OTP конфигурациясы

Егер сіз Rutoken OTP пайдалансаңыз, сізге Rutoken OTP қолданбасы орнатылған Android мобильді құрылғысы қажет. Android мобильді құрылғысы келесі талаптарға сай болуы керек:

- Операциялық жүйе – Android 7 немесе одан жаңа.
- NFC модулі – қолжетімді және қосылған.

Rutoken OTP қолданбасында келесі параметрлерді конфигурациялау керек:

- Екі сатылы конфигурация шеберінде көрсетілген QR кодын сканерлеу.
- Уақыт аралығын 30 секундқа орнатыңыз.
- Алгоритм ретінде SHA1 таңдаңыз.

Rutoken OTP конфигурациялау үшін:

1. Rutoken OTP құрылғысын NFC модулі бар мобильдік құрылғының жанына қойыңыз.
2. Rutoken OTP қолданбасында **Қосылу токенін** басыңыз.
3. Rutoken OTP қолданбасында **Параметрлерді конфигурациялау** түймесін басып, **Құпия кілтті сақтау** түймесін басыңыз.

Токен мобильдік құрылғыға сәтті қосылған болса, Rutoken OTP қолданбасы келесі күй хабарларын көрсетеді:

- **Токен қосылды.**
- **Параметрлер конфигурацияланды.**
- **Құпия кілт сақталды.**

4. Rutoken OTP құрылғысында түймені басыңыз.

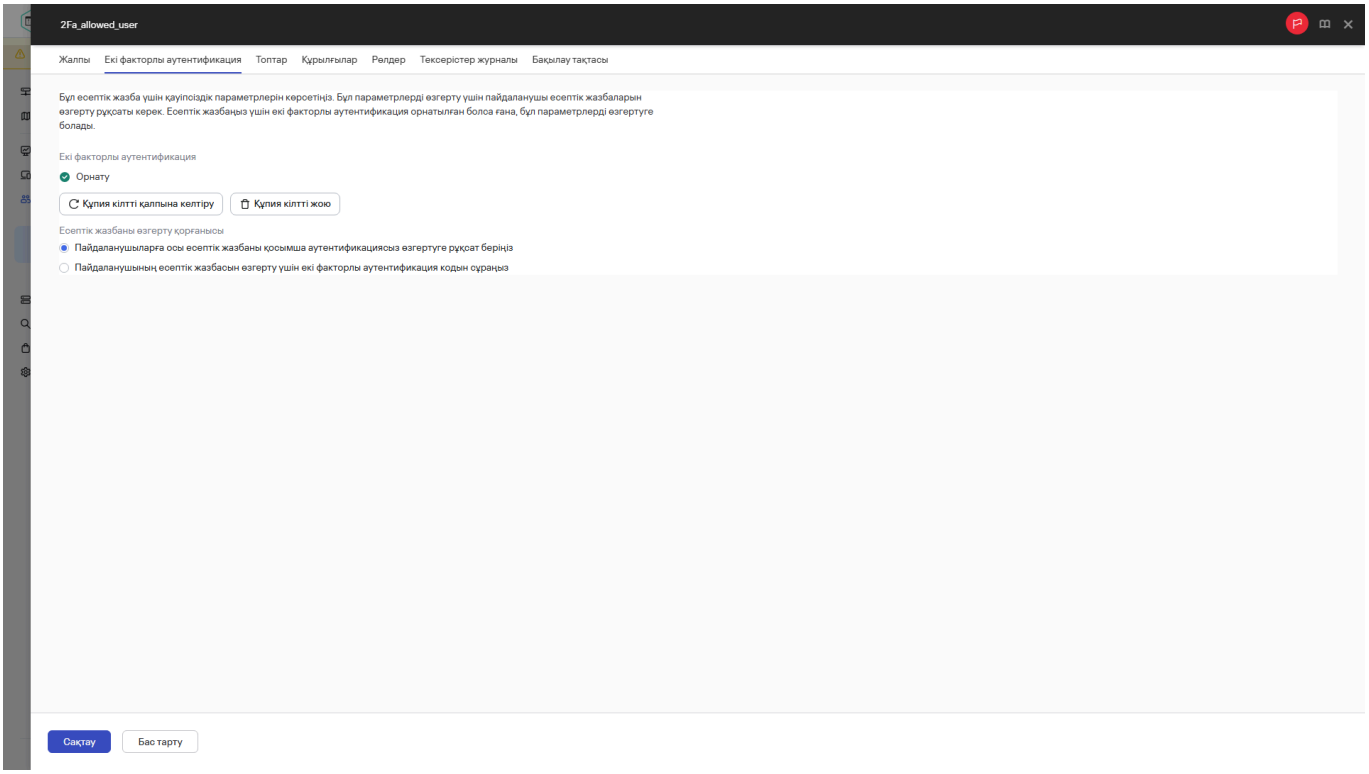
   Құрылғыда қауіпсіздік коды көрсетіледі.

5. Kaspersky Security Center Web Console веб-консолінде екі қадамдық тексеру терезесінде қауіпсіздік кодын енгізіңіз.

Есептік жазбаңыздың құпия кілті өзгертілді.

4. Егер сіз басқа есептік жазбаның құпия кілтін қалпына келтіргіңіз келсе:

   a. **Екі факторлы аутентификация** қойындысында **Құпия кілтті қалпына келтіру** түймесін басыңыз.



Басқа пайдаланушы есептік жазбасы үшін екі факторлы аутентификация құпия кілтін қалпына келтіру

   a. Пайдаланушы есептік жазбасы рұқсатсыз өзгертуден қорғалған болса, осы есептік жазбаны өзгертуге рұқсатыңыз бар екенін растауыңыз қажет. **Есептік жазба қорғанысы** терезесінде өз есептік жазбаңыздың есептік жазба деректерін және екі факторлы аутентификация үшін бір реттік қауіпсіздік кодын көрсетіңіз.

   b. Құпия кілтті қалпына келтіруді растаңыз, содан кейін өзгерістерді сақтаңыз.

Басқа пайдаланушы есептік жазбасы үшін құпия кілтті қалпына келтірген кезде, бар құпия кілт жойылады және пайдаланушы есептік жазбасы Басқару серверінің қасиеттеріндегі екі факторлы аутентификация рұқсат тізіміне қосылады. Келесі кіру кезінде пайдаланушы жаңа құпия кілт жасай алады.

Пайдаланушы есептік жазбасы құпия кілті қалпына келтіріледі.

Пайдаланушының Web Console веб-консоліне кіруіне толығымен тыйым салу және пайдаланушының Басқару серверіне кіруіне жол бермеу үшін құпия кілтті жоюға болады.

Құпия кілтті жою үшін:

1. Бағдарламаның негізгі терезесінде **Пайдаланушылар және рөлдер** → **Пайдаланушылар және топтар** бөліміне өтіп, **Пайдаланушылар** қойындысын таңдаңыз.
2. Аралық құпия кілтті жойғыңыз келетін пайдаланушы есептік жазбасының атын басыңыз.

   Сіз өз есептік жазбаңыз үшін құпия кілтті жоя алмайсыз.

3. **Екі факторлы аутентификация** қойындысында **Құпия кілтті жою** түймесін басыңыз.
4. Пайдаланушы есептік жазбасы рұқсатсыз өзгертуден қорғалған болса, осы есептік жазбаны өзгертуге рұқсатыңыз бар екенін растауыңыз қажет. **Есептік жазба қорғанысы** терезесінде өз есептік жазбаңыздың есептік жазба деректерін және екі факторлы аутентификация үшін бір реттік қауіпсіздік кодын көрсетіңіз.
5. Құпия кілттің жойылуын растаңыз, содан кейін өзгерістерді сақтаңыз.

   Пайдаланушы есептік жазбасының құпия кілті жойылады.

Пайдаланушыны Басқару серверінің қасиеттерінде екі факторлы аутентификацияға рұқсат тізіміне қосу арқылы кіруді қалпына келтіре аласыз. Бұл жағдайда, келесі кіру кезінде пайдаланушы жаңа құпия кілт жасай алады.

Есептік жазбаларды екі факторлы аутентификациядан алып тастау

Қажет болса, екі факторлы аутентификацияны конфигурацияламаған болса да, пайдаланушы аккаунттарын екі факторлы аутентификациядан шығарыңыз, бұл оларға Басқару серверіне кіруге мүмкіндік береді. Екі факторлы аутентификациядан есептік жазбаларды шығару аутентификация кезінде бір реттік қауіпсіздік коды кодын бере алмайтын интеграция есептік жазбалары үшін қажет болуы мүмкін. Интеграция есептік жазбалары OpenAPI арқылы сценарийлерді іске қосу үшін пайдаланылады.

Егер сіздің аккаунтыңыз үшін екі факторлы аутентификация конфигурацияланған болса және сізде **Жалпы функционал**: **Пайдаланушы рұқсаттары** функционалдық аймағында нысан ACL өзгерту болса, алып тастау тізімін өзгерте аласыз.

Пайдаланушы есептік жазбасын екі факторлы аутентификациядан шығару үшін:

1. Негізгі мәзірдегі басқару серверінің атауын басыңыз.

   Басқару серверінің сипаттары терезесі ашылады.

2. **Екі факторлы аутентификация** үшін ерекшеліктер кестесіндегі сипаттар терезесінің **Екі факторлы аутентификацияны орындау** қойыншасында **Қосу** түймесін басыңыз.

3. Ашылған терезеде:

   a. Жойғыңыз келетін пайдаланушы есептік жазбаларын таңдаңыз.

   b. Пайдаланушы есептік жазбасы рұқсатсыз өзгертуден қорғалған болса, осы есептік жазбаны өзгертуге рұқсатыңыз бар екенін растауыңыз қажет. **Есептік жазба қорғанысы** терезесінде өз тіркелгіңіздің есептік жазбаның деректерін және екі факторлы аутентификация үшін бір реттік қауіпсіздік кодын көрсетіңіз.

   c. Өзгерістерді сақтаңыз.

Таңдалған пайдаланушы есептік жазбалары екі факторлы аутентификациядан алынып тасталады, ал егер бар болса, олардың құпия кілттері жойылады. Басқару сервері 16.1 жүйесінде сақтық көшірмені қалпына келтіргенде немесе Басқару серверін 16.1 немесе одан кейінгі нұсқасына жаңартқанда алынып тасталған есептік жазбалардың тізімі өзгермейді. Егер алып тастау тізіміндегі тіркелгілерде Басқару серверінің алдыңғы нұсқасында құпиялар болса, бұл құпия кілттер 16.1 нұсқасында жойылады.

Пайдаланушылардың Web Console веб-консоліне кіруіне толығымен тыйым салу және пайдаланушылардың Басқару серверіне кіруіне жол бермеу үшін пайдаланушы есептік жазбаларын алып тастау тізімінен жоюға болады.

Пайдаланушы есептік жазбаларын алып тастау тізімінен жою үшін:

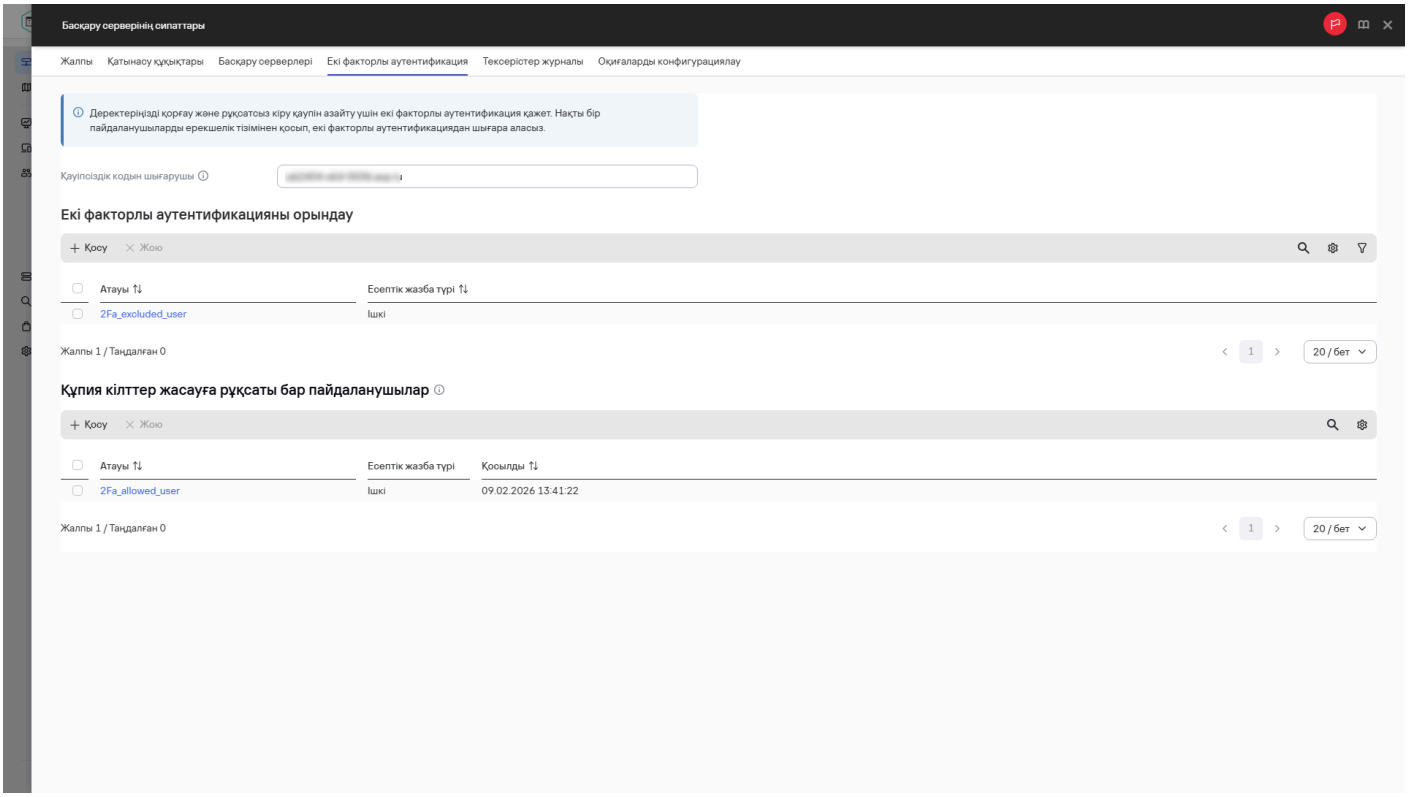
1. Негізгі мәзірдегі басқару серверінің атауын басыңыз.

   Басқару серверінің сипаттары терезесі ашылады.

2. Сипаттар терезесінің **Екі факторлы аутентификация** қойындысында, **Екі факторлы аутентификацияны орындау** кестесінде жойғыңыз келетін пайдаланушы есептік жазбаларын таңдап, **Жою** түймесін басыңыз.

3. Пайдаланушы есептік жазбасы рұқсатсыз өзгертуден қорғалған болса, осы есептік жазбаны өзгертуге рұқсатыңыз бар екенін растауыңыз қажет. **Есептік жазба қорғанысы** терезесінде өз тіркелгіңіздің есептік жазбаның деректерін және екі факторлы аутентификация үшін бір реттік қауіпсіздік кодын көрсетіңіз.

Таңдалған пайдаланушы есептік жазбалары ерекшеліктер тізімінен жойылады.



Екі факторлы аутентификацияны алып тастау тізімін конфигурациялау

Қауіпсіздік кодын шығарушының атын өзгерту

Әртүрлі Басқару серверлері үшін бірнеше идентификаторға (эмитенттер деп аталатын) ие бола аласыз. Қауіпсіздік кодын шығарушының атын өзгертуге болады, мысалы, егер Басқару сервері басқа Басқару сервері үшін ұқсас қауіпсіздік кодын шығарушының атын қолданса. Әдепкі бойынша, қауіпсіздік кодын шығарушының аты Басқару серверінің атымен бірдей.

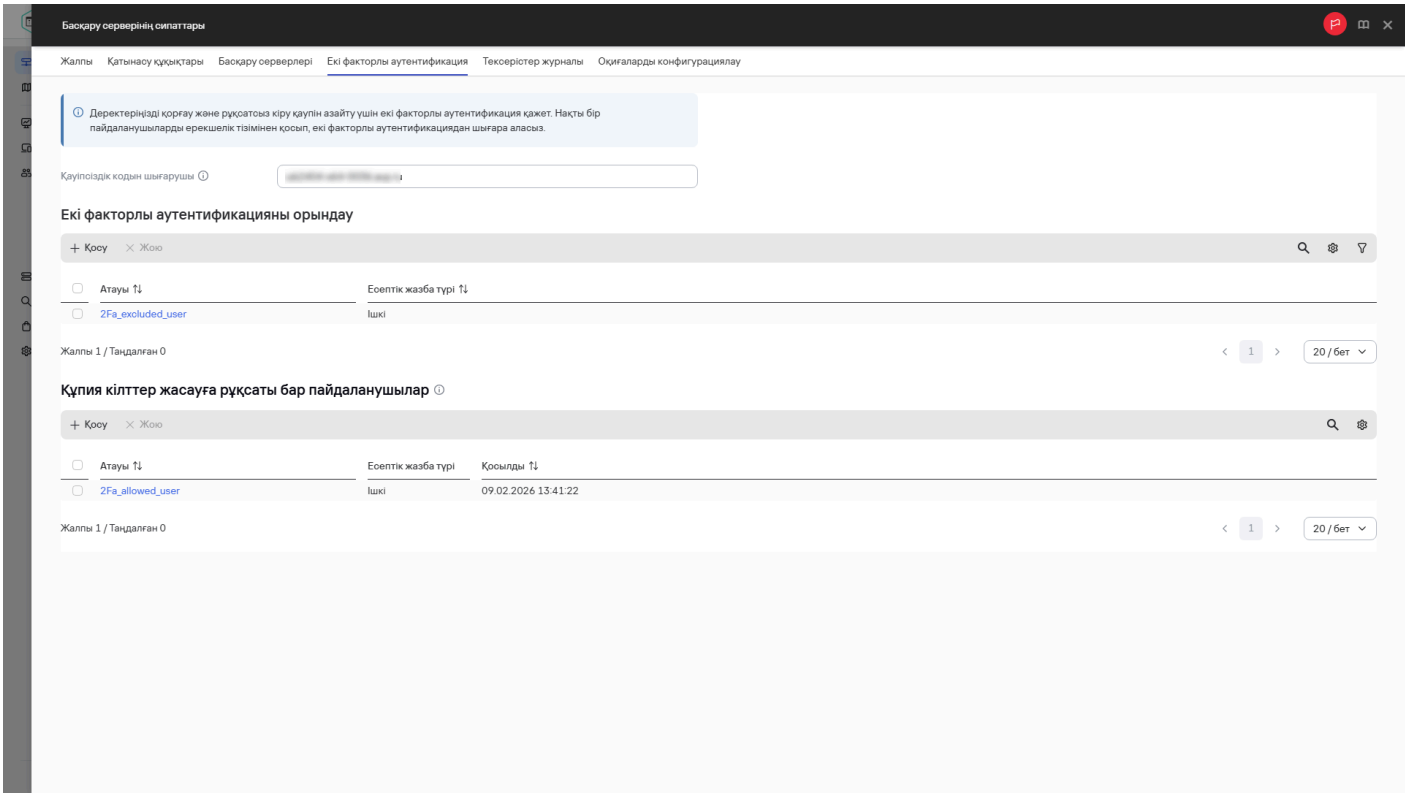
Қауіпсіздік кодын шығарушының жаңа атын көрсету үшін:

1. Негізгі мәзірдегі басқару серверінің атауын басыңыз.

   Басқару серверінің сипаттары терезесі ашылады.

2. Сипаттар терезесінің **Екі факторлы аутентификация** қойындысында **Қауіпсіздік кодын шығарушы** өрісіне жаңа атау енгізіңіз, содан кейін өзгертулерді сақтаңыз.

Келесі кіруден кейін Басқару серверіне жаңа қауіпсіздік коды шығарушысының атауы тағайындалады.



Қауіпсіздік кодын шығарушының атын белгілеу

Құпиясөзді енгізу әрекеттерінің санын өзгерту

Kaspersky Security Center Linux пайдаланушысы құпиясөзді шектеулі рет енгізе алады. Осыдан кейін, пайдаланушы есептік жазбасы бір сағатқа бұғатталады.

Әдепкі бойынша, енгізу әрекеттерінің максималды саны 10-ға тең. Төмендегі нұсқауларды орындау арқылы құпиясөзді енгізу әрекеттерінің санын өзгертуге болады.

Құпиясөзді енгізу әрекеттерінің санын өзгерту үшін келесі әрекеттерді орындаңыз:

1. Басқару сервері орнатылған құрылғыда Linux пәрмен жолын іске қосыңыз.

2. klscflag утилитасы үшін келесі пәрменді орындаңыз:

   ```
   sudo /opt/kaspersky/ksc64/sbin/klscflag -fset -pv klserver -n SrvSplPpcLogonAttempts -t d -v N
   ```

мұндағы N – құпиясөзді енгізу әрекеттерінің саны.

3. Өзгерістер күшіне енуі үшін Басқару сервері қызметін қайта іске қосыңыз.

Құпиясөзді енгізу әрекеттерінің максималды саны өзгертілді.

Пайдаланушыларды немесе қауіпсіздік топтарын жою

Ішкі пайдаланушыларды немесе қауіпсіздік топтарын ғана жоюға болады.

Пайдаланушыларды немесе қауіпсіздік топтарын жою:

1. Қолданбаның негізгі терезесінде **Пайдаланушылар және рөлдер** → **Пайдаланушылар және топтар** бөліміне өтіп, **Пайдаланушылар** немесе **Топтар** қойындысын таңдаңыз.

2. Жойғыңыз келетін пайдаланушы атының немесе қауіпсіздік тобының жанындағы жалаушаны қойыңыз.

   Әрқашан кем дегенде бір пайдаланушы екі факторлы аутентификацияны конфигурациялаған болуы керек, сонда бұл пайдаланушы екі факторлы аутентификацияның рұқсат етілген тізімін және алып тастау тізімін басқара алады.

3. **Жою** түймесін басыңыз.

4. Пайда болған терезеде **ОК** түймесін басыңыз.

Пайдаланушы немесе қауіпсіздік тобы жойылды.

Пайдаланушы есептік жазбасының құпиясөзін өзгерту

Ағымдағы құпиясөз мерзімі аяқталуға жақын болса немесе оны күштірегіне өзгерткіңіз келсе, есептік жазбаның немесе басқа пайдаланушының есептік жазбасының құпиясөзін өзгерту қажет болуы мүмкін.

Құпиясөз келесі ережелерге сәйкес келуі керек:

- Құпиясөздің ұзындығы 8-ден 256 таңбаға дейін болуы керек.
- Құпиясөзде төмендегі тізімдегі кемінде үш топтың таңбалары болуы керек:
  - Бас әріптер (A-Z)
  - Кіші әріптер (a-z)

- Сандар (0-9)
- Арнайы таңбалар (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)

- Құпиясөзде бос орындар, Юникод таңбалары немесе "." таңбасы "@" алдында тұрған кезде "." және "@" тіркесімі болмауы тиіс.

Өз есептік жазбасының құпиясөзін өзгерту

Есептік жазбаңыздың құпиясөзін өзгерту үшін:

1. Жоғарғы панельде есептік жазба атын басу арқылы есептік жазба мәзіріне өтіңіз.
2. Ашылмалы тізімнен **Құпиясөзді өзгерту** опциясын таңдаңыз.
3. Ашылатын оң жақ панельде Kaspersky Security Center Linux қолданбасына қосылу үшін ағымдағы құпиясөзді енгізіп, жаңа құпиясөзді көрсетіңіз.

   Енгізілген құпиясөзді көру үшін түймесін басыңыз.
4. Пайдаланушы есептік жазбасы рұқсатсыз өзгертуден қорғалған болса, осы есептік жазбаны өзгертуге рұқсатыңыз бар екенін растауыңыз қажет. **Есептік жазба қорғанысы** терезесінде "**Жалпы функционал**: **Пайдаланушы рұқсаттары**" функционалдық аймағында есептік жазбаңыздың деректерін немесе Нысандарға қол жеткізуді басқару тізімдерін өзгерту құқығы бар есептік жазба деректерін көрсетіңіз.
5. Ұялы құрылғыдағы аутентификация қолданбасы арқылы жасалған бір реттік қауіпсіздік кодын енгізіңіз.

Ішкі пайдаланушының есептік жазбасының құпиясөзін өзгерту

Ішкі пайдаланушы есептік жазбасының құпиясөзін өзгерту үшін:

1. Қолданбаның негізгі терезесінде **Пайдаланушылар және рөлдер** → **Пайдаланушылар және топтар** бөліміне өтіп, **Пайдаланушылар** қойындысын таңдаңыз.
2. Өзгерту қажет болған реттелетін есептік жазбасын таңдаңыз.
3. Ашылатын пайдаланушы сипаттары терезесінде **Жалпы** қойындысындағы **Құпиясөзді өзгерту** түймесін басыңыз.
4. Пайдаланушыны Kaspersky Security Center Linux-ке қосуға арналған жаңа құпиясөзді орнатыңыз.

   Енгізілген құпиясөзді көру үшін түймесін басыңыз.
5. Қажет болса, пайдаланушының келесі аутентификациясында құпиясөзді өзгертуге мәжбүрлеу үшін **Пайдаланушы бірінші кірген кезде құпиясөзді өзгертуі керек** параметрін қосыңыз.

6. Егер пайдаланушы есептік жазбасы рұқсатсыз өзгертуден қорғалған болса, осы есептік жазбаны өзгертуге рұқсатыңыз бар екенін растауыңыз қажет. **Есептік жазба қорғанысы** терезесінде "**Жалпы функционал**: **Пайдаланушы рұқсаттары**" функционалдық аймағында Нысандарға қол жеткізуді басқару тізімдерін өзгерту құқығы бар есептік жазба деректерін көрсетіңіз.

7. Ұялы құрылғыдағы аутентификация қолданбасы арқылы жасалған бір реттік қауіпсіздік кодын енгізіңіз.

Сервер жалаушалары көмегімен құпиясөзді өзгерту параметрлерін реттеу

Klscflag утилитасын пайдаланып, келесі пәрмендер арқылы құпиясөзді өзгертуді реттеуге болады:

- Құпиясөзді ауыстыру кезеңін орнату (`LP_SplPwdChangePeriodDays` жалаушасы).

  ```
  klscflag -fset -pv .core/.independent -s KLLIM -n LP_SplPwdChangePeriodDays -t d -v <айналу_мерзімі>
  ```

  бұл жерде `<айналу_мерзімі>` — пайдаланушы құпиясөзінің мерзімі аяқталатын кезең (күнмен берілген). Ықтимал мәндер: 0–730. Параметр мәні 0 болса, құпиясөзді өзгерту өшірілген.

- Құпиясөзді өзгерту қажеттігі туралы алдыңғы ескерту уақытын конфигурациялау (`LP_SplPwdChangeNotificationHours` жалаушасы)

  ```
  klscflag -fset -pv .core/.independent -s KLLIM -n LP_SplPwdChangeNotificationHours -t d -v <ескерту_уақыт>
  ```

  бұл жерде `<ескерту_уақыт>` — пайдаланушы құпиясөзінің мерзімі аяқталатын кезең (сағатпен берілген). Осы уақыт ішінде құпиясөзді өзгертуді сұрайтын хабарландыру көрсетіледі. Ықтимал мәндер: 0–17520. Параметр мәні 0 болса, ескерту уақыты құпиясөзді ауыстыру кезеңінің 25%-ын құрайды.

- **Пайдаланушы бірінші кірген кезде құпиясөзді өзгертуі керек** параметрі (`LP_SplPwdForceChange` жалаушасы) үшін әдепкі мән нұсқауы.

  ```
  klscflag -fset -pv .core/.independent -s KLLIM -n LP_SplPwdForceChange -t d -v <мән>
  ```

  `<мән>` жалаушасының ықтимал мәндері мына жерде:

  `1` — **Пайдаланушы бірінші кірген кезде құпиясөзді өзгертуі керек** опциясы қосылған.

  `0` — **Пайдаланушы бірінші кірген кезде құпиясөзді өзгертуі керек** опциясы өшірілген.

Жалаушаның ағымдағы мәнін көру үшін келесі пәрменді орындаңыз:

```
klscflag -fget -pv .core/.independent -s KLLIM -n <жалауша> -t d
```

Мұндағы `<жалауша>` – `LP_SplPwdChangePeriodDays`, `LP_SplPwdChangeNotificationHours` немесе `LP_SplPwdForceChange` жалаушасы.

Пайдаланушы рөлін жасау

Пайдаланушы рөлін жасау үшін:

1. Бағдарламаның негізгі терезесінде **Пайдаланушылар және рөлдер** → **Рөлдер** бөліміне өтіңіз.

2. **Қосу** түймесін басыңыз.

3. Ашылған **Жаңа рөл аты** терезесінде жаңа рөл атауын көрсетіңіз.

4. Өзгерістерді қолдану үшін **OK** түймесін басыңыз.

5. Ашылған терезеде рөл параметрлерін өзгертіңіз:

   - **Жалпы** қойыншасында рөл атауын өзгертіңіз.

     Типтік рөл атауларын өзгерте алмайсыз.

   - **Параметрлер** қойыншасында рөлдің әрекет ету ауқымын, сондай-ақ рөлмен байланысты саясаттар мен саясат профильдерін өзгертіңіз.

   - **Қатынасу құқықтары** қойыншасында Kaspersky бағдарламаларына қатынасу құқықтарын өзгертіңіз.

6. Өзгерістерін сақтау үшін **Сақтау** түймесін басыңыз.

Жасалған рөл пайдаланушы рөлдері тізімінде пайда болады.

Пайдаланушы рөлін өзгерту

Пайдаланушы рөлін өзгерту үшін:

1. Бағдарламаның негізгі терезесінде **Пайдаланушылар және рөлдер** → **Рөлдер** бөліміне өтіңіз.

2. Өзгерту қажет рөлді таңдаңыз.

3. Ашылған терезеде рөл параметрлерін өзгертіңіз:

   - **Жалпы** қойыншасында рөл атауын өзгертіңіз.

     Типтік рөл атауларын өзгерте алмайсыз.

   - **Параметрлер** қойыншасында рөлдің әрекет ету ауқымын, сондай-ақ рөлмен байланысты саясаттар мен саясат профильдерін өзгертіңіз.

   - **Қатынасу құқықтары** қойыншасында Kaspersky бағдарламаларына қатынасу құқықтарын өзгертіңіз.

4. Өзгерістерін сақтау үшін **Сақтау** түймесін басыңыз.

Жаңартылған рөл пайдаланушы рөлдері тізімінде пайда болады.

Пайдаланушы рөлі үшін аймақты өзгерту

Пайдаланушы рөлі ауқымы – бұл пайдаланушылар мен басқару топтарының тіркесімі. Пайдаланушы рөліне қатысты параметрлер тек осы рөл тағайындалған пайдаланушыларға тиесілі құрылғыларға қолданылады және бұл құрылғылар осы рөл тағайындалған топтарға, соның ішінде еншілес топтарға жататын болса ғана қолданылады.

Пайдаланушыларды, қауіпсіздік топтарын және басқару топтарын пайдаланушы рөлінің аймағына қосу үшін келесі тәсілдердің бірін пайдаланыңыз:

1-тәсіл:

1. Қолданбаның негізгі терезесінде **Пайдаланушылар және рөлдер** → **Пайдаланушылар және топтар** бөліміне өтіп, **Пайдаланушылар** немесе **Топтар** қойындысын таңдаңыз.
2. Рөл аймағына қосу қажет пайдаланушы аттары немесе қауіпсіздік топтарына қарама-қарсы жалаушыларды қойыңыз.
3. **Рөлді тағайындау** түймесін басыңыз.

   Рөлді тағайындау шебері іске қосылады. Шебердің жұмысын жалғастыру үшін **Келесі** түймесін басыңыз.
4. **Рөлді таңдау** қадамында тағайындау қажет рөлді таңдаңыз.
5. **Ауқымды анықтау** бетінде, рөл аймағына қосу қажет басқару тобын таңдаңыз.
6. Шебер терезесін жабу үшін **Рөлді тағайындау** түймесін басыңыз.

Таңдалған пайдаланушылар, қауіпсіздік топтары және басқару топтары рөл аймағына қосылды.

2-тәсіл:

1. Бағдарламаның негізгі терезесінде **Пайдаланушылар және рөлдер** → **Рөлдер** бөліміне өтіңіз.
2. Аймақты белгілеуді қажет ететін рөлді таңдаңыз.
3. Ашылған рөл сипаттары терезесінде **Параметрлер** қойыншасын таңдаңыз.
4. **Рөл ауқымы** бөлімінде **Қосу** түймесін басыңыз.

   Рөлді тағайындау шебері іске қосылады. Шебердің жұмысын жалғастыру үшін **Келесі** түймесін басыңыз.
5. **Ауқымды анықтау** бетінде, рөл аймағына қосу қажет басқару тобын таңдаңыз.
6. **Пайдаланушыларды таңдау** бетінде, рөл аймағына қосу қажет пайдаланушылар мен қауіпсіздік топтарын таңдаңыз.
7. Шебер терезесін жабу үшін **Рөлді тағайындау** түймесін басыңыз.
8. Басқару сервері сипаттары терезесін жабу үшін **Жабу** (⨯) түймесін басыңыз.

Таңдалған пайдаланушылар, қауіпсіздік топтары және басқару топтары рөл аймағына қосылды.

3-тәсіл:

1. Негізгі мәзірдегі басқару серверінің атауын басыңыз.

   Басқару серверінің сипаттары терезесі ашылады.
2. **Қатынасу құқықтары** қойындысында теңшелетін рөл ауқымын қосқыңыз келетін пайдаланушы немесе қауіпсіздік тобы атының жанындағы құсбелгіні қойып, **Рөлдер** түймесін басыңыз.

   Бір уақытта бірнеше пайдаланушыны немесе қауіпсіздік тобын таңдау мүмкін емес. Бірнеше нысанды таңдасаңыз, **Рөлдер** түймесі өшірулі болады.

3. **Рөлдер** терезесінде тағайындау, қолдану және өзгертулерді сақтағыңыз келетін реттелетін рөлді таңдаңыз.

   Таңдалған пайдаланушылар немесе қауіпсіздік топтары рөлдер ауқымына қосылады.

Пайдаланушы рөлін жою

Пайдаланушы рөлін жою үшін:

1. Бағдарламаның негізгі терезесінде **Пайдаланушылар және рөлдер** → **Рөлдер** бөліміне өтіңіз.
2. Жойғыңыз келетін рөлге қарама-қарсы жалаушаны қойыңыз.
3. **Жою** түймесін басыңыз.
4. Пайда болған терезеде **OK** түймесін басыңыз.

Пайдаланушы рөлі жойылады.

Саясат профильдерінің рөлдермен байланысы

Сіз рөлдерді саясат профильдерімен байланыстыра аласыз. Бұл жағдайда, саясат профилі үшін белсендіру ережесі рөлге байланысты анықталады: саясат профилі белгілі бір рөлі бар пайдаланушы үшін белсенді болады.

Мысалы, саясат басқару тобының барлық құрылғылары үшін қалалық навигациялық бағдарламаларды іске қосуға тыйым салады. Қалалық навигация бағдарламалары "Пайдаланушылар" басқару тобында курьер рөлін атқаратын пайдаланушының бір ғана құрылғысының жұмыс істеуі үшін қажет. Бұл жағдайда, бұл құрылғының иесіне "Курьер" рөлін тағайындауға және иелеріне "Курьер" рөлі тағайындалған құрылғыларда қалалық навигация бағдарламаларын қолдануға рұқсат беретін саясат профилін жасауға болады. Барлық басқа саясат параметрлері өзгеріссіз қалады. Тек "Курьер" рөлі бар пайдаланушыларға қалалық навигация бағдарламаларын пайдалануға рұқсат етіледі. Содан кейін, басқа қызметкерге "Курьер" рөлі тағайындалса, онда бұл қызметкер сіздің ұйымыңызға тиесілі құрылғыда қалалық навигациялық бағдарламаларды қолдана алады. Алайда, осы басқару тобының басқа құрылғыларында қалалық навигациялық бағдарламаларды пайдалануға тыйым салынады.

Рөлді саясат профилімен байланыстыру үшін:

1. Бағдарламаның негізгі терезесінде **Пайдаланушылар және рөлдер** → **Рөлдер** бөліміне өтіңіз.
2. Саясат профилімен байланыстырылатын рөлді таңдаңыз.

   Жалпы қойыншасында рөл сипаттары терезесі ашылады.
3. **Параметрлер** қойыншасына өтіп, **Саясаттар** бөліміне дейін төменге айналдырыңыз.
4. **Өңдеу** түймесін басыңыз.

5. Рөлді осымен байланыстыру үшін:

   - **Қолданыстағы саясат профилімен** – қажетті саясаттың атауының жанындағы (>) белгішесін басыңыз, содан соң рөлді байланыстырғыңыз келетін саясат профилінің жанында жалаушаны қойыңыз.
   - **Жаңа саясат профилі**:

     a. Саясат профилін жасағыңыз келетін саясаттың жанында жалауша қойыңыз.

     b. **Жаңа саясат профилі** түймесін басыңыз.

     c. Жаңа саясат профилінің атауын көрсетіңіз және саясат профилінің параметрлерін конфигурациялаңыз.

     d. **Сақтау** түймесін басыңыз.

     e. Жаңа саясат профилінің жанында жалауша қойыңыз.

6. **Рөлге тағайындау** түймесін басыңыз.

Таңдалған саясат профилі рөлмен байланысып, рөлдің сипаттарында пайда болады. Профиль, иелеріне осы рөл тағайындалған барлық құрылғыларға автоматты түрде қолданылады.

Қосалқы Басқару серверлеріне пайдаланушы рөлдерін тарату

Әдепкі бойынша, негізгі және қосалқы Басқару серверлерінің пайдаланушы рөлдерінің тізімдері тәуелсіз болып саналады. Негізгі Басқару серверінде жасалған пайдаланушы рөлдерін барлық Басқару серверіне автоматты түрде тарату үшін бағдарламаларды орнатуға болады. Пайдаланушы рөлдері қосалқы Басқару серверінен өзінің қосалқы Басқару серверлеріне де таралуы мүмкін.

Пайдаланушы рөлдерін негізгі Басқару серверінен қосалқы Басқару серверлеріне тарату үшін:

1. Негізгі мәзірдегі басқару серверінің атауын басыңыз.

   Жалпы қойыншасында Басқару сервері сипаттары терезесі ашылады.

2. **Басқару серверлерінің иерархиясы** бөліміне өтіңіз.

3. **Рөлдердің тізімін әрі қарай қосалқы Басқару серверлеріне жіберу** опциясын қосыңыз, содан кейін **Сақтау** түймесін басыңыз.

   Бағдарлама негізгі Басқару сервері пайдаланушыларының рөлдерін қосалқы Басқару серверлеріне көшіреді.

Рөлдердің тізімін әрі қарай қосалқы Басқару серверлеріне жіберу опциясы қосулы және пайдаланушы рөлдері таратылған болса, оларды қосалқы басқару серверінде өңдеу немесе жою мүмкін емес. Негізгі Басқару серверінде рөл жасағанда немесе қолданыстағы рөлді өзгерткенде, өзгерістер автоматты түрде қосалқы Басқару серверлеріне көшіріледі. Негізгі Басқару серверінде пайдаланушы рөлін жойған кезде, бұл рөл қосалқы Басқару серверінде қалады және оны өзгертуге немесе жоюға болады.

Басты серверден қосалқы басқару серверіне таралатын рөлдер жасыл құсбелгілер (✓) арқылы көрсетіледі. Сіз бұл рөлдерді қосалқы Басқару серверінде өзгерте алмайсыз.

Егер рөл негізгі Басқару серверінде жасалса және қосалқы Басқару серверінде бірдей атауы бар рөл болса, жаңа рөл қосалқы Басқару серверіне көшіріледі және оның атына жақшаға нөмір қосылады, мысалы, ~~1, ~~2 (нөмірі кездейсоқ болуы мүмкін).

Рөлдердің тізімін әрі қарай қосалқы Басқару серверлеріне жіберу опциясын өшірсеңіз, барлық пайдаланушы рөлі қосалқы басқару серверлерінде қала береді, бірақ негізгі басқару серверіндегі рөлдерден тәуелсіз болады. Қосалқы Басқару серверлеріндегі рөлдер тәуелсіз болған кезде, оларды өзгертуге немесе жоюға болады.

Есептік жазбаның құпиясөзін ауыстыру

Жергілікті есептік жазбаның құпиясөзін өзгертуге болады, мысалы, пайдаланушы жергілікті есептік жазба құпиясөзін ұмытып қалғанда немесе құпиясөзді кесте бойынша өзгерту үшін.

Құпиясөзді өзгерту пайдаланушы есептік жазбаға кірмеген жағдайда да қолданылады. Сондай-ақ, root жергілікті есептік жазбасы үшін құпиясөзді өзгертуге болады.

Бұл тапсырманы тек Linux басқаруымен жұмыс істейтін құрылғыларда орындауға болады.

Белгілі бір құрылғыларда жергілікті есептік жазба құпиясөзін өзгерту үшін:

1. Бағдарламаның негізгі терезесінде **Тапсырмалар** бөліміне өтіңіз.
2. **Қосу** түймесін басыңыз.

   Жаңа тапсырма жасау шебері іске қосылады.
3. **Тапсырма түрі** өрісінде **Есептік жазба құпиясөзін өзгерту (тек Linux)** тармағын таңдаңыз.
4. Келесі нұсқалардың бірін таңдаңыз:

   - **Басқару тобына тапсырманы белгілеу**

     Тапсырма бұрын жасалған басқару тобына кіретін құрылғыларға тағайындалады. Бар топтардың бірін көрсетуге немесе жаңа топ құруға болады.

     Мысалы, хабар белгілі бір басқару тобындағы құрылғыларға арналған болса, пайдаланушыларға хабар жіберу тапсырмасын іске қосу үшін осы параметрді пайдалануға болады.

     Тапсырма Басқару тобына тағайындалса, **Қауіпсіздік** қойындысы тапсырма сипаттары терезесінде көрсетілмейді, себебі топтық тапсырмалар олар тиесілі болып саналатын қауіпсіздік топтарының параметрлеріне бағынады.

   - **Құрылғының мекенжайларын қолмен белгілеу немесе тізімнен импорттау**

     Сіз DNS атауларын, IP мекенжайларын, сондай-ақ тапсырманы тағайындауды қажет ететін құрылғылардың IP мекенжайы ауқымдарын белгілей аласыз.

     Бұл параметрді белгіленген ішкі желі үшін тапсырманы орындау үшін пайдалануға болады. Мысалы, сіз бухгалтерлердің құрылғыларына белгілі бір бағдарламаны орната аласыз немесе вирус жұқтыруы мүмкін ішкі желідегі құрылғыларды тексере аласыз.

   - **Құрылғы таңдауына тапсырманы белгілеу**

     Тапсырма құрылғы таңдауларына кіретін құрылғыларға тағайындалады. Қолданыстағы таңдаулардың бірін көрсетуге болады.

Мысалы, операциялық жүйенің белгілі бір нұсқасы бар құрылғыларда тапсырманы іске қосу үшін осы параметрді пайдалануға болады.

Есептік жазба құпиясөзін өзгерту (тек Linux) тапсырмасы көрсетілген құрылғылар үшін жасалады. **Басқару тобына тапсырманы белгілеу** параметрін таңдаған болсаңыз, тапсырма топтық болып саналады.

5. **Тапсырма ауқымы** қадамында басқару тобын, нақты мекенжайлары бар құрылғыларды немесе құрылғылар таңдауын көрсетіңіз.

   Қолжетімді параметрлер алдыңғы қадамда таңдалған параметрлерге байланысты.

6. **Есептік жазба аты мен жаңа құпиясөзді енгізіңіз** қадамында келесі параметрлерді көрсетіңіз:

   - **Есептік жазбаның атауы** өрісінде құпиясөзді өзгерткіңіз келетін есептік жазбаның атауын енгізіңіз.
   - **Жаңа құпиясөз** жолында алдыңғы өрісте көрсетілген есептік жазба үшін орнатылатын құпиясөзді енгізіңіз.

     Енгізген құпиясөзді қарау үшін **Көрсету** түймесін басып тұрыңыз.
   - Қажет болса, **Бір реттік құпиясөз ретінде орнату (пайдаланушы есептік жазбаға бірінші кіргеннен кейін, құпиясөзді өзгертуі керек)** құсбелгісін қойыңыз.

     - **Бір реттік құпиясөз ретінде орнату (пайдаланушы есептік жазбаға бірінші кіргеннен кейін, құпиясөзді өзгертуі керек)**

       Егер бұл құсбелгі таңдалса, пайдаланушыдан бірінші рет кіргеннен кейін жаңа құпиясөзді өзгерту сұралады.

       Бұл құсбелгі алынып тасталса, пайдаланушыдан бірінші рет кіргеннен кейін жаңа құпиясөзді өзгерту сұралмайды.

       Әдепкі бойынша, жалауша алынып тасталған.

7. Тапсырма жасау және шеберді абу үшін **Тапсырманы жасауды аяқтау** қадамында **Аяқтау** түймесін басыңыз.

   Жасап болған соң, тапсырма туралы мәліметтерді ашу параметрі қосулы болса, тапсырма параметрлері терезесі ашылады. Бұл терезеде тапсырма параметрлерін тексеруге, оларды өзгертуге немесе қажет болса, тапсырманы іске қосу кестесін конфигурациялауға болады.

8. Тапсырмалар тізімінде жасалған тапсырманы таңдап, **Іске қосу** түймесін басыңыз.

   Немесе тапсырма параметрлерінде көрсетілген кестеге сәйкес тапсырманың іске қосылуын күтіңіз.

Есептік жазба құпиясөзін өзгерту тапсырмасы аяқталғанда, құпиясөз таңдалған құрылғыларда көрсетілген жергілікті есептік жазба үшін өзгертіледі.

Есептік жазба құпиясөзін өзгерту тапсырмаларының дұрыс жұмыс істеуін қамтамасыз ету үшін пайдаланушы құрылғысында SELinux өшірілуі керек.

Жергілікті әкімші құқықтарын кері қайтарып алу

Есептік жазбалар үшін жергілікті әкімші құқықтарын жоюға болады. Бұл пайдаланушы есептік жазбаларын бақылаудың қосымша деңгейін береді. Мысалы, бір реттік тапсырманы орындағаннан кейін жергілікті әкімші құқықтарын жоя аласыз.

Бұл тапсырма іске қосылғанда, көрсетілген жергілікті есептік жазба Желілік агент саясатының параметрлерінде анықталған әкімшілердің жергілікті топтарына жататынын-жатпайтынын тексеру үшін тексеріледі. Әкімшілердің жергілікті топтары тізімін Желілік агент саясатының параметрлерінде конфигурациялай аласыз. Сондай-ақ, артықшылықты пайдаланушы есептік жазбаларының тізімін **Артықшылықтары бар құрылғы пайдаланушылары туралы есеп (тек Linux)** арқылы тексеруге болады.

Бұл тапсырманы тек Linux басқаруымен жұмыс істейтін құрылғыларда орындауға болады.

Белгілі бір құрылғылардағы жергілікті әкімші құқықтарын жою үшін:

1. Бағдарламаның негізгі терезесінде **Тапсырмалар** бөліміне өтіңіз.
2. **Қосу** түймесін басыңыз.

   Жаңа тапсырма жасау шебері іске қосылады.
3. **Тапсырма түрі** өрісінде **Жергілікті әкімші құқықтарын қайтарып алу (тек Linux)** таңдаңыз.
4. Келесі нұсқалардың бірін таңдаңыз:

   - **Басқару тобына тапсырманы белгілеу**

     Тапсырма бұрын жасалған басқару тобына кіретін құрылғыларға тағайындалады. Бар топтардың бірін көрсетуге немесе жаңа топ құруға болады.

     Мысалы, хабар белгілі бір басқару тобындағы құрылғыларға арналған болса, пайдаланушыларға хабар жіберу тапсырмасын іске қосу үшін осы параметрді пайдалануға болады.

     Тапсырма Басқару тобына тағайындалса, **Қауіпсіздік** қойындысы тапсырма сипаттары терезесінде көрсетілмейді, себебі топтық тапсырмалар олар тиесілі болып саналатын қауіпсіздік топтарының параметрлеріне бағынады.

   - **Құрылғының мекенжайларын қолмен белгілеу немесе тізімнен импорттау**

     Сіз DNS атауларын, IP мекенжайларын, сондай-ақ тапсырманы тағайындауды қажет ететін құрылғылардың IP мекенжайы ауқымдарын белгілей аласыз.

     Бұл параметрді белгіленген ішкі желі үшін тапсырманы орындау үшін пайдалануға болады. Мысалы, сіз бухгалтерлердің құрылғыларына белгілі бір бағдарламаны орната аласыз немесе вирус жұқтыруы мүмкін ішкі желідегі құрылғыларды тексере аласыз.

   - **Құрылғы таңдауына тапсырманы белгілеу**

     Тапсырма құрылғы таңдауларына кіретін құрылғыларға тағайындалады. Қолданыстағы таңдаулардың бірін көрсетуге болады.

     Мысалы, операциялық жүйенің белгілі бір нұсқасы бар құрылғыларда тапсырманы іске қосу үшін осы параметрді пайдалануға болады.

   Көрсетілген құрылғылар үшін тапсырма жасалады: *Жергілікті әкімші құқықтарын кері қайтарып алу (тек Linux үшін)*. **Басқару тобына тапсырманы белгілеу** параметрін таңдаған болсаңыз, тапсырма топтық болып саналады.
5. **Тапсырма ауқымы** қадамында басқару тобын, нақты мекенжайлары бар құрылғыларды немесе құрылғылар таңдауын көрсетіңіз.

   Қолжетімді параметрлер алдыңғы қадамда таңдалған параметрлерге байланысты.

6. Шебердің осы қадамында келесі параметрлерді көрсетіңіз:

   - **Жұмыс режимі** параметрлер тобында жұмыс режимін таңдаңыз:

     - **Берілген есептік жазбалардан жергілікті әкімші құқықтарын қайтарып алу**

       Бұл параметр таңдалса, жергілікті әкімші құқықтары көрсетілген жергілікті есептік жазбалар үшін жойылады.

       Әдепкі бойынша, осы нұсқа таңдалған.

     - **Жергілікті әкімші құқықтарын қайтарып алудан берілген есептік жазбаларды шығару**

       Бұл параметр таңдалса, жергілікті әкімші құқықтары көрсетілгендерден басқа барлық жергілікті есептік жазбалар үшін жойылады.

       Әдепкі бойынша нұсқа таңдалмаған.

   - Жергілікті есептік жазбаларды көрсетіңіз:

     - **Қосу** түймесін басыңыз.

     - Ашылған терезеде келесі әрекеттердің бірін орындаңыз:

       - **Есептік жазбаның атауы** өрісінде жергілікті есептік жазбаңыздың атауын көрсетіңіз.

       - **Есептік жазба әрекеті** параметрлер тобында (**Берілген есептік жазбалардан жергілікті әкімші құқықтарын қайтарып алу** параметрі таңдалған жағдайда қолжетімді) әрекетті таңдаңыз.

       - **Есептік жазбаны сақтау**

         Бұл параметр таңдалса, жергілікті әкімші құқықтары жойылғаннан кейін жергілікті есептік жазба жойылмайды.

         Әдепкі бойынша, осы нұсқа таңдалған.

       - **Есептік жазбаны жою**

         Бұл параметр таңдалса, жергілікті есептік жазба жергілікті әкімші құқықтарының бар-жоғына қарамастан жойылады.

         Әдепкі бойынша нұсқа таңдалмаған.

7. Тапсырма жасау және шеберді абу үшін **Тапсырманы жасауды аяқтау** қадамында **Аяқтау** түймесін басыңыз.

   Жасап болған соң, тапсырма туралы мәліметтерді ашу параметрі қосулы болса, тапсырма параметрлері терезесі ашылады. Бұл терезеде тапсырма параметрлерін тексеруге, оларды өзгертуге немесе қажет болса, тапсырманы іске қосу кестесін конфигурациялауға болады.

8. Тапсырмалар тізімінде жасалған тапсырманы таңдап, **Іске қосу** түймесін басыңыз.

   Немесе тапсырма параметрлерінде көрсетілген кестеге сәйкес тапсырманың іске қосылуын күтіңіз.

Тапсырма аяқталғаннан кейін таңдалған құрылғылардағы көрсетілген жергілікті есептік жазбалар үшін жергілікті әкімші құқықтары жойылады.

Kerberos домен аутентификациясын конфигурациялау

Kaspersky Security Center Linux бағдарламасы Kerberos протоколы арқылы домен аутентификациясын пайдалануға мүмкіндік береді. Домен аутентификациясы корпоративтік желіде құпиясөзді қайта енгізбей (бірыңғай кіру), Kaspersky Security Center Web Console серверінде қауіпсіз аутентификацияны қосуға мүмкіндік береді.

Алдымен домен контроллерін Kerberos пайдалану және пернетақта файлын жасау үшін конфигурациялау керек. Қосымша ақпарат алу үшін домен контроллеріне арналған құжаттаманы қараңыз.

Microsoft Active Directory үшін SCRIL (өзара әрекетті кіру үшін смарт карталар қажет) қолдау көрсетіледі.

FreeIPA және AldPro үшін пернетақта файлын жасау

Пернетақта файлын жасау үшін:

1. Домен контроллеріне кіру үшін IAM пайдаланатын пайдаланушы есептік жазбасын жасаңыз.
2. Басқару сервері FreeIPA/AldPro доменінен тыс болса, DNS жазбасын және хост жазбасын қосыңыз:

   ```
   ipa dnsrecord-add <zoneName> <recordName> --a-rec < Басқару сервері IP мекенжайы >
   ipa host-add --password=<password> < Басқару сервері хост мекенжайы >
   ```

3. Басқару серверіне арналған HTTP қызметін жасаған кезде, PAC түрін көрсетіңіз:

   ```
   ipa service-add HTTP/< Басқару сервері хосты FQDN >@< ДОМЕН БАС ӘРІПТЕРМЕН ЖАЗЫЛҒАН > --ok-to-auth-as-delegate=true --pac-type PAD
   ```

4. Аутентификация үшін пайдаланушы есептік жазбасын көрсетіңіз:

   ```
   ipa service-allow-retrieve-keytab HTTP/< Басқару сервері хостының мекенжайы >@< ДОМЕН БАС ӘРІПТЕРМЕН ЖАЗЫЛҒАН > --user=<user>
   ```

5. Пернетақта файлын экспорттаңыз:

   ```
   ipa-getkeytab -s < домендік контроллер мекенжайы > -p HTTP/< Басқару сервері хосты мекенжайы >@< ДОМЕН БАС ӘРІПТЕРМЕН ЖАЗЫЛҒАН > -k /tmp/h.keytab
   ```

Microsoft Active Directory үшін пернетақта файлын жасау

Пернетақта файлын жасау үшін:

1. IAM домен контроллерімен байланысу үшін қолданатын пайдаланушы есептік жазбасын жасаңыз.
2. Пайдаланушы есептік жазбасы үшін келесі опцияларды қосыңыз:
   - **Пайдаланушы құпиясөзді өзгерте алмайды**
   - **Kerberos AES 256 разрядты шифрлау**

   Құпиясөз мерзімі аяқталған сайын пернетақта файлын қайта шығаруға жол бермеу үшін **Құпиясөз мерзімі ешқашан аяқталмайды** опциясын қосуға болады.
3. Пайдаланушы есептік жазбасына қызметтің негізгі атауын (SPN) қосыңыз:

   ```
   setspn -S HTTP/< Басқару сервері хосты FQDN > < ДОМЕН БАС ӘРІПТЕРМЕН ЖАЗЫЛҒАН >\<user>
   ```
4. Пернетақта файлын экспорттаңыз:

   ```
   ktpass -out C:\<folder>\< keytab файлы атауы > -princ HTTP/< Басқару сервері хосты FQDN >@< ДОМЕН БАС ӘРІПТЕРМЕН ЖАЗЫЛҒАН > -mapuser < ДОМЕН БАС ӘРІПТЕРМЕН ЖАЗЫЛҒАН >\<user> -crypto AES256-SHA1 -ptype KRB5_NT_PRINCIPAL -pass <password> -mapop set
   ```

Samba үшін пернетақта файлын жасау

Пернетақта файлын жасау үшін:

1. IAM домен контроллерімен байланысу үшін қолданатын пайдаланушы есептік жазбасын жасаңыз:

   ```
   samba-tool user add <user>
   ```
2. SPN-ді пайдаланушы есептік жазбасына қосыңыз:

   ```
   samba-tool spn add HTTP/< Басқару сервері хосты FQDN > <user>
   ```
3. Пернетақта файлын экспорттаңыз:

   ```
   samba-tool domain exportkeytab /tmp/file.keytab --principal=HTTP/< Басқару сервері хосты FQDN >
   ```

Kerberos домен аутентификациясын қосу

Kerberos домен аутентификациясын қосу үшін:

1. Домен контроллері сауалнамасын жүргізіңіз.
2. Негізгі мәзірдегі **Параметрлер** → **Бірыңғай кіру** бөліміне өтіңіз.

3. **Kerberos аутентификациясы** опциясын қосыңыз.

4. Пернетақта файлын жүктеп салыңыз.

5. Kaspersky Security Center Web Console-ге кіруге мүмкіндік беретін рөлді домен пайдаланушыларына тағайындаңыз.

   Kerberos домен аутентификациясы домен пайдаланушылары үшін қосылған.

Kaspersky дерекқорлары мен бағдарламаларын жаңарту

Бұл бөлімде тұрақты жаңартулар үшін орындау керек қадамдар сипатталған:

- Kaspersky дерекқорлары мен бағдарламалық модульдері;
- Kaspersky Security Center Linux құрамдастары мен қауіпсіздік бағдарламаларын қоса алғанда, Kaspersky орнатылған бағдарламалары.

Жаңарту функционалдығы (антивирустық қолтаңба жаңартуларын және код дерекқоры жаңартуларын қоса) және KSN функционалдығы АҚШ аймағындағы бағдарламада қолжетімді болмауы мүмкін.

Сценарий: Kaspersky бағдарламалары мен дерекқорларын үнемі жаңартып тұру

Бұл бөлімде Kaspersky дерекқорлары, бағдарламалық модульдері мен бағдарламаларын үнемі жаңартып тұру сценарийі ұсынылған. Сіз Ұйымның желісінде қорғанысты конфигурациялау сценарийін аяқтағаннан кейін, Басқару серверлері мен басқарылатын құрылғыларды түрлі қауіптерден, сонымен қатар вирустардан, желілік шабуылдардан және фишингтік шабуылдардан қорғауды қамтамасыз ету үшін қорғаныс жүйесінің сенімділігін қамтамасыз етуге тиіссіз.

Желі қорғанысына, келесіні үнемі жаңартып тұру арқылы қолдау көрсетіледі:

- Kaspersky дерекқорлары мен бағдарламалық модульдері;
- Kaspersky Security Center Linux құрамдастары мен қауіпсіздік бағдарламаларын қоса алғанда, Kaspersky орнатылған бағдарламалары.

Сіз осы сценарийді аяқтағаннан кейін, келесіге сенімді бола аласыз:

- Сіздің желіңіз Kaspersky Security Center Linux құрамдастары мен қауіпсіздік бағдарламаларын қоса алғанда, Kaspersky ең соңғы бағдарламалық жасақтамасымен қорғалған.
- Желі қауіпсіздігі үшін критикалық тұрғыдан маңызды болып саналатын Kaspersky антивирустық дерекқорлары мен басқа да дерекқорлары, әрдайым өзекті.

Алдын ала талаптар

Басқарылатын құрылғылардың Басқару серверімен қосылымы болуы тиіс. Құрылғылардың қосылымы болмаса, Kaspersky дерекқорлары, бағдарламалық модульдері мен бағдарламаларын қолмен немесе тікелей Kaspersky жаңарту серверлерінен жаңарту мүмкіндігін қарастырып көріңіз.

Басқару серверінің интернетке қосылымы болуы тиіс.

Бастамас бұрын, келесі әрекеттерді орындағаныңызға көз жеткізіңіз:

1. Kaspersky Security Center Web Console көмегімен Kaspersky бағдарламалық жасақтамасын орналастыру сценарийіне сәйкес басқарылатын құрылғыларда Kaspersky қауіпсіздік бағдарламалары орналастырылды.

2. Желі қорғанысын конфигурациялау сценарийіне сәйкес барлық қажетті саясаттар, саясат профильдері және тапсырмалар жасалған және конфигурацияланған.

3. Басқарылатын құрылғылардың санына және желі топологиясына сәйкес тарату нүктелерінің тиісті саны тағайындалған.

Kaspersky бағдарламалары мен дерекқорларын жаңарту келесі кезеңдерден тұрады:

1. **Жаңарту схемасын таңдау**

   Қауіпсіздік бағдарламаларына арналған жаңартуларды орнату үшін пайдалануға болатын бірнеше схема бар. Желіңіздің талаптарына бәрінен жақсы сай келетін схеманы немесе бірнеше схеманы таңдап алыңыз.

2. **Жаңартуларды Басқару серверінің қоймасына жүктеп алу үшін тапсырма жасау**

   Бұл тапсырма Kaspersky Security Center бағдарламаны жылдам іске қосу шеберінде автоматты түрде жасалады. Бағдарламаны жылдам іске қосу шеберін іске қоспаған болсаңыз, тапсырманы дәл қазір жасаңыз.

   Бұл тапсырма жаңартуларды Kaspersky жаңартулар серверлерінен Басқару сервері қоймасына, сондай-ақ Kaspersky Security Center Linux үшін дерекқорлар мен бағдарламалық модульдердің жаңартуларын жүктеп алуға қажет. Жаңартуларды жүктегеннен кейін, оларды басқарылатын құрылғыларға таратуға болады.

   Сіздің желіңізде тарату нүктелері тағайындалған болса, жаңартулар Басқару серверінің қоймасынан тарату нүктелерінің қоймаларына автоматты түрде жүктеледі. Бұл жағдайда, тарату нүктесінің ауқымына кіретін басқарылатын құрылғылар Басқару серверінің қоймасы орнына жаңартуларды тарату нүктелерінің қоймаларынан жүктеп алады.

   Нұсқаулар: Жаңартуларды Басқару серверінің қоймасына жүктеп алу үшін тапсырма жасау.

3. **Жаңартуларды тарату орындарының қоймаларына жүктеп алу тапсырмасын жасау (қажет болса)**

   Әдепкі бойынша, жаңартулар Басқару сервері қоймасынан тарату нүктелерінің қоймаларына жүктеледі. Сіз Kaspersky Security Center Linux бағдарламасын, тарату нүктелері жаңартуларды тікелей Kaspersky жаңарту серверлерінен жүктейтін етіп конфигурациялай аласыз. Басқару сервері мен тарату нүктелері арасындағы трафик Kaspersky жаңарту серверлері мен тарату нүктелері арасындағы трафиктен қымбатырақ болса немесе Басқару серверіңізде интернетке қатынасу мүмкіндігі болмаса, жаңартулары тарату нүктелерінің қоймаларынан жүктеп алу артық көрінеді.

   Сіздің желіңізге тарату нүктелері тағайындалып, *Жаңартуларды тарату нүктесінің қоймаларына жүктеп алу* тапсырмасы жасалған кезде, тарату нүктелері жаңартуларды Басқару сервері қоймасынан емес, Kaspersky жаңарту серверлерінен жүктейді.

   Нұсқаулар: Жаңартуларды тарату орындарының қоймаларына жүктеп алу тапсырмасын жасау

4. **Тарату нүктелерін конфигурациялау**

   Сіздің желіңізге тарату нүктелері тағайындалған болса, **Қосулы** параметрі барлық қажетті тарату нүктелеріндегі сипаттарда қосылғанына көз жеткізіңіз. Егер бұл параметр тарату нүктесі үшін өшірулі болса, тарату нүктесінің ауқымына қосылған құрылғылар Басқару сервері қоймасынан жаңартуларды жүктейді.

5 Жаңарту процесін айырмашылық файлдары арқылы оңтайландыру (қажет болса)

Басқару сервері мен басқарылатын құрылғылар арасындағы трафикті айырмашылық файлдарын пайдаланып оңтайландыруға болады. Бұл функция қосылған кезде, Басқару сервері немесе тарату нүктесі Kaspersky бүкіл дерекқор файлдарының немесе бағдарламалық модульдерінің орнына айырмашылық файлдарын жүктейді. Айырмашылықтар файлы дерекқор немесе бағдарламалық модуль файлдарының екі нұсқасы арасындағы айырмашылықтарды сипаттайды. Сондықтан, айырмашылық файлдары бүкіл файлдарға қарағанда аз орын алады. Нәтижесінде, Басқару сервері немесе тарату нүктелері және басқарылатын құрылғылар арасындағы трафик азаяды. Бұл функцияны пайдалану үшін *Жаңартуларды Басқару серверінің қоймасына жүктеп алу* және/немесе *Жаңартуларды тарату нүктесінің қоймаларына жүктеп алу* тапсырмасының сипаттарындағы **diff файлдарды жүктеп алу** параметрін қосыңыз.

Нұсқаулар: Kaspersky дерекқорлары мен бағдарламалық модульдерін жаңарту үшін айырмашылық файлдарын пайдалану

6 Қауіпсіздік бағдарламалары үшін жаңартуларды автоматты түрде орнатуды конфигурациялау

Kaspersky бағдарламалық модульдерін және дерекқорларын, соның ішінде антивирустық базаларды уақтылы жаңартуды қамтамасыз ету мақсатында, басқарылатын бағдарламалар үшін *Жаңарту* тапсырмасын жасаңыз. Уақтылы жаңарту үшін тапсырмалар кестесін конфигурациялау кезінде **Қоймаға жаңа жаңартуларды жүктеп алу уақыты** опциясын таңдау ұсынылады.

Егер жаңарту Лицензиялық келісімнің шарттарын қабылдауды талап етсе, алдымен Лицензиялық келісімнің шарттарын оқып, қабылдауыңыз қажет. Осыдан кейін, жаңартулар басқарылатын құрылғыларға таратылуы мүмкін.

7 Kaspersky басқаратын қолданбаларының жаңартуларын мақұлдау және қабылдамау

Әдепкі бойынша, жүктелген бағдарламалық жасақтама жаңартулары *Анықталмаған* күйіне ие. Жаңарту күйін *Расталды* немесе *Қабылданбады* күйіне өзгертуге болады. Бекітілген жаңартулар әрқашан орнатылады. Kaspersky басқаратын қолданбалары жаңарту Лицензиялық келісімнің шарттарын қабылдауды талап етсе, алдымен Лицензиялық келісімнің шарттарын оқып, қабылдау керек. Осыдан кейін, жаңартулар басқарылатын құрылғыларға таратылуы мүмкін. Сіз *Қабылданбады* деп белгілеген жаңартулар, басқарылатын құрылғыларға орнатылмайды. Егер басқарылатын қолданба үшін бұрын қабылданбаған жаңарту орнатылған болса, Kaspersky Security Center Linux барлық қолданбасы құрылғылардан жаңартуларды жоюға тырысады.

Жаңартуларды мақұлдау және қабылдамау Windows операциялық жүйесімен жұмыс істейтін клиент құрылғыларына орнатылған желілік агент пен Kaspersky басқарылатын қолданбалары үшін ғана қолжетімді. Басқару серверін, Kaspersky Security Center Web Console веб-консолін және веб-басқару плагиндерін үздіксіз жаңартуға қолдау көрсетілмейді.

Нұсқаулар: Бағдарламалық жасақтама жаңартуын мақұлдау және қабылдамау.

Кейде желілік агент жаңартуынан кейін сізден басқарылатын құрылғыларды қайта іске қосу сұралуы мүмкін. Қайта іске қосу қажеттігі туралы көрсетілген хабарландырудағы **Құрылғыларды көру** сілтемесін басыңыз, қайта іске қосылатын құрылғылардың жанындағы құсбелгі ұяшықтарын таңдаңыз, содан кейін желілік агент жаңартуын аяқтау үшін **Қайта іске қосу** түймесін басыңыз.

Нәтижелер

Сценарий аяқталғаннан кейін Kaspersky Security Center Linux жүйесі жаңартулар Басқару серверінің қоймасына жүктелгеннен кейін Kaspersky дерекқорларын жаңарту үшін конфигурацияланды. Енді сіз желі жұмысын бақылауға кірісе аласыз.

Kaspersky дерекқорларын, бағдарламалық модульдерін және бағдарламаларын жаңарту туралы

Басқару серверлері мен басқарылатын құрылғыларды қорғау жаңартылған күйде екеніне көз жеткізу үшін келесі жаңартуларды уақтылы ұсыну керек:

- Kaspersky дерекқорлары мен бағдарламалық модульдері;

  Kaspersky Security Center Linux бағдарламасы Kaspersky дерекқорлары мен бағдарламалық модульдерін жүктемес бұрын Kaspersky серверлерінің қолжетімділігін тексереді. Жүйелік DNS арқылы серверлерге қатынасу мүмкін болмаса, бағдарлама жалпыға ортақ DNS серверлерін пайдаланады. Бұл антивирустық дерекқорларды жаңарту және басқарылатын құрылғылардың қауіпсіздік деңгейін сақтау үшін қажет.

- Kaspersky Security Center Linux құрамдастары мен қауіпсіздік бағдарламаларын қоса алғанда, Kaspersky орнатылған бағдарламалары.

  Kaspersky Security Center Linux сізге Windows жүйесімен жұмыс істейтін клиент құрылғыларына орнатылған Желілік агент пен Kaspersky қолданбаларын автоматты түрде жаңартуға мүмкіндік береді. Басқару серверін, Kaspersky Security Center Web Console веб-консолін және веб-басқару плагиндерін үздіксіз жаңартуға қолдау көрсетілмейді. Бұл компоненттерді жаңарту үшін, олардың соңғы нұсқаларын Kaspersky сайтынан жүктеп алу және қолмен орнату керек.

Желіңіздің конфигурациясына байланысты сіз келесі жүктеу схемаларын қолдана аласыз және басқарылатын құрылғыларға қажетті жаңартуларды тарата аласыз:

- Бір тапсырмамен: *Жаңартуларды Басқару серверінің қоймасына жүктеп алу*
- Екі тапсырманың көмегімен:
  - *Жаңартуларды Басқару серверінің қоймасына жүктеп алу* тапсырмалары.
  - *Жаңартуларды тарату нүктесінің қоймаларына жүктеп алу* тапсырмалары.
- Жергілікті қалта, ортақ қатынасы бар қалта немесе FTP сервері арқылы қолмен
- Басқарылатын құрылғылардағы Kaspersky Endpoint Security үшін Kaspersky жаңарту серверлерінен тікелей
- Басқару сервері интернетке қатынаса алмаса, жергілікті немесе желілік қалта арқылы

Жаңартуларды Басқару серверінің қоймасына жүктеп алу тапсырмасын пайдалану

Бұл схемада Kaspersky Security Center Linux жаңартуларды *Жаңартуларды Басқару серверінің қоймасына жүктеп алу* тапсырмасы арқылы жүктейді. Желінің бір сегментінде 300-ден аз басқарылатын құрылғы немесе әр сегментте оннан аз басқарылатын құрылғы бар шағын желілерде, жаңартулар басқарылатын құрылғыларға тікелей Басқару серверінің қоймасынан таралады (төмендегі суретті қараңыз).



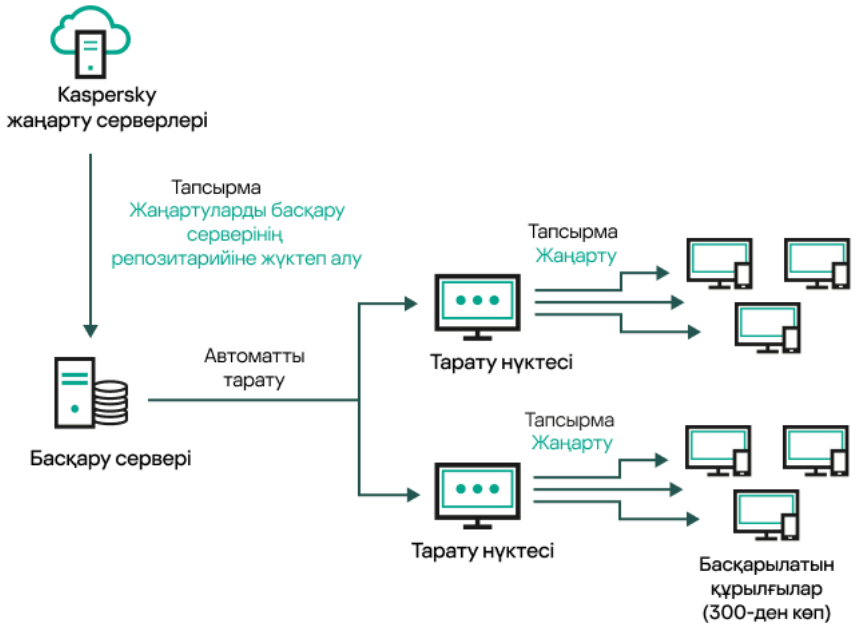
Жаңартуларды Басқару серверінің қоймасына жүктеп алу тапсырмасын қолдану арқылы және тарату нүктелерінсіз жаңарту

Жаңарту көзі ретінде сіз Kaspersky жаңарту серверлерін ғана емес, сонымен қатар жергілікті немесе желілік қалтаны да пайдалана аласыз.

Әдепкі бойынша, Басқару сервері Kaspersky жаңарту серверлерімен өзара әрекеттеседі және HTTPS жаңартуларын жүктейді. Басқару серверін HTTPS орнына HTTP протоколын пайдалану үшін конфигурациялауға болады.

Егер сіздің желіңізде бір желі сегментінде 300-ден астам басқарылатын құрылғы болса немесе сіздің желіңізде тоғыздан астам басқарылатын құрылғысы бар бірнеше сегмент болса, жаңартуларды басқарылатын құрылғыларға тарату үшін тарату нүктелерін пайдалануды ұсынамыз (төмендегі суретті қараңыз). Тарату нүктелері Басқару серверіне түсетін жүктемені азайтады және Басқару сервері мен басқарылатын құрылғылар арасындағы трафикті оңтайландырады. Тарату нүктелерінің санын және олардың желіңізге қажетті конфигурациясын есептеуіңізге болады.

Бұл схемада жаңартулар Басқару сервері қоймасынан тарату нүктесінің қоймаларына автоматты түрде жүктеледі. Тарату нүктесінің ауқымына кіретін басқарылатын құрылғылар Басқару серверінің қоймасы орнына жаңартуларды тарату нүктелерінің қоймаларынан жүктеп алады.



Тарату нүктелері бар *Жаңартуларды Басқару серверінің қоймасына жүктеп алу* тапсырмасын қолдану арқылы жаңарту

Жаңартуларды Басқару серверінің қоймасына жүктеп алу тапсырмасын орындағаннан кейін Kaspersky дерекқорларының жаңартулары және Kaspersky Endpoint Security үшін бағдарламалық модульдер Басқару серверінің қоймасына жүктелген. Бұл жаңартулар Kaspersky Endpoint Security *Жаңарту* тапсырмасы арқылы орнатылады.

> *Жаңартуларды Басқару серверінің қоймасына жүктеп алу* тапсырмасы жүктеп алу тапсырмасы виртуалды Басқару серверлерінде қолжетімді емес. Виртуалды сервердің қоймасы негізгі Басқару серверіне жүктелген жаңартуларды көрсетеді.

Алынған жаңартуларды жұмысқа жарамдылық тұрғысынан және сынақ құрылғыларының жиынтығында қателердің болуы тұрғысынан тексеруге конфигурациялауға болады. Егер тексеру сәтті болса, жаңартулар басқа басқарылатын құрылғыларға таралады.

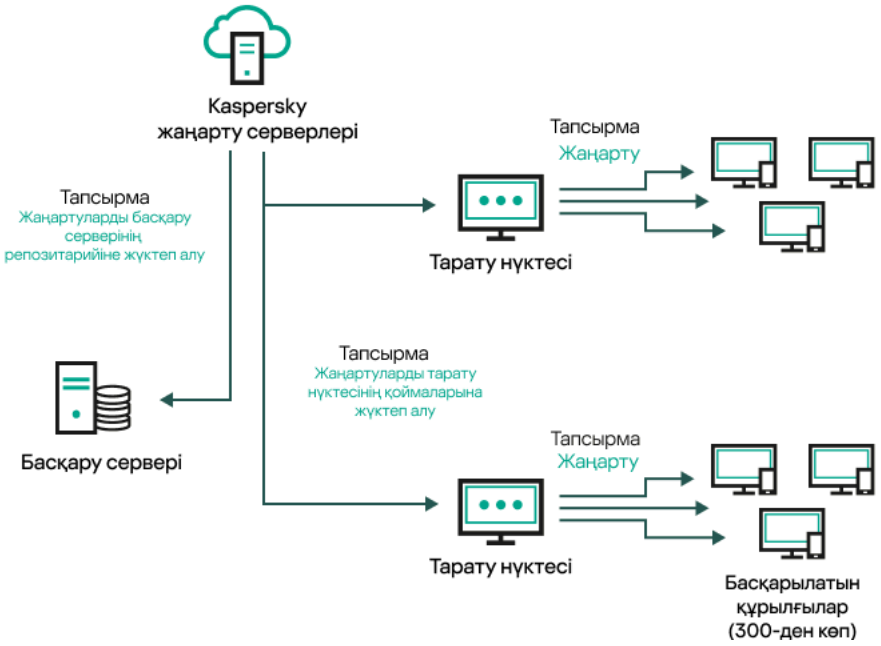
Әрбір басқарылатын Kaspersky бағдарламасы Басқару серверінен қажетті жаңартуларды сұрайды. Басқару сервері осы сұрауларды біріктіреді және тек бағдарламалар сұрайтын жаңартуларды жүктейді. Осылайша, тек қажетті жаңартулар және тек бір рет қана жүктелетіні қамтамасыз етіледі. *Жаңартуларды Басқару серверінің қоймасына жүктеп алу* тапсырмасын орындау кезінде Kaspersky дерекқорлары мен бағдарламалық модульдерінің қажетті нұсқаларының жүктелуін қамтамасыз ету үшін Kaspersky жаңарту серверлеріне автоматты түрде Басқару сервері мынадай ақпаратты жібереді:

- Бағдарламаның идентификаторы және нұсқасы
- Бағдарламаны орнату идентификаторы
- Белсенді кілт идентификаторы
- *Жаңартуларды Басқару серверінің қоймасына жүктеп алу* тапсырмасын іске қосу идентификаторы

Берілетін ақпарат дербес деректерді және басқа да құпия деректерді қамтымайды. АО "Лаборатория Касперского" алынған ақпаратты заңда белгіленген талаптарға сәйкес қорғайды.

Екі тапсырманы пайдалану: Жаңартуларды Басқару серверінің қоймасына жүктеп алу және Жаңартуларды тарату нүктесінің қоймаларына жүктеп алу

Тарату нүктелерінің қоймаларына жаңартуларды Басқару сервері қоймасының орнына тікелей Kaspersky жаңарту серверлерінен жүктеп алуға болады, содан кейін жаңартуларды басқарылатын құрылғыларға таратуға болады (төмендегі суретті қараңыз). Басқару сервері мен тарату нүктелері арасындағы трафик Kaspersky жаңарту серверлері мен тарату нүктелері арасындағы трафиктен қымбатырақ болса немесе Басқару серверіңізде интернетке қатынасу мүмкіндігі болмаса, жаңартулары тарату нүктелерінің қоймаларынан жүктеп алу артық көрінеді.



Тапсырманы пайдаланып жаңарту *Жаңартуларды Басқару серверінің қоймасына жүктеп алу* және тапсырма *Жаңартуларды тарату нүктесінің қоймаларына жүктеп алу*

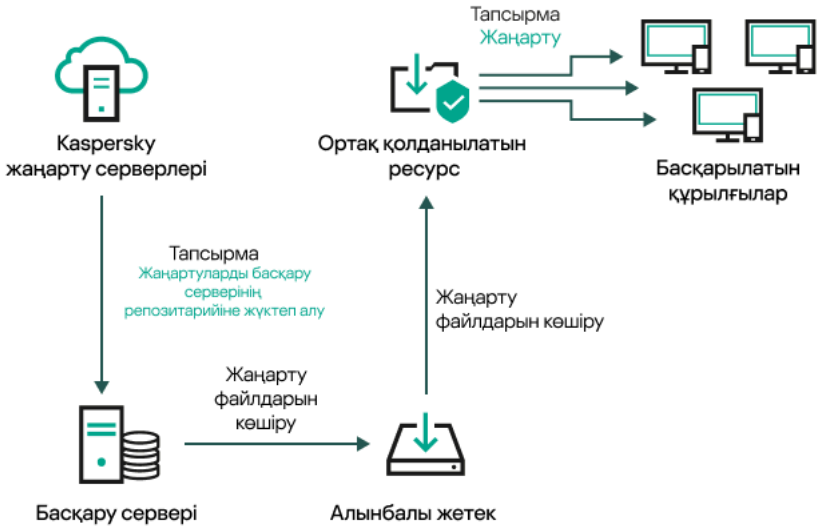
Әдепкі бойынша, Басқару сервері мен тарату нүктелері Kaspersky жаңарту серверлерімен өзара әрекеттеседі және HTTPS жаңартуларын жүктейді. Басқару серверін және/немесе тарату нүктелерін HTTPS орнына HTTP протоколын пайдалану үшін конфигурациялауға болады.

Бұл схеманы іске асыру үшін *Жаңартуларды Басқару серверінің қоймасына жүктеп алу* тапсырмасына қосымша ретінде *Жаңартуларды тарату нүктесінің қоймаларына жүктеп алу* тапсырмасын жасаңыз. Осыдан кейін, тарату нүктелері жаңартуларды Басқару серверінің қоймасынан емес, Kaspersky жаңарту серверлерінен жүктейді.

Бұл схема үшін де *Жаңартуларды Басқару серверінің қоймасына жүктеп алу* тапсырмасы керек, себебі бұл тапсырма Kaspersky Security Center Linux үшін Kaspersky дерекқорлары мен бағдарламалық модульдерін жүктеу үшін қолданылады.

Жергілікті қалта, ортақ қатынасы бар қалта немесе FTP сервері арқылы қолмен

Егер клиент құрылғылары Басқару серверіне қосылмаған болса, сіз жергілікті қалтаны немесе ортақ ресурсты Kaspersky дерекқорларын, бағдарламалық модульдерін және бағдарламаларын жаңарту көзі ретінде пайдалана аласыз. Бұл схемада қажетті жаңартуларды Басқару сервері қоймасынан алынбалы дискіге көшіру керек, содан кейін жаңартуларды жергілікті қалтаға немесе Kaspersky Endpoint Security параметрлерінде жаңарту көзі ретінде көрсетілген ортақ ресурсқа көшіру керек (төмендегі суретті қараңыз).



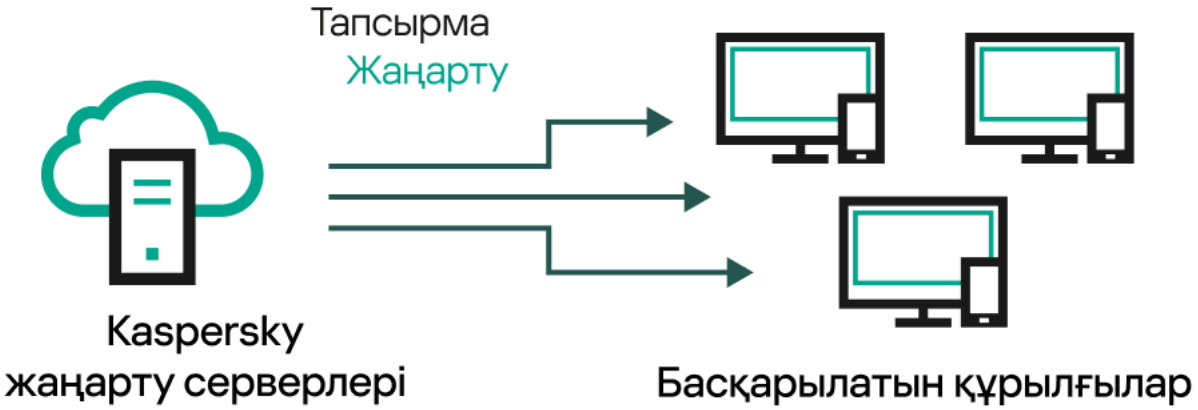
Жергілікті қалта, ортақ қатынасы бар қалта немесе FTP сервері арқылы жаңарту

Kaspersky Endpoint Security бағдарламасындағы жаңарту көздері туралы қосымша ақпарат алу үшін келесі анықтамаларды қараңыз:

- Kaspersky Endpoint Security for Linux онлайн-анықтамасы
- Kaspersky Endpoint Security for Windows онлайн-анықтамасы

Басқарылатын құрылғылардағы Kaspersky Endpoint Security үшін Kaspersky жаңарту серверлерінен тікелей

Басқарылатын құрылғыларда сіз Kaspersky Endpoint Security бағдарламасын Kaspersky жаңарту серверлерінен тікелей жаңартуларды алу үшін конфигурациялай аласыз (төмендегі суретті қараңыз).



Қауіпсіздік бағдарламаларын тікелей Kaspersky жаңарту серверлерінен жаңарту

Бұл схемада қауіпсіздік бағдарламасы Kaspersky Security Center Linux ұсынған қойманы пайдаланбайды. Жаңартуларды тікелей Kaspersky жаңарту серверлерінен алу үшін қауіпсіздік бағдарламасында жаңарту көзі ретінде Kaspersky жаңарту серверлерін көрсетіңіз. Осы параметрлер туралы қосымша ақпарат алу үшін анықтаманың келесі бөлімдерін қараңыз:

- Kaspersky Endpoint Security for Linux онлайн-анықтамасы
- Kaspersky Endpoint Security for Windows онлайн-анықтамасы

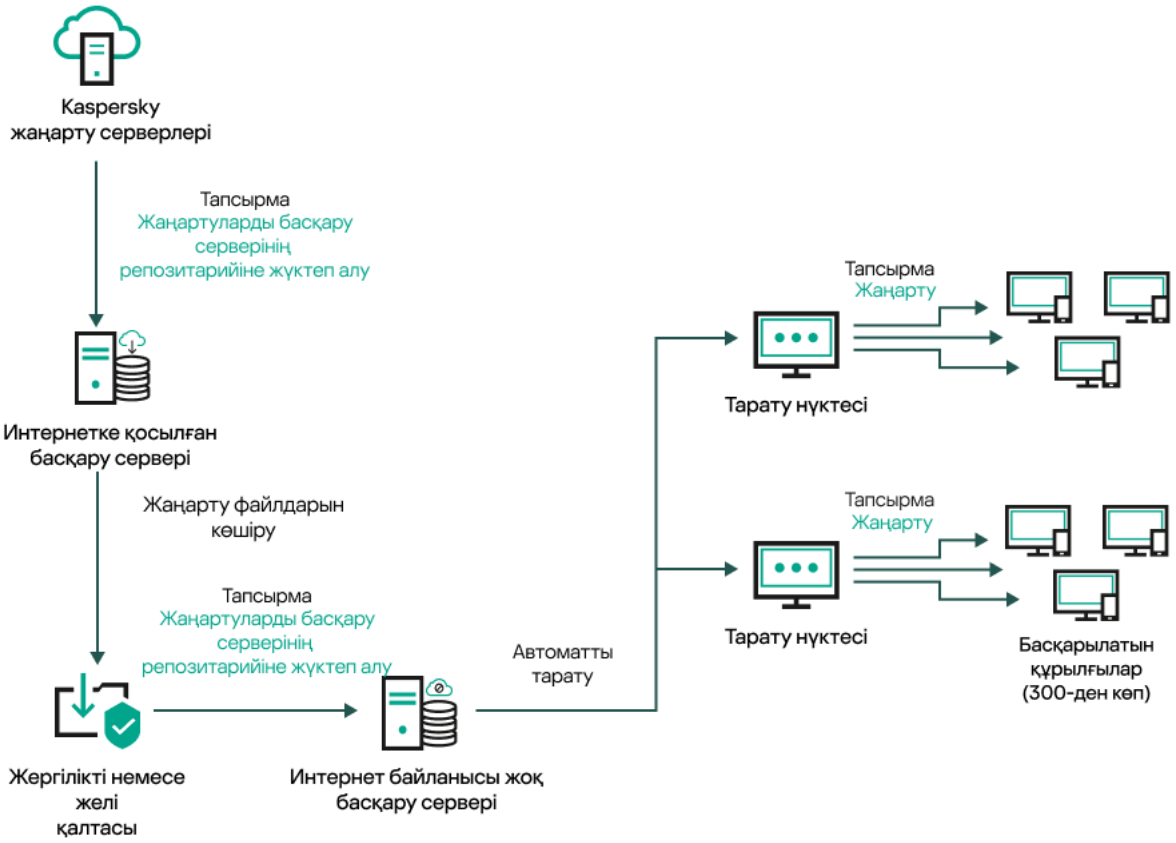
Басқару сервері интернетке қатынаса алмаса, жергілікті немесе желілік қалта арқылы

Басқару серверінде интернет қосылымы болмаса, жергілікті немесе желілік қалтадан жаңартуларды жүктеу үшін *Жаңартуларды Басқару серверінің қоймасына жүктеп алу* тапсырмасын конфигурациялауға болады. Бұл жағдайда, қажетті жаңарту файлдарын көрсетілген қалтаға мезгіл-мезгіл көшіріп тұру қажет. Мысалы, қажетті жаңарту файлдарын келесі көздердің бірінен көшіруге болады:

- Интернетке кіру мүмкіндігі бар Басқару сервері (төмендегі суретті қараңыз).

  Басқару сервері тек қауіпсіздік бағдарламалары сұрайтын жаңартуларды жүктейтіндіктен, Басқару серверлері басқаратын қауіпсіздік бағдарламаларының жиынтығы (интернетке қосылған және қосылмаған) сәйкес келуі керек.

  Сіз жаңартуларды жүктеу үшін қолданатын Басқару серверінің нұсқасы 13.2 немесе одан да бұрынғы болса, *Жаңартуларды Басқару серверінің қоймасына жүктеп алу* тапсырмасының сипаттарын ашып, **Ескі схеманы пайдаланып, жаңартуларды жүктеп алу** параметрін қосыңыз.



Басқару сервері интернетке қатынаса алмаса, жергілікті немесе желілік қалта арқылы жаңарту

- Kaspersky Update Utility

  Утилита жаңартуларды жүктеу үшін ескі схеманы қолданатындықтан, *Жаңартуларды Басқару серверінің қоймасына жүктеп алу* тапсырмасының сипаттарын ашып, *Ескі схеманы пайдаланып, жаңартуларды жүктеп алу* параметрін қосыңыз. Қажет болса, Kaspersky жаңарту утилитасы қажетті жаңартуларды жүктеп алуы үшін, *Жаңарту сұрауының файлын автоматты түрде жүктеп алу* опциясын конфигурациялауға да болады.

Жаңартуларды Басқару серверінің қоймасына жүктеп алу тапсырмасын жасау

Жаңартуларды Басқару серверінің қоймасына жүктеп алу тапсырма Kaspersky қауіпсіздік бағдарламасының дерекқорлары мен бағдарламалық модульдерінің жаңартуларын Kaspersky жаңарту серверлерінен Басқару серверінің қоймасына жүктеп алуға мүмкіндік береді.

Kaspersky Security Center бағдарламаны жылдам іске қосу шебері Басқару серверінің *Жаңартуларды Басқару серверінің қоймасына жүктеп алу* тапсырмасын автоматты түрде жасайды. Тапсырмалар тізімінде тек бір *Жаңартуларды Басқару серверінің қоймасына жүктеп алу* тапсырмасы болуы керек. Басқару сервері тапсырмаларының тізімінен жойылса, бұл тапсырманы қайта жасауға болады.

Жаңартуларды Басқару серверінің қоймасына жүктеп алу тапсырманы аяқтағаннан және жаңартуларды жүктегеннен кейін, оларды басқарылатын құрылғыларға таратуға болады.

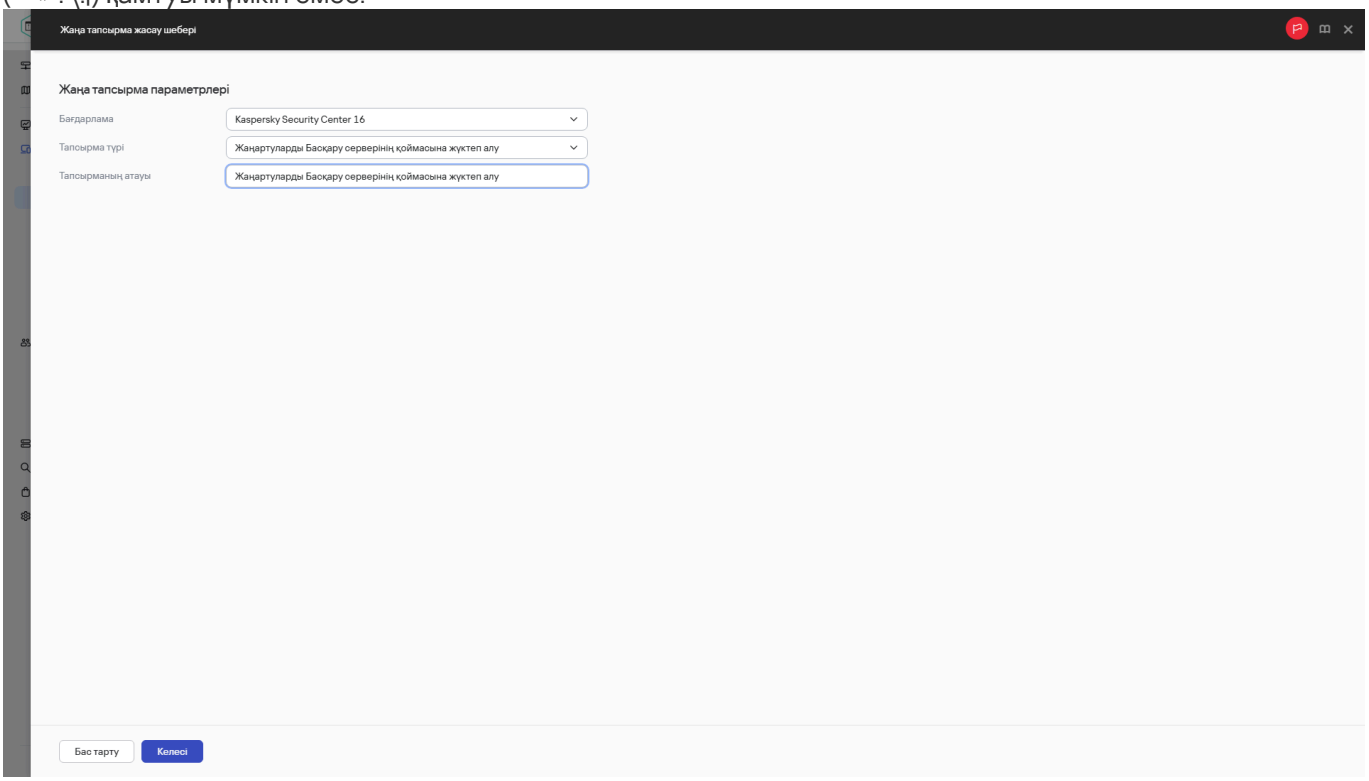
Жаңартуларды басқарылатын құрылғыларға таратпас бұрын, сіз *Жаңартуларды тексеру* тапсырмасын орындай аласыз. Соның арқасында, Басқару сервері жүктелген жаңартуларды дұрыс орнататындығына және қауіпсіздік деңгейі жаңартулардан төмендемейтіндігіне көз жеткізе аласыз. Таратудың алдында жаңартуларды тексеру үшін, *Жаңартуларды Басқару серверінің қоймасына жүктеп алу* тапсырмасының сипаттарында **Жаңарту тексерісін іске қосу** параметрін конфигурациялаңыз.

Жаңартуларды Басқару серверінің қоймасына жүктеп алу тапсырмасын жасау үшін:

1. Бағдарламаның негізгі терезесінде **Тапсырмалар** бөліміне өтіңіз.
2. **Қосу** түймесін басыңыз.

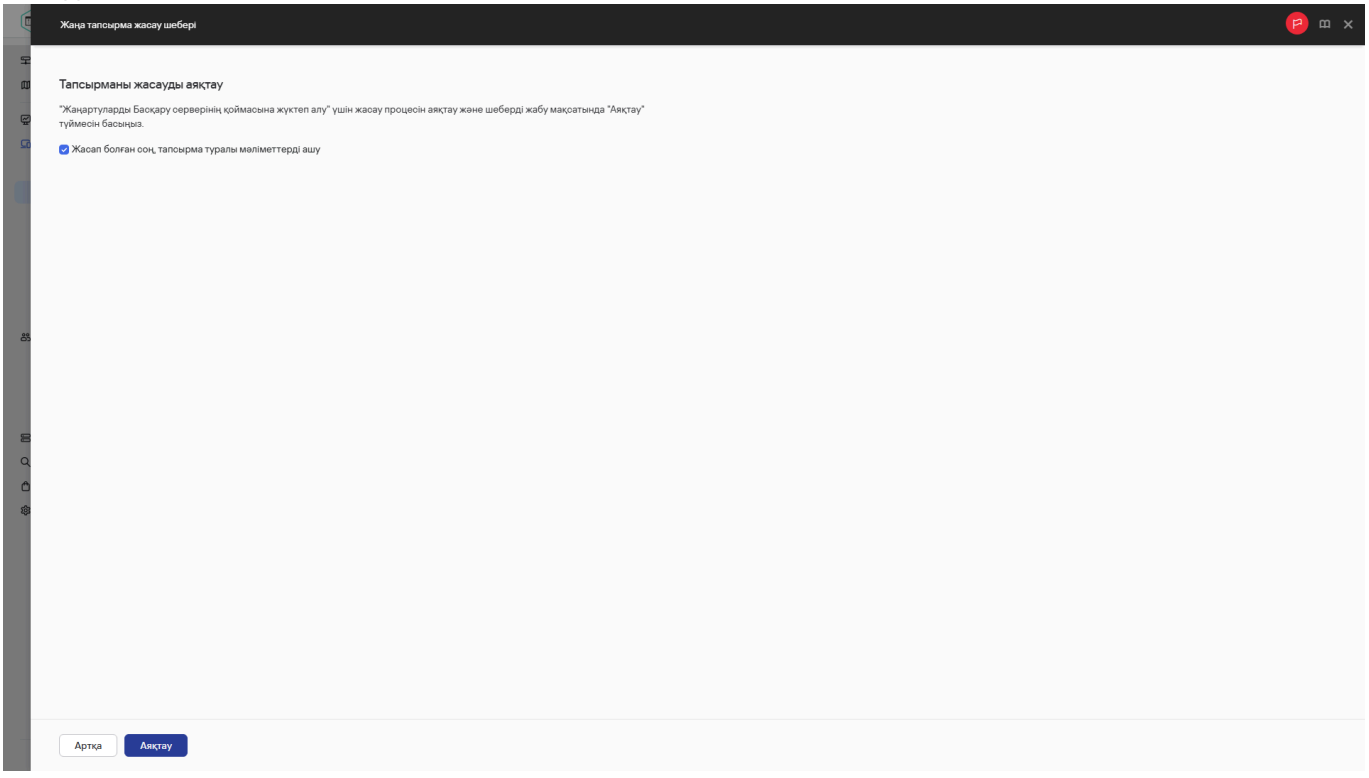
   Жаңа тапсырма жасау шебері іске қосылады. Содан кейін, шебердің нұсқауларын орындаңыз.
3. Kaspersky Security Center бағдарламасы үшін **Жаңартуларды Басқару серверінің қоймасына жүктеп алу** тапсырма түрін таңдаңыз.

4. Жасап жатқан тапсырманың атын көрсетіңіз. Тапсырма атауы 100 таңбадан асуы және арнайы таңбаларды ("*<>?\:|) қамтуы мүмкін емес.



Жаңартуларды Басқару серверінің қоймасына жүктеп алу тапсырмасын жасау

5. **Тапсырманы жасауды аяқтау** бетінде, тапсырма сипаттары терезесін ашу үшін **Жасап болған соң, тапсырма туралы мәліметтерді ашу** параметрін қосып, әдепкі бойынша тапсырма параметрлерін өзгертуге болады. Сондай-ақ, тапсырма параметрлерін кейінірек, кез келген уақытта конфигурациялауға болады.



Тапсырманы жасауды аяқтау

6. **Аяқтау** түймесін басыңыз.

   Тапсырма жасалып, тапсырмалар тізімінде көрсетіледі.

7. Тапсырма сипаттары терезесін ашу үшін жасалған тапсырманың атын басыңыз.

8. Тапсырма сипаттары терезесінде **Бағдарлама параметрлері** қойыншасында келесі параметрлерді көрсетіңіз:

- **Жаңартулардың көздері**

  Жаңарту көзі ретінде мыналарды пайдалануға болады:

  - Kaspersky жаңарту серверлері (әдепкі бойынша таңдалған)
  - Негізгі Басқару сервері

    Бұл ресурс қосалқы немесе виртуалды Басқару сервері үшін жасалған тапсырмаларға қатысты қолданылады.
  - Жергілікті немесе желілік қалта

    Соңғы жаңартуларды қамтитын жергілікті немесе желілік қалта. Желілік қалта FTP сервері, HTTP сервері немесе SMB жалпы ресурсы болуы мүмкін.

    Жергілікті қалтаны таңдағанда, Басқару сервері орнатылған құрылғыдағы қалтаны көрсету қажет. Қалтаға апаратын жол құрылғының амалдық жүйесіне байланысты. Жергілікті қалта Linux негізіндегі Басқару серверінде орналасқандықтан, POSIX жолын көрсету керек, мысалы: /path/to/dir.

    Жаңарту көзі ретінде SMB желілік қалтасын таңдаған кезде, қалтаны таңдамас бұрын оны Басқару сервері орнатылған құрылғыға монтаждаңыз. Содан кейін монтаждалған қалтаның жолын оның жергілікті файлдық жүйедегі жолын пайдаланып көрсетіңіз. Қалтаға қатынасу SMB протоколы арқылы жүзеге асырылады.

    > Жаңарту көзі ретінде пайдаланылатын жергілікті немесе желілік қалтада, FTP немесе HTTP серверінде Kaspersky жаңарту серверлеріндегі қалта құрылымына сәйкес келетін қалта құрылымы болуы керек. Бұл құрылымды Kaspersky Update Utility көмегімен алуға болады.

  > *Басқару серверінің қоймасына жаңартуларды жүктеп алу* және *Тарату нүктелерінің қоймаларына жаңартуларды жүктеп алу* тапсырмаларында, егер жаңарту көзі ретінде құпиясөзбен қорғалған жергілікті немесе желілік қалта таңдалған болса, пайдаланушының аутентификациясы жұмыс істемейді. Бұл мәселені шешу үшін алдымен құпиясөзбен қорғалған қалтаны жөндеңіз, содан кейін қажетті есептік деректерді (мысалы, операциялық жүйенінің құралдарымен) көрсетіңіз. Осыдан кейін жаңартуларды жүктеу тапсырмасында жаңарту көзі ретінде осы қалтаны таңдауға болады. Kaspersky Security Center Linux сізден есептік деректерді енгізуді талап етпейді.

- **Жаңартулар сақталатын қалта**

  Сақталған жаңартуларды сақтау үшін көрсетілген қалтаға апаратын жол. Көрсетілген қалтаға апаратын жолды алмасу буферіне көшіруге болады. Топтық тапсырма үшін көрсетілген қалтаға апаратын жолды өзгерте алмайсыз.

- **Қосалқы Басқару серверлерін мәжбүрлеп жаңарту**

  Параметр қосылса, Басқару сервері жаңартуларды алғаннан кейін бірден бағыныңқы Басқару серверлерінде жаңартуларды алу тапсырмаларын іске қосады. Жаңарту тапсырмалары Басқару серверлеріндегі тапсырма сипаттамаларында конфигурацияланған жаңарту көзі арқылы іске қосылады.

  Егер бұл параметр өшірулі болса, қосалқы Басқару серверлеріндегі жаңарту тапсырмалары кестеге сәйкес басталады.

  Әдепкі бойынша, параметр өшірулі.

- **Алынған жаңартуларды қосымша қалталарға көшіру**

  Егер жалауша қойылса, жаңартуларды алғаннан кейін, Басқару сервері жаңартуларды көрсетілген қалталарға көшіреді. Құрылғыңыздағы жаңартуларды қолмен басқарғыңыз келсе, осы параметрді пайдаланыңыз.

  Мысалы, сіз бұл параметрді келесі жағдайда пайдалана аласыз: ұйым желісінде бірнеше тәуелсіз ішкі желілер бар және әр ішкі желідегі құрылғылар басқа ішкі желіге қатынаса алмайды. Бұл жағдайда, барлық ішкі желілердегі құрылғылар ортақ желілік қалтаға қатынаса алады. Бұл жағдайда, ішкі желілердің біріндегі Басқару сервері үшін Kaspersky жаңарту серверлерінен жаңартуларды жүктеуді көрсетіңіз, осы параметрді қосыңыз және осы желілік қалтаны көрсетіңіз. Басқару сервері үшін жаңартуларды қоймаға жүктеу тапсырмасында дәл осы желілік қалтаны жаңартулар көзі ретінде көрсетіңіз.

  Жүктелген жаңартуларды жергілікті қалтаға көшіруді таңдасаңыз, құрылғыда Басқару сервері орнатылған қалтаны көрсетуіңіз керек. Қалтаға апаратын жол құрылғының амалдық жүйесіне байланысты. Жергілікті қалта Linux негізіндегі Басқару серверінде орналасқандықтан, POSIX жолын көрсету керек, мысалы: /path/to/dir.

  Linux негізіндегі Басқару серверінде орналасқан желілік қалтаны таңдағанда, қалтаны іске қосу арқылы Басқару сервері орнатылған құрылғыдан желілік қалтаға қатынасуды алдын ала қамтамасыз ету керек. Қалтаға қатынасу SMB протоколы арқылы жүзеге асырылады.

  Әдепкі бойынша, параметр өшірулі.

- **diff файлдарды жүктеп алу**

  Бұл параметр айырмашылық файлдарын жүктеп алу функциясын қосады.

  Әдепкі бойынша, параметр өшірулі.

- **Ескі схеманы пайдаланып, жаңартуларды жүктеп алу**

  14-ші нұсқадан бастап, Kaspersky Security Center бағдарламасы дерекқорлар мен бағдарлама модульдері жаңартуларын жаңа схема бойынша жүктеп алады. Бағдарлама жаңартуларды жаңа схеманың көмегімен жүктей алуы үшін, жаңарту көзі жаңа схемамен үйлесімді метадеректері бар жаңарту файлдарын қамтуы керек. Жаңарту көзінде тек ескі схемамен үйлесімді метадеректері бар жаңарту файлдары болса, **Ескі схеманы пайдаланып, жаңартуларды жүктеп алу** параметрін қосыңыз. Әйтпесе, жаңартуларды жүктеу тапсырмасы қатемен аяқталады.

  Мысалы, жаңарту көзі ретінде жергілікті немесе желілік қалта көрсетілсе және осы қалтадағы жаңарту файлдары келесі бағдарламалардың бірімен жүктелген болса, осы параметрді қосу керек:

  - Kaspersky Update Utility

    Бұл утилита жаңартуларды ескі схема бойынша жүктейді.

  - Kaspersky Security Center 13 Linux

    Мысалы, бір Басқару серверінің интернетке қосылымы жоқ. Бұл жағдайда, сіз интернетке қосылған екінші Басқару сервері арқылы жаңартуларды жүктей аласыз, содан кейін жаңартуларды бірінші Сервер үшін жаңарту көзі ретінде пайдалану үшін жергілікті немесе желілік қалтаға орналастыра аласыз. Егер екінші Басқару серверінің нұсқа нөмірі 13 болса, бірінші Басқару серверіне арналған тапсырмада **Ескі схеманы пайдаланып, жаңартуларды жүктеп алу** параметрін қосыңыз.

  Әдепкі бойынша, параметр өшірулі.

- **Жаңарту тексерісін іске қосу**

  Егер жалауша қойылса, Басқару сервері жаңартуларды көзден көшіреді, оларды уақытша қоймада сақтайды және **Жаңартуларды тексеру тапсырмасы** өрісінде көрсетілген Жаңартуларды тексеру тапсырмасын іске қосады. Бұл тапсырма сәтті орындалған жағдайда, жаңартулар уақытша қоймадан Басқару серверінің ортақ қатынас бар қалтасына көшіріледі және Басқару сервері жаңартулардың көзі болып табылатын құрылғыларға таратылады (**Қоймаға жаңартуларды жүктеу кезінде** кесте түрі бар тапсырмалар іске қосылады). Жаңартуларды қоймаға жүктеу тапсырмасы, тек *Жаңартуларды тексеру* тапсырмасы аяқталғаннан кейін аяқталған болып саналады.

  Әдепкі бойынша, параметр өшірулі.

- **Жаңарту сұрауының файлын автоматты түрде жүктеп алу**

  Kaspersky жаңарту утилитасы тиісті конфигурацияға тек қажетті жаңартуларды жүктеп алғанын қаласаңыз, осы опцияны қосып, Kaspersky Security Center Linux жүктеп алынатын жаңартулар туралы ақпараты бар жаңарту сұрауының файлын жасайтын жолды көрсетіңіз. Жаңарту сұрауының файлында уақыт белгісі мен нұсқаны басқаруға арналған MD5 хэші болады.

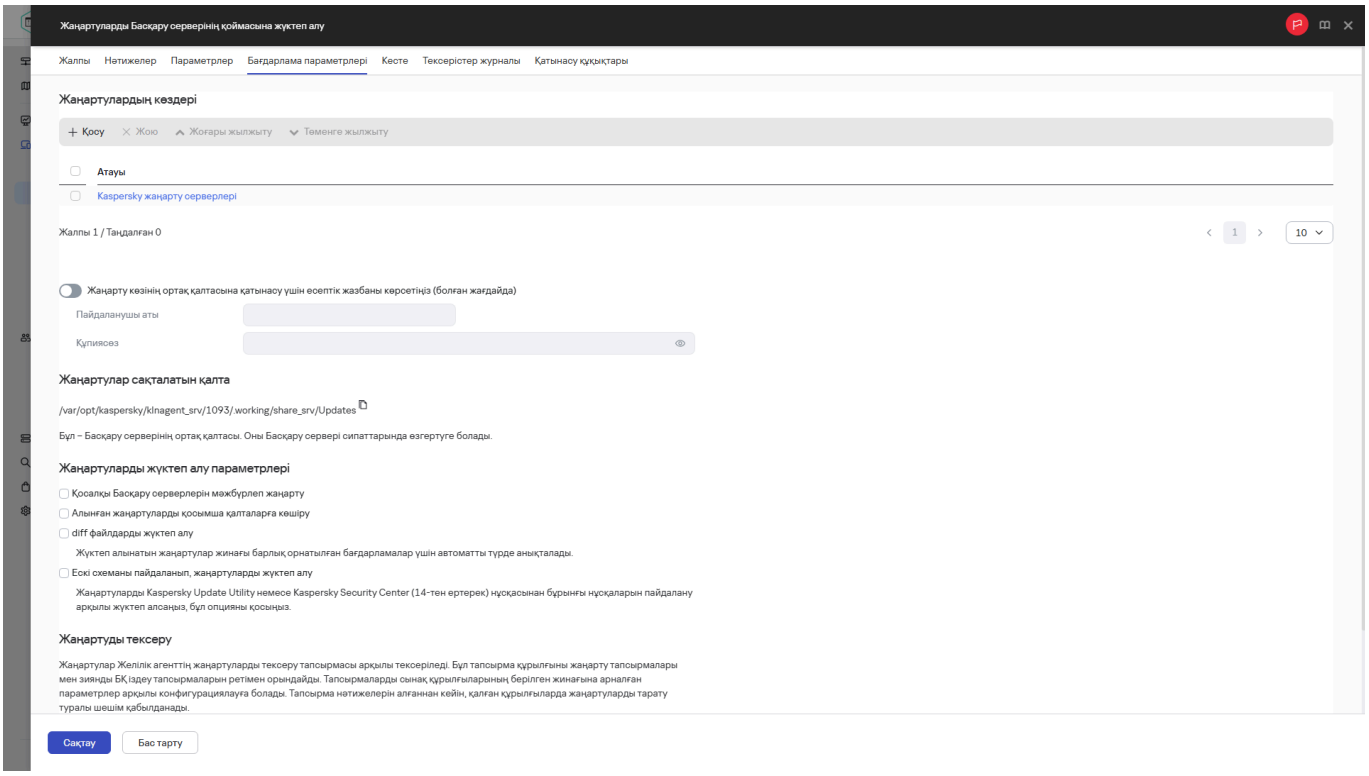
  Ескі схеманы пайдаланып, жаңартуларды жүктеп алу опциясының өшірілгеніне көз жеткізіңіз.

  Сондай-ақ Kaspersky жаңарту утилитасына жаңартуды жүктеп алуды конфигурациялау керек.

  Әдепкісінше келесі жол көрсетіледі: /var/opt/kaspersky/klnagent_srv/1093/.working/share_srv/retranslation_request.xml. Қажет болса, әдепкі атауды (retranslation_request) және жолды өзгертуге болады.

  > Сұрау файлын жергілікті немесе ортақ қалтаға орналастыруға болады. Ортақ қалтаны пайдаланған кезде, осы қалтаға басқару сервері орнатылған құрылғыдан кіру рұқсатын қамтамасыз ету керек. Қол жеткізуді қамтамасыз ету жолдары мен қолданылатын құралдар инфрақұрылымыңызға байланысты.

  Жаңартуларды басқару серверінің қоймасына жүктеп алу тапсырмасын орындаған кезде, Kaspersky Security Center Linux сіз көрсеткен жолда .xml форматындағы жаңарту сұрауының файлын жасайды. Kaspersky жаңарту файлы сұрау файлынан ақпаратты автоматты түрде алып, тек қажетті жаңартуларды жүктеп алады. Kaspersky жаңарту утилитасы ақпаратты автоматты түрде ала алмаса (мысалы, Kaspersky Security Center Linux сұрау файлын жасаған қалтаға Kaspersky жаңарту утилитасы қол жеткізе алмаса), файлды үшінші тарап құралдары арқылы тасымалдауыңыз керек.



Басқару серверінің қоймасына жаңартуларды жүктеп алу тапсырмасының сипаттарын көрсету

9. Тапсырма сипаттары терезесінде, **Кесте** қойыншасында тапсырманы іске қосу кестесін жасаңыз. Қажет болса, келесі параметрлерді конфигурациялаңыз:

   - **Тапсырманы бастау**:

     - **Қолмен** (әдепкі бойынша таңдалған)

       Тапсырма автоматты түрде іске қосылмайды. Тапсырманы тек қолмен іске қосуға болады.

       Әдепкі бойынша, осы нұсқа таңдалған.

     - **N минут сайын**

       Тапсырма жүйелі түрде, тапсырма жасалған күні көрсетілген уақыттан бастап, минуттар түрінде белгіленген аралықпен орындалады.

       Әдепкі бойынша, тапсырма ағымдағы жүйелік уақыттан бастап 30 минут сайын іске қосылады.

     - **N сағат сайын**

       Тапсырма көрсетілген күн мен уақыттан бастап, сағат түрінде белгіленген аралықпен жүйелі түрде орындалады.

       Әдепкі бойынша, тапсырма ағымдағы жүйелік күн мен уақыттан бастап 6 сағат сайын іске қосылып тұрады.

     - **N күн сайын**

       Тапсырма, күндер түрінде белгіленген аралықпен жүйелі түрде орындалады. Сондай-ақ, сіз тапсырманы бірінші рет іске қосу күні мен уақытын да көрсете аласыз. Бұл қосымша параметрлерге сіз тапсырма жасап жатқан бағдарлама қолдау көрсетсе, олар қолжетімді болады.

       Әдепкі бойынша, тапсырма ағымдағы жүйелік күн мен уақыттан бастап күн сайын іске қосылады.

- **Апта күндері бойынша**

  Тапсырма жүйелі түрде, аптаның көрсетілген күндерінде, көрсетілген уақытта орындалады.

  Әдепкі бойынша, тапсырма жұма сайын, сағат 18:00:00-де іске қосылады.

- **Ай сайын**

  Тапсырма жүйелі түрде, айдың көрсетілген күнінде, көрсетілген уақытта орындалады.

  Көрсетілген күні жоқ айларда тапсырма соңғы күні орындалады.

  Әдепкі бойынша, тапсырма әр айдың бірінші күнінде, ағымдағы жүйелік уақытта орындалады.

- **Таңдалған апта күні ай сайын**

  Тапсырма жүйелі түрде, әр айдың көрсетілген күндерінде, көрсетілген уақытта орындалады.

  Әдепкі бойынша, басталу уақыты 18:00 және айдың күндері таңдалмайды.

  > Айдағы нақты күнді де, апта нөмірін де (айдың бірінші, екінші аптасын) емес, ай ішіндегі апта күнінің реттік нөмірін таңдайтыныңызды ескеріңіз. Мысалы, егер сіз курсорды **Сс** жолдың **Бірінші** ұяшығына орнатсаңыз, бұл тапсырма әр жаңа айдың бірінші сейсенбісінде орындалатынын білдіреді.

  Аптаның бірнеше күнін таңдай аласыз.

- **Басқа тапсырманы аяқтағанда**

  Ағымдағы тапсырма басқа тапсырма аяқталғаннан кейін іске қосылады. Екі тапсырма да бір құрылғы арқылы тағайындалса ғана, осы параметр жұмыс істейді. Мысалы, *Құрылғыларды басқару* тапсырмасын **Құрылғыны қосу** параметрінің көмегімен іске қоса аласыз және ол аяқталғаннан кейін *Вирустарды іздеу* тапсырмасын іске қоса аласыз.

  Кестеден іске қосу тапсырмасын және осы тапсырма орындалатын күйді таңдау керек (**Сәтті аяқталды** немесе **Сәтсіз аяқталды**).

  Қажет болса, кестедегі тапсырмаларды төмендегідей іздеуге, сұрыптауға және сүзуге болады:

  - Тапсырманы атауы бойынша іздеу үшін іздеу өрісіне тапсырма атауын енгізіңіз.
  - Тапсырмаларды атауы бойынша сұрыптау үшін сұрыптау белгішесін басыңыз.

    Әдепкі бойынша, тапсырмалар өсу ретімен әліпбилік ретпен сұрыпталады.
  - Сүзгі белгішесін басыңыз және ашылатын терезеде тапсырмаларды топтар бойынша сүзіңіз, содан кейін **Қолдану** түймесін басыңыз.

- Тапсырманың қосымша параметрлері:

  - **Өткізіп алынған тапсырмаларды іске қосу**

    Бұл параметр, тапсырма басталғалы тұрған кезде клиент құрылғысы желіде көрсетілмесе, тапсырманың жүріс-тұрысын анықтайды.

    Параметр қосулы болса, клиент құрылғысында Kaspersky бағдарламасын кезекті рет іске қосу кезінде тапсырманы іске қосу әрекеті жасалады. Тапсырманың кестесінде **Қолмен**, **Бір рет** немесе **Дереу** іске қосу көрсетілсе, онда тапсырма желіде құрылғы көзге көрінетін болғаннан кейін немесе құрылғы тапсырманың әрекет ету ауқымына қосылғаннан кейін бірден іске қосылады.

Егер параметр өшірулі болса, клиент құрылғыларында тапсырманы іске қосу тек кесте бойынша орындалатын болады. **Қолмен**, **Бір рет** және **Дереу** кестесі үшін тапсырмалар желіде көрінетін клиенттік құрылғыларда ғана орындалады. Мысалы, сіз бұл параметрді тек жұмыс уақытынан тыс уақытта іске қосқыңыз келетін ресурстарды қажетсінетін тапсырма үшін өшіре аласыз.

Әдепкі бойынша, параметр өшірулі.

- **Тапсырманы бастау үшін автоматты түрде араластырылған кідірісті пайдалану**

  Параметр қосулы болса, тапсырма клиент құрылғыларында белгілі бір уақыт аралығында кездейсоқ іске қосылады, яғни *тапсырманың таратылған іске қосылуы* орын алады. Тапсырманың таратылған іске қосылуы, тапсырманы кесте бойынша іске қосу кезінде көптеген клиент құрылғыларының Басқару серверіне бір уақытта жүгінуіне жол бермейді.

  Таратылған іске қосылу кезеңі, тапсырма тағайындалған клиент құрылғыларының санына байланысты тапсырманы жасау кезінде автоматты түрде есептеледі. Кейінірек, тапсырма әрқашан есептелген іске қосу уақытында іске қосылады. Алайда, тапсырма параметрлеріне түзетулер енгізілгенде немесе тапсырма қолмен іске қосылғанда, тапсырманы іске қосу уақытының есептелген мәні өзгереді.

  Егер параметр өшірулі болса, клиент құрылғыларында тапсырманы іске қосу кесте бойынша орындалады.

- **Тапсырманы бастауға арналған келесі аралықтағы автоматты кездейсоқ кідірісті пайдалану**

  Параметр қосулы болса, тапсырма клиент құрылғыларында белгілі бір уақыт аралығында кездейсоқ іске қосылады. Тапсырманың таратылған іске қосылуы, тапсырманы кесте бойынша іске қосу кезінде көптеген клиент құрылғыларының Басқару серверіне бір уақытта жүгінуіне жол бермейді.

  Егер параметр өшірулі болса, клиент құрылғыларында тапсырманы іске қосу кесте бойынша орындалады.

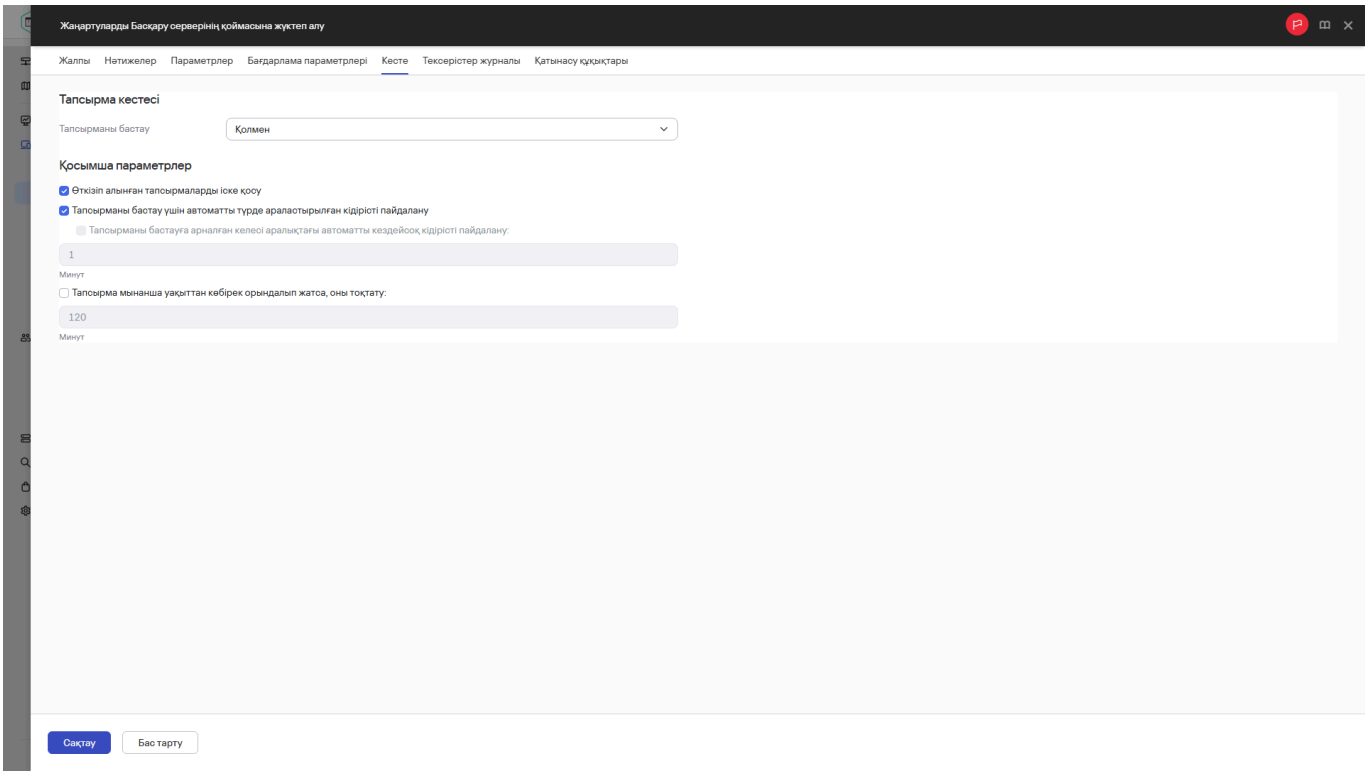
  Әдепкі бойынша, параметр өшірулі. Әдепкі бойынша, уақыт аралығы бір минутқа тең.

- **Тапсырма мынанша уақыттан көбірек орындалып жатса, оны тоқтату**

  Белгіленген уақыттан кейін, тапсырма аяқталғанына немесе аяқталмағанына қарамастан автоматты түрде тоқтатылады.

  Егер сіз тым ұзақ орындалатын тапсырмаларды үзгіңіз келсе (немесе тоқтатқыңыз келсе), осы параметрді қосыңыз.

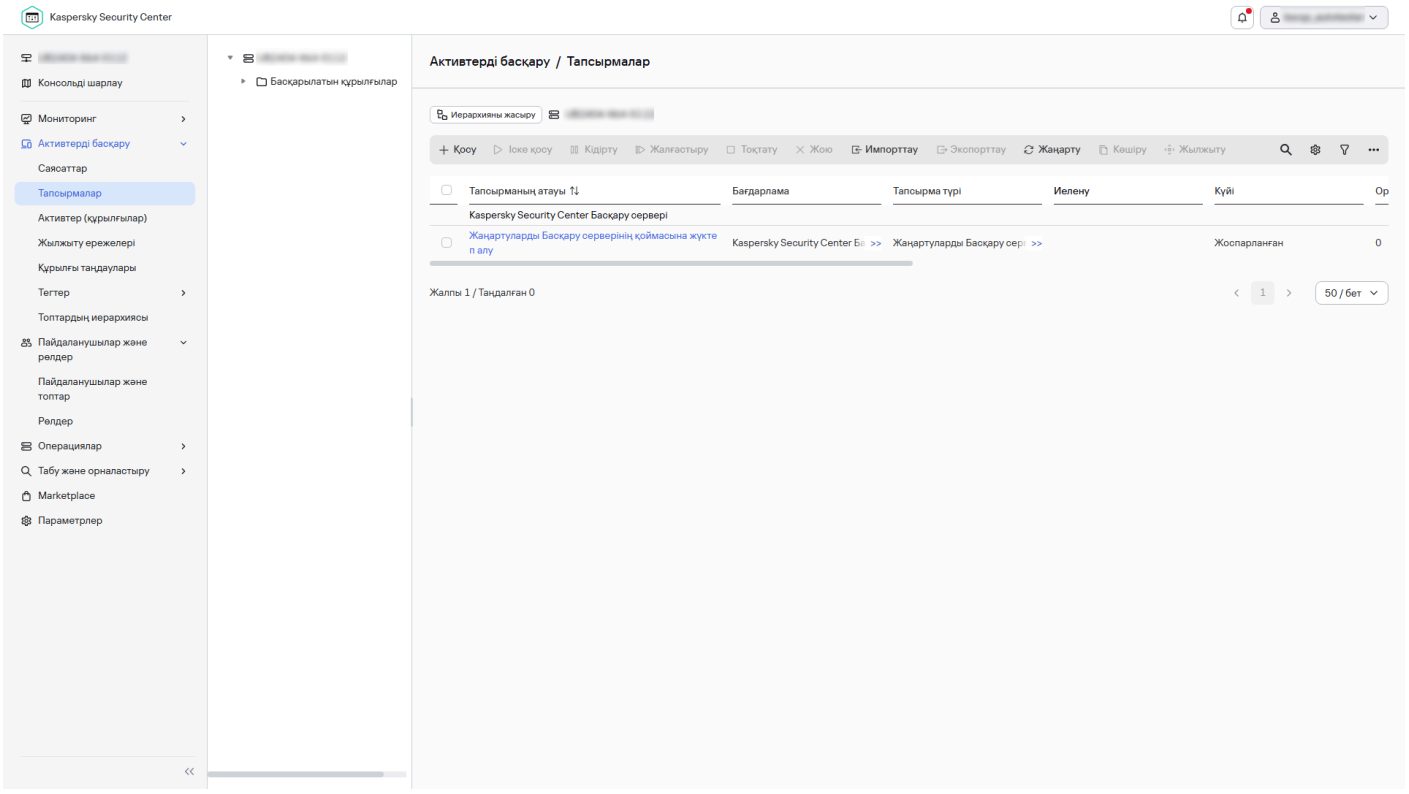
  Әдепкі бойынша, параметр өшірулі. Әдепкі бойынша тапсырманы орындау уақыты – 120 минут.



Басқару серверінің қоймасына жаңартуларды жүктеп алу тапсырмасының кестесін көрсету

10. **Сақтау** түймесін басыңыз.

Тапсырма жасалды және конфигурацияланды.



Тапсырмалар тізімі

Жаңартуларды Басқару серверінің қоймасына жүктеп алу тапсырмасын орындау нәтижесінде, деректқорлар мен бағдарламалық модульдердің жаңартулары жаңарту көзінен көшіріледі және Басқару серверінің ортақ қатынасы бар қалтасына орналастырылады. Егер тапсырма басқару тобы үшін жасалса, онда ол тек көрсетілген басқару тобына кіретін Желілік агенттерге қолданылады.

Ортақ қатынасы бар қалтадан жаңартулар клиент құрылғыларына және қосалқы Басқару серверлеріне таратылады.

Алынған жаңартуларды тексеру

Басқарылатын құрылғыларға жаңартуларды орнатудың алдында, оларды алдымен *Жаңартуды тексеру* тапсырмасының көмегімен жұмысқа жарамдылығы мен қателері тұрғысынан тексере аласыз. *Жаңартуды тексеру* тапсырмасы *Жаңартуларды Басқару серверінің қоймасына жүктеп алу* тапсырмасы аясында автоматты түрде орындалады. Басқару сервері жаңартуларды көзден жүктейді, оларды уақытша қоймада сақтайды және *Жаңартуды тексеру* тапсырмасын іске қосады. Бұл тапсырма сәтті орындалған жағдайда, жаңартулар уақытша қоймадан Басқару серверінің ортақ қатынасы бар қалтасына көшіріледі. Жаңартулар Басқару сервері жаңарту көзі болып табылатын клиент құрылғыларына қолданылады.

Жаңартуды тексеру тапсырмасын орындау нәтижесінде уақытша қоймадағы жаңартулар қате деп танылса немесе *Жаңартуды тексеру* тапсырмасы қатемен аяқталса, мұндай жаңартулар ортақ қалтаға көшірілмейді. Басқару серверінде алдыңғы жаңартулар жиынтығы қалады. **Қоймаға жаңартуларды жүктеу кезінде** кесте түрі бар тапсырмаларды іске қосу да орындалмайды. Жаңа жаңартулар жиынтығын тексеру сәтті аяқталса, бұл операциялар *Жаңартуларды Басқару серверінің қоймасына жүктеп алу* тапсырмасы келесі рет іске қосылған кезде орындалады.

Егер сынақ құрылғыларының кем дегенде біреуінде келесі шарттардың бірі орындалса, жаңартулар жиынтығы дұрыс емес болып саналады:

- жаңарту тапсырмасын орындау кезінде қате пайда болды;
- жаңартуларды қолданғаннан кейін, қауіпсіздік бағдарламасының тұрақты қорғаныс күйі өзгерді;
- талап бойынша тексеру тапсырмасын орындау барысында жұқтырған нысан табылды;
- Kaspersky бағдарламасының жұмыс қатесі туындады.

Егер сынақ құрылғыларының ешқайсысында аталған шарттардың ешбірі орындалмаса, жаңартулар жиынтығы дұрыс деп танылады және *Жаңартуларды тексеру* тапсырмасы сәтті орындалды деп саналады.

Жаңартуды тексеру тапсырмасын жасауға кіріспес бұрын, алдын ала шарттарды орындаңыз:

1. Бірнеше сынақ құрылғысы бар басқару тобын құрыңыз. Жаңартуларды тексеру үшін сізге бұл топ қажет болады.

   Сынақ құрылғылары ретінде ұйымның желісінде ең көп таралған бағдарламалық конфигурациясы бар жақсы қорғалған құрылғыларды пайдалану ұсынылады. Бұл тәсілдеме, тексеру кезінде вирустарды анықтаудың сапасы мен ықтималдығын арттырады, сонымен қатар жалған іске қосылу қаупін азайтады. Сынақ құрылғыларында вирустар табылған кезде *Жаңартуды тексеру* тапсырмасы сәтсіз аяқталды деп саналады.

2. Kaspersky Endpoint Security for Linux сияқты Kaspersky Security Center Linux қолдайтын кейбір бағдарлама үшін жаңарту және зиянды БҚ іздеу тапсырмаларын жасаңыз. Жаңарту тапсырмаларын жасау және зиянды БҚ іздеу кезінде сынақ құрылғылары бар басқару тобын көрсетіңіз.

   Жаңартуды тексеру тапсырмасы барлық жаңартулардың жаңартылғанына көз жеткізу үшін сынақ құрылғыларында жаңарту және зиянды БҚ іздеу тапсырмаларын дәйекті түрде іске қосады. Сондай-ақ, *Жаңартуды тексеру* тапсырмасын жасау кезінде жаңарту және зиянды БҚ іздеу тапсырмаларын көрсету қажет.

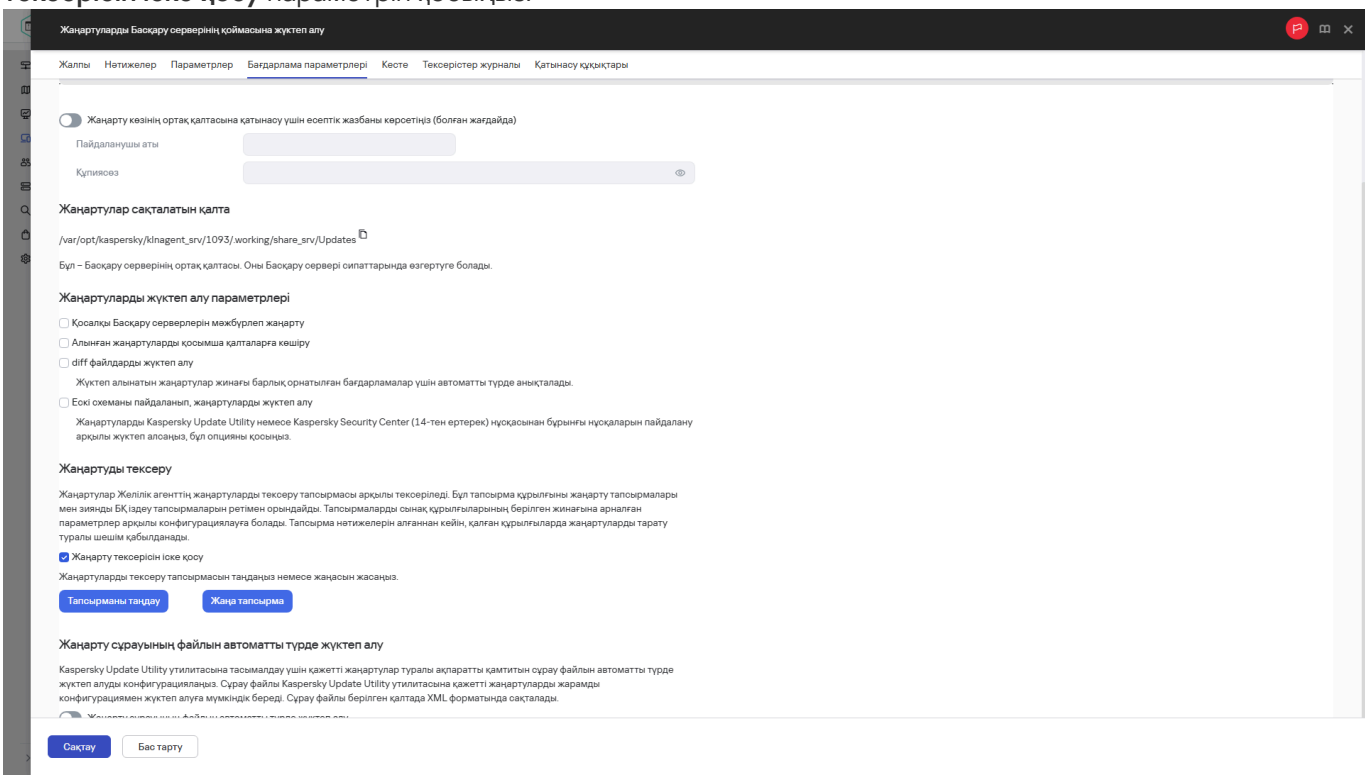
3. *Жаңартуларды Басқару серверінің қоймасына жүктеп алу* тапсырмасын жасаңыз.

Kaspersky Security Center Linux бағдарламасы клиент құрылғыларына таратпас бұрын алынған жаңартуларды тексеруі үшін:

1. Бағдарламаның негізгі терезесінде **Тапсырмалар** бөліміне өтіңіз.

2. **Жаңартуларды Басқару серверінің қоймасына жүктеп алу** тапсырмасының атын басыңыз.

3. Ашылған тапсырма сипаттары терезесінде **Бағдарлама параметрлері** қойыншасына өтіп, **Жаңарту тексерісін іске қосу** параметрін қосыңыз.



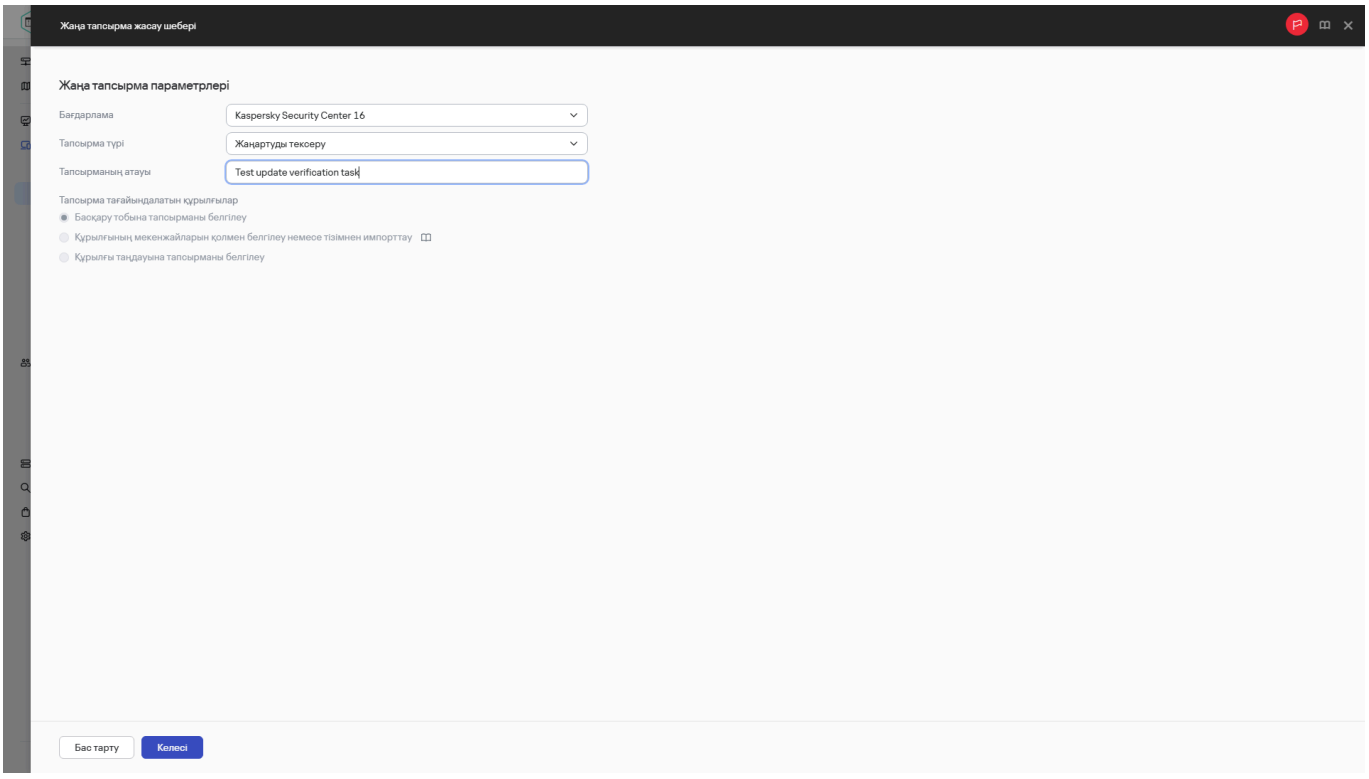
Жаңартуларды Басқару серверінің қоймасына жүктеп алу тапсырмасының сипаттары

4. *Жаңартуларды тексеру* тапсырмасы бар болса, **Тапсырманы таңдау** түймесін басыңыз. Сынақ құрылғылары бар басқару тобында ашылған *Жаңартуларды тексеру* тапсырмасы терезесінде.

5. *Жаңартуларды тексеру* тапсырмасын бұған дейін жасамаған болсаңыз, келесі әрекеттерді орындаңыз:

a. **Жаңа тапсырма** түймесін басыңыз.

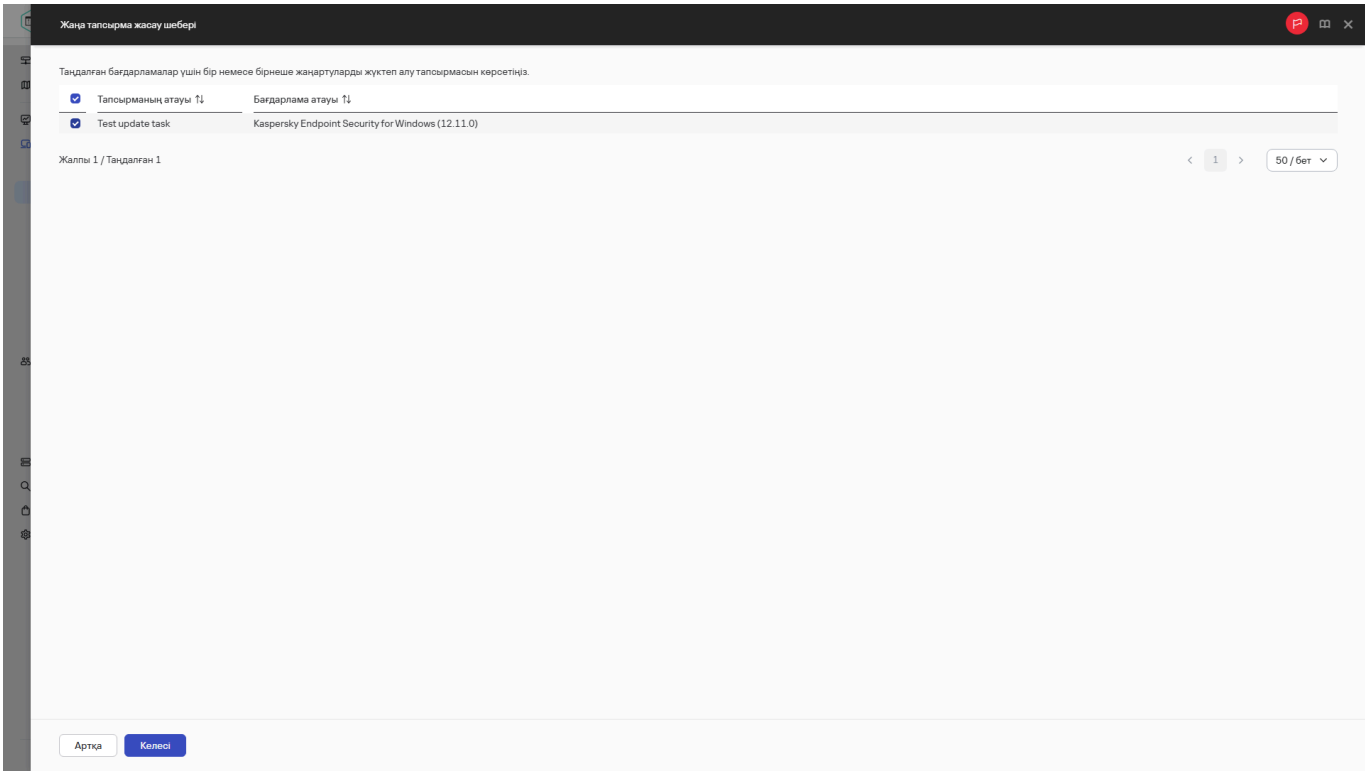
b. Ашылған тапсырма жасау шеберінде алдын ала орнатылған атауды өзгерткіңіз келсе, тапсырманың атын көрсетіңіз.



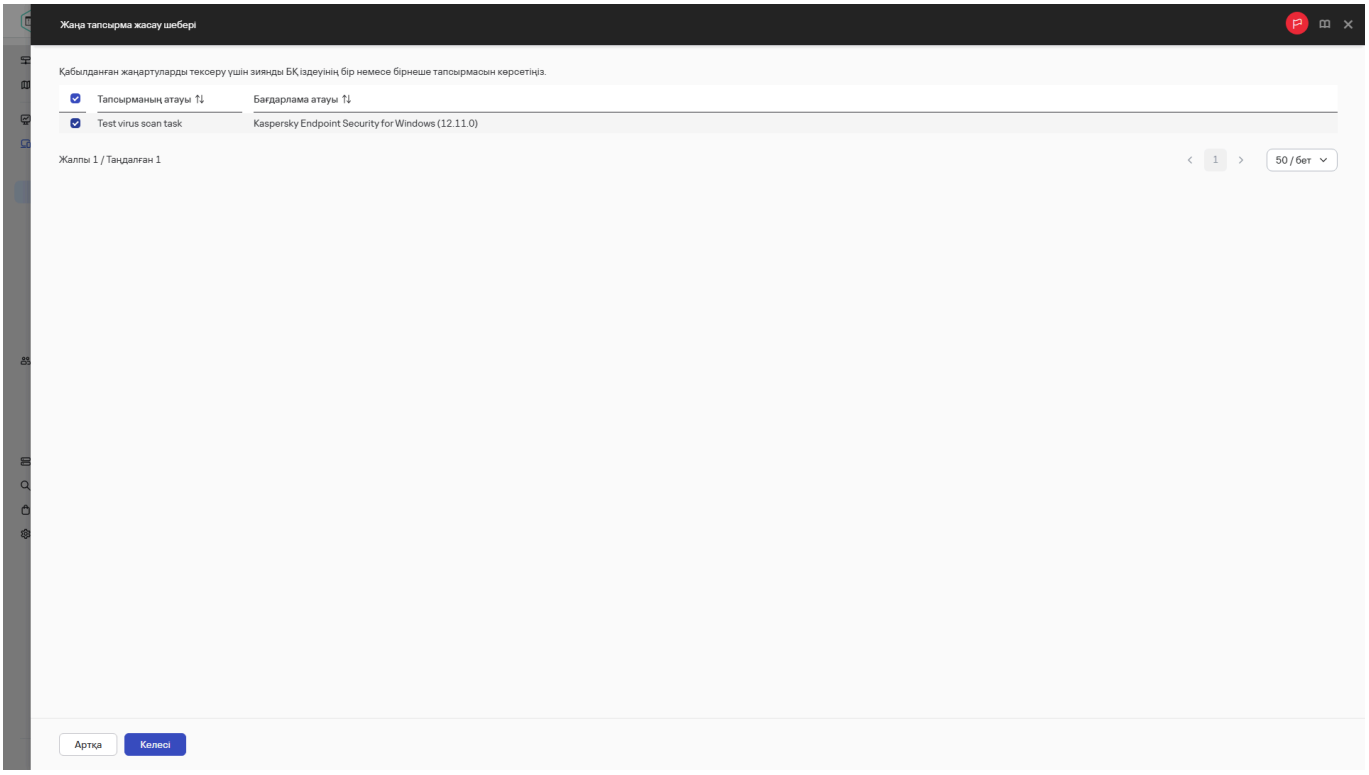
Жаңартуларды тексеру тапсырмасын жасау

a. Бұрын жасалған сынақ құрылғылары бар басқару тобын таңдаңыз.

b. Kaspersky Security Center Linux қолдау көрсететін қажетті қолданбаның жаңарту тапсырмасын таңдаңыз.



a. Kaspersky Security Center Linux қолдау көрсететін қажетті қолданбаның зиянды БҚ іздеу тапсырмасын таңдаңыз.



Зиянды БҚ іздеу тапсырмасын таңдау

Осыдан кейін, келесі параметрлер пайда болады. Оларды қосулы күйде қалдыру ұсынылады:

- **Дерекқорды жаңартудан кейін құрылғыны өшіріп қайта іске қосу**

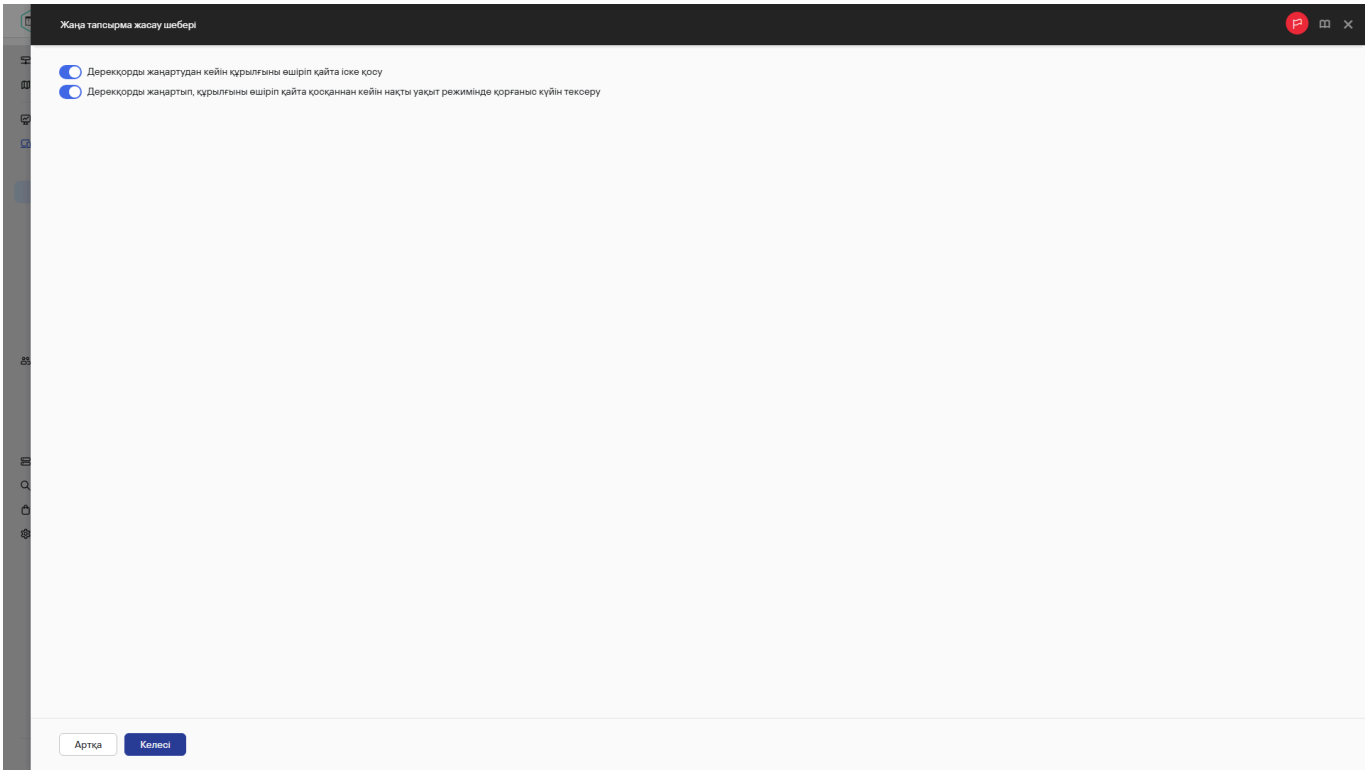
  Құрылғыдағы антивирустық дерекқорларды жаңартқаннан кейін, құрылғыны қайта іске қосу ұсынылады.

  Әдепкі бойынша, параметр қосулы.

- **Дерекқорды жаңартып, құрылғыны өшіріп қайта қосқаннан кейін нақты уақыт режимінде қорғаныс күйін тексеру**

  Егер бұл параметр қосулы болса, *Жаңартуларды тексеру* тапсырмасы Басқару сервері қоймасына жүктелген жаңартулардың өзектілігін және антивирустық дерекқорды жаңартып, құрылғыны қайта іске қосқаннан кейін қорғаныс деңгейінің төмендегенін тексереді.

Әдепкі бойынша, параметр қосулы.



Тапсырма параметрлерін көрсету

a. *Жаңартуларды тексеру* тапсырмасы іске қосылатын есептік жазбаны көрсетіңіз. Сіз өзіңіздің есептік жазбаңызды қолданып, **Әдепкі есептік жазба** параметрін қосулы күйде қалдыра аласыз. Сонымен қатар, тапсырма қажетті қатынасу құқықтары бар басқа есептік жазбада орындалуы керек екенін көрсетуге болады. Ол үшін **Есептік жазбаны көрсету** параметрін таңдап, сол есептік жазбаның есептік деректерін енгізіңіз.

6. *Жаңартуларды Басқару серверінің қоймасына жүктеп алу* тапсырмасының сипаттар терезесін жабу үшін **Сақтау** түймесін басыңыз.

Жаңартуларды автоматты түрде тексеру қосылған. Енді сіз *Жаңартуларды Басқару серверінің қоймасына жүктеп алу* тапсырмасын іске қоса аласыз, сонда ол жаңартуларды тексеруден басталады.

Жаңартуларды тарату орындарының қоймаларына жүктеп алу тапсырмасын жасау

Басқару тобы үшін *Жаңартуларды тарату орындарының қоймаларына жүктеп алу* тапсырмасын жасай аласыз. Мұндай тапсырма, көрсетілген басқару тобына кіретін тарату нүктелері үшін орындалады.

Бұл тапсырманы, мысалы, Басқару сервері мен тарату нүктелері арасындағы трафик Kaspersky жаңарту серверлері мен тарату нүктелері арасындағы трафиктен қымбатырақ болса немесе Басқару серверіңізде интернетке қатынасу мүмкіндігі болмаса пайдалана аласыз.

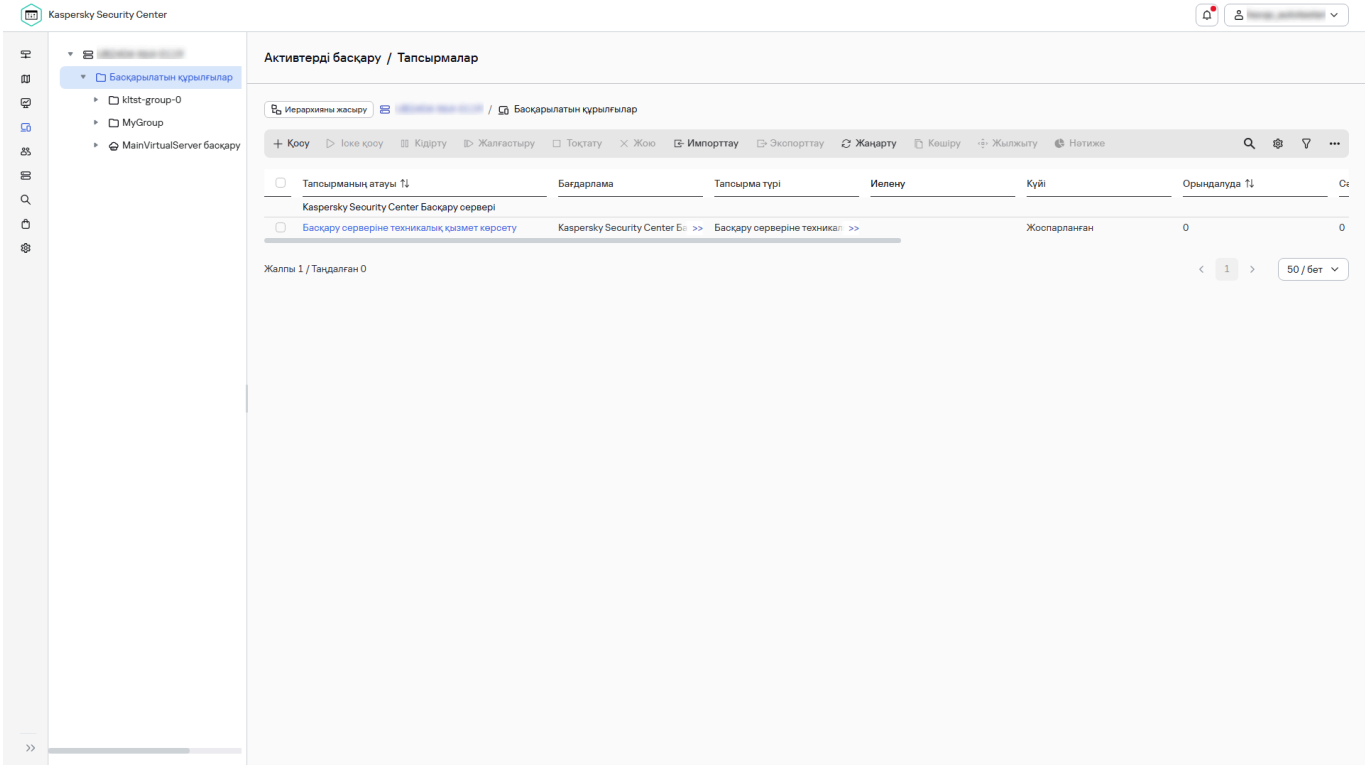
Бұл тапсырма Kaspersky жаңарту серверлерінен тарату нүктелері қоймалары жаңартуларды жүктеу үшін қажет. Жаңартулардың тізіміне мыналар кіреді:

- Kaspersky қауіпсіздік бағдарламаларына арналған дерекқорлар мен бағдарламалық модульдер жаңартулары;
- Kaspersky Security Center құрамдастарын жаңарту;
- Kaspersky қауіпсіздік бағдарламалары жаңартулары.

Жаңартуларды жүктегеннен кейін, оларды басқарылатын құрылғыларға таратуға болады.

*Таңдалған басқару тобына **Жаңартуларды тарату нүктесінің қоймаларына жүктеп алу** тапсырмасын жасау үшін:*

1. Бағдарламаның негізгі терезесінде **Тапсырмалар** бөліміне өтіңіз.



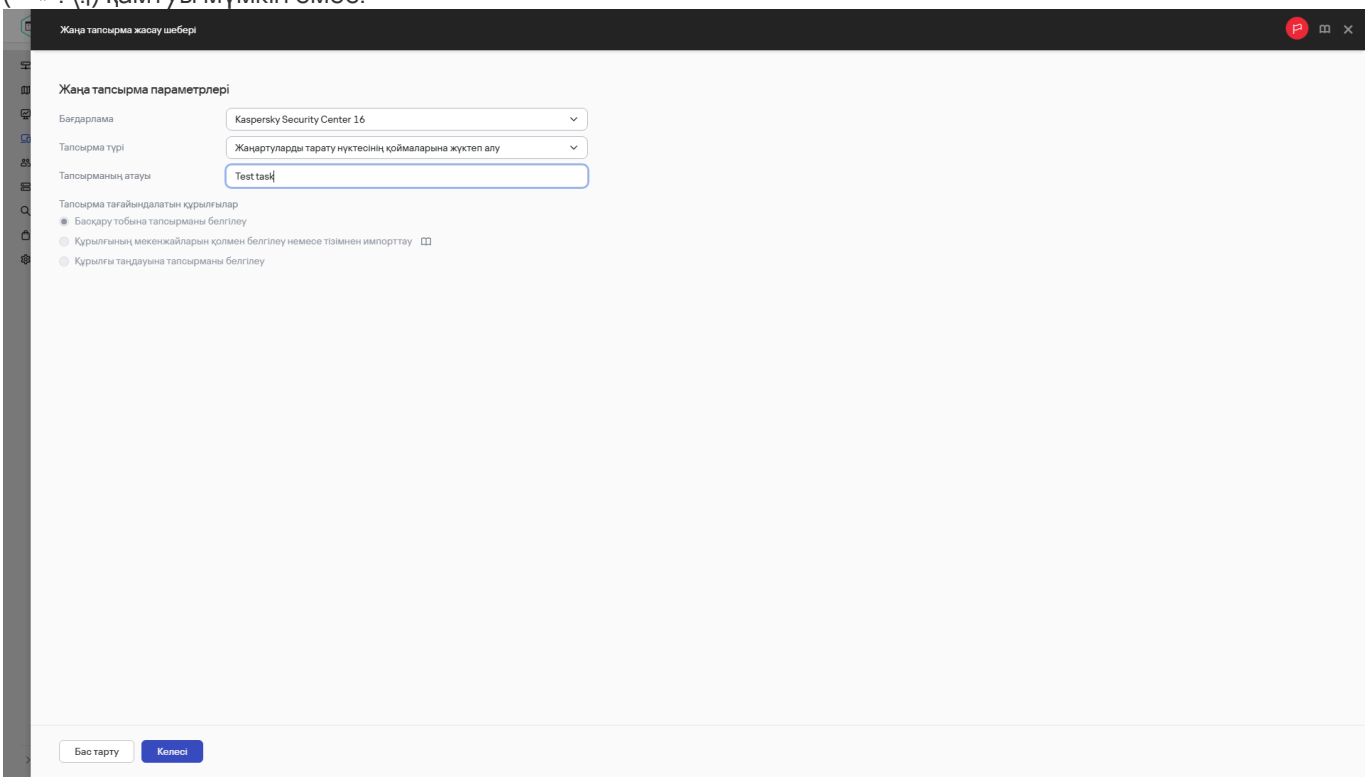
Тапсырмалар бөлімі

2. **Қосу** түймесін басыңыз.

   Жаңа тапсырма жасау шебері іске қосылады. Содан кейін, шебердің нұсқауларын орындаңыз.

3. Kaspersky Security Center бағдарламасы үшін **Task type** өрісінен **Жаңартуларды тарату нүктесінің қоймаларына жүктеп алу** тармағын таңдаңыз.

4. Жасап жатқан тапсырманың атын көрсетіңіз. Тапсырма атауы 100 таңбадан асуы және арнайы таңбаларды ("*<>?\:|) қамтуы мүмкін емес.



Жаңартуларды тарату нүктесінің қоймаларына жүктеп алу тапсырмасын жасау

5. Басқару тобын, тапсырма қолданылатын құрылғылар немесе құрылғы таңдауын көрсету үшін таңдау түймесін басыңыз.

6. **Тапсырманы жасауды аяқтау** қадамында, әдепкі бойынша тапсырма параметрлерін өзгерткіңіз келсе, **Жасап болған соң, тапсырма туралы мәліметтерді ашу** параметрін қосыңыз. Егер сіз бұл параметрді қоспасаңыз, тапсырма әдепкі бойынша белгіленген параметр мәндерімен жасалады. Әдепкі бойынша параметр мәндерін кейінірек кез келген уақытта өзгертуге болады.

7. **Жасау** түймесін басыңыз.

   Тапсырма жасалып, тапсырмалар тізімінде көрсетіледі.

8. Тапсырма сипаттары терезесін ашу үшін жасалған тапсырманың атын басыңыз.

9. Тапсырма сипаттары терезесінің **Бағдарлама параметрлері** қойыншасында келесі параметрлерді көрсетіңіз:

   - **Жаңартулардың көздері**

     Тарату нүктелері үшін жаңарту көзі ретінде келесі ресурстарды пайдалануға болады:

     - Kaspersky жаңарту серверлері

       Kaspersky бағдарламаларына дерекқорлар мен модульдердің жаңартуларын жіберетін Kaspersky HTTP серверлері мен HTTPS серверлері.

       Әдепкі бойынша, осы нұсқа таңдалады.

     - Жергілікті немесе желілік қалта

       Соңғы жаңартуларды қамтитын жергілікті немесе желілік қалта. Желілік қалта ретінде тек орнатылған ортақ SMB қалтасын пайдалануға болады. Жергілікті қалтаны таңдағанда, Басқару сервері орнатылған құрылғыдағы қалтаны көрсету қажет.

Басқару серверінің қоймасына жаңартуларды жүктеп алу және *Тарату нүктелерінің қоймаларына жаңартуларды жүктеп алу* тапсырмаларында, егер жаңарту көзі ретінде құпиясөзбен қорғалған жергілікті немесе желілік қалта таңдалған болса, пайдаланушының аутентификациясы жұмыс істемейді. Бұл мәселені шешу үшін алдымен құпиясөзбен қорғалған қалтаны жөндеңіз, содан кейін қажетті есептік деректерді (мысалы, операциялық жүйенің құралдарымен) көрсетіңіз. Осыдан кейін жаңартуларды жүктеу тапсырмасында жаңарту көзі ретінде осы қалтаны таңдауға болады. Kaspersky Security Center Linux сізден есептік деректерді енгізуді талап етпейді.

- **Жаңартулар сақталатын қалта**

  Сақталған жаңартуларды сақтау үшін көрсетілген қалтаға апаратын жол. Көрсетілген қалтаға апаратын жолды алмасу буферіне көшіруге болады. Топтық тапсырма үшін көрсетілген қалтаға апаратын жолды өзгерте алмайсыз.

- **diff файлдарды жүктеп алу**

  Бұл параметр айырмашылық файлдарын жүктеп алу функциясын қосады.

  Әдепкі бойынша, параметр өшірулі.

- **Ескі схеманы пайдаланып, жаңартуларды жүктеп алу**

  14-ші нұсқадан бастап, Kaspersky Security Center бағдарламасы дерекқорлар мен бағдарлама модульдері жаңартуларын жаңа схема бойынша жүктеп алады. Бағдарлама жаңартуларды жаңа схеманың көмегімен жүктей алуы үшін, жаңарту көзі жаңа схемамен үйлесімді метадеректері бар жаңарту файлдарын қамтуы керек. Жаңарту көзінде тек ескі схемамен үйлесімді метадеректері бар жаңарту файлдары болса, **Ескі схеманы пайдаланып, жаңартуларды жүктеп алу** параметрін қосыңыз. Әйтпесе, жаңартуларды жүктеу тапсырмасы қатемен аяқталады.

  Мысалы, жаңарту көзі ретінде жергілікті немесе желілік қалта көрсетілсе және осы қалтадағы жаңарту файлдары келесі бағдарламалардың бірімен жүктелген болса, осы параметрді қосу керек:

  - Kaspersky Update Utility

    Бұл утилита жаңартуларды ескі схема бойынша жүктейді.

  - Kaspersky Security Center 13 Linux

    Мысалы, тарату нүктесі жергілікті немесе желілік қалтадан жаңартуларды алу үшін конфигурацияланған. Бұл жағдайда, сіз интернетке қосылған Басқару серверін пайдалану арқылы жаңартуларды жүктей аласыз, содан кейін жаңартуларды тарату нүктесіндегі жергілікті қалтаға орналастыра аласыз. Басқару сервері нұсқасының нөмірі 13 болса, *Тарату нүктелерінің қоймаларына жаңартуларды жүктеу* тапсырмасында **Ескі схеманы пайдаланып, жаңартуларды жүктеп алу** опциясын қосыңыз.

  Әдепкі бойынша, параметр өшірулі.

10. Тапсырманы іске қосу кестесін жасаңыз. Қажет болса, келесі параметрлерді конфигурациялаңыз:

- **Тапсырманы бастау**:

  - **Қолмен** (әдепкі бойынша таңдалған)

    Тапсырма автоматты түрде іске қосылмайды. Тапсырманы тек қолмен іске қосуға болады.

    Әдепкі бойынша, осы нұсқа таңдалған.

- **N минут сайын**

  Тапсырма жүйелі түрде, тапсырма жасалған күні көрсетілген уақыттан бастап, минуттар түрінде белгіленген аралықпен орындалады.

  Әдепкі бойынша, тапсырма ағымдағы жүйелік уақыттан бастап 30 минут сайын іске қосылады.

- **N сағат сайын**

  Тапсырма көрсетілген күн мен уақыттан бастап, сағат түрінде белгіленген аралықпен жүйелі түрде орындалады.

  Әдепкі бойынша, тапсырма ағымдағы жүйелік күн мен уақыттан бастап 6 сағат сайын іске қосылып тұрады.

- **N күн сайын**

  Тапсырма, күндер түрінде белгіленген аралықпен жүйелі түрде орындалады. Сондай-ақ, сіз тапсырманы бірінші рет іске қосу күні мен уақытын да көрсете аласыз. Бұл қосымша параметрлерге сіз тапсырма жасап жатқан бағдарлама қолдау көрсетсе, олар қолжетімді болады.

  Әдепкі бойынша, тапсырма ағымдағы жүйелік күн мен уақыттан бастап күн сайын іске қосылады.

- **Апта күндері бойынша**

  Тапсырма жүйелі түрде, аптаның көрсетілген күндерінде, көрсетілген уақытта орындалады.

  Әдепкі бойынша, тапсырма жұма сайын, сағат 18:00:00-де іске қосылады.

- **Ай сайын**

  Тапсырма жүйелі түрде, айдың көрсетілген күнінде, көрсетілген уақытта орындалады.

  Көрсетілген күні жоқ айларда тапсырма соңғы күні орындалады.

  Әдепкі бойынша, тапсырма әр айдың бірінші күнінде, ағымдағы жүйелік уақытта орындалады.

- **Таңдалған апта күні ай сайын**

  Тапсырма жүйелі түрде, әр айдың көрсетілген күндерінде, көрсетілген уақытта орындалады.

  Әдепкі бойынша, басталу уақыты 18:00 және айдың күндері таңдалмайды.

  > Айдағы нақты күнді де, апта нөмірін де (айдың бірінші, екінші аптасын) емес, ай ішіндегі апта күнінің реттік нөмірін таңдайтыныңызды ескеріңіз. Мысалы, егер сіз курсорды **Сс** жолдың **Бірінші** ұяшығына орнатсаңыз, бұл тапсырма әр жаңа айдың бірінші сейсенбісінде орындалатынын білдіреді.

  Аптаның бірнеше күнін таңдай аласыз.

- **Вирустық шабуылды анықтағанда**

  Тапсырманы *Вирустың тарауы* оқиғасы туындағаннан кейін іске қосуға болады. Вирустық шабуылдарды қадағалайтын бағдарлама түрлерін таңдаңыз. Бағдарламалардың келесі түрлері қолжетімді:

  - жұмыс станциялары мен файлдық серверлерге арналған вирусқа қарсы бағдарламалар;
  - периметрлік қорғанысқа арналған вирусқа қарсы бағдарламалар;
  - пошталық жүйелерге арналған вирусқа қарсы бағдарламалар.

Әдепкі бойынша, бағдарламалардың барлық түрлері таңдалған.

Вирустық шабуыл туралы хабарлайтын қауіпсіздік бағдарламасының түріне байланысты әртүрлі тапсырмаларды іске қосуға болады. Бұл жағдайда, сізге қажет емес бағдарлама түрлерін таңдауды алып тастаңыз.

- **Басқа тапсырманы аяқтағанда**

  Ағымдағы тапсырма басқа тапсырма аяқталғаннан кейін іске қосылады. Екі тапсырма да бір құрылғы арқылы тағайындалса ғана, осы параметр жұмыс істейді. Мысалы, *Құрылғыларды басқару* тапсырмасын **Құрылғыны қосу** параметрінің көмегімен іске қоса аласыз және ол аяқталғаннан кейін *Вирустарды іздеу* тапсырмасын іске қоса аласыз.

  Кестеден іске қосу тапсырмасын және осы тапсырма орындалатын күйді таңдау керек (**Сәтті аяқталды** немесе **Сәтсіз аяқталды**).

  Қажет болса, кестедегі тапсырмаларды төмендегідей іздеуге, сұрыптауға және сүзуге болады:

  - Тапсырманы атауы бойынша іздеу үшін іздеу өрісіне тапсырма атауын енгізіңіз.
  - Тапсырмаларды атауы бойынша сұрыптау үшін сұрыптау белгішесін басыңыз.

    Әдепкі бойынша, тапсырмалар өсу ретімен әліпбилік ретпен сұрыпталады.
  - Сүзгі белгішесін басыңыз және ашылатын терезеде тапсырмаларды топтар бойынша сүзіңіз, содан кейін **Қолдану** түймесін басыңыз.

- **Өткізіп алынған тапсырмаларды іске қосу**

  Бұл параметр, тапсырма басталғалы тұрған кезде клиент құрылғысы желіде көрсетілмесе, тапсырманың жүріс-тұрысын анықтайды.

  Параметр қосулы болса, клиент құрылғысында Kaspersky бағдарламасын кезекті рет іске қосу кезінде тапсырманы іске қосу әрекеті жасалады. Тапсырманың кестесінде **Қолмен**, **Бір рет** немесе **Дереу** іске қосу көрсетілсе, онда тапсырма желіде құрылғы көзге көрінетін болғаннан кейін немесе құрылғы тапсырманың әрекет ету ауқымына қосылғаннан кейін бірден іске қосылады.

  Егер параметр өшірулі болса, клиент құрылғыларында тапсырманы іске қосу тек кесте бойынша орындалатын болады. **Қолмен**, **Бір рет** және **Дереу** кестесі үшін тапсырмалар желіде көрінетін клиенттік құрылғыларда ғана орындалады. Мысалы, сіз бұл параметрді тек жұмыс уақытынан тыс уақытта іске қосқыңыз келетін ресурстарды қажетсінетін тапсырма үшін өшіре аласыз.

  Әдепкі бойынша, параметр өшірулі.

- **Тапсырманы бастау үшін автоматты түрде араластырылған кідірісті пайдалану**

  Параметр қосулы болса, тапсырма клиент құрылғыларында белгілі бір уақыт аралығында кездейсоқ іске қосылады, яғни *тапсырманың таратылған іске қосылуы* орын алады. Тапсырманың таратылған іске қосылуы, тапсырманы кесте бойынша іске қосу кезінде көптеген клиент құрылғыларының Басқару серверіне бір уақытта жүгінуіне жол бермейді.

  Таратылған іске қосылу кезеңі, тапсырма тағайындалған клиент құрылғыларының санына байланысты тапсырманы жасау кезінде автоматты түрде есептеледі. Кейінірек, тапсырма әрқашан есептелген іске қосу уақытында іске қосылады. Алайда, тапсырма параметрлеріне түзетулер енгізілгенде немесе тапсырма қолмен іске қосылғанда, тапсырманы іске қосу уақытының есептелген мәні өзгереді.

  Егер параметр өшірулі болса, клиент құрылғыларында тапсырманы іске қосу кесте бойынша орындалады.

- **Тапсырманы бастауға арналған келесі аралықтағы автоматты кездейсоқ кідірісті пайдалану**

  Параметр қосулы болса, тапсырма клиент құрылғыларында белгілі бір уақыт аралығында кездейсоқ іске қосылады. Тапсырманың таратылған іске қосылуы, тапсырманы кесте бойынша іске қосу кезінде көптеген клиент құрылғыларының Басқару серверіне бір уақытта жүгінуіне жол бермейді.

  Егер параметр өшірулі болса, клиент құрылғыларында тапсырманы іске қосу кесте бойынша орындалады.

  Әдепкі бойынша, параметр өшірулі. Әдепкі бойынша, уақыт аралығы бір минутқа тең.

11. **Сақтау** түймесін басыңыз.

Тапсырма жасалды және конфигурацияланды.

Тапсырманы жасау кезінде көрсетілетін параметрлерге қосымша ретінде, сіз осы тапсырманың басқа параметрлерін өзгерте аласыз.

Жаңартуларды тарату нүктесінің қоймаларына жүктеп алу тапсырмасын орындау нәтижесінде, дерекқорлар мен бағдарламалық модульдердің жаңартулары жаңарту көзінен көшіріледі және ортақ қатынасы бар қалтаға орналастырылады. Жүктелген жаңартуларды тек көрсетілген басқару тобына кіретін және жаңартуларды алу үшін нақты белгіленген тапсырмасы жоқ тарату нүктелері ғана пайдаланады.

Басқару серверінің қоймасына жаңартуларды жүктеп алу тапсырмасы үшін жаңарту көздерін қосу

Басқару серверінің қоймасына жаңартуларды жүктеп алу тапсырмасын жасағанда немесе пайдаланған кезде келесі жаңарту көздерін таңдауға болады:

- Kaspersky жаңарту серверлері
- Негізгі Басқару сервері

  Бұл ресурс қосалқы немесе виртуалды Басқару сервері үшін жасалған тапсырмаларға қатысты қолданылады.

- Жергілікті немесе желілік қалта

> *Басқару серверінің қоймасына жаңартуларды жүктеп алу* және *Тарату нүктелерінің қоймаларына жаңартуларды жүктеп алу* тапсырмаларында, егер жаңарту көзі ретінде құпиясөзбен қорғалған жергілікті немесе желілік қалта таңдалған болса, пайдаланушының аутентификациясы жұмыс істемейді. Бұл мәселені шешу үшін алдымен құпиясөзбен қорғалған қалтаны жөндеңіз, содан кейін қажетті есептік деректерді (мысалы, операциялық жүйенінің құралдарымен) көрсетіңіз. Осыдан кейін жаңартуларды жүктеу тапсырмасында жаңарту көзі ретінде осы қалтаны таңдауға болады. Kaspersky Security Center Linux сізден есептік деректерді енгізуді талап етпейді.

Kaspersky жаңарту серверлері әдепкі бойынша пайдаланылады, бірақ жаңартуларды жергілікті немесе желілік қалтадан жүктеп алуға да болады. Желіде интернетке кіру мүмкіндігі болмаса, бұл қалтаны пайдалануға болады. Бұл жағдайда Kaspersky жаңарту серверлерінен жаңартуларды қолмен жүктеп алуға және жүктелген файлдарды қажетті қалтаға орналастыруға болады. Жергілікті немесе желілік қалтаға бір ғана жолды көрсетуге болады.

Жергілікті қалтаны таңдағанда, Басқару сервері орнатылған құрылғыдағы қалтаны көрсету қажет. Қалтаға апаратын жол құрылғының амалдық жүйесіне байланысты. Жергілікті қалта Linux негізіндегі Басқару серверінде орналасқандықтан, POSIX жолын көрсету керек, мысалы: /path/to/dir.

Желілік қалта ретінде тек орнатылған ортақ SMB қалтасын пайдалануға болады. Егер SMB үлесі аутентификацияны қажет етсе, ол қажетті есептік деректерімен жүйеге алдын ала қосылуы керек. SMB1 протоколын пайдалану ұсынылмайды, себебі ол қауіпті.

Жаңарту көздерін қосу үшін:

1. Бағдарламаның негізгі терезесінде **Тапсырмалар** бөліміне өтіңіз.
2. **Жаңартуларды Басқару серверінің қоймасына жүктеп алу** түймесін басыңыз.
3. **Бағдарлама параметрлері** қойыншасына өтіңіз.
4. **Жаңартулардың көздері** кестесінде **Қосу** түймесін басыңыз.
5. Ашылған терезеде қажетті жаңарту көздерін қосып, **Сақтау** түймесін басыңыз.

   Егер сіз **Жергілікті немесе желілік қалта** жалаушасын орнатсаңыз, қалтаға жолды көрсетіңіз.
6. Тапсырма терезесінде **Сақтау** түймесін басыңыз.

Жаңартулар енді Басқару серверінің қоймасына көрсетілген көздерден жүктеледі.

Kaspersky жаңарту серверлерін, сондай-ақ жергілікті немесе желілік қалтаны қоссаңыз, жаңартуларға басымдықтарды орнатуға болады. Мұны істеу үшін, **Жаңартулардың көздері** кестесінде басымдылығын өзгерткіңіз келетін жаңартудың жанына құсбелгіні қойып, **Жоғары жылжыту** немесе **Төменге жылжыту** түймесін басыңыз.

Бағдарламалық жасақтама жаңартуын мақұлдау және қабылдамау

Жаңартуларды орнату тапсырмасының параметрлері, орнатылуы тиісті жаңартуларды мақұлдауды талап етуі мүмкін. Орнату қажет болған жаңартуларды растай аласыз немесе орнатылмауы тиісті жаңартулардан бас тарта аласыз.

Мысалы, сіз алдымен жаңартуларды сынақ ортасында орнатуды тексеріп, олар құрылғылардың жұмысына кедергі келтірмейтіндігіне көз жеткізіп алып, содан кейін осы жаңартуларды клиент құрылғыларына орната аласыз.

Жаңартуларды мақұлдау және қабылдамау Windows жүйесінде орнатылған клиенттік құрылғыларда орнатылған Желілік агент және басқарылатын қолданбалар үшін ғана қолжетімді. Басқару серверін, Kaspersky Security Center Web Console веб-консолін және веб-басқару плагиндерін үздіксіз жаңартуға қолдау көрсетілмейді. Бұл компоненттерді жаңарту үшін, олардың соңғы нұсқаларын Kaspersky сайтынан жүктеп алу және қолмен орнату керек.

Бір немесе бірнеше жаңартуды растау немесе болдырмау үшін:

1. Бағдарламаның негізгі терезесінде **Бағдарламалық жасақтаманы басқару** → **Kaspersky бағдарламалары** → **Байқалмайтын жаңартулар** бөліміне өтіңіз.

Қолжетімді жаңартулар тізімі көрсетіледі.

Басқарылатын бағдарламаларды жаңарту үшін Kaspersky Security Center бағдарламасының белгілі бір ықшам нұсқасын орнату қажет болуы мүмкін. Бұл нұсқа сіздің қазіргі нұсқаңыздан да соңғы болса, бұл жаңартулар көрсетілсе де, оларды мақұлдау мүмкін емес. Сондай-ақ, Kaspersky Security Center жаңартпайынша, осындай жаңартулардан орнату пакеттерін жасау мүмкін емес. Сізге Kaspersky Security Center данасын қажетті ықшам нұсқаға дейін жаңарту ұсынылады.

2. Қажет болса, **Лицензиялық келісімдерді қарап шығу және қабылдау** түймесін басу арқылы Лицензиялық келісімді қабылдаңыз.

3. Растау немесе қабылдамау қажет болған жаңартуларды таңдаңыз.

4. Таңдалған жаңартуды мақұлдау үшін **Бекіту** түймесін басыңыз немесе таңдалған жаңартуды қабылдамау үшін **Қабылдамау** түймесін басыңыз.

   Әдепкі бойынша, *Анықталмаған* мәні орнатылған.

Расталды күйі белгіленген жаңартулар орнатуға кезекке қойылады.

Қабылданбады күйі белгіленген жаңартулар, бұған дейін орнатылған құрылғылардан жойылады (бұл мүмкін болса). Сондай-ақ, олар құрылғыларға кейінірек орнатылмайды.

Kaspersky бағдарламаларына арналған жаңартулардың кейбірін жою мүмкін емес. Оларға *Қабылданбады* күйін белгілеген болсаңыз, Kaspersky Security Center Linux қолданбасы осы жаңартуларды бұған дейін орнатылған құрылғылардан жоймайды. Мұндай жаңартулар болашақта құрылғыларға ешқашан орнатылмайды.

Үшінші тарап бағдарламалық жасақтамасының жаңартулары үшін *Қабылданбады* күйін белгілеп жатсаңыз, бұл жаңартулар орнатылуы жоспарланған, бірақ әлі орнатылмаған құрылғыларға орнатылмайды. Жаңартулар әлдеқашан орнатылған құрылғыларда қала береді. Жаңартуларды жою қажет болса, мұны жергілікті түрде қолмен орындай аласыз.

Kaspersky Endpoint Security for Windows жаңартуларын автоматты түрде орнату

Клиент құрылғыларында Kaspersky Endpoint Security for Windows бағдарламасының дерекқорлары мен модульдерін автоматты түрде жаңартуды конфигурациялауға болады.

Kaspersky Endpoint Security for Windows жаңартуларын құрылғыларға жүктеуді және автоматты түрде орнатуды конфигурациялау үшін:

1. Бағдарламаның негізгі терезесінде **Тапсырмалар** бөліміне өтіңіз.

2. **Қосу** түймесін басыңыз.

   Жаңа тапсырма жасау шебері іске қосылады. Содан кейін, шебердің нұсқауларын орындаңыз.

3. Kaspersky Endpoint Security for Windows бағдарламасы үшін **Жаңарту** тапсырмасы ішкі түрін таңдаңыз.

4. Жасап жатқан тапсырманың атын көрсетіңіз. Тапсырма атауы 100 таңбадан асуы және арнайы таңбаларды ("*<>?\:|) қамтуы мүмкін емес.

5. Тапсырманың әрекет ету ауқымын таңдаңыз.

6. Тапсырма қолданылатын басқару тобын, құрылғылар немесе құрылғы таңдауын көрсетіңіз.

7. **Тапсырманы жасауды аяқтау** қадамында, әдепкі бойынша тапсырма параметрлерін өзгерткіңіз келсе, **Жасап болған соң, тапсырма туралы мәліметтерді ашу** параметрін қосыңыз. Егер сіз бұл параметрді қоспасаңыз, тапсырма әдепкі бойынша белгіленген параметр мәндерімен жасалады. Әдепкі бойынша параметр мәндерін кейінірек кез келген уақытта өзгертуге болады.

8. **Жасау** түймесін басыңыз.

   Тапсырма жасалып, тапсырмалар тізімінде көрсетіледі.

9. Тапсырма сипаттары терезесін ашу үшін жасалған тапсырманың атын басыңыз.

10. Жаңарту тапсырмасы сипаттары терезесінде, **Бағдарлама параметрлері** қойыншасында жергілікті немесе ұялы режимді көрсетіңіз:

    - **Жергілікті режим**: құрылғы мен Басқару сервері арасында байланыс орнатылған.
    - **Ұялы режим**: құрылғы мен Kaspersky Security Center Linux арасында байланыс орнатылмаған (мысалы, құрылғы интернетке қосылмаған болса).

11. Kaspersky Endpoint Security for Windows бағдарламасының дерекқорлары мен модульдерін жаңарту үшін пайдаланғыңыз келетін жаңарту көздерін қосыңыз. Тізімдегі жаңарту көздерінің орнын өзгерту қажет болса, **Жоғары жылжыту** және **Төменге жылжыту** түймелерін пайдаланыңыз. Бірнеше жаңарту көздері қосылған болса, Kaspersky Endpoint Security for Windows бағдарламасы оларға бір-бірлеп, тізімнің жоғарғы жағынан бастап қосылуға тырысады және бірінші қолжетімді көзден жаңарту пакетін алып шығару арқылы жаңарту тапсырмасын орындайды.

12. Бағдарлама модульдерінің жаңартуларын бағдарлама дерекқорларымен бірге жүктеу және орнату үшін **Бағдарлама модульдерінің жаңартуларын орнату** параметрін қосыңыз.

    Егер параметр қосулы болса, Kaspersky Endpoint Security for Windows бағдарламасы пайдаланушыға бағдарлама модульдерінің қолжетімді жаңартулары туралы хабарлайды және жаңарту тапсырмасы орындалған кезде бағдарлама модульдерінің жаңартуларын жаңарту пакетіне қосады. Kaspersky Endpoint Security for Windows бағдарламасы тек сіз *Расталды* күйін орнатқан жаңартуларды орнатады; жаңартулар қолданба интерфейсі арқылы немесе Kaspersky Security Center Linux арқылы жергілікті түрде орнатылады.

    Сондай-ақ, **Бағдарлама модулінің критикалық жаңартуларын автоматты түрде орнату** параметрін қосуға да болады. Бағдарлама модульдерінің жаңартулары болған кезде, Kaspersky Endpoint Security for Windows бағдарламасы *Критикалық* күйі бар жаңартуларды автоматты түрде орнатады; бағдарлама модульдерінің қалған жаңартуларын – әкімші оларды орнатуды мақұлдағаннан кейін.

    Егер бағдарлама модульдерін жаңарту Лицензиялық келісімнің және Құпиялылық саясатының ережелерімен танысуды және келісуді көздейтін болса, онда пайдаланушы Лицензиялық келісімнің және Құпиялылық саясатының ережелерімен келіскеннен кейін, бағдарлама жаңартуды белгілейді.

13. Бағдарлама жүктелген жаңартуларды қалтаға сақтайтын **Жаңартуларды қалтаға көшіру** жалаушасын қойыңыз, содан кейін қалта жолын көрсетіңіз.

14. Тапсырманы бастау кестесін белгілеңіз. Уақтылы жаңартуды қамтамасыз ету үшін, **Қоймаға жаңартуларды жүктеу кезінде** нұсқасын таңдау ұсынылады.

15. **Сақтау** түймесін басыңыз.

Жаңарту тапсырмасын орындау кезінде, бағдарлама Kaspersky жаңартулар серверлеріне сұрау салады.

Кейбір жаңартулар басқарылатын бағдарлама плагиндерінің соңғы нұсқаларын орнатуды талап етеді.

Kaspersky дерекқорлары мен бағдарламалық модульдерін жаңарту үшін айырмашылық файлдарын пайдалану туралы

Kaspersky Security Center Linux бағдарламасы Kaspersky жаңартулар серверлерінен жаңартуларды жүктеп алғанда, ол трафикті айырмашылық файлдары арқылы оңтайландырады. Сондай-ақ, желіңіздегі басқа құрылғылардан жаңартуларды қабылдайтын құрылғылардың (Басқару серверлері, тарату нүктелері және клиент құрылғылары) айырмашылық файлдарын пайдалануын қосуға болады.

Айырмашылық файлдарын жүктеу функциясы туралы

Айырмашылықтар файлы дерекқор немесе бағдарламалық модуль файлдарының екі нұсқасы арасындағы айырмашылықтарды сипаттайды. Айырмашылық файлдарын пайдалану трафикті ұйымыңыздың желісінде сақтайды, өйткені айырмашылық файлдары бүкіл дерекқор және бағдарламалық модуль файлдарына қарағанда аз орын алады. *diff файлдарды жүктеп алу* функциясы Басқару сервері немесе тарату нүктесі үшін қосылса, айырмашылық файлдары сол Басқару серверінде немесе тарату нүктесінде сақталады. Нәтижесінде, осы Басқару серверінен немесе тарату нүктелерінен жаңартулар алатын құрылғылар өздерінің дерекқорлары мен бағдарламалық модульдерін жаңарту үшін сақталған айырмашылық файлдарын пайдалана алады.

Айырмашылық файлдарын пайдалануды оңтайландыру үшін құрылғыны жаңарту кестесін Басқару серверінің жаңарту кестесімен немесе сол құрылғы жаңартуларды алатын тарату нүктелерімен синхрондау ұсынылады. Дегенмен, құрылғылар Басқару серверіне немесе құрылғы жаңартуларды алатын тарату нүктелеріне қарағанда бірнеше есе аз жаңартылса да, трафикті сақтауға болады.

Тарату нүктелері айырмашылық файлдарын автоматты түрде тарату үшін көп мекенжайлы IP таратылымын пайдаланбайды.

Айырмашылық файлдарын жүктеу функциясын қосу

Кезеңдер

1. **Басқару серверіндегі функцияны қосу**

   Жаңартуларды басқару серверінің қоймасына жүктеп алу тапсырмасының параметрлерінде мүмкіндікті қосыңыз.

2. **Тарату нүктесі үшін функцияны қосу**

   Жаңартуларды тарату орындарының қоймаларына жүктеу тапсырмасының көмегімен жаңартуларды алып тұратын тарату нүктесі үшін функцияны іске қосу.

   Содан кейін басқару серверінен жаңартуларды алатын тарату нүктесі үшін Желілік агенттің саясат параметрлерінде функцияны іске қосыңыз.

   Басқару серверінен жаңартуларды алып тұратын тарату нүктесі үшін функцияны қосыңыз.

   Бұл функция Желілік агент саясатының параметрлерінде және (тарату нүктелері қолмен тағайындалған болса және саясат параметрлерін қайта анықтағыңыз келсе) басқару серверінің сипаттарындағы **Тарату нүктелері** бөлімінде қосылады.

Айырмашылық файлдарын жүктеу функциясы сәтті қосылғанын тексеру үшін сценарийді орындағанға дейін және одан кейін ішкі трафикті өлшеуге болады.

Тарату нүктелері арқылы жаңартуларды жүктеп алу

Kaspersky Security Center Linux бағдарламасы, тарату нүктелеріне Басқару серверінен, Kaspersky серверлерінен, жергілікті немесе желілік қалтадан жаңартулар алып тұруға мүмкіндік береді.

Тарату нүктесі үшін жаңартулар алуды конфигурациялау үшін келесі әрекеттерді орындаңыз:

1. Негізгі мәзірдегі басқару серверінің атауын басыңыз.

   Басқару серверінің сипаттары терезесі ашылады.

2. **Жалпы** қойыншасында **Тарату нүктелері** бөлімін таңдаңыз.

3. Топтағы клиенттік құрылғыларға жаңартулар жеткізілетін тарату нүктесінің атауын басыңыз.

4. Тарату нүктесі сипаттары терезесінде **Жаңартулар көзі** бөлімін таңдаңыз.

5. Тарату нүктесі үшін жаңартулар көзін таңдаңыз:

   - **Жаңартулар көзі**

     Тарату нүктесі үшін жаңартулар көзін таңдаңыз:

     - Тарату нүктесі Басқару серверінен жаңартулар алып тұруы үшін, **Басқару серверінен шығарып алу** нұсқасын таңдаңыз.

     - Тарату нүктесіне тапсырма арқылы жаңартуларды алуға рұқсат беру үшін, **Жаңартуды жүктеп алу тапсырмасын пайдалану** тармағын таңдаңыз және *Жаңартуларды тарату нүктелерінің қоймаларына жүктеу* тапсырмасын көрсетіңіз:

       - Егер мұндай тапсырма құрылғы үшін бұрыннан бар болса, тізімнен тапсырманы таңдаңыз.

       - Егер құрылғы үшін мұндай тапсырма әлі болмаса, тапсырманы жасау үшін **Тапсырма жасау** сілтемесінен өтіңіз. Жаңа тапсырма жасау шебері іске қосылады. Содан кейін, шебердің нұсқауларын орындаңыз.

   - **diff файлдарды жүктеп алу**

     Бұл параметр айырмашылық файлдарын жүктеп алу функциясын қосады.

     Әдепкі бойынша, параметр қосулы.

Нәтижесінде, тарату нүктесі көрсетілген көзден жаңартулар алып тұрады.

Автономды құрылғыларда Kaspersky дерекқорлары мен бағдарламалық жасақтама модульдеріне арналған жаңартулар

Басқарылатын құрылғыларда Kaspersky дерекқорлары мен бағдарламалық жасақтама модульдеріне арналған жаңартулар, құрылғыларды вирустар мен басқа да қауіптерден қорғауды қамтамасыз етуге арналған маңызды тапсырма болып табылады. Әкімші Басқару сервері қоймасының көмегімен тұрақты жаңартуды конфигурациялайды.

Басқару серверіне (негізгі немесе қосалқы), тарату нүктесіне немесе интернетке қосылмаған құрылғыдағы (немесе құрылғылар тобындағы) дерекқорлар мен бағдарламалық модульдерді жаңарту қажет болғанда, FTP сервері немесе жергілікті қалта сияқты баламалы жаңарту көздерін пайдалану керек. Бұл жағдайда, флеш-дискі немесе сыртқы қатты диск сияқты жаппай сақтау құрылғысы арқылы қажетті жаңартулар файлдарын жеткізу керек.

Қажетті жаңартуларды осыдан көшіруге болады:

- Басқару сервері.

  Басқару сервері қоймасында автономды құрылғыда орнатылған қауіпсіздік бағдарламасына қажетті жаңартулар болуы үшін, басқарылатын желілік құрылғылардың кем дегенде біреуінде осы қауіпсіздік бағдарламасы орнатылуы керек. Бұл бағдарлама *Жаңартуларды Басқару серверінің қоймасына жүктеп алу* тапсырмасы арқылы Басқару сервері қоймасынан жаңартуларды алу үшін конфигурациялануы керек.

- Бірдей қауіпсіздік бағдарламасы орнатылған және Басқару сервері қоймасынан, тарату нүктесі қоймасынан немесе тікелей Kaspersky жаңарту серверлерінен жаңартулар алуға конфигурацияланған кез келген құрылғы.

Төменде Басқару сервері қоймасынан көшіру арқылы дерекқорлар мен бағдарламалық модульдер жаңартуларын орнатудың мысалы келтірілген.

Автономды құрылғылардағы Kaspersky дерекқоры мен бағдарламалық модульдерін жаңарту үшін:

1. Алынбалы жетекті Басқару сервері орнатылған құрылғыға қосыңыз.

2. Жаңарту файлдарын алынбалы жетекке көшіріңіз.

   Әдепкісінше жаңартулар мына жерде орналасқан: /var/opt/kaspersky/klnagent_srv/1093/.working/share_srv/Updates/.

   Сондай-ақ, сіз Kaspersky Security Center Linux бағдарламасында жаңартуларды өзіңіз таңдаған қалтаға үнемі көшіруді конфигурациялай аласыз. Бұл үшін, *Жаңартуларды Басқару серверінің қоймасына жүктеп алу* тапсырмасының сипаттарында **Алынған жаңартуларды қосымша қалталарға көшіру** параметрін қолданыңыз. Егер сіз жаппай сақтау құрылғысында немесе сыртқы қатты дискіде орналасқан қалтаны осы параметрдің мақсатты қалтасы ретінде көрсетсеңіз, бұл жаппай сақтау құрылғысында әрқашан жаңартулардың соңғы нұсқасы болады.

3. Автономды құрылғыларда жергілікті қалтадан немесе FTP сервері немесе ортақ қалтасы сияқты ортақ ресурстан жаңартуларды алу үшін Kaspersky Endpoint Security конфигурациялаңыз.

   Нұсқаулар:

   - Kaspersky Endpoint Security for Linux онлайн-анықтамасы
   - Kaspersky Endpoint Security for Windows онлайн-анықтамасы

4. Жаңарту файлдарын алынбалы жетектен жергілікті қалтаға немесе жаңартулар көзі ретінде пайдаланғыңыз келетін ортақ ресурсқа көшіріңіз.

5. Жаңартуларды орнатуды қажет ететін автономды құрылғыда автономды құрылғының операциялық жүйесіне байланысты Kaspersky Endpoint Security for Linux немесе Kaspersky Endpoint Security for Windows *Жаңарту* тапсырмасын іске қосыңыз.

Жаңарту тапсырмасы аяқталғаннан кейін, Kaspersky дерекқорлары мен бағдарламалық модульдері құрылғыда жаңартылады.

Мониторинг, есеп беру және аудит

Бұл бөлімде, Kaspersky Security Center Linux-те есептермен жұмыс істеу және мониторинг жүргізу функциялары сипатталған. Бұл функциялар желіңіздің инфрақұрылымы, қорғаныс күйі, сондай-ақ статистика туралы мәлімет алуға мүмкіндік береді.

Kaspersky Security Center Linux бағдарламасын орналастыру немесе оның жұмыс істеуі барысында мониторинг функцияларын және есеп параметрлерін конфигурациялауға болады.

Сценарий: Бақылау және есеп беру

Бұл бөлімде Kaspersky Security Center Linux бағдарламасында бақылау және есеп беру конфигурациясы сценарийі берілген.

Алдын ала талаптар

Kaspersky Security Center Linux бағдарламасын ұйымның желісіне орналастырғаннан кейін, сіз Kaspersky Security Center көмегімен желінің қауіпсіздік күйін мониторингтеуге және есептерді қалыптастыруға кірісе аласыз.

Ұйымның желісіндегі бақылау және есептермен жұмыс келесі кезеңдерден тұрады:

1. **Құрылғылардың күйлерін ауыстыруды конфигурациялау**

   Нақты жағдайларға байланысты құрылғы күйлері параметрлерімен танысыңыз. Осы параметрлерді өзгерту арқылы, сіз *Критикалық* немесе *Ескерту* маңызды деңгейлері бар оқиғалар санын өзгерте аласыз. Құрылғының күйін ауыстырып қосуды конфигурациялау кезінде мынаны тексеріңіз:

   - жаңа параметрлер сіздің ұйымыңыздың ақпараттық қауіпсіздік саясатына қарама-қайшы келмейді;
   - сіз өз ұйымыңыздың желісіндегі маңызды қауіпсіздік оқиғаларына уақтылы жауап бере аласыз.

2. **Клиент құрылғыларындағы оқиғалар туралы хабарландыру параметрлерін конфигурациялау**

   Нұсқаулар:

   Клиент құрылғыларындағы оқиғалар туралы хабарландыруларды (электрондық пошта, SMS немесе орындалатын файлды іске қосу арқылы) конфигурациялау.

3. **Критикалық және ескерту хабарландырулары үшін ұсынылатын әрекеттерді орындау**

   Нұсқаулар:

   Ұйымыңыздың желісі үшін ұсынылатын әрекеттерді орындаңыз.

4. **Ұйымыңыздың желі қауіпсіздігі күйін қарау**

Нұсқаулар:

- Қорғаныс күйі веб-виджетін қарау.
- Қорғаныс жағдайы туралы есеп есебін жасау және қарау.
- Қателер туралы есеп есебін жасау және қарау.

5. **Қорғалмаған клиент құрылғыларын табу**

   Нұсқаулар:

   - Жаңа құрылғылар веб-виджетін қарау.
   - Қорғаныс орналастыру туралы есеп есебін жасау және қарау.

6. **Клиент құрылғылары қорғанысын тексеру**

   Нұсқаулар:

   - Қорғаныс күйі және Қауіптер статистикасы санаттарынан есепті жасау және қарау.
   - Маңызды оқиғалар таңдауын іске қосу және қарау.

7. **Дерекқорға оқиғаларды жүктеуді бағалау және шектеу**

   Басқарылатын бағдарламалар жұмыс істеп тұрған кезде туындайтын оқиғалар туралы ақпарат клиент құрылғысынан беріледі және Басқару серверінің дерекқорында тіркеледі. Басқару серверіне түсетін жүктемені азайту үшін дерекқорда сақталуы мүмкін оқиғалардың ең көп санын бағалаңыз және шектеңіз.

   Нұсқаулар:

   - Оқиғалардың ең көп санын шектеу

8. **Лицензия мәліметтерін қарау**

   Нұсқаулар:

   - Бақылау тақтасына Лицензиялық кілтті пайдалану веб-виджетін қосу және қарау
   - Лицензиялық кілттерді пайдалану туралы есеп есебін жасау және қарау

Нәтижелер

Сценарий аяқталғаннан кейін, сіз өз ұйымыңыздың желісін қорғау туралы хабардар боласыз және осылайша, одан әрі қорғау үшін әрекеттерді жоспарлай аласыз.

Бақылау түрлері және есеп беру туралы

Ұйым желісіндегі қауіпсіздік оқиғалары туралы ақпарат Басқару сервері дерекқорында сақталады. Kaspersky Security Center Web Console веб-консолі ұйымыңыздың желісінде бақылау және есеп берудің келесі түрлерін ұсынады:

- Бақылау тақтасы
- Есептер
- Оқиғалар таңдау
- Хабарландырулар

Бақылау тақтасы

Бақылау тақтасы ақпаратты графикалық түрде ұсыну арқылы ұйымның желісіндегі қауіпсіздік күйін бақылауға мүмкіндік береді.

Есептер

Есептер бұл ақпаратты файлға сақтау, электрондық пошта арқылы жіберу және басып шығару үшін ұйымыңыздың желісінің қауіпсіздігі туралы толық сандық ақпаратты алуға мүмкіндік береді.

Оқиғалар таңдау

Оқиғаларды таңдау, экранда Басқару серверінің дерекқорынан таңдалған аталған оқиғалар жиынтығын көруге арналған. Осы оқиға түрлері келесі санаттар бойынша топтастырылған:

- Маңыздылық деңгейі: **Маңызды оқиғалар**, **Функционалдық ақаулар**, **Ескертулер** және **Ақпараттық оқиғалар**.
- Уақыт: **Соңғы оқиғалар**.
- Түрі: **Пайдаланушылардың сұраулары** және **Аудит оқиғалары**.

Kaspersky Security Center Web Console интерфейсінде конфигурациялауға қолжетімді параметрлер негізінде пайдаланушы тарапынан айқындалған оқиғалар таңдауын жасай аласыз және көре аласыз.

Хабарландырулар

Хабарландырулар оқиғалар туралы ескертуге және сіз сәйкес деп санайтын ұсынылған әрекеттерді орындау арқылы осы оқиғаларға жауап беру жылдамдығыңызды арттыруға көмектесу үшін жасалған.

Ережелердің Смарт оқыту режимінде іске қосылуы

Бұл бөлімде клиент құрылғыларындағы Kaspersky Endpoint Security for Windows Аномалияларды бейімделумен басқару ережелері орындаған анықтаулар туралы ақпарат берілген.

Ережелер клиент құрылғыларындағы қалыптан тыс жүріс-тұрысты анықтайды және оны бұғаттай алады. Егер ережелер Смарт оқыту режимінде жұмыс істесе, олар қалыптан тыс мінез-құлықты анықтайды және әрбір осындай жағдай туралы есептерді Басқару серверіне жібереді. Анықталған аномалиялық әрекет туралы есептерді көру үшін **Қоймалар → "Смарт оқыту" күйіндегі ереже триггерлері** тармағына өтіңіз. Сіз анықтауды дұрыс деп растай аласыз немесе оны ерекшеліктерге қоса аласыз, содан кейін жүріс-тұрыстың бұл түрі қалыптан тыс болып саналмайды.

Анықтау туралы ақпарат Басқару серверіндегі оқиғалар журналында (қалған оқиғалармен бірге) және Аномалияларды бейімделумен басқару есебінде сақталады.

Аномалияларды бейімделумен басқару, оның ережелері, олардың режимдері мен күйлері туралы толық ақпарат Kaspersky Endpoint Security for Windows анықтамасында берілген.

Аномалияларды бейімделумен басқару ережелері арқылы орындалған анықтау әрекеттерін қарау және растау

Аномалияларды бейімделумен басқару ережелері арқылы орындалған анықтау тізімін қарау үшін:

1. Негізгі мәзірде **Қоймалар → "Смарт оқыту" күйіндегі ереже триггерлері** тармағына өтіңіз.

   Тізімде Аномалияларды бейімделумен басқару ережелері арқылы орындалатын келесі анықтау ақпарат көрсетіледі:

   - **Басқару тобы**

     Құрылғы қосылған басқару тобының атауы.

   - **Виртуалды Басқару сервері**

     Құрылғыны басқаратын виртуалды басқару сервері.

   - **Құрылғы атауы**

     Ереже қолданылған клиент құрылғысының атауы.

   - **Атауы**

     Қолданылған ереже атауы.

- **Күйі**

  Ерекшелік – егер әкімші бұл анықтауды өңдеп, оны ережелерден ерекшелік ретінде қосқан болса. Бұл күй, клиент құрылғысы Басқару серверімен синхрондалмайынша қала береді; синхрондалғаннан кейін анықтау тізімнен жоғалады.

  Растау – егер әкімші бұл анықтауды өңдеп, оны расталған болса. Бұл күй, клиент құрылғысы Басқару серверімен синхрондалмайынша қала береді; синхрондалғаннан кейін анықтау тізімнен жоғалады.

  Бос – егер әкімші бұл анықтауды өңдемеген болса.

- **Анықтамалар саны**

  Бір эвристикалық ережені, бір процесті және бір клиент құрылғысын анықтау саны. Бұл санды Kaspersky Endpoint Security есептеп шығарған.

- **Пайдаланушы аты**

  Анықтауды тудырған процесті іске қосқан клиент құрылғысының пайдаланушы аты.

- **Бастапқы өңдеу жолы**

  Бастапқы өңдеу жолы, яғни әрекетті орындаған процеске апаратын жол (толық ақпаратты Kaspersky Endpoint Security анықтамасынан қараңыз).

- **Бастапқы өңдеу хэші**

  Бастапқы процесс файлының SHA256 хэші (толық ақпаратты Kaspersky Endpoint Security анықтамасынан қараңыз).

- **Бастапқы нысан жолы**

  Процесті іске қосқан нысанға апаратын жол (толық ақпаратты Kaspersky Endpoint Security анықтамасынан қараңыз).

- **Бастапқы нысан хэші**

  Бастапқы файлдың SHA256 хэші (толық ақпаратты Kaspersky Endpoint Security анықтамасынан қараңыз).

- **Мақсатты өңдеу жолы**

  Мақсатты процеске апаратын жол (толық ақпаратты Kaspersky Endpoint Security анықтамасынан қараңыз).

- **Мақсатты өңдеу хэші**

  Мақсатты файлдың SHA256 хэші (толық ақпаратты Kaspersky Endpoint Security анықтамасынан қараңыз).

- **Мақсатты нысан жолы**

  Мақсатты нысанға апаратын жол (толық ақпаратты Kaspersky Endpoint Security анықтамасынан қараңыз).

- **Мақсатты нысан хэші**

  Мақсатты файлдың SHA256 хэші (толық ақпаратты Kaspersky Endpoint Security анықтамасынан қараңыз).

- **Өңделді**

  Аномалияның анықталған күні.

Анықтау сипаттарын көру үшін:

1. Негізгі мәзірде **Қоймалар → "Смарт оқыту" күйіндегі ереже триггерлері** тармағына өтіңіз.
2. Келесі әрекеттердің бірін орындаңыз:
   - **Атауы** бағанында көргіңіз келетін анықтау атауы бар сілтемені басыңыз.
   - Анықтаулар тізімінде көргіңіз келетін анықтаудың жанындағы құсбелгіні қойып, **Сипаттар** түймесін басыңыз.

   Таңдалған анықтау сипаттары терезесі ашылып, ол туралы ақпаратты көрсетеді.

Аномалияларды бейімделумен басқару ережелерінің анықтаулар тізімінен немесе таңдалған анықтау әрекеттерінің сипаттар терезесінен кез келген анықтау әрекетін растауға болады.

Анықтауды растау үшін:

- Анықтау тізімінде бір немесе бірнеше анықтауды таңдап, **Растау** түймесін басыңыз.
- Таңдалған анықтау әрекетінің сипаттар терезесін ашып, **Растау** түймесін басыңыз.

Анықтау күйі **Расталуда** күйіне өзгертіледі. Клиент құрылғысы басқару серверімен келесіде синхрондалғаннан кейін, анықтау әрекеті анықтаулар тізімінен жойылады.

Сіздің растауыңыз ережелерде қолданылатын статистикаға үлес қосады. Қосымша ақпаратты Kaspersky Endpoint Security for Windows анықтамасынан қараңыз.

Аномалияларды бейімделумен басқару ережесіне ерекшеліктер қосу

Аномалияларды бейімделумен басқару ерекшеліктеріне қосу шебері Kaspersky Endpoint Security үшін аномалияларды бейімделумен басқару ережелерінен ерекшеліктерді қосуға мүмкіндік береді.

Аномалияларды бейімделумен басқару ережелерінен шебер арқылы ерекше жағдайлар қосу үшін:

1. Шеберді келесі тәсілдердің бірімен іске қосыңыз:
   - Негізгі мәзірде **Қоймалар → "Смарт оқыту" күйіндегі ереже триггерлері** тармағына өтіп, бір немесе бірнеше анықтауды таңдап, **Есептен шығару** түймесін басыңыз.

     Бір уақытта 1000-ға дейін ерекшелік қосуға болады.

     Анықтауды ерекшеліктерге қоспай тұрып, анықтау атын немесе **Сипаттар** түймесін басу арқылы анықтау сипаттарын көруге болады. Ашылатын анықтау сипаттары терезесінде **Есептен шығару** түймесін басуға болады.
   - Негізгі мәзірде **Мониторинг → Оқиғаларды таңдау** тармағына өтіп, қажетті оқиға таңдауы бар сілтемені басыңыз, шығарғыңыз келетін анықтаудың жанындағы құсбелгіні қойыңыз, содан кейін **Аномалияларды бейімделумен басқарудан шығарып тастау** түймесін басыңыз.

Аномалияларды бейімделумен басқару ерекшеліктеріне қосу шебері іске қосылады. Шебердің жұмысын жалғастыру үшін **Келесі** түймесін басыңыз.

2. Ерекшеліктер қосқыңыз келетін саясаттар мен саясат профильдерін таңдаңыз.

   Иеленген саясаттарды жаңарту мүмкін емес. Саясатты өзгертуге құқықтарыңыз болмаса, саясат жаңартылмайды.

3. Шеберді жабу үшін **Дайын** түймесін басыңыз.

Анықтау күйі **Шығаруда** күйіне өзгертіледі. Клиент құрылғысы басқару серверімен келесіде синхрондалғаннан кейін, анықтау әрекеті анықтаулар тізімінен жойылады. Аномалияларды бейімделумен басқару ережесінің ерекшелігі конфигурацияланған және қолданылады.

Бақылау тақтасы және веб-виджеттер

Бұл бөлімде бақылау тақтасы және бақылау тақтасында көрсетілген веб-виджеттер туралы ақпарат бар. Бөлімде веб-виджеттерді басқару және веб-виджеттерді конфигурациялау бойынша нұсқаулар бар.

Бақылау тақтасын қолдану

Бақылау тақтасы ақпаратты графикалық түрде ұсыну арқылы ұйымның желісіндегі қауіпсіздік күйін бақылауға мүмкіндік береді.

Бақылау тақтасы Kaspersky Security Center Web Console бағдарламасында **Мониторинг** → **Бақылау тақтасы** бөлімінде қолжетімді.

Бақылау тақтасында конфигурацияланатын веб-виджеттер бар. Сіз дөңгелек диаграммалар, кестелер, графиктер, гистограммалар және тізімдер түрінде ұсынылған көптеген веб-виджеттерді таңдай аласыз. Веб-виджеттерде көрсетілген ақпарат автоматты түрде жаңартылады, жаңарту кезеңі бір-екі минутты құрайды. Жаңартулар арасындағы уақыт аралығы веб-виджет түріне байланысты өзгереді. Веб-виджет деректерін кез келген уақытта мәзір арқылы қолмен жаңартуға болады.

Әдепкі бойынша, веб-виджеттер Басқару сервері дерекқорында сақталатын оқиғалар туралы ақпаратты қамтиды.

Әдепкі бойынша, Kaspersky Security Center Web Console бағдарламасы келесі санаттарға арналған веб-виджеттер жиынтығына ие:

- **Қорғаныс күйі**
- **Орналастыру**
- **Жаңарту**
- **Қауіптер статистикасы**
- **Басқа**

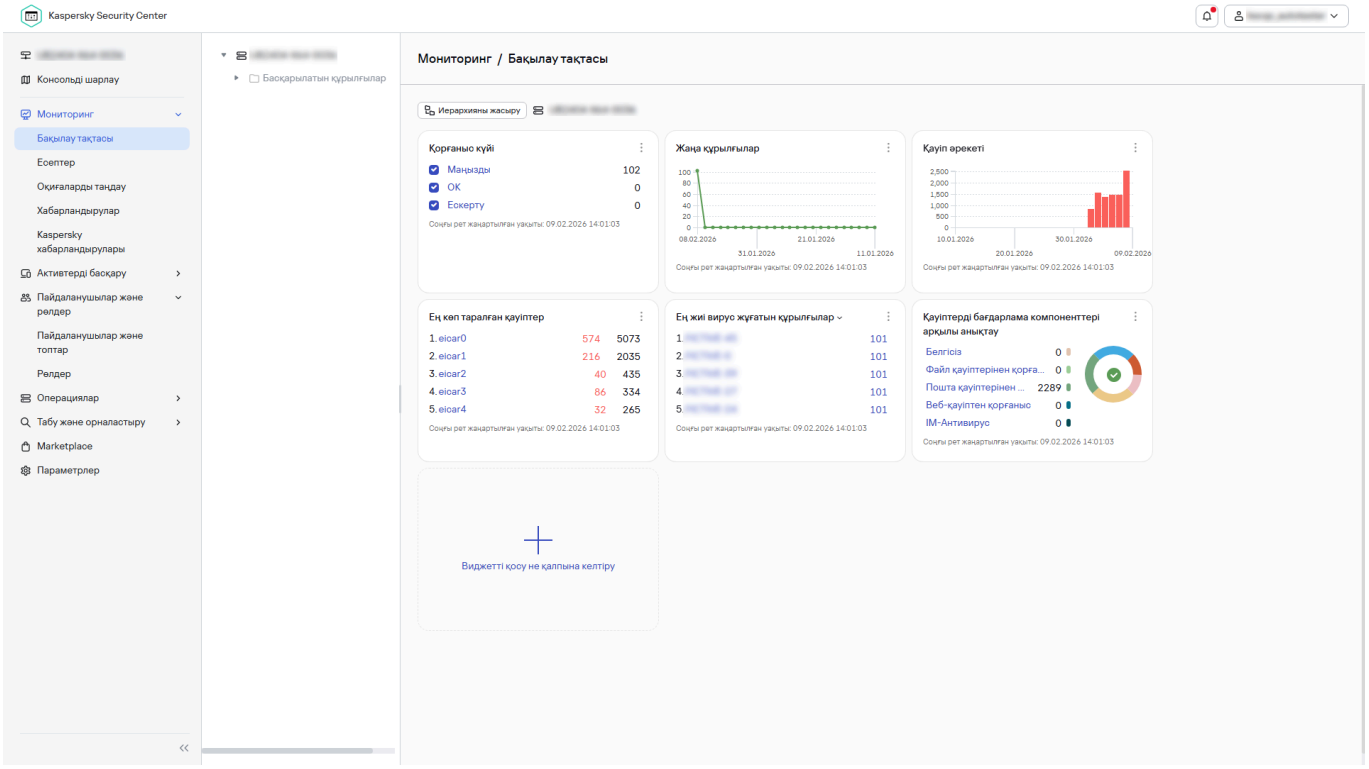
Кейбір веб-виджеттерде сілтемелі мәтін бар. Толық ақпаратты көру үшін мына сілтемеге өтіңіз.

Бақылау тақтасын конфигурациялау кезінде қажетті веб-виджеттерді қосуға, веб-виджеттерді жасыруға, сондай-ақ веб-виджеттердің сыртқы түрін немесе өлшемін өзгертуге, веб-виджеттерді жылжытуға және веб-виджеттердің параметрлерін өзгертуге болады.

Ақпараттық тақтаға веб-виджетті қосу

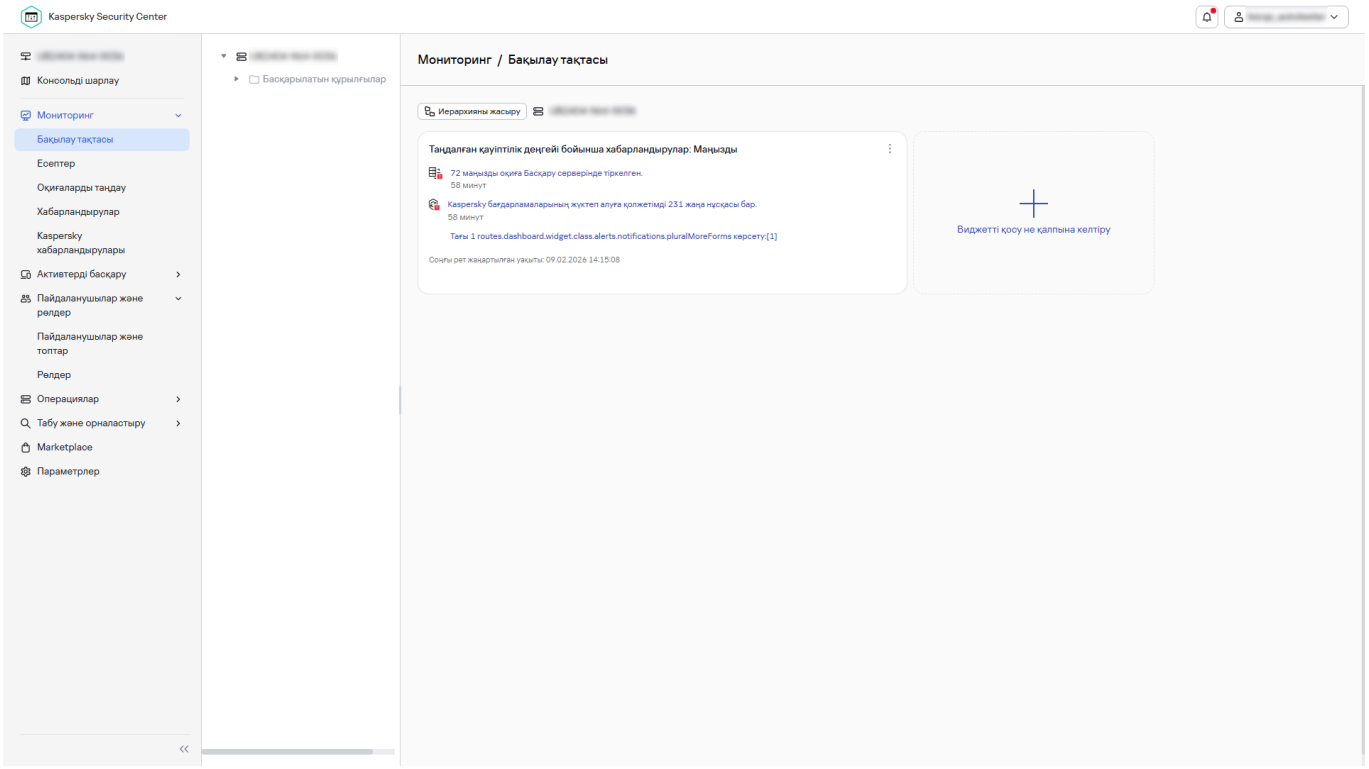
Веб-виджетті ақпараттық тақтаға қосу үшін:

1. Қолданбаның негізгі терезесінде **Мониторинг → Бақылау тақтасы** бөліміне өтіңіз.



Виджеттері бар бақылау тақтасы

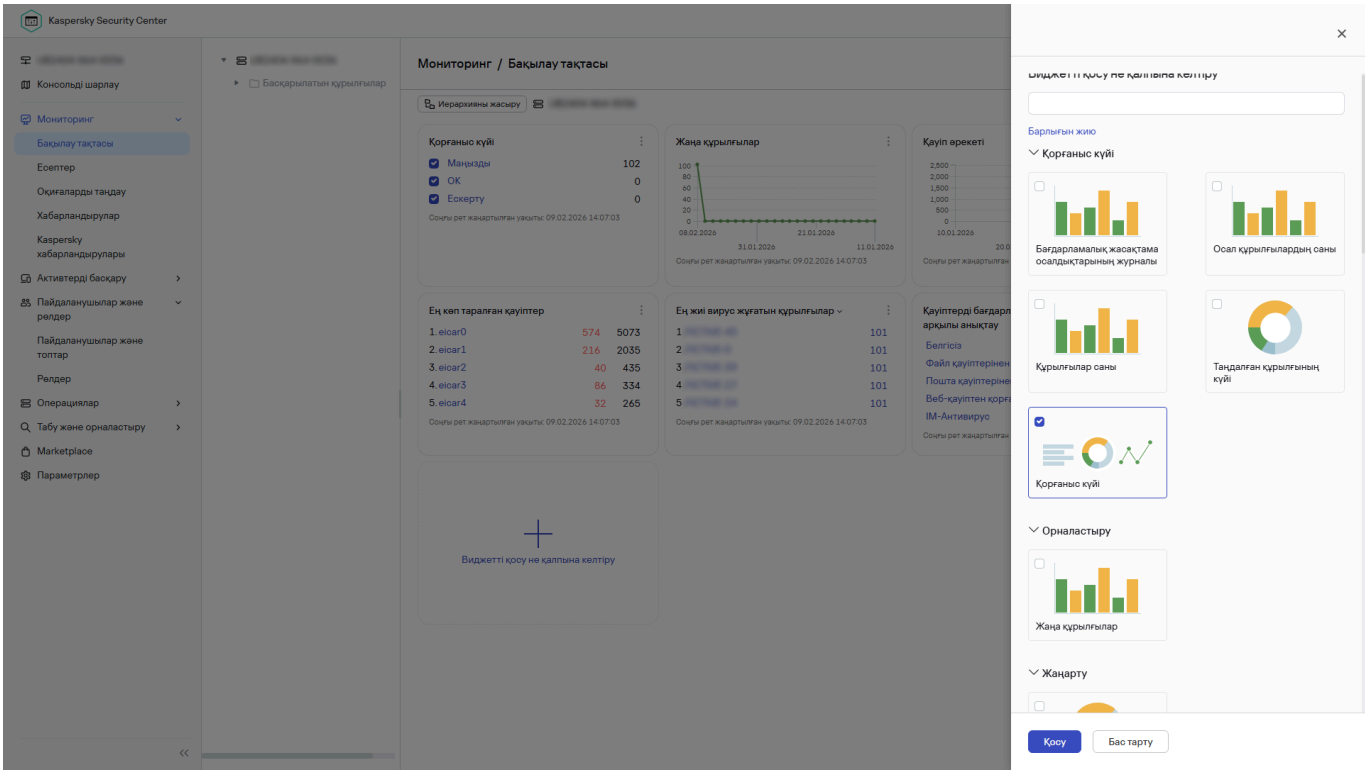
2. **Виджетті қосу не қалпына келтіру** түймесін басыңыз.



Виджет қосу

3. Қолжетімді веб-виджеттер тізімінен ақпараттық тақтаға қосу қажет веб-виджетті таңдаңыз.

Веб-виджеттер санаттар бойынша топтастырылған. Санатқа қандай веб-виджеттердің кіретінін көру үшін санаттың атауы жанындағы шеврон (>) белгішесін басыңыз.



Виджет түрін таңдау

4. **Қосу** түймесін басыңыз.

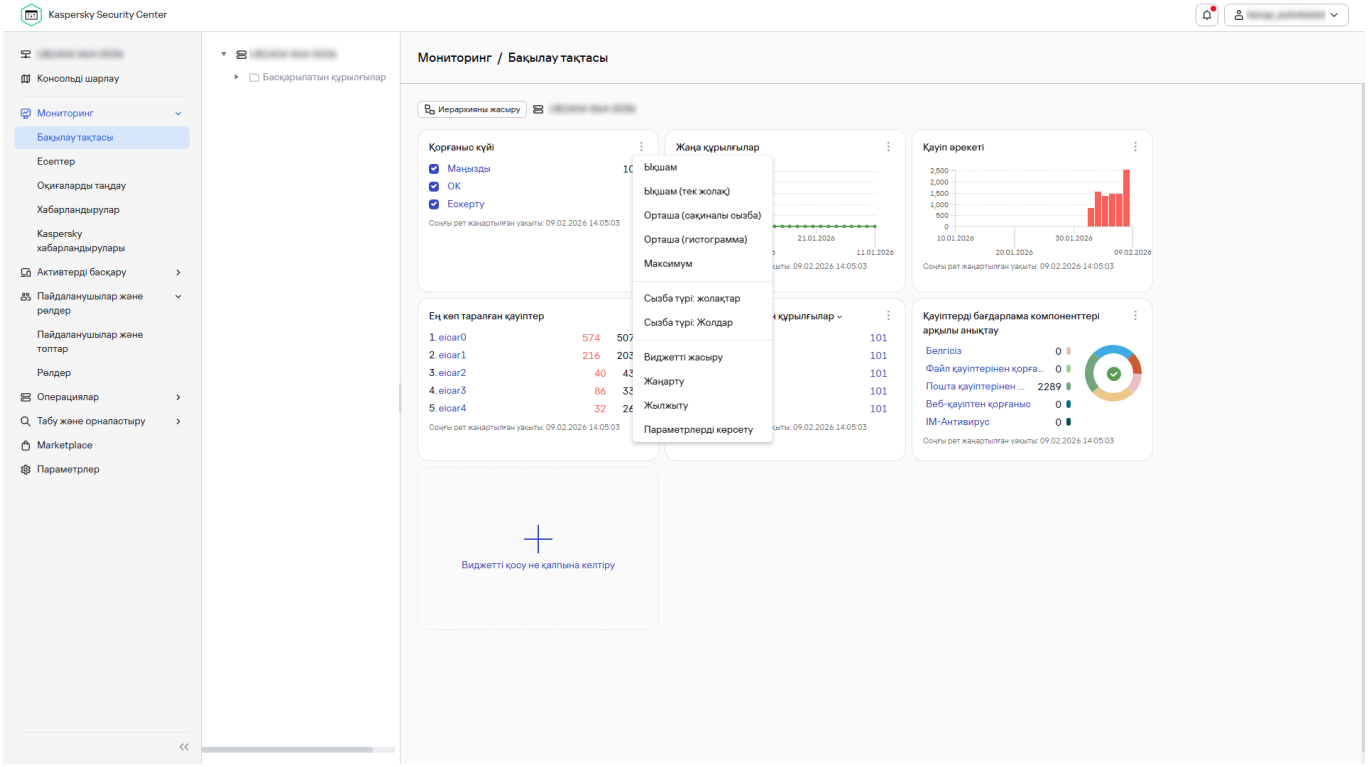
Таңдалған веб-виджеттер ақпараттық тақтаның соңына қосылады.

Қосылған веб-виджеттердің сыртқы түрі мен параметрлерін өзгертуге болады.

Веб-виджетті ақпараттық тақтадан жою

Веб-виджетті ақпараттық тақтадан жою үшін:

1. Бағдарламаның негізгі терезесінде **Мониторинг → Бақылау тақтасы** бөліміне өтіңіз.
2. Жою қажет веб-виджеттің жанындағы параметрлер (⚙) белгішесін басыңыз.



Виджет мәзірі

3. **Виджетті жасыру** таңдаңыз.
4. Пайда болған **Ескерту** терезеде **ОК** түймесін басыңыз.

Таңдалған веб-виджет ақпараттық тақтадан жойылады. Алдағыда, веб-виджетті ақпараттық тақтаға қайтадан қосуға болады.

Веб-виджетті ақпараттық тақтадан жылжыту

Веб-виджетті ақпараттық тақтадан жылжыту үшін:

1. Бағдарламаның негізгі терезесінде **Мониторинг → Бақылау тақтасы** бөліміне өтіңіз.
2. Жылжыту қажет веб-виджеттің жанындағы параметрлер (⚙) белгішесін басыңыз.

3. **Жылжыту** таңдаңыз.

4. Веб-виджетті жылжыту қажет орынды көрсетіңіз. Тек басқа веб-виджетті таңдауға болады.

Таңдалған веб-виджеттер орындарын ауыстырады.

Виджеттің өлшемін немесе сыртқы түрін өзгерту

Веб-виджеттердің сыртқы түрін өзгертуге болады: бағаналы немесе сызықтық диаграмманы таңдаңыз. Кейбір веб-виджеттер үшін өлшемін өзгертуге болады: шағын, орташа немесе ірі.

Веб-виджеттің сыртқы түрін өзгерту үшін:

1. Бағдарламаның негізгі терезесінде **Мониторинг** → **Бақылау тақтасы** бөліміне өтіңіз.

2. Өзгерту қажет веб-виджеттің жанындағы параметрлер (⚙) белгішесін басыңыз.

3. Келесі әрекеттердің бірін орындаңыз:

   - Веб-виджет бағандық диаграмма ретінде көрсетілуі үшін **Сызба түрі: жолақтар** тармағын таңдаңыз.
   - Веб-виджет сызықтық диаграмма ретінде көрсетілуі үшін **Сызба түрі: Жолдар** тармағын таңдаңыз.
   - Веб-виджет алып жатқан аймақтың өлшемін ауыстыру үшін келесі мәндердің бірін таңдаңыз:
     - **Ықшам**
     - **Ықшам (тек жолақ)**
     - **Орташа (сақиналы сызба)**
     - **Орташа (гистограмма)**
     - **Максимум**

Таңдалған веб-виджеттің сыртқы түрі өзгертіледі.

Веб-виджет параметрлерін өзгерту

Веб-виджет параметрлерін өзгерту үшін:

1. Бағдарламаның негізгі терезесінде **Мониторинг** → **Бақылау тақтасы** бөліміне өтіңіз.

2. Өзгерту қажет веб-виджеттің жанындағы параметрлер (⚙) белгішесін басыңыз.

3. **Параметрлерді көрсету** таңдаңыз.

4. Ашылған веб-виджет параметрлері терезесінде веб-виджеттің қажетті параметрлерін өзгертіңіз.

5. Өзгерістерін сақтау үшін **Сақтау** түймесін басыңыз.

Таңдалған веб-виджеттің параметрлері өзгертіледі.

Параметрлер жиынтығы нақты веб-виджетке байланысты. Төменде кейбір жалпы параметрлер берілген:

- **Виджет ауқымы** – веб-виджет ақпаратты көрсететін нысандар жиынтығы; мысалы, басқару тобы немесе құрылғылар таңдауы.
- **Тапсырманы таңдау** – веб-виджет ақпаратты көрсететін тапсырма.
- **Уақыт аралығы** – веб-виджетте ақпарат көрсетілетін кезең; мысалы, белгіленген күннен бастап қазіргі уақытқа дейін немесе көрсетілген күндер саны ішінде қазіргі уақытқа дейін белгіленген екі күн арасында.
- **Келесі параметрлер көрсетілген болса, "Критикалық" күйіне орнату** және **Келесі параметрлер көрсетілген болса, "Ескерту" күйіне орнату** – күй графигінде түстер тағайындалатын ережелер.

Веб-виджет параметрлерін өзгерткеннен кейін веб-виджет деректерін қолмен жаңартуға болады.

Веб-виджет деректерін жаңарту үшін:

1. Бағдарламаның негізгі терезесінде **Мониторинг** → **Бақылау тақтасы** бөліміне өтіңіз.
2. Жылжыту қажет веб-виджеттің жанындағы параметрлер (⚙) белгішесін басыңыз.
3. **Жаңарту** түймесін басыңыз.

Веб-виджет деректері жаңартылды.

Тек бақылау тақтасын қарау режимі туралы

Желіні басқармайтын, бірақ Kaspersky Security Center Linux-те желі қорғанысы статистикасын көргісі келетін қызметкерлер үшін "Тек бақылау тақтасы" режимін конфигурациялауға болады (мысалы, бұл топ-менеджер болуы мүмкін). Пайдаланушыда осы режим қосулы болғанда, пайдаланушыда алдын ала анықталған веб-виджеттер жиынтығы бар бақылау тақтасы ғана көрсетіледі. Осылайша, пайдаланушы веб-виджеттерде көрсетілген статистиканы, мысалы, барлық басқарылатын құрылғылардың қорғаныс күйін, жақында табылған қауіптер санын немесе желідегі ең көп таралған қауіптер тізімін көре алады.

Пайдаланушы Тек бақылау тақтасын қарау режимінде жұмыс істеген кезде келесі шектеулер қолданылады:

- Бас мәзір көрсетілмейді, сондықтан пайдаланушы желіні қорғау параметрлерін өзгерте алмайды.
- Пайдаланушы веб-виджеттермен байланысты әрекеттерді орындай алмайды, мысалы, оларды қоса немесе жасыра алмайды. Сондықтан, пайдаланушыға қажет барлық веб-виджеттерді бақылау тақтасына орналастырып, оларды конфигурациялау керек, мысалы, нысандарды санау ережесін белгілеу немесе кезеңді көрсету қажет.

Сіз "Тек бақылау тақтасы" режимін өзіңізге тағайындай алмайсыз. Егер осы режимде жұмыс істегіңіз келсе, жүйе әкімшісіне, провайдерге (MSP) немесе **Жалпы функциялар: Пайдаланушы құқықтары** функционалдық аймағында Нысан ACL параметрлерін өзгерту құқықтары бар пайдаланушыға жүгініңіз.

Тек бақылау тақтасын қарау режимін конфигурациялау

Тек бақылау тақтасын қарау режимін конфигурациялауды бастау алдында, келесі алдын ала талаптардың орындалғанына көз жеткізіңіз:

- Сізде **Жалпы функциялар: Пайдаланушы құқықтары** функционалды аймағында **Modify object ACLs** құқығы бар. Егер сізде бұл құқық болмаса, режимді конфигурациялау үшін қойынша болмайды.
- **Жалпы функционал: Базалық функционал** аймағындағы **Оқу** құқығы бар пайдаланушы.

> Егер сіздің желіңізде Басқару серверлері иерархиясы құрылған болса, Тек бақылау тақтасын қарау режимін конфигурациялау үшін **Пайдаланушылар** в разделе **Пайдаланушылар және рөлдер** → **Пайдаланушылар және топтар** бөлімінде пайдаланушы есептік жазбасы қолжетімді Серверге өтіңіз. Бұл басты Сервер немесе физикалық қосалқы Сервер болуы мүмкін. Виртуалды Басқару серверінде "Тек бақылау тақтасы" режимін конфигурациялау мүмкін емес.

"Тек бақылау тақтасы" режимін конфигурациялау үшін:

1. Қолданбаның негізгі терезесінде **Пайдаланушылар және рөлдер** → **Пайдаланушылар және топтар** бөліміне өтіп, **Пайдаланушылар** қойындысын таңдаңыз.
2. Веб-виджеттері бар құралдар тақтасын конфигурациялағыңыз келетін пайдаланушы есептік жазбасының атын басыңыз.
3. Есептік жазба сипаттары терезесі ашылғанда **Бақылау тақтасы** қойыншасын таңдаңыз.

   Ашылған қойыншада пайдаланушыға да арналған бақылау тақтасын көрсетіледі.
4. **"Тек бақылау тақтасы" режимін көрсету** параметрі қосулы болса, оны қосқыш арқылы өшіріңіз.

   Бұл параметр қосылған кезде де бақылау тақтасын өзгерту мүмкін емес. Параметрді өшіргеннен кейін веб-виджеттерді басқаруға болады.
5. Бақылау тақтасының сыртқы түрін конфигурациялаңыз. **Бақылау тақтасы** қойыншасында дайындалған веб-виджеттер жиынтығы, конфигурацияланатын есептік жазбасы бар пайдаланушы үшін қолжетімді. Мұндай есептік жазбасы бар пайдаланушы веб-виджеттердің параметрлерін немесе өлшемін өзгерте алмайды, бақылау тақтасына веб-виджеттерді қоса алмайды немесе одан жоя алмайды. Сондықтан, оларды желіні қорғау статистикасын көре алатындай етіп пайдаланушыға бейімдеп конфигурациялаңыз. Осы мақсатта, **Бақылау тақтасы** қойыншасында **Мониторинг** → **Бақылау тақтасы** бөліміндегідей әрекеттерді орындауға болады:
   - Бақылау тақтасына веб-виджеттерді қосу.
   - Пайдаланушыға қажет емес веб-виджеттерді жасыру.
   - Белгіленген тәртіпте веб-виджеттерді жылжыту.
   - Веб-виджеттердің өлшемін немесе сыртқы түрін өзгерту.
   - Веб-виджет параметрлерін өзгерту.
6. **"Тек бақылау тақтасы" режимін көрсету** параметрін қосу үшін қосқышты ауыстырып қосыңыз.

Осыдан кейін, пайдаланушыға тек бақылау тақтасы қолжетімді болады. Пайдаланушы статистиканы көре алады, бірақ желіні қорғау параметрлерін және бақылау тақтасының сыртқы түрін өзгерте алмайды. Пайдаланушы үшін бірдей бақылау тақтасы көрсетілгендіктен, сіз бақылау тақтасын да өзгерте алмайсыз.

Бұл параметрді өшірулі күйде қалдырсаңыз, пайдаланушыда бас мәзір көрсетіледі, сондықтан ол Kaspersky Security Center Linux бағдарламасында әртүрлі әрекеттерді орындай алады, соның ішінде қауіпсіздік параметрлері мен веб-виджеттерді өзгерте алады.

7. Тек бақылау тақтасын қарау режимін конфигурациялауды аяқтағаннан кейін **Сақтау** түймесін басыңыз. Осыдан кейін ғана дайындалған бақылау тақтасы пайдаланушыда көрсетіледі.

8. Егер пайдаланушы қолдау көрсетілетін Kaspersky бағдарламаларының статистикасын көргісі келсе және оған қатынасу құқығы қажет болса, сол пайдаланушыға құқықтарды конфигурациялаңыз. Осыдан кейін, Kaspersky бағдарламаларының деректері пайдаланушыда осы бағдарламалардың веб-виджеттерінде көрсетіледі.

Енді пайдаланушы Kaspersky Security Center Linux бағдарламасына конфигурацияланатын есептік жазбамен кіре алады және тек бақылау тақтасын Қарау режимінде желіні қорғау статистикасын көре алады.

Басқару және қорғау есептері

Бұл бөлімде есептерді пайдалану, пайдаланушы есептерінің үлгілерін басқару, есептерді жасау үшін үлгілерді пайдалану және есептерді жеткізу тапсырмаларын жасау тәсілі сипатталған.

Есептерді қолдану

Есептер бұл ақпаратты файлға сақтау, электрондық пошта арқылы жіберу және басып шығару үшін ұйымыңыздың желісінің қауіпсіздігі туралы толық сандық ақпаратты алуға мүмкіндік береді.

Есептер Kaspersky Security Center Web Console бағдарламасында **Мониторинг** → **Есептер** бөлімінде қолжетімді.

Әдепкі бойынша, есептер соңғы 30 күндегі ақпаратты қамтиды.

Әдепкі бойынша, Kaspersky Security Center Linux келесі санаттарға арналған есептер жиынтығына ие:

- **Қорғаныс күйі**
- **Орналастыру**
- **Жаңарту**
- **Қауіптер статистикасы**
- **Басқа**

Сіз пайдаланушылық есеп үлгілерін жасай аласыз, есеп үлгілерін өңдеп, жоя аласыз.

Есептерді қолданыстағы үлгілер негізінде жасай аласыз, есептерді файлға экспорттай аласыз және есептерді жеткізу тапсырмаларын жасай аласыз.

Есеп үлгісін жасау

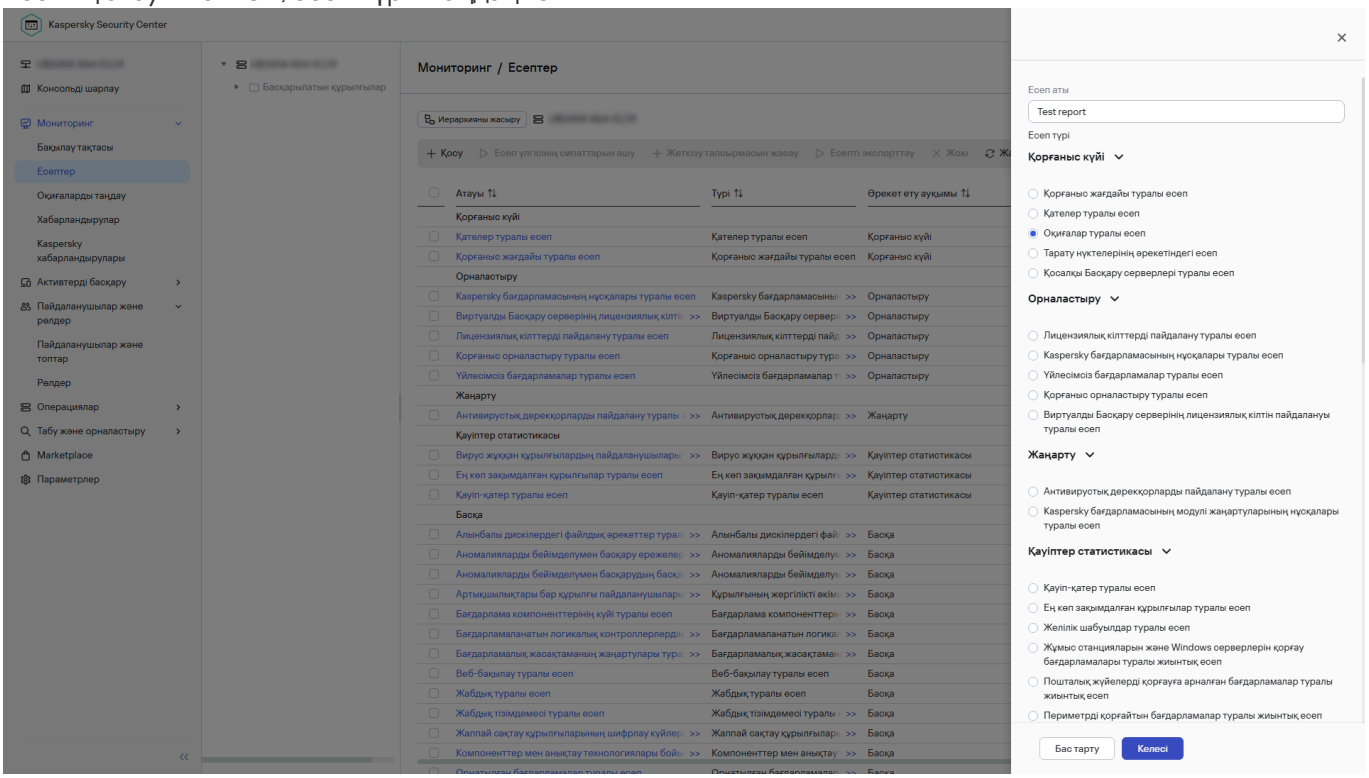
Есеп үлгісін жасау үшін:

1. Бағдарламаның негізгі терезесінде **Мониторинг** → **Есептер** бөліміне өтіңіз.

2. **Қосу** түймесін басыңыз.

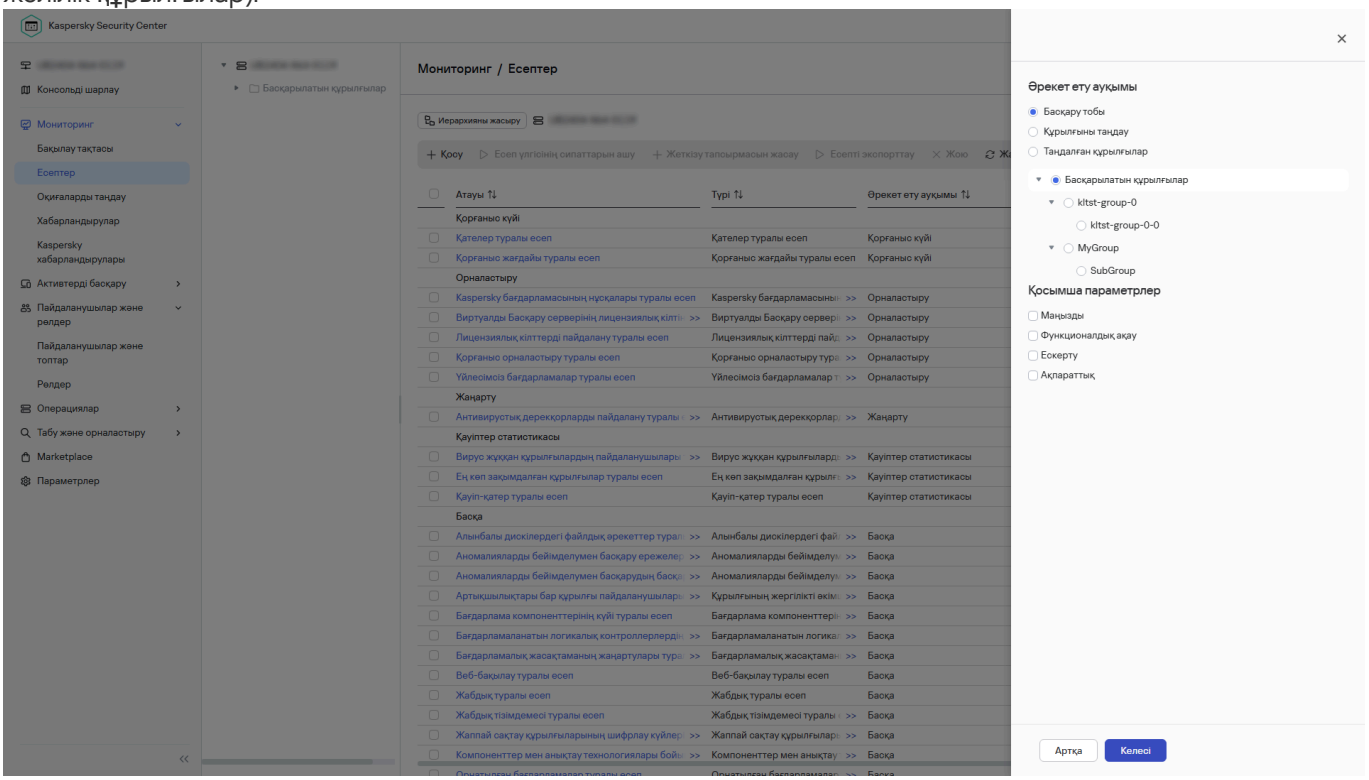
   Нәтижесінде, есеп үлгісін жасау шебері іске қосылады. Шебердің жұмысын жалғастыру үшін **Келесі** түймесін басыңыз.

3. Есептің атауын енгізіп, есеп түрін таңдаңыз.



Есеп атауын көрсету және есеп түрін таңдау

4. Шебердің **Әрекет ету ауқымы** қадамында, осы үлгі негізінде жасалған есептерде көрсетілетін деректері бар клиент құрылғылары жиынтығын таңдаңыз (басқару топтары, құрылғылар таңдауы немесе барлық желілік құрылғылар).

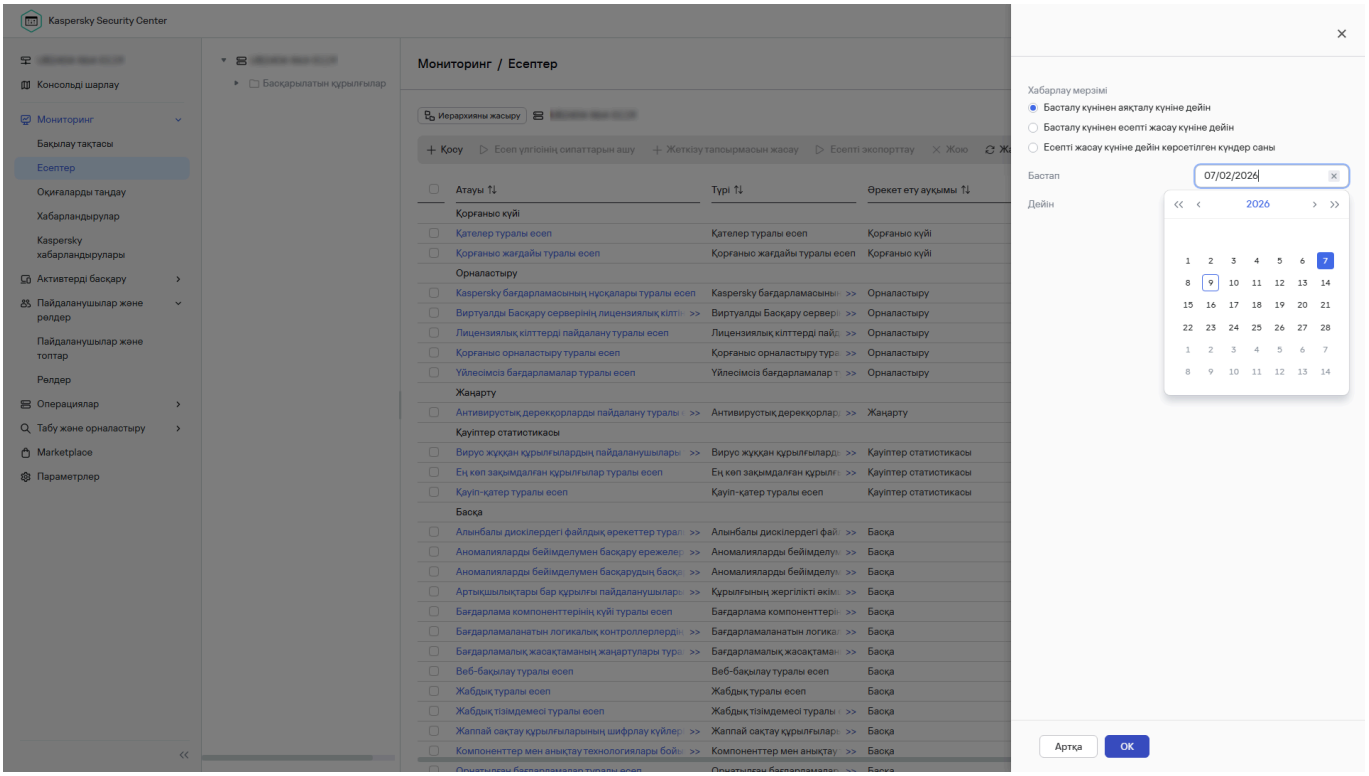


Есеп ауқымын көрсету

5. Шебердің **Хабарлау мерзімі** бетінде есеп жасалатын кезеңді көрсетіңіз. Қолжетімді мәндері:

   - екі көрсетілген күн арасында;
   - көрсетілген күннен есеп жасалған күнге дейін;
   - есеп жасалған күннен бастап, минус көрсетілген күндер саны, есеп жасалған күнге дейін.

Кейбір есептерде бұл бет көрсетілмеуі мүмкін.



Есеп беру кезеңін көрсету

6. Шебердің жұмысын аяқтау үшін **OK** түймесін басыңыз.

7. Келесі әрекеттердің бірін орындаңыз:

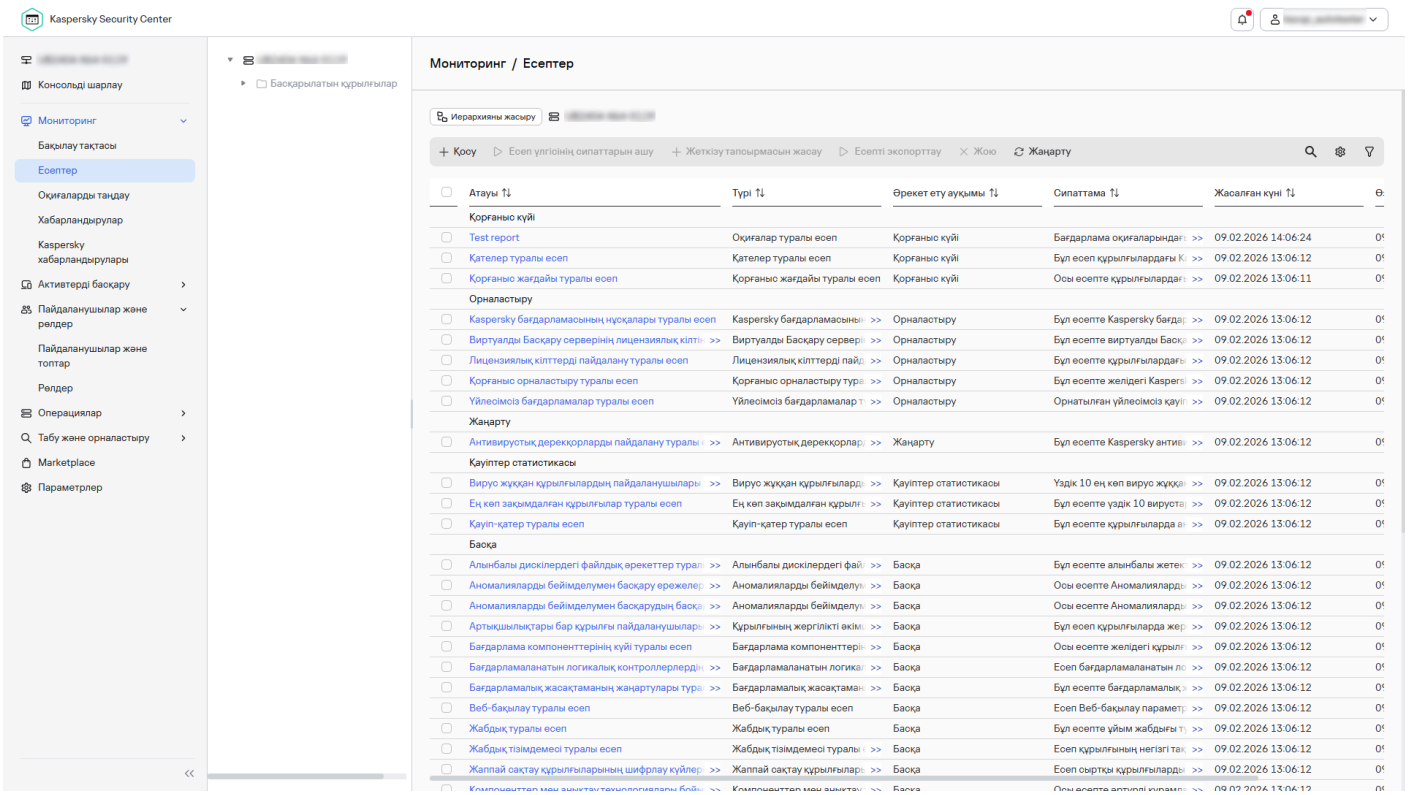
   - Жаңа есеп үлгісін сақтау және оның негізінде есеп жасауды бастау үшін **Сақтау және іске қосу** түймесін басыңыз.

     Есеп үлгісі сақталады. Есеп құрастырылады.

   - Жаңа есеп үлгісін сақтау үшін **Сақтау** түймесін басыңыз.

     Есеп үлгісі сақталады.

Жасалған үлгіні есептерді қалыптастыру және қарау үшін пайдалануға болады.



Есептер тізімі

Есеп үлгісінің сипаттарын қарау және өзгерту

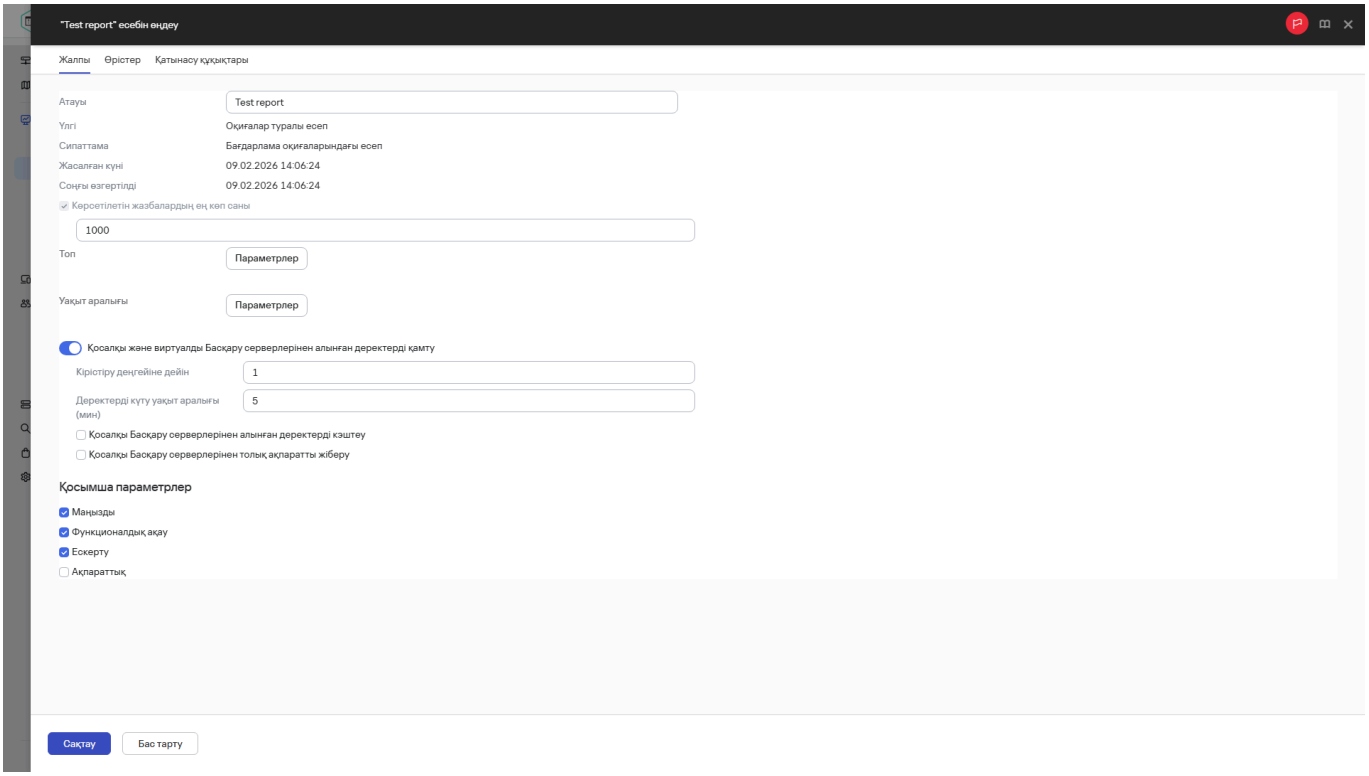
Есеп үлгісінің негізгі сипаттарын, мысалы, есеп үлгісінің атауын немесе есепте көрсетілетін өрістерді қарауға және өзгертуге болады.

Есеп үлгісінің сипаттарын қарау және өзгерту үшін:

1. Бағдарламаның негізгі терезесінде **Мониторинг** → **Есептер** бөліміне өтіңіз.
2. Сипаттарын көргіңіз және өзгерткіңіз келетін есеп үлгісіне қарама-қарсы жалауша қойыңыз.

   Балама ретінде, алдымен есепті құрастырып, кейін **Өңдеу** түймесін басуға болады.
3. **Есеп үлгісінің сипаттарын ашу** түймесін басыңыз.

Жалпы қойыншасында **<есеп атауы> есебін өзгерту** терезесі ашылады.



Есеп үлгісінің сипаттары

4. Есеп үлгісі сипаттарын өзгертіңіз:

   - **Жалпы** қойыншасы:

     - Есеп үлгісінің атауы

     - **Көрсетілетін жазбалардың ең көп саны**

       Егер бұл параметр қосылса, есептің егжей-тегжейлі деректері бар кестеде көрсетілетін жазбалар саны көрсетілген мәннен аспайды. Бұл параметр есепті файлға экспорттау кезінде есепке қосуға болатын оқиғалардың ең көп санына әсер етпейтінін ескеріңіз.

       Есеп жазбалары алдымен есеп үлгісі сипаттарының **Өрістер** → **Мәліметтер өрістері** бөлімінде көрсетілген ережелерге сай сұрыпталады, содан соң қорытқы жазбалардың бірінші бөлігі ғана сақталады. Есептің егжей-тегжейлі деректері бар кесте тақырыбында, көрсетілетін жазбалар саны және есеп үлгісінің басқа параметрлеріне сәйкес келетін жазбалардың жалпы саны көрсетілген.

       Егер бұл параметр өшірулі болса, есептің егжей-тегжейлі деректері бар кестеде барлық жазбалар көрсетіледі. Бұл параметрді өшіру ұсынылмайды. Көрсетілетін есеп жазбаларының санын шектеу дерекқорды басқару жүйесіне түсетін жүктемені және есепті қалыптастыру мен экспорттауға кететін уақытты азайтады. Кейбір есептерде тым көп жазбалар бар. Мұндай жағдайларда барлық жазбаларды қарау және талдау тым көп еңбекті қажет етуі мүмкін. Сондай-ақ мұндай есепті жасау кезінде құрылғыңыздың жады таусылуы мүмкін, демек есепті көре алмайсыз.

       Әдепкі бойынша, параметр қосулы. Әдепкі бойынша, 1000 мәні көрсетілген.

     - **Топ**

       Есеп жасалатын клиент құрылғылары жиынтығын өзгерту үшін **Параметрлер** түймесін басыңыз. Есептердің кейбір түрлері үшін түйме қолжетімді болмауы мүмкін. Нақты деректер есеп үлгісін жасау кезінде көрсетілген параметрлер мәндеріне байланысты.

     - **Уақыт аралығы**

Есеп жасалатын кезеңді өзгерту үшін **Параметрлер** түймесін басыңыз. Есептердің кейбір түрлері үшін түйме қолжетімді болмауы мүмкін. Қолжетімді мәндері:

- екі көрсетілген күн арасында;
- көрсетілген күннен есеп жасалған күнге дейін;
- есеп жасалған күннен бастап, минус көрсетілген күндер саны, есеп жасалған күнге дейін.

- **Қосалқы және виртуалды Басқару серверлерінен алынған деректерді қамту**

  Бұл параметр өшірулі болса, есеп есеп үлгісі жасалған Басқару серверіне бағынатын қосалқы және виртуалды Басқару серверлерінен алынған ақпаратты қамтиды.

  Тек ағымдағы Басқару серверінің деректерін ғана қарағыңыз келсе, осы параметрді өшіріңіз.

  Әдепкі бойынша, параметр қосулы.

- **Кірістіру деңгейіне дейін**

  Есепте, ағымдағы Басқару серверінің астында, көрсетілген мәннен төмен немесе оған тең тіркеме деңгейінде орналасқан қосалқы және виртуалды Басқару серверлерінің деректері бар.

  Әдепкі бойынша, 1 мәні көрсетілген. Егер сіз есепте ағаштың ең төменгі деңгейінде орналасқан қосалқы Басқару серверлері туралы ақпаратты көргіңіз келсе, бұл мәнді өзгерте аласыз.

- **Деректерді күту уақыт аралығы (мин)**

  Есеп үлгісі жасалған Басқару сервері есепті жасау үшін көрсетілген уақыт ішінде қосалқы Басқару серверлерінен деректерді күтеді. Егер деректер көрсетілген уақыт аралығында қосалқы Басқару серверінен алынбаса, есеп кез келген жағдайда іске қосылады. Есепте нақты деректердің орнына кэштен алынған деректер (егер **Қосалқы Басқару серверлерінен алынған деректерді кэштеу** параметрі қосулы болса) не болмаса **N/A** (қолжетімді емес) көрсетіледі.

  Әдепкі бойынша күту уақыты – 5 минут.

- **Қосалқы Басқару серверлерінен алынған деректерді кэштеу**

  Қосалқы Басқару серверлері деректерді үнемі есеп үлгісі жасалған негізгі Басқару серверіне жібереді. Берілген деректер кэште сақталады.

  Басқару сервері есепті құру кезінде қосалқы Басқару серверінің деректерін ала алмаса, есеп кэштегі деректерді көрсетеді. Бұл жағдайда, деректер кэшке жіберілген күн көрсетіледі.

  Бұл параметрді қосу арқасында өзекті деректерді алу мүмкін болмаса да, қосалқы Басқару серверлерінен алынған ақпаратты көруге мүмкіндік беріледі. Алайда, көрсетілетін деректер ескірген болуы мүмкін.

  Әдепкі бойынша, параметр өшірулі.

- **Кэшті жаңарту жиілігі (сағ)**

  Қосалқы Басқару серверлері деректерді үнемі есеп үлгісі жасалған негізгі Басқару серверіне жібереді. Сіз осы кезеңді сағат түрінде көрсете аласыз. Егер 0 мәні белгіленсе, деректер тек есеп шығару кезінде беріледі.

  Әдепкі бойынша, 0 мәні көрсетілген.

- **Қосалқы Басқару серверлерінен толық ақпаратты жіберу**

  Жасалған есепте егжей-тегжейлі деректер кестесі есеп үлгісі жасалған негізгі Басқару серверінің қосалқы Басқару серверлерінен алынған ақпаратты қамтиды.

Егер бұл параметр қосылса, онда есепті құру баяулайды және Басқару серверлері арасындағы трафик артады. Дегенмен, сіз барлық деректерді бір есепте көре аласыз.

Бұл параметрді қоспау үшін сіз ақаулы қосалқы Басқару серверін табу үшін есеп деректерін талдай аласыз, содан кейін бірдей есепті тек сол ақаулы Басқару сервері үшін жасай аласыз.

Әдепкі бойынша, параметр өшірулі.

- **Өрістер** қойынша

  Есепте көрсетілетін өрістерді таңдап, осы өрістердің ретін өзгерту үшін **Жоғары жылжыту** және **Төменге жылжыту** түймелерін пайдаланыңыз. **Қосу** және **Өңдеу** түймелерінің көмегімен есептегі ақпарат таңдалған өрістер бойынша сүзгіленетінін немесе сұрыпталатынын көрсетіңіз.

  Сондай-ақ, **Мәліметтер өрісінің сүзгілері** бөлімінде, кеңейтілген сүзгілеу пішімін қолдана бастау үшін **Түрлендіру сүзгілері** түймесін баса аласыз. Бұл пішім логикалық НЕМЕСЕ көмегімен әртүрлі өрістерде көрсетілген сүзгілеу шарттарын біріктіруге мүмкіндік береді. **Түрлендіру сүзгілері** түймесін басқаннан кейін, оң жақта тақта ашылады. Лицензияны қайтарып алуды растайтын **Түрлендіру сүзгілері** түймесін басыңыз. Енді сіз логикалық НЕМЕСЕ көмегімен қолданылатын **Мәліметтер өрістері** бөлімінен шарттары бар түрлендірілген сүзгіні анықтай аласыз.

  Есепті күрделі сүзгілеу шарттарын қолдайтын пішімге түрлендіру салдарынан, ол Kaspersky Security Center (11 және одан төмен) алдыңғы нұсқаларымен үйлесімсіз болады. Сондай-ақ, түрлендірілген есепте үйлесімсіз нұсқалары бар қосалқы Басқару серверлерінен алынған деректер болмайды.

5. Өзгерістерін сақтау үшін **Сақтау** түймесін басыңыз.

6. **<Есеп атауы> есебін өңдеу** терезесін жабыңыз.

Өзгертілген есеп үлгісі есеп үлгілерінің тізімінде пайда болады.

Есепті файлға экспорттау

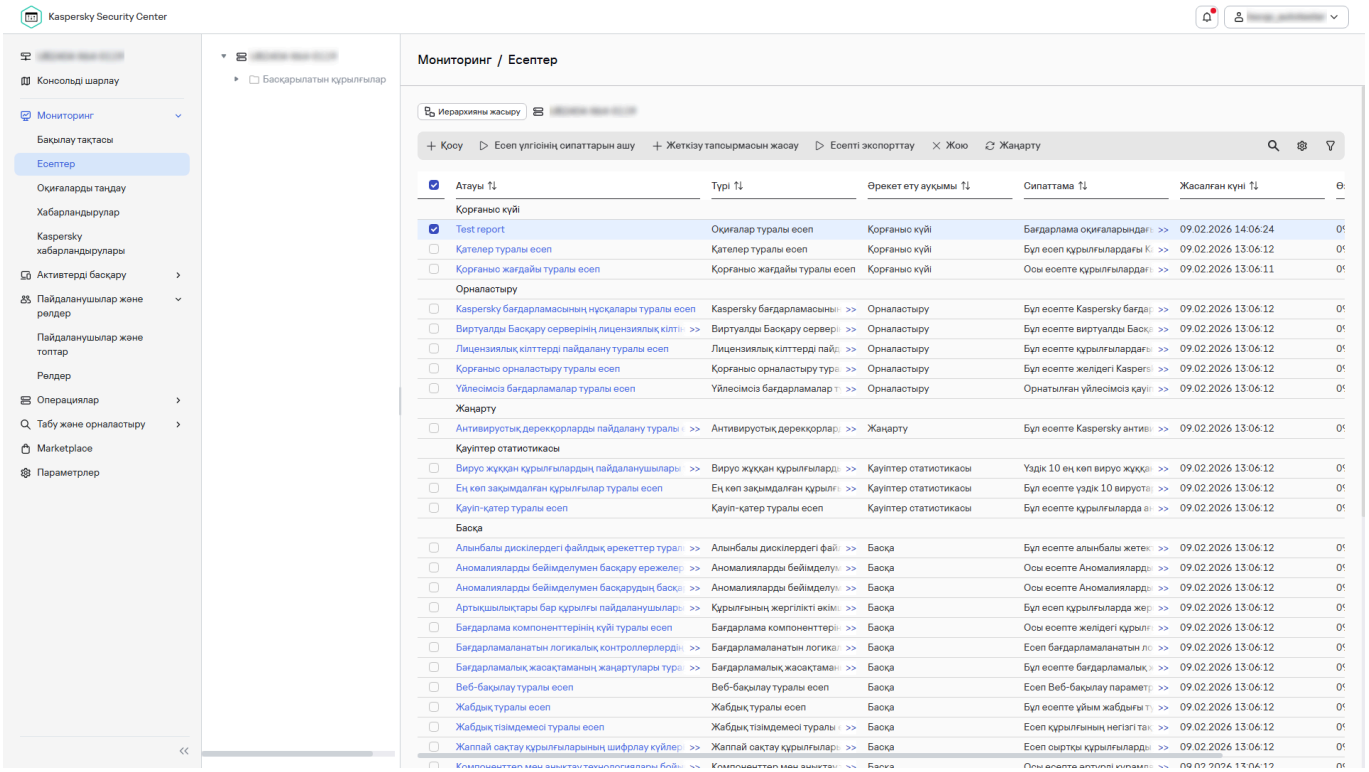
Бір немесе бірнеше есепті XML, HTML немесе PDF пішімінде сақтауға болады. Kaspersky Security Center Linux көрсетілген пішімдегі файлдарға бір уақытта 10 есепті экспорттауға мүмкіндік береді.

Есепті файлға экспорттау үшін:

1. Бағдарламаның негізгі терезесінде **Мониторинг** → **Есептер** бөліміне өтіңіз.

2. Экспорттағыңыз келетін есептерді таңдаңыз.

Оннан астам есеп таңдасаңыз, **Есепті экспорттау** түймесі өшірулі болады.



Есептер тізімі

3. **Есепті экспорттау** түймесін басыңыз.

4. Ашылған терезеде келесі экспорттау параметрлерді конфигурациялаңыз:

   - **Файл атауы**.

     Экспорттау үшін бір есепті таңдасаңыз, есеп файлына ат беріңіз.

     Бірнеше есеп таңдаған болсаңыз, есеп файлының атаулары таңдалған есеп үлгілерімен бірдей болады.

   - **Жазбалардың максималды саны**.

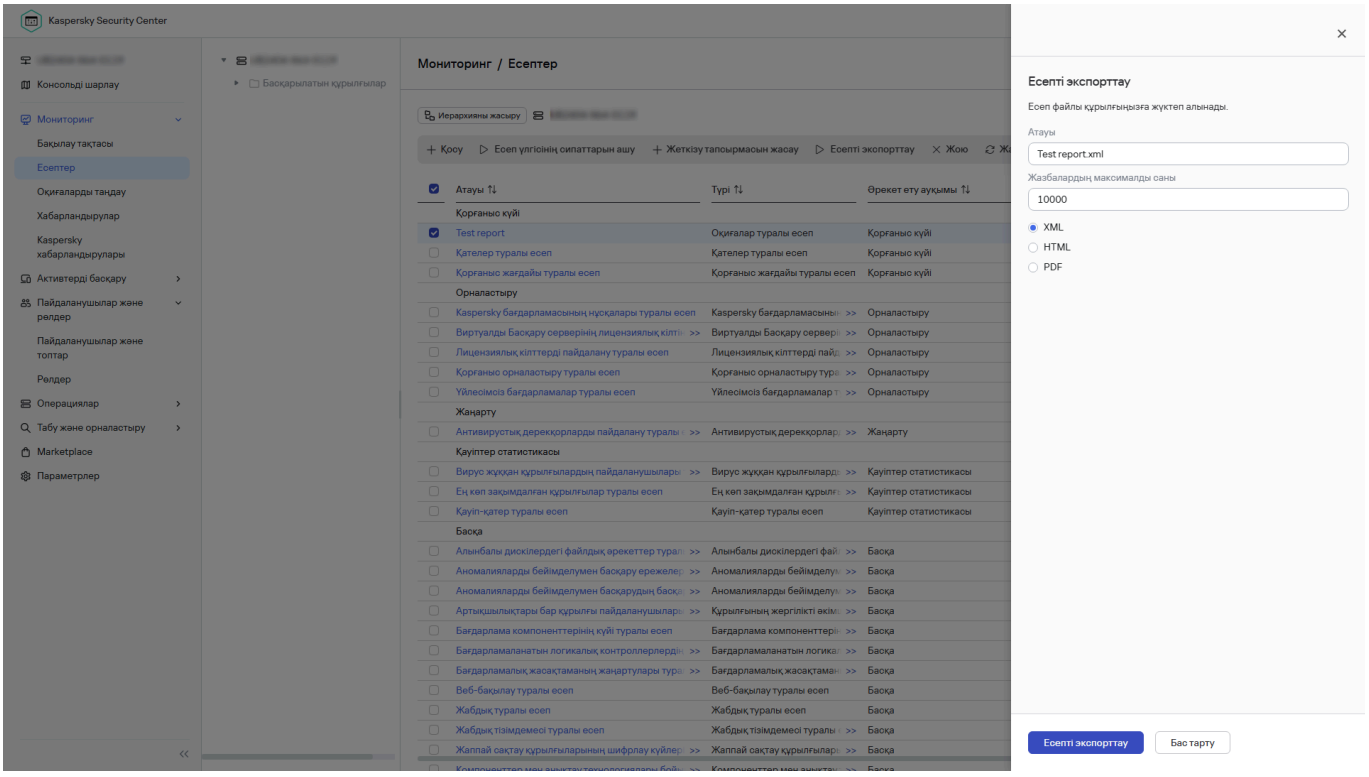
     Есеп файлына қосылатын жазбалардың ең көп санын көрсетіңіз. Әдепкі бойынша, 10,000 мәні көрсетілген.

     Есепті жазбалардың шексіз санымен экспорттауға болады. Есепте жазбалар көп болса, есепті жасау және экспорттау үшін қажет уақыт артатынын ескеріңіз.

   - **Файл пішімі**.

     Есеп файлының пішімін таңдаңыз: XML, HTML немесе PDF. Бірнеше есепті экспорттаған кезде, барлық таңдалған есептер көрсетілген пішімде бөлек файлдар ретінде сақталады.

wkhtmltopdf құралы есепті PDF пішіміне түрлендіру үшін қажет. PDF параметрі таңдалғанда, Басқару сервері wkhtmltopdf утилитасы құрылғыда орнатылғанын тексереді. Құрал орнатылмаған болса, бағдарлама оны Басқару серверінде орнату қажет екендігі туралы хабарламаны көрсетеді. Құралды қолмен орнатып, келесі қадамға өтіңіз.



Есепті экспорттау параметрлерін көрсету

5. **Есепті экспорттау** түймесін басыңыз.

Есеп файлға көрсетілген пішімде сақталады.

Есепті жасау және қарау

Есепті жасау және қарау үшін:

1. Бағдарламаның негізгі терезесінде **Мониторинг** → **Есептер** бөліміне өтіңіз.
2. Есепті жасау үшін пайдаланғыңыз келетін есеп үлгісінің атауын басыңыз.

   Жасалған есеп таңдалған үлгіні пайдаланып көрсетіледі.

Есеп деректері Басқару серверінің локализация тіліне сәйкес көрсетіледі.

Жасалған есептердегі кейбір қаріптер диаграммаларда дұрыс көрсетілмеуі мүмкін. Бұған жол бермеу үшін fontconfig кітапханасы орнатыңыз. Сондай-ақ операциялық жүйеде операциялық жүйеңіздің тіл стандартына сәйкес келетін қаріптер орнатылғанын тексеріңіз.

Есепте келесі деректер көрсетіледі:

- **Жиынтық ақпарат** қойыншасында:
  - Есептің түрі мен атауы, оның қысқаша сипаттамасы мен есепті кезеңі және есептің қай құрылғылар тобы үшін жасалғаны туралы ақпарат.
  - Есептің анағұрлым тән деректері бар графикалық диаграмма.
  - Есептелетін есеп көрсеткіштері бар жиынтық кесте.
- **Мәліметтер** қойыншасында есептің егжей-тегжейлі деректері бар кесте көрсетіледі.

Есептерді жеткізу тапсырмасын жасау

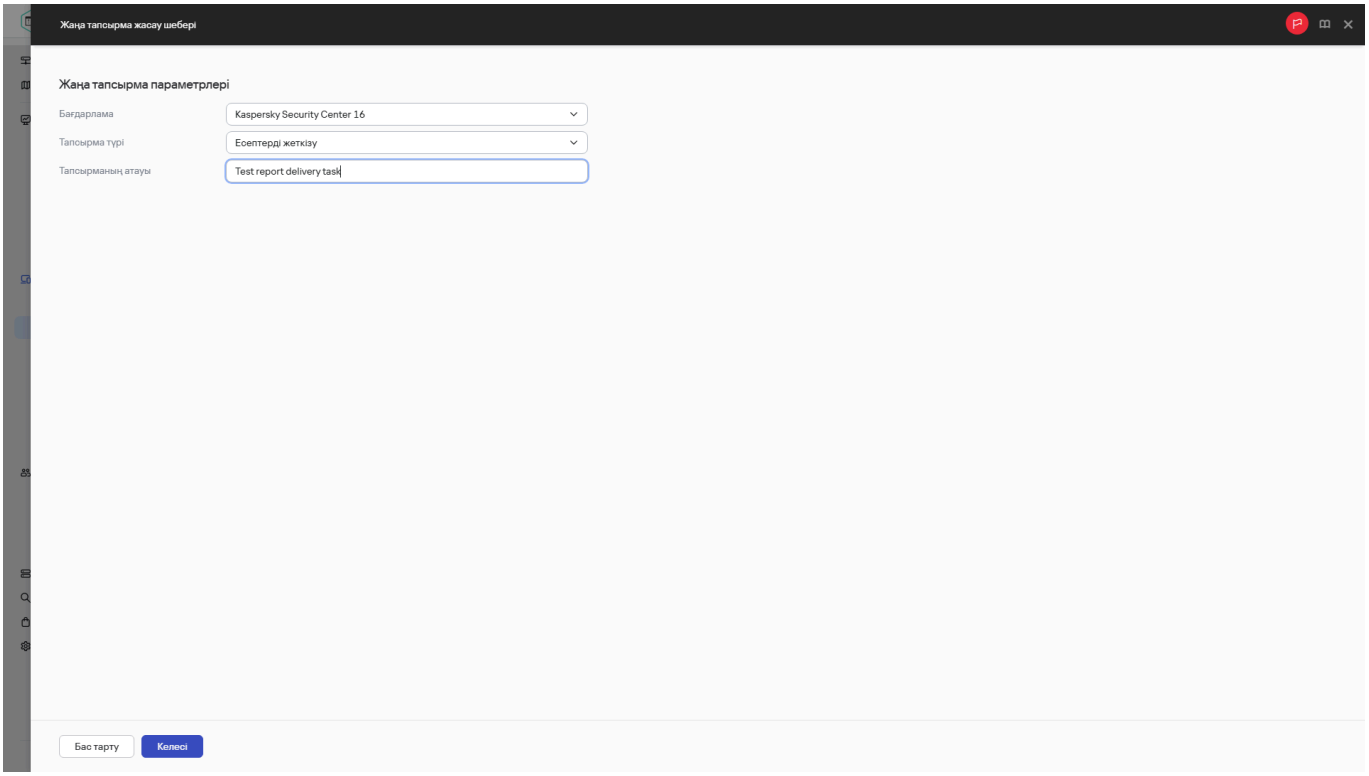
Таңдалған есептерді жеткізу тапсырмасын жасауға болады.

Есептерді жеткізу тапсырмасын жасау үшін:

1. Бағдарламаның негізгі терезесінде **Мониторинг → Есептер** бөліміне өтіңіз.
2. Есептерді жеткізу тапсырмасын жасағыңыз келетін есеп үлгілерінің жанына жалаушаларды қойыңыз.
3. **Жеткізу тапсырмасын жасау** түймесін басыңыз.

   Жаңа тапсырма жасау шебері іске қосылады. Шебердің жұмысын жалғастыру үшін **Келесі** түймесін басыңыз.
4. Шебердің **Жаңа тапсырма параметрлері** қадамында тапсырманың атауын енгізіңіз.

   Әдепкі тапсырма атауы – **Есептерді жеткізу болып табылады.** Егер аттас тапсырма бұрыннан бар болса, тапсырма атауына сериялық нөмір қосылады (<N>).



Есептерді жеткізу тапсырмасын жасау

5. Шебердің **Есеп конфигурациясы** қадамында келесі параметрлерді көрсетіңіз:

   a. Тапсырма арқылы жіберілетін есеп үлгілері.

   b. Есеп пішімі: HTML, XLS немесе PDF.

      wkhtmltopdf құралы есепті PDF пішіміне түрлендіру үшін қажет. PDF параметрі таңдалғанда, Басқару сервері wkhtmltopdf утилитасы құрылғыда орнатылғанын тексереді. Құрал орнатылмаған болса, бағдарлама оны Басқару серверінде орнату қажет екендігі туралы хабарламаны көрсетеді. Құралды қолмен орнатып, келесі қадамға өтіңіз.

   c. Есептер электрондық пошта арқылы жіберіле ме, сондай-ақ пошта хабарландыруларының параметрлері.

      Сіз ең көбі 20 электрондық пошта мекенжайын енгізе аласыз. Электрондық пошта мекенжайларын бөлу үшін **Enter** пернесін басыңыз. Сондай-ақ, үтірмен бөлінген электрондық пошта мекенжайларының тізімін қойып, **Enter** пернесін бассаңыз да болады.

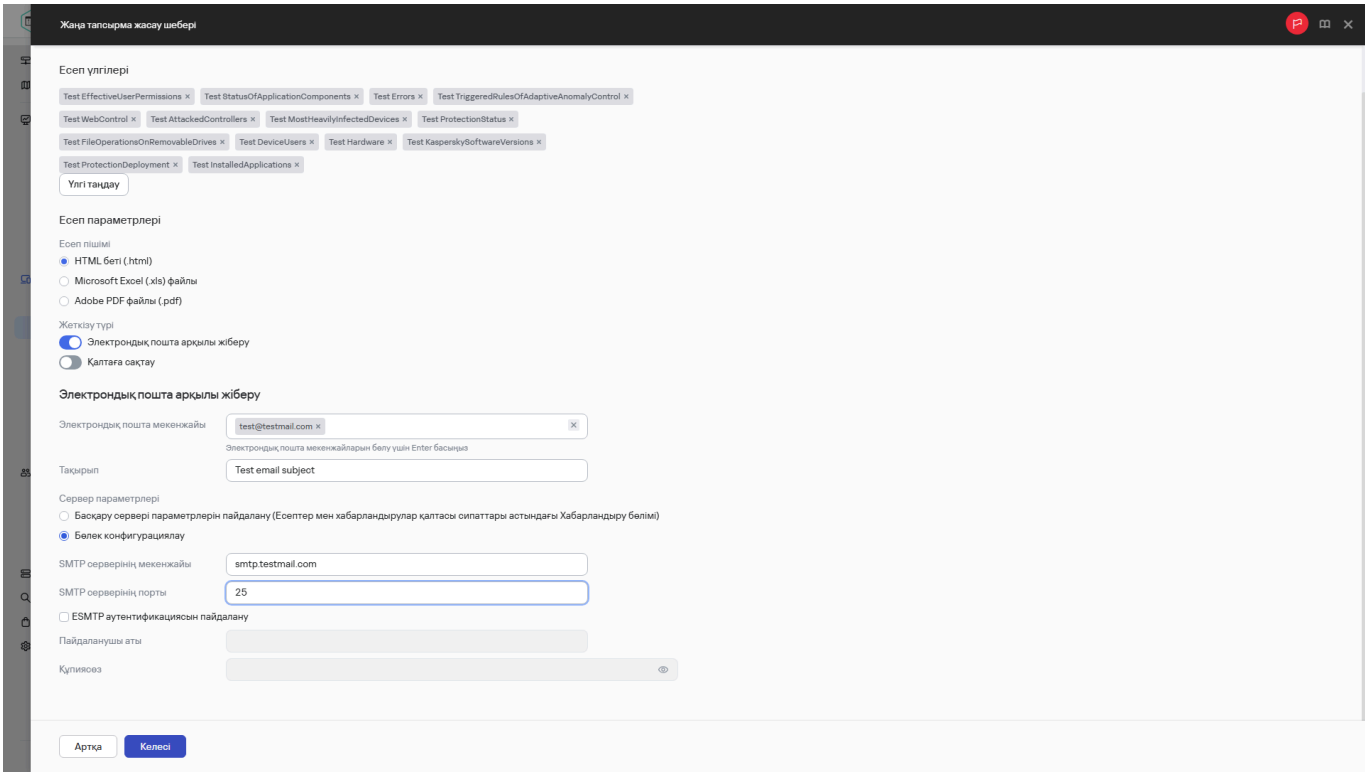
   d. Есептерді сәйкес параметрлермен бірге қалтаға сақтау қажеттігі.

      Қалтаға сақтау опциясын қосқаннан кейін, қалтаға апаратын POSIX жолын көрсетуіңіз керек. Есептерді ортақ қалтаға сақтағыңыз келсе, **Ортақ қалтаға қатынасу үшін есептік жазбаны белгілеу** құсбелгі ұяшығын таңдап, сол қалтаға кіруге арналған пайдаланушы есептік жазбасы мен құпиясөзін де көрсетуіңіз керек.

      > Есептерді ортақ қалтаға сақтауды таңдасаңыз, басқару сервері орнатылған құрылғыдан осы қалтаға кіру мүмкіндігін қамтамасыз етуіңіз керек. Қол жеткізуді қамтамасыз ету жолдары мен қолданылатын құралдар инфрақұрылымыңызға байланысты.

      Есептерді жергілікті қалтаға сақтаған кезде әдетте кіру деректері қажет емес, себебі басқару сервері іске қосылған есептік жазбада сол қалтаға кіру рұқсаты болады. Қажет болса, шебердің **Тапсырманы іске қосу үшін есептік жазбаны таңдау** қадамында пайдаланушының кіру деректерін көрсете аласыз.

Қалта таңдауына қарамастан, жаңа есеп файлының алдыңғы тапсырманы іске қосқан кезде есептер қалтасына сақталған файлдың үстінен жазылғанын қаласаңыз, **Бір түрдегі бұрынғы есептердің үстінен жазу** құсбелгі ұяшығын таңдай аласыз.



Тапсырма параметрлерін көрсету

6. Шебердің **Тапсырма кестесін конфигурациялау** қадамында тапсырманы іске қосу кестесін таңдаңыз.

   Тапсырманы іске қосу кестесінің келесі нұсқалары қолжетімді:

   - **Қолмен**

     Тапсырма автоматты түрде іске қосылмайды. Тапсырманы тек қолмен іске қосуға болады.

     Әдепкі бойынша, осы нұсқа таңдалған.

   - **N минут сайын**

     Тапсырма жүйелі түрде, тапсырма жасалған күні көрсетілген уақыттан бастап, минуттар түрінде белгіленген аралықпен орындалады.

     Әдепкі бойынша, тапсырма ағымдағы жүйелік уақыттан бастап 30 минут сайын іске қосылады.

   - **N сағат сайын**

     Тапсырма көрсетілген күн мен уақыттан бастап, сағат түрінде белгіленген аралықпен жүйелі түрде орындалады.

     Әдепкі бойынша, тапсырма ағымдағы жүйелік күн мен уақыттан бастап 6 сағат сайын іске қосылып тұрады.

   - **N күн сайын**

     Тапсырма, күндер түрінде белгіленген аралықпен жүйелі түрде орындалады. Сондай-ақ, сіз тапсырманы бірінші рет іске қосу күні мен уақытын да көрсете аласыз. Бұл қосымша параметрлерге сіз тапсырма жасап жатқан бағдарлама қолдау көрсетсе, олар қолжетімді болады.

     Әдепкі бойынша, тапсырма ағымдағы жүйелік күн мен уақыттан бастап күн сайын іске қосылады.

- **N апта сайын**

  Тапсырма жүйелі түрде, апта түрінде белгіленген аралықпен, аптаның көрсетілген күнінде және көрсетілген уақытта орындалады.

  Әдепкі бойынша, тапсырма жұма сайын, ағымдағы жүйелік уақытта іске қосылады.

- **Ай сайын**

  Тапсырма жүйелі түрде, айдың көрсетілген күнінде, көрсетілген уақытта орындалады.

  Көрсетілген күні жоқ айларда тапсырма соңғы күні орындалады.

  Әдепкі бойынша, тапсырма әр айдың бірінші күнінде, ағымдағы жүйелік уақытта орындалады.

- **Белгіленген күндері**

  Тапсырма жүйелі түрде, әр айдың көрсетілген күндерінде, көрсетілген уақытта орындалады.

  Әдепкі бойынша, басталу уақыты 18:00 және айдың күндері таңдалмайды.

  > Айдағы нақты күнді де, апта нөмірін де (айдың бірінші, екінші аптасын) емес, ай ішіндегі апта күнінің реттік нөмірін таңдайтыныңызды ескеріңіз. Мысалы, егер сіз курсорды **Сс** жолдың **Бірінші** ұяшығына орнатсаңыз, бұл тапсырма әр жаңа айдың бірінші сейсенбісінде орындалатынын білдіреді.

  Аптаның бірнеше күнін таңдай аласыз.

- **Вирустық шабуылды анықтағанда**

  Тапсырманы *Вирустың тарауы* оқиғасы туындағаннан кейін іске қосуға болады. Вирустық шабуылдарды қадағалайтын бағдарлама түрлерін таңдаңыз. Бағдарламалардың келесі түрлері қолжетімді:

  - жұмыс станциялары мен файлдық серверлерге арналған вирусқа қарсы бағдарламалар;
  - периметрлік қорғанысқа арналған вирусқа қарсы бағдарламалар;
  - пошталық жүйелерге арналған вирусқа қарсы бағдарламалар.

  Әдепкі бойынша, бағдарламалардың барлық түрлері таңдалған.

  Вирустық шабуыл туралы хабарлайтын қауіпсіздік бағдарламасының түріне байланысты әртүрлі тапсырмаларды іске қосуға болады. Бұл жағдайда, сізге қажет емес бағдарлама түрлерін таңдауды алып тастаңыз.

- **Басқа тапсырманы аяқтағанда**

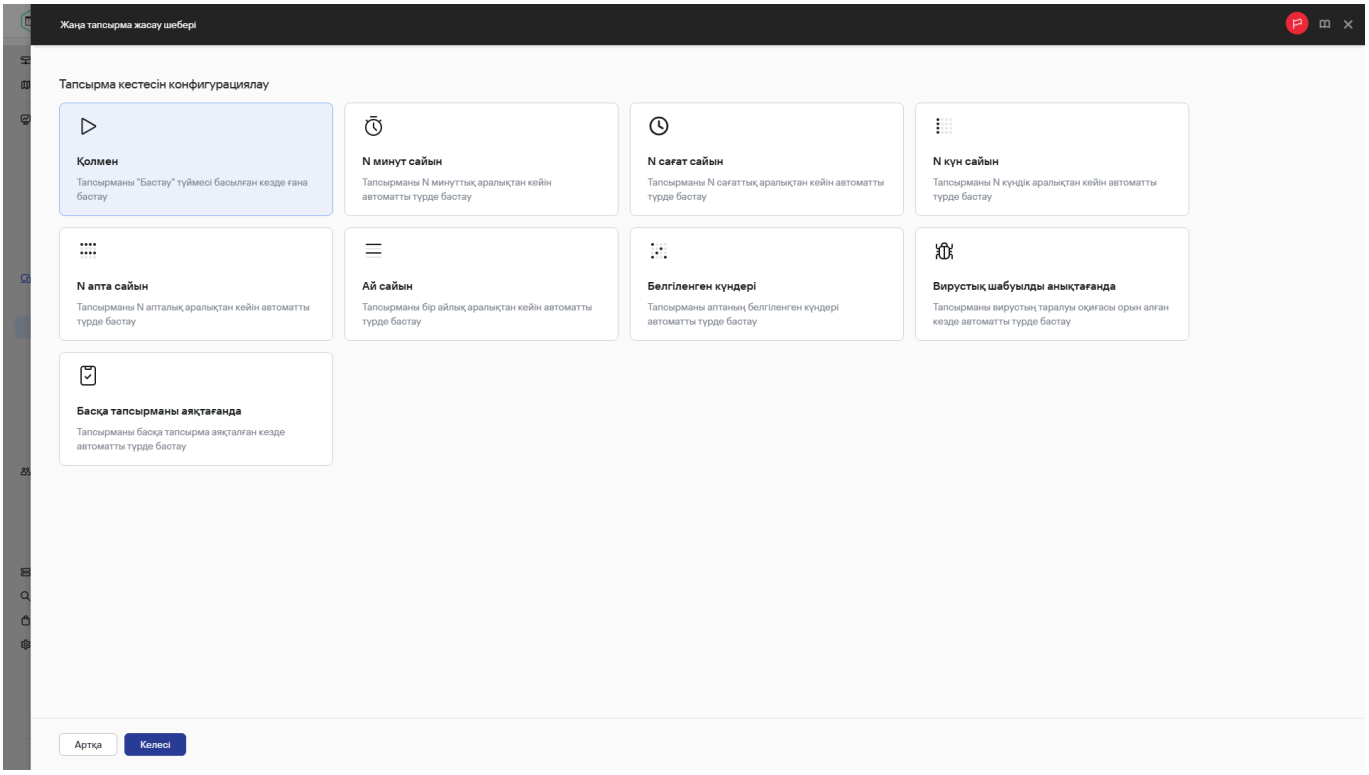
  Ағымдағы тапсырма басқа тапсырма аяқталғаннан кейін іске қосылады. Екі тапсырма да бір құрылғы арқылы тағайындалса ғана, осы параметр жұмыс істейді. Мысалы, *Құрылғыларды басқару* тапсырмасын **Құрылғыны қосу** параметрінің көмегімен іске қоса аласыз және ол аяқталғаннан кейін *Вирустарды іздеу* тапсырмасын іске қоса аласыз.

  Кестеден іске қосу тапсырмасын және осы тапсырма орындалатын күйді таңдау керек (**Сәтті аяқталды** немесе **Сәтсіз аяқталды**).

Қажет болса, кестедегі тапсырмаларды төмендегідей іздеуге, сұрыптауға және сүзуге болады:

- Тапсырманы атауы бойынша іздеу үшін іздеу өрісіне тапсырма атауын енгізіңіз.
- Тапсырмаларды атауы бойынша сұрыптау үшін сұрыптау белгішесін басыңыз.

  Әдепкі бойынша, тапсырмалар өсу ретімен әліпбилік ретпен сұрыпталады.
- Сүзгі белгішесін басыңыз және ашылатын терезеде тапсырмаларды топтар бойынша сүзіңіз, содан кейін **Қолдану** түймесін басыңыз.



Тапсырманы бастау кестесін таңдау

7. Шебердің осы қадамында тапсырманы іске қосу кестесінің басқа параметрлерін конфигурациялаңыз:

- **Тапсырма кестесі** бөлімінде бұрын таңдалған кестені тексеріңіз немесе қайта конфигурациялаңыз және кезеңді, ай немесе апта күндерін орнатыңыз, вирус шабуылының шартын немесе тапсырманы іске қосу ретінде басқа тапсырманың орындалуын белгілеңіз. Бұл бөлімде қолайлы кесте таңдалған болса, басталу уақытын да көрсетуге болады.
- **Қосымша параметрлер** бөлімінде келесі параметрлерді көрсетіңіз:
  - **Өткізіп алынған тапсырмаларды іске қосу**

    Бұл параметр, тапсырма басталғалы тұрған кезде клиент құрылғысы желіде көрсетілмесе, тапсырманың жүріс-тұрысын анықтайды.

    Параметр қосулы болса, клиент құрылғысында Kaspersky бағдарламасын кезекті рет іске қосу кезінде тапсырманы іске қосу әрекеті жасалады. Тапсырманың кестесінде **Қолмен**, **Бір рет** немесе **Дереу** іске қосу көрсетілсе, онда тапсырма желіде құрылғы көзге көрінетін болғаннан кейін немесе құрылғы тапсырманың әрекет ету ауқымына қосылғаннан кейін бірден іске қосылады.

    Егер параметр өшірулі болса, клиент құрылғыларында тапсырманы іске қосу тек кесте бойынша орындалатын болады. **Қолмен**, **Бір рет** және **Дереу** кестесі үшін тапсырмалар желіде көрінетін клиенттік құрылғыларда ғана орындалады. Мысалы, сіз бұл параметрді тек жұмыс уақытынан тыс уақытта іске қосқыңыз келетін ресурстарды қажетсінетін тапсырма үшін өшіре аласыз.

    Әдепкі бойынша, параметр өшірулі.

- **Тапсырманы бастау үшін автоматты түрде араластырылған кідірісті пайдалану**

  Параметр қосулы болса, тапсырма клиент құрылғыларында белгілі бір уақыт аралығында кездейсоқ іске қосылады, яғни *тапсырманың таратылған іске қосылуы* орын алады. Тапсырманың таратылған іске қосылуы, тапсырманы кесте бойынша іске қосу кезінде көптеген клиент құрылғыларының Басқару серверіне бір уақытта жүгінуіне жол бермейді.

  Таратылған іске қосылу кезеңі, тапсырма тағайындалған клиент құрылғыларының санына байланысты тапсырманы жасау кезінде автоматты түрде есептеледі. Кейінірек, тапсырма әрқашан есептелген іске қосу уақытында іске қосылады. Алайда, тапсырма параметрлеріне түзетулер енгізілгенде немесе тапсырма қолмен іске қосылғанда, тапсырманы іске қосу уақытының есептелген мәні өзгереді.

  Егер параметр өшірулі болса, клиент құрылғыларында тапсырманы іске қосу кесте бойынша орындалады.

- **Тапсырманы бастауға арналған келесі аралықтағы автоматты кездейсоқ кідірісті пайдалану**

  Параметр қосулы болса, тапсырма клиент құрылғыларында белгілі бір уақыт аралығында кездейсоқ іске қосылады. Тапсырманың таратылған іске қосылуы, тапсырманы кесте бойынша іске қосу кезінде көптеген клиент құрылғыларының Басқару серверіне бір уақытта жүгінуіне жол бермейді.

  Егер параметр өшірулі болса, клиент құрылғыларында тапсырманы іске қосу кесте бойынша орындалады.

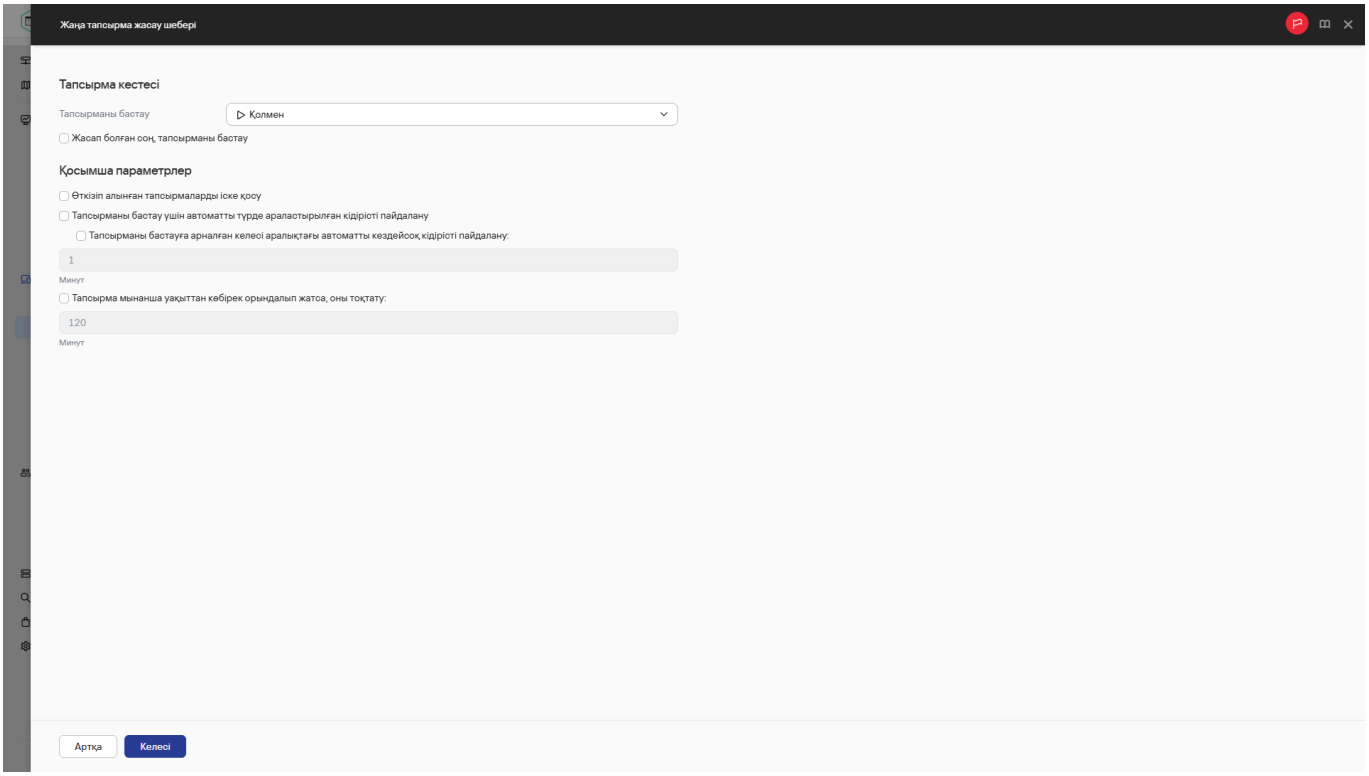
  Әдепкі бойынша, параметр өшірулі. Әдепкі бойынша, уақыт аралығы бір минутқа тең.

- **Тапсырма мынанша уақыттан көбірек орындалып жатса, оны тоқтату**

  Белгіленген уақыттан кейін, тапсырма аяқталғанына немесе аяқталмағанына қарамастан автоматты түрде тоқтатылады.

  Егер сіз тым ұзақ орындалатын тапсырмаларды үзгіңіз келсе (немесе тоқтатқыңыз келсе), осы параметрді қосыңыз.

  Әдепкі бойынша, параметр өшірулі. Әдепкі бойынша тапсырманы орындау уақыты – 120 минут.

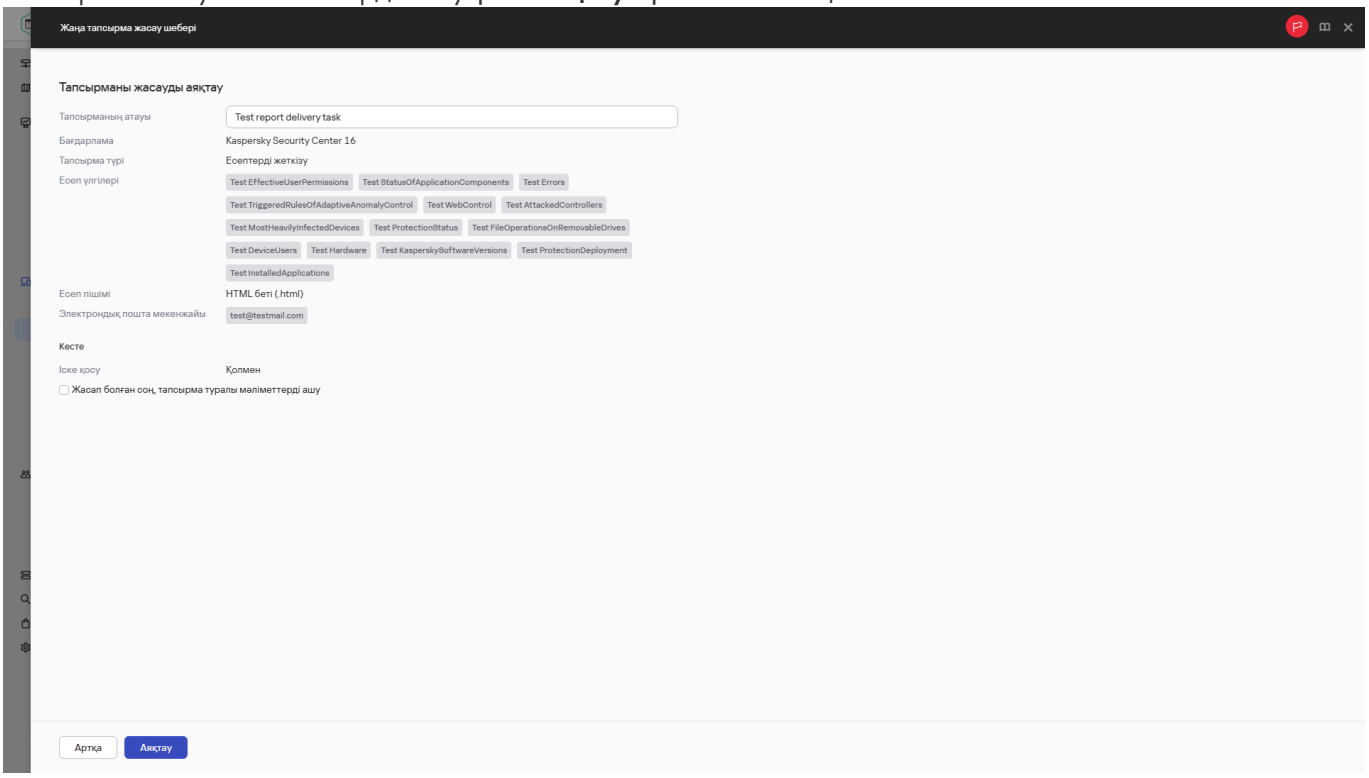


Тапсырмалар кестесінің параметрлерін көрсету

8. Шебердің **Тапсырманы іске қосу үшін есептік жазбаны таңдау** қадамында тапсырманы іске қосу үшін пайдаланылатын есептік жазба деректерін көрсетіңіз.

9. Тапсырманы жасағаннан кейін, оның басқа параметрлерін өзгерту қажет болса, шебердегі **Тапсырманы жасауды аяқтау** қадамында **Жасап болған соң, тапсырма туралы мәліметтерді ашу** опциясын қосыңыз (әдепкісінше бұл опция қосулы болады).

10. Тапсырма жасау және шеберді жабу үшін **Аяқтау** түймесін басыңыз.



Тапсырманы жасауды аяқтау

Есепті жіберу тапсырмасы жасалады. **Жасап болған соң, тапсырма туралы мәліметтерді ашу** параметрі қосылса, тапсырма параметрлері терезесі ашылады.

Есеп үлгілерін жою

Есеп үлгілерін жою үшін:

1. Бағдарламаның негізгі терезесінде **Мониторинг** → **Есептер** бөліміне өтіңіз.

2. Жойғыңыз келетін есеп үлгілеріне қарсы жалаушаларды қойыңыз.

3. **Жою** түймесін басыңыз.

4. Пайда болған терезеде таңдауыңызды растау үшін **OK** түймесін басыңыз.

Таңдалған есеп үлгілері жойылады. Егер бұл есеп үлгілері есептерді жіберу тапсырмаларына енгізілген болса, олар да осы тапсырмалардан жойылады.

Қорғаныс деңгейінің индикаторы

Қорғаныс деңгейінің индикаторы сіздің Басқару серверіңіз бен тарату нүктелерін қорғау туралы жаңартылған ақпаратты көрсетеді. Бұл сізге Қауіпсіздікті күшейту жөніндегі нұсқаулықтың орындалуын бақылауға мүмкіндік береді. Индикатор **Мониторинг** → **Бақылау тақтасы** көрсетіледі және оны жасыруға немесе Web Console мәзірінің басқа бөліміне орналастыруға болмайды. Индикаторды басу арқылы сіз Қауіпсіздікті күшейту орталығына өтіп, Басқару сервері мен тарату нүктелерінің қорғау параметрлерінің күйлерін көре аласыз. Инфрақұрылымыңыздың қауіпсіздігін арттыру үшін, егер бар болса, көрсетілген мәселелерді шешуіңіз керек.

Индикатор келесі күйлердің бірінде мыналар болуы мүмкін:

- Қорғаныс конфигурацияланған.
- Қорғаныс жартылай конфигурацияланған.
- Қорғаныс конфигурацияланбаған.

Қорғаныс деңгейі туралы егжей-тегжейлі ақпаратты қалай көруге болады

Жалпы индикатор күйі қорғаныс параметрлерінің күйлерімен қалыптасады.

Параметрлерді көру үшін индикаторды басыңыз.

Ашылған **Қауіпсіздікті күшейту орталығы** терезесінде параметрлер қорғалған нысандар бойынша топтастырылады: Басқару сервері және тарату нүктелері.

Әрбір қорғау параметрі сіздің қатынасу құқықтарыңызға байланысты күйлердің бірінде көрсетіледі:

- егер шешілетін мәселелер болмаса немесе сізде қажетті қатынасу құқықтары болмаса.
- ⚠ немесе ✖, егер шешілуі тиіс мәселелер болса.

Келесі параметрлер тек Басқару сервері үшін көрсетіледі:

- Сақтық көшірме конфигурацияланған
- Басқару серверіне техникалық қызмет көрсету тапсырмасы
- TLS шифрлау қосылған

Келесі параметрлер Басқару сервері және тарату нүктелері үшін көрсетіледі:

- Қауіпсіздік бағдарламасы орнатылған
- Қолданылған саясат
- Антивирустық дерекқорларды жаңарту схемасы

Басқару серверіне арналған мүмкіндіктер:

- Барлық қорғау параметрлері тек физикалық Басқару сервері үшін есептеледі және виртуалды серверлерге қолданылмайды.

  Егер сізде бірнеше Басқару серверлерінің иерархиялық құрылымы болса, қорғау деңгейінің индикаторы әрбір физикалық сервер үшін бөлек есептеледі.

- **Орнатылған қауіпсіздік бағдарламасы**, **Қолданылған саясат**, **Антивирустық дерекқорларды жаңарту конфигурацияланған** параметрлері Басқару сервері орнатылған құрылғы үшін есептеледі.

- Kaspersky Security Center Linux ақауларға төзімді кластерін орналастырған кезде, **орнатылған қауіпсіздік қолданбасы**, **Қолданылған саясат**, **Антивирустық дерекқорларды жаңарту конфигурацияланған** параметрлері әрбір түйін үшін есептеледі. Түйін индикатор күйін есептеу кезінде тек белсенді болғаннан кейін ғана ескеріледі.

Индикатор күйі қалай есептеледі

Индикатор күйі кестеде сипатталғандай есептеледі.

Индикатор күйі	Шарт
Қорғаныс конфигурацияланған.	Барлық қорғаныс параметрлері күйінде.
Қорғаныс жартылай конфигурацияланған.	**Антивирустық дерекқорларды жаңарту конфигурацияланған** параметрі күйінде, ал басқа барлық параметрлер күйінде.
Қорғаныс конфигурацияланбаған.	Егер келесі қорғаныс параметрлерінің кем дегенде біреуі күйінде болса.

Қауіпсіздік бағдарламасы орнатылған

Қауіпсіздік қолданбалары құрылғыларыңызды желілік, фишингтік және алаяқтық шабуылдарды қоса алғанда, әртүрлі қауіптерден қорғауға мүмкіндік береді.

Параметр, төмендегі шарттардың бірі орындалған кезде күйінде көрсетіледі:

- Құрылғыларға қатынасу құқығыңыз жоқ.

- Құрылғыларға Желілік агент пен қауіпсіздік бағдарламасы орнатылған кезде, **Оқу** → **Жалпы функционал** функционалдық аймағында **Базалық функционалдылық** құқығыңыз бар.

  > Бұл шарт сіздің қатынасу құқықтарыңызға негізделген барлық құрылғыларда орындалуы керек, антивирустық қорғауды қажет етпейтін орнатылған қолданбасы бар құрылғыларды қоспағанда (мысалы, қорғалған операциялық жүйе, құрылғы туралы ақпарат Басқару серверінде 24 сағаттан аз уақыт бұрын пайда болғандықтан), Желілік агент орнатылмаған құрылғылар және Басқару серверіне соңғы рет 7 немесе одан да көп күн бұрын қосылған офлайн құрылғылар.

Параметр, төмендегі шарттардың кем дегенде біреуі орындалған кезде күйінде көрсетіледі.

Сіз **«Құрылғыларды қарау»** түймесін басып, көрсетілген құрылғылар үшін кестеде сипатталған әрекеттерді орындауыңыз керек.

Шарт	Шешім
Құрылғыға Желілік агент орнатылмаған	Желілік агентті орнату. Басқару сервері құрылғысы үшін Желілік агентті орнатудың ең қарапайым жолы — жеке орнату пакетін пайдалану.
Құрылғы **«Тағайындалмаған құрылғылар»** тобына кіреді	Құрылғыны «Басқарылатын құрылғылар» тобына немесе оның кіші тобына жылжытыңыз
Қауіпсіздік бағдарламалары табылмады немесе орнатылған қауіпсіздік бағдарламасы үшін нақты уақыттағы қорғаныс жұмыс істемейді	Қауіпсіздік бағдарламасын орнатыңыз. Қолданба қорғаныс күйі туралы деректерді Басқару серверіне жібереді. Құрылғының қорғаныс күйін келесі құрылғы параметрлерінен көре аласыз: **Жалпы** бөлім → **Құрылғының күйі**. Басқару серверінің құрылғысында Kaspersky Endpoint Security for Linux орнатуыңыз керек.

Қолданылған саясат

Саясат – басқару тобы мен оның ішкі тобына қатысты қолданылатын қауіпсіздік бағдарламасының параметрлері жиынтығы.

Параметр, төмендегі шарттардың бірі орындалған кезде күйінде көрсетіледі:

- Құрылғыларға қатынасу құқығыңыз жоқ.
- Құрылғыларыңызға қауіпсіздік бағдарламасы орнатылған кезде және құрылғыларға осы қауіпсіздік бағдарламасының белсенді саясаты қолданылатын кезде, **Оқу** → **Жалпы функционал** функционалдық аймағында **Базалық функционалдылық** құқығыңыз бар.

  Бұл шарт сіздің қатынасу құқықтарыңызға негізделген барлық құрылғыларда орындалуы керек, антивирустық қорғауды қажет етпейтін орнатылған қолданбасы бар құрылғыларды қоспағанда (мысалы, қорғалған операциялық жүйе, құрылғы туралы ақпарат Басқару серверінде 24 сағаттан аз уақыт бұрын пайда болғандықтан), Желілік агент орнатылмаған құрылғылар және Басқару серверіне соңғы рет 7 немесе одан да көп күн бұрын қосылған офлайн құрылғылар.

Параметр, төмендегі шарттардың кем дегенде біреуі орындалған кезде күйінде көрсетіледі.

Сіз **«Құрылғыларды қарау»** түймесін басып, көрсетілген құрылғылар үшін кестеде сипатталған әрекеттерді орындауыңыз керек.

Шарт	Шешім
Қауіпсіздік бағдарламасы құрылғыға орнатылған.	Қауіпсіздік бағдарламасы орнатылған қорғау параметрін таңдағанда құрылғылардың жоқ екеніне көз жеткізіңіз.

Құрылғыға саясат қолданылмаған.	Құрылғы тиесілі басқару тобы үшін саясат жасалғанына көз жеткізіңіз. Егер жоқ болса, саясатты жасап, белсендіріңіз. Егер иә болса, мынаған көз жеткізіңіз: • Жасалған саясат белсенді. Егер жоқ болса, саясатты белсендіріңіз. • Саясатты тарату күйі **сәтті қолданылды**. Егер күй **қатемен қолданылған** болса, мәселе қауіпсіздік бағдарламасы жағында шешілуі керек.

Антивирустық дерекқорларды жаңарту схемасы

Антивирустық дерекқорлар құрылғыларыңызды қауіптерден қорғайтындықтан, құрылғылардағы дерекқорларды үнемі және уақтылы жаңартып отыруыңыз керек.

Параметр, төмендегі шарттардың бірі орындалған кезде ✅ күйінде көрсетіледі:

- Құрылғыларға қатынасу құқығыңыз жоқ.
- Оқу → Жалпы функционал функционалдық аймағында Базалық функционалдылық құқығыңыз бар, ал құрылғылардағы вирусқа қарсы дерекқорлар жаңартылады.

  Бұл шарт сіздің қатынасу құқықтарыңызға негізделген барлық құрылғыларда орындалуы керек, антивирустық қорғауды қажет етпейтін орнатылған қолданбасы бар құрылғыларды қоспағанда (мысалы, қорғалған операциялық жүйе, құрылғы туралы ақпарат Басқару серверінде 24 сағаттан аз уақыт бұрын пайда болғандықтан), Желілік агент орнатылмаған құрылғылар және Басқару серверіне соңғы рет 7 немесе одан да көп күн бұрын қосылған офлайн құрылғылар.

Параметр, антивирустық дерекқорлар құрылғыда соңғы рет 3 күннен астам уақыт бұрын жаңартылған болса, ⚠️ күйінде көрсетіледі.

Параметр, антивирустық дерекқорлар құрылғыда соңғы рет 7 күннен астам уақыт бұрын жаңартылған болса, ❌ күйінде көрсетіледі.

Мәселелерді шешу үшін:

1. Параметрдің жанындағы «Құрылғыларды қарау» түймесін басыңыз.
2. Көрсетілген құрылғылар үшін келесі әрекеттерді орындаңыз:
   a. Желілік агент пен Басқару сервері арасында байланыс орнатылғанына көз жеткізіңіз.

      Егер олай болмаса, келесі мақалаларды қараңыз:

      Kaspersky Endpoint Security for Linux антивирустық дерекқорларын жаңарту кезіндегі мәселелерді шешу

      Kaspersky Security Center қоймасынан антивирустық дерекқорларды жаңарту кезіндегі мәселелер

   b. Сіз тексеріп жатқан антивирустық дерекқорлары Kaspersky қолданбасының тоқтатылмағанына көз жеткізіңіз.

      Егер қолданба тоқтатылған болса, оны іске қосыңыз.

   c. Құрылғыда жаңартудан кейін пайда болған қателерді қараңыз.

Сақтық көшірме конфигурацияланған

Басқару сервері деректерінің сақтық көшірмесін жасау бойынша ұсыныстар алу үшін Басқару сервері деректерінің сақтық көшірмесін жасау және қалпына келтіру бөлімін қараңыз.

Параметр, төмендегі шарттардың бірі орындалған кезде күйінде көрсетіледі:

- Сізде Басқару серверінің деректерін сақтық көшірмелеу тапсырмасымен жұмыс істеуге рұқсат жоқ.
- Сізде **Жалпы функционал** → **Басқару серверіне қатысты әрекеттер** функционалдық аймағында **Оқу, Жазу** және **Орындау** құқықтары бар, ал сақтық көшірме жасау тұрақты түрде конфигурацияланған және орындалады.

Параметр, төмендегі шарттардың кем дегенде біреуі орындалған кезде күйінде көрсетіледі.

Шарт	Шешім
Басқару серверінің деректерін сақтық көшірмелеу тапсырмасы жасалмаған.	Тапсырманы жасау.
Басқару серверінің деректерін сақтық көшірмелеу тапсырмасы үшін қажетті кесте параметрлері конфигурацияланбаған.	Басқару серверінің техникалық қызмет көрсету тапсырмасында **Вирустық шабуылды анықтағанда** және **Қолмен** нұсқаларынан басқа **Тапсырманы бастау** параметрлерін көрсетіңіз.

Басқару серверіне техникалық қызмет көрсету тапсырмасы

Басқару серверіне техникалық қызмет көрсету Басқару серверінің қалтасында орын босатуға, сондай-ақ дерекқор өлшемін азайтуға мүмкіндік береді. Бұл сұранысты өңдеуді жеделдетуге және жүйенің жалпы тұрақтылығын арттыруға көмектеседі.

Параметр, төмендегі шарттардың бірі орындалған кезде күйінде көрсетіледі:

- Сізде Басқару серверіне техникалық қызмет көрсету тапсырмасымен жұмыс істеуге рұқсат жоқ.
- Сізде **Жалпы функционал** → **Басқару серверіне қатысты әрекеттер** функционалдық аймағында **Оқу, Жазу** және **Орындау** құқықтары бар, ал Басқару серверіне техникалық қызмет көрсету тұрақты түрде конфигурацияланған және орындалады.

  Құқықтар Басқару сервері деңгейінде орнатылуы керек.

Параметр, төмендегі шарттардың кем дегенде біреуі орындалған кезде күйінде көрсетіледі.

Шарт	Шешім
Басқару серверіне техникалық қызмет көрсету тапсырмасы жасалмаған.	Тапсырманы жасау.
Басқару серверіне техникалық қызмет көрсету тапсырмасы үшін қажетті кесте параметрлері конфигурацияланбаған.	Басқару серверінің техникалық қызмет көрсету тапсырмасында **Вирустық шабуылды анықтағанда** және **Қолмен** нұсқаларынан басқа **Тапсырманы бастау** параметрлерін көрсетіңіз.

TLS шифрлау қосылған

TLS хаттамасының тек 1.2 және 1.3 нұсқаларына рұқсат етілгеніне көз жеткізуіңіз керек. Алдыңғы нұсқаларға рұқсат беру деректер қауіпсіздігінде елеулі осалдық тудырады және жүйелерді шабуылдарға осал етеді.

Параметр, TLS хаттамасының тек 1.2 және 1.3 нұсқаларына ғана рұқсат етілсе ғана ✅ күйінде көрсетіледі.

Параметр, 1.2 нұсқасынан бұрынғы ескірген TLS нұсқаларына рұқсат етілсе ғана ❌ күйінде көрсетіледі.

Мәселені шешу үшін сіз `SrvUseStrictSslSettings` жалаушасының мәнін `4` немесе `5` деп белгілеуіңіз керек.

Оқиғалар және оқиғаларды таңдау

Бұл бөлімде оқиғалар мен оқиғаларды таңдау, Kaspersky Security Center Linux құрамдастарында орын алған оқиғалар түрлері және жиі болатын оқиғаларды бұғаттауды басқару туралы ақпарат бар.

Kaspersky Security Center Linux-тегі оқиғалар туралы

Kaspersky Security Center Linux бағдарламасы, басқарылатын бағдарламаларға орнатылған Kaspersky Басқару сервері мен бағдарламаларының жұмысы барысында орын алған оқиғалар туралы ақпаратты алуға мүмкіндік береді. Оқиғалар туралы ақпарат Басқару серверінің дерекқорында сақталады.

Түрі бойынша оқиғалар

Kaspersky Security Center Linux-те хабарландырулардың келесі түрлері бар:

- Жалпы оқиғалар. Бұл оқиғалар барлық Kaspersky басқарылатын бағдарламаларында туындайды. Мысалы, Вирустың тарауы жалпы оқиға. Жалпы оқиғалар қатаң белгіленген синтаксис пен семантикаға ие. Жалпы оқиғалар, мысалы, есептер мен мониторинг тақтасында қолданылады.

- Kaspersky басқарылатын бағдарламаларының айрықша оқиғалары. Kaspersky әрбір басқарылатын бағдарламасы өзіндік оқиғалар жиынтығына ие.

Дереккөз бойынша оқиғалар

Бағдарлама жасай алатын оқиғалардың толық тізімі бағдарлама саясаты сипаттарындағы **Оқиғаларды конфигурациялау** қойыншасында келтірілген. Басқару сервері үшін, Басқару серверінің сипаттарындағы оқиғалар тізімін қосымша түрде қарап шығуға болады.

Оқиғалар келесі бағдарламалар тарапынан жасалуы мүмкін:

- Kaspersky Security Center Linux бағдарламасының құрамдастары:
  - Басқару сервері
  - Желілік агент
- Kaspersky басқарылатын бағдарламалары

  Kaspersky басқарылатын бағдарламалары жасайтын оқиғалар туралы толығырақ ақпарат тиісті бағдарламаның құжаттасында келтірілген.

Маңыздылық дәрежесі бойынша оқиғалар

Әрбір оқиғаның өзіндік маңыздылық деңгейі бар. Туындау шарттарына байланысты, оқиғаға түрлі маңыздылық деңгейлері белгіленуі мүмкін. Оқиғалар маңыздылығының төрт деңгейі бар:

- *Критикалық оқиға* – деректерді жоғалтуға, жұмыстағы ақауға немесе критикалық қатеге әкелуі мүмкін критикалық мәселенің туындағанын білдіретін оқиға.
- *Функционалдық ақау* – қолданбаның жұмысы немесе рәсімді орындау барысында туындаған күрделі мәселенің, қатенің немесе ақаудың орын алғанын білдіретін оқиға.
- *Ескерту* – міндетті түрде күрделі болып саналмаса да, болашақта мәселенің туындауы мүмкін екенін білдіретін оқиға. Оқиғалар туындағаннан кейін бағдарламаның жұмысы деректерді немесе функционалдық мүмкіндіктерді жоғалтпай қалпына келтіріле алса, осы оқиғалар көбінесе Ескертулерге қатысты болып келеді.
- *Ақпараттық хабарлар* – операцияның сәтті орындалуы, бағдарламаның дұрыс жұмыс істеуі немесе рәсімнің аяқталуы туралы хабарлау мақсатында туындайтын оқиға.

Әрбір оқиға үшін Kaspersky Security Center Linux-де қарап шығуға немесе өзгертуге болатын сақтау уақыты белгіленген. Кейбір оқиғалар Басқару серверінің дерекқорында әдепкі бойынша сақталмайды, себебі олар үшін белгіленген уақыт нөлге тең. Сыртқы жүйелерге, Басқару серверінің дерекқорында кемінде бір күн бойы сақталатын оқиғалар ғана экспортталуы мүмкін.

Оқиғалар: Kaspersky Security Center Linux құрамдасы

Kaspersky Security Center Linux әрбір құрамдасының өзіндік оқиғалар түрлерінің жиынтығы бар. Бұл бөлімде Басқару серверінде және Желілік агентте орын алатын оқиғалардың түрлері берілген. Kaspersky бағдарламаларында орын алатын оқиғалар түрлері бұл бөлімде атап көрсетілмеген.

Бағдарлама жасай алатын әрбір оқиға үшін, бағдарлама саясаты сипаттарындағы **Оқиғаларды конфигурациялау** қойындысында хабарландыру параметрлерін және сақтау параметрлерін көрсетуге болады. Басқару сервері үшін, Басқару серверінің сипаттарындағы оқиғалар тізімін қосымша түрде қарап шығуға және конфигурациялауға болады. Барлық оқиғалар үшін хабарландыру параметрлерін бірден конфигурациялау қажет болса, Басқару сервері сипаттарында жалпы хабарландыру параметрлерін конфигурациялаңыз.

Оқиға түрі сипаттамасы деректерінің құрылымы

Оқиғалардың әр түрі үшін оның аты, идентификаторы, әріптік коды, сипаттамасы және әдепкі бойынша сақтау уақыты көрсетіледі.

- **Оқиға түрінің көрсетілетін атауы**. Бұл мәтін Kaspersky Security Center Linux бағдарламасында оқиғаларды орнатқан кезде және олар пайда болған кезде көрсетіледі.
- **Оқиға түрі идентификаторы**. Бұл сандық код үшінші тарап оқиғаларын талдау құралдарын қолдана отырып, оқиғаларды өңдеуде қолданылады.
- **Оқиға түрі** (әріптік код). Бұл код Kaspersky Security Center Linux дерекқорының жария көріністерін пайдалана отырып, оқиғаларды қарау және өңдеу кезінде және оқиғаларды SIEM жүйелеріне экспорттау кезінде пайдаланылады.
- **Сипаттамасы**. Бұл мәтінде оқиға болған кездегі жағдайдың сипаттамасы және бұл жағдайда не істеуге болатыны туралы сипаттама келтірілген.
- **Әдепкі бойынша сақтау мерзімі**. Бұл, оқиға Басқару серверінің дерекқорында сақталатын және Басқару сервері оқиғаларының тізімінде көрсетілетін күндер саны. Осы кезең аяқталғаннан кейін, оқиға жойылады. Егер оқиғаны сақтау уақытының мәні 0 болып көрсетілсе, мұндай оқиғалар тіркеледі, бірақ Басқару сервері оқиғалары тізімінде көрсетілмейді. Егер сіз осындай оқиғаларды операциялық жүйенің оқиғалар журналында сақтауды конфигурациялаған болсаңыз, оларды сол жерден таба аласыз.

  Оқиғалар үшін сақтау орны мерзімін өзгертуге болады: Оқиға үшін сақтау орны мерзімін орнату

Басқару сервері оқиғалары

Бұл бөлімде Басқару сервері оқиғалары туралы ақпарат бар.

Басқару серверінің критикалық оқиғалары

Төмендегі кестеде **Маңызды** маңыздылық деңгейіндегі Басқару серверінің оқиғалары берілген.

Бағдарлама жасай алатын әрбір оқиға үшін, бағдарлама саясаты сипаттарындағы **Оқиғаларды конфигурациялау** қойындысында хабарландыру параметрлерін және сақтау параметрлерін көрсетуге болады. Басқару сервері үшін, Басқару серверінің сипаттарындағы оқиғалар тізімін қосымша түрде қарап шығуға және конфигурациялауға болады. Барлық оқиғалар үшін хабарландыру параметрлерін бірден конфигурациялау қажет болса, Басқару сервері сипаттарында жалпы хабарландыру параметрлерін конфигурациялаңыз.

Оқиға түрінің көрсетілетін атауы	Оқиға түрі идентификаторы	Оқиға түрі	Сипаттамасы	Әдепкі бойынша сақтау мерзімі
Мобильдік құрылғыларға арналған басқару сервері сертификатының мерзімі аяқталды	6129	KLSRV_EV_SRV_CERT_EXPIRED_DN	Осы түрдегі оқиғалар мобильдік құрылғылар мен UEFI құрылғыларына арналған басқару сервері сертификаттарының жарамдылық мерзімі аяқталғанда туындайды. Сізге жарамдылық мерзімі бітейін деп жатқан сертификатты жаңарту керек.	180 күн
Аудит: SIEM серверіне экспорттау сәтсіз аяқталды	5130	KLAUD_EV_SIEM_EXPORT_ERROR	Осы түрдегі оқиғалар, SIEM жүйесіне оқиғаларды экспорттау SIEM жүйесіне қосылу қатесіне байланысты сәтсіз аяқталғанда орын алады.	180 күн
Құрылғы басқарылмайтын күйге айналды	4111	KLSRV_HOST_OUT_CONTROL	Осы түрдегі оқиғалар, басқарылатын құрылғы желіде көрініп тұрса да, Басқару сервері белгіленген кезең ішінде қосылмаған жағдайда туындайды. Құрылғыда Желілік агенттің дұрыс жұмыс істеуіне не кедергі келтіретінін анықтаңыз. Ықтимал себептеріне желі ақаулары және құрылғыдан Желілік агентті жою кіруі мүмкін.	180 күн
Құрылғының күйі: "Маңызды"	4113	KLSRV_HOST_STATUS_CRITICAL	Осы түрдегі оқиғалар, басқарылатын құрылғыға *Критикалық* күйі тағайындалса туындайды. Құрылғы күйі *Критикалық* болып өзгеретін шарттарды конфигурациялауға болады.	180 күн
Лицензияның қолданылу мерзімі жақында аяқталады	4129	KLSRV_EV_LICENSE_SRV_EXPIRE_SOON	Осы түрдегі оқиғалар, коммерциялық лицензияның жарамдылық мерзімінің аяқталу күні жақындаса туындайды. Күніне бір рет Kaspersky Security Center Linux бағдарламасы лицензияның лицензия мерзімінің өтпегенін тексеріп тұрады. Осы түрдегі оқиғалар 30 күн, 15 күн, 5 күн және 1 күн бұрын, лицензия мерзімі аяқталғанға дейін жарияланады. Бұл күндер санын өзгерту мүмкін емес. Басқару сервері лицензияның жарамдылық мерзімінің аяқталу күніне дейін көрсетілген күні өшірілсе, оқиға келесі күнге дейін жарияланбайды. Коммерциялық лицензияның мерзімі аяқталғаннан кейін, Kaspersky Security Center Linux бағдарламасы Базалық функционалдылық режимінде жұмыс істейді. Сіз оқиғаға келесі тәсілдермен жауап бере аласыз: • Резервттегі лицензиялық кілт Басқару серверіне қосылғанына көз жеткізіңіз. • Жазылымды қолдансаңыз, оның мерзімін ұзартыңыз. Провайдерге алғы төлем уақтылы төленген болса, шектелмеген жазылым автоматты түрде ұзартылады.	180 күн

Оқиға түрінің көрсетілетін атауы	Оқиға түрі идентификаторы	Оқиға түрі	Сипаттамасы	Әдепкі бойынша сақтау мерзімі
Лицензиялық шектеу асырылды	4099	KLSRV_EV_LICENSE_CHECK_MORE_110	Күніне бір рет Kaspersky Security Center Linux бағдарламасы лицензиялық шектеулердің асып кетпегенін тексеріп тұрады. Осы түрдегі оқиғалар, Басқару сервері клиент құрылғыларына орнатылған Kaspersky бағдарламаларының лицензиялық шектеуінің асып кеткенін тіркесе және бір лицензияның қолданылатын лицензиялық бірліктерінің саны лицензия қамтитын лицензиялық бірліктердің жалпы санының 110%-нан асса туындайды. Осы оқиға туындаса да, клиент құрылғылары қорғалған. Сіз оқиғаға келесі тәсілдермен жауап бере аласыз: • Басқарылатын құрылғылардың тізімін қарап шығыңыз. Қолданылмайтын құрылғыларды жойыңыз. • Көптеген құрылғыларға лицензия беріңіз (Басқару серверіне басқа жарамды белсендіру кодын немесе кілт файлын қосыңыз). Kaspersky Security Center Linux бағдарламасы, лицензиялық шектеуден асып кеткен жағдайда оқиғаларды жасау ережесін айқындайды.	180 күн
Шектелген функционалдылық режимі	4130	KLSRV_EV_LICENSE_SRV_LIMITED_MODE	Осы түрдегі оқиғалар, Kaspersky Security Center Linux бағдарламасы Ұялы құрылғыларды басқару және Осалдықтар мен патчтарды басқару мүмкіндігінің қолдауынсыз, базалық функционалдылық режимінде жұмыс істей бастаса туындайды. Төменде себептер және оқиғаға берілген тиісті жауаптар келтірілген: • Лицензия мерзімі өтті. Kaspersky Security Center Linux толық функционалдылығына лицензия беріңіз (Басқару серверіне белсендіру кодын немесе кілт файлын қосыңыз). • Басқару сервері ұсынылған лицензия бойынша қолданылуы мүмкін саннан көп құрылғылар санын басқарады. Құрылғыларды бір Сервердің басқару топтарының құрамынан басқа Сервердің басқа топтарына жылжытыңыз (басқа Сервердің лицензиялық шектеуі асып кетпесе).	180 күн
MDM сертификатының мерзімі аяқталды	4132	KLSRV_CERTIFICATE_EXPIRED	Бұл түрдегі оқиғалар мобильдік құрылғылардағы клиент сертификатының мерзімі аяқталғанда орын алады.	180 күн

Оқиға түрінің көрсетілетін атауы	Оқиға түрі идентификаторы	Оқиға түрі	Сипаттамасы	Әдепкі бойынша сақтау мерзімі
Кілт файлы қара тізімге қосылды	4124	KLSRV_LICENSE_BLACKLISTED	Осы түрдегі оқиғалар, Kaspersky бағдарламасы сіз қолданып жатқан белсендіру кодын немесе лицензиялық кілтті тыйым салынғандар тізіміне қосқан болса туындайды. Толығырақ ақпарат алу үшін Техникалық қолдау қызметіне жүгініңіз.	180 күн
Kaspersky бағдарламасының модульдеріне арналған жаңартулар қайтарылды	4142	KLSRV_SEAMLESS_UPDATE_REVOKED	Kaspersky техникалық қолдау қызметінің мамандары үзіліссіз жаңартуларды қайтарып алса (бұл жаңартулар үшін *Қайтарылған* күйі көрсетіледі); мысалы, оларды жаңа нұсқаға жаңарту қажет болса, осы түрдегі оқиғалар пайда болады. Оқиға Kaspersky Security Center Linux патчтарына қатысты емес және Kaspersky басқарылатын қолданба модульдеріне жатпайды. Оқиға жаңартулардың орнатылмауы себебін қамтиды.	180 күн
Вирустың тарауы	• 26 (Файл қауіптерінен қорғаныс құрамдасы үшін) • 27 (Пошта қауіптерінен қорғаныс құрамдасы үшін) • 28 (желілік экран үшін)	GNRL_EV_VIRUS_OUTBREAK	Осы түрдегі оқиғалар, бірнеше басқарылатын құрылғыда қысқа кезең ішінде анықталған зиянды нысандардың саны белгіленген шекті мәндерден асып кетсе туындайды. Сіз оқиғаға келесі тәсілдермен жауап бере аласыз: • Басқару серверінің сипаттарында шекті мәндерді конфигурациялаңыз. • Белсендірілетін аса қатаң саясатты жасаңыз немесе осы оқиға туындаған кезде іске қосылатын тапсырманы жасаңыз.	

Басқару серверінің функционалдық ақауы оқиғалары

Төмендегі кестеде маңыздылық деңгейі **Функционалдық ақау** Басқару серверінің оқиғалары берілген.

Бағдарлама жасай алатын әрбір оқиға үшін, бағдарлама саясаты сипаттарындағы **Оқиғаларды конфигурациялау** қойындысында хабарландыру параметрлерін және сақтау параметрлерін көрсетуге болады. Басқару сервері үшін, Басқару серверінің сипаттарындағы оқиғалар тізімін қосымша түрде қарап шығуға және конфигурациялауға болады. Барлық оқиғалар үшін хабарландыру параметрлерін бірден конфигурациялау қажет болса, Басқару сервері сипаттарында жалпы хабарландыру параметрлерін конфигурациялаңыз.

Оқиға түрінің көрсетілетін атауы	Оқиға түрі идентификаторы	Оқиға түрі	Сипаттамасы	Әдепкі бойынша сақтау мерзімі
Белгіленген қалтаға жаңартуларды көшіру мүмкін болмады	4123	KLSRV_UPD_REPL_FAIL	Бағдарламалық жасақтама жаңартулары ортақ қатынасы бар қалтаға (немесе қалталарға) көшірілсе, осы түрдегі оқиғалар туындайды. Сіз оқиғаға келесі тәсілдермен жауап бере аласыз: • Қалтаға (немесе қалталарға) қатынасу үшін пайдаланылатын пайдаланушы есептік жазбасының жазу құқығы бар-жоғын тексеріңіз. • Қалта(лар)ға арналған пайдаланушы аты және/немесе құпиясөз өзгергенін тексеріңіз. • Интернет қосылымын тексеріңіз, себебі бұл оқиғаның себебі болуы мүмкін. Деректқорлар мен бағдарламалық модульдерді жаңарту жөніндегі нұсқауларды орындаңыз.	180 күн
Бұлттық сегментте сауалнаманы орындау мүмкін болмады	4143	KLSRV_KLCLOUD_SCAN_ERROR	Осы түрдегі оқиғалар, Басқару сервері бұлтты ортадағы желі сегментінде сауалнама өткізе алмаған жағдайда туындайды. Оқиғаның сипаттамасындағы ақпаратты оқып, оларға тиісінше ден қойыңыз.	Сақталмайды
Лицензиялы бағдарламалар топтарының біреуі үшін орнатулар санының шектеуі асырылды	4126	KLSRV_INVLICPROD_EXCEDED	Басқару сервері осындай түрдегі оқиғаларды мерзімді түрде (сағат сайын) жасайды. Kaspersky Security Center Linux бағдарламасында үшінші тарап қолданбаларының лицензиялық кілттерін басқарсаңыз және орнату саны үшінші тарап қолданбасының лицензиялық кілтінде белгіленген шектен асып кетсе, осы түрдегі оқиғалар туындайды. Сіз оқиғаға келесі тәсілдермен жауап бере аласыз: • Басқарылатын құрылғылардың тізімін қарап шығыңыз. Үшінші тарап бағдарламасын, ол қолданылмайтын құрылғылардан жойыңыз. • Үшінші тарап лицензиясын көптеген құрылғыларға қолданыңыз. Лицензиялы қолданбалар топтарыныңының функционалдығы арқылы үшінші тарап қолданбаларының лицензиялық кілттерін басқара аласыз. Лицензиялы бағдарламалар тобына, сіз белгілеген өлшемшарттарға сай келетін үшінші тарап бағдарламалары кіреді.	180 күн

Оқиға түрінің көрсетілетін атауы	Оқиға түрі идентификаторы	Оқиға түрі	Сипаттамасы	Әдепкі бойынша сақтау мерзімі
Дискіде бос орын жоқ	4107	KLSRV_DISK_FULL	Бұл түрдегі оқиғалар, Басқару сервері орнатылған құрылғының қатты дискісінде диск кеңістігі таусылып бара жатқан жағдайда туындайды. Құрылғыдағы диск кеңістігін босатыңыз.	180 күн
Басқару серверінің дерекқорында бос орын жоқ	4110	KLSRV_DATABASE_FULL	Бұл түрдегі оқиғалар Басқару сервері дерекқорында бос орын болмаса пайда болады. Басқару серверінің дерекқоры толып кетсе және дерекқорға одан әрі жазу мүмкін болмаса, Басқару сервері жұмыс істемейді. Төменде, қолданылатын ДҚБЖ жүйесіне тәуелді оқиғаның туындау себептері және оқиғаға ден қоюдың тиісті тәсілдері келтірілген: • Басқару серверінің дерекқорында сақталатын оқиғалар санын шектеңіз. • Басқару сервері дерекқорында бағдарламаларды басқару құрамдасы жіберген оқиғалар өте көп. Басқару серверінің дерекқорында Бағдарламаларды басқару құрамдасының оқиғаларын сақтауға қатысты Kaspersky Endpoint Security саясатының параметрлерін өзгертуге болады. ДҚБЖ таңдау туралы ақпаратты қарап шығыңыз.	180 күн
Орындау уақытының қатесі	4125	KLSRV_RUNTIME_ERROR	Осы түрдегі оқиғалар белгісіз мәселелерден туындайды. Көбінесе бұл ДҚБЖ мәселелері, желімен байланысты мәселелер, сондай-ақ бағдарламалық және аппараттық жасақтамамен байланысты басқа да мәселелер. Оқиға туралы толық ақпаратты оның сипаттамасынан табуға болады.	180 күн
Ортақ қалта қолжетімсіз	4108	KLSRV_SHARED_FOLDER_UNAVAILABLE	Осы түрдегі оқиғалар, Басқару серверінің ортақ қатынасы бар қалтасы қолжетімді болмағанда туындайды. Сіз оқиғаға келесі тәсілдермен жауап бере аласыз: • Басқару серверінің (ортақ қатынасы бар қалта орналасқан) қосулы және қолжетімді екеніне көз жеткізіңіз. • Қалтаға арналған пайдаланушы аты және/немесе құпиясөз өзгертілгенін тексеріңіз. • Желі қосылымын тексеріңіз.	180 күн

Оқиға түрінің көрсетілетін атауы	Оқиға түрі идентификаторы	Оқиға түрі	Сипаттамасы	Әдепкі бойынша сақтау мерзімі
Басқару серверінің дерекқоры қолжетімсіз	4109	KLSRV_DATABASE_UNAVAILABLE	Осы түрдегі оқиғалар Басқару сервері дерекқоры қолжетімсіз болған жағдайда пайда болады. Сіз оқиғаға келесі тәсілдермен жауап бере аласыз: • ДҚБЖ орнатылған қашықтағы сервердің қолжетімді екенін тексеріңіз. • ДҚБЖ оқиғалар журналдарын қарап шығыңыз және Басқару сервері дерекқорының қолжетімсіздігінің себебін табыңыз.	180 күн

Басқару серверінің ескерту оқиғалары

Төмендегі кестеде **Ескерту** маңыздылық деңгейіндегі Басқару серверінің оқиғалары берілген.

Бағдарлама жасай алатын әрбір оқиға үшін, бағдарлама саясаты сипаттарындағы **Оқиғаларды конфигурациялау** қойындысында хабарландыру параметрлерін және сақтау параметрлерін көрсетуге болады. Басқару сервері үшін, Басқару серверінің сипаттарындағы оқиғалар тізімін қосымша түрде қарап шығуға және конфигурациялауға болады. Барлық оқиғалар үшін хабарландыру параметрлерін бірден конфигурациялау қажет болса, Басқару сервері сипаттарында жалпы хабарландыру параметрлерін конфигурациялаңыз.

Басқару серверінің ескерту оқиғалары

Оқиға түрінің көрсетілетін атауы	Оқиға түрі идентификаторы	Оқиға түрі	Сипаттамасы	Әдепкі бойынша сақтау мерзімі
Мобильдік құрылғыларға арналған басқару сервері сертификатының мерзімі аяқталуға жақын	6128	KLSRV_EV_SRV_CERT_EXPIRES_SOON	Осы түрдегі оқиғалар мобильдік құрылғылар мен UEFI құрылғыларына арналған басқару сервері сертификаттарының жарамдылық мерзімі аяқталғанда туындайды. Сізге жарамдылық мерзімі бітейін деп жатқан сертификатты жаңарту керек.	90 күн
APN сертификатының жарамдылық мерзімі жақында аяқталады	4136	KLSRV_APN_CERTIFICATE_EXPIRES_SOON	Егер APNs сертификатының жарамдылық мерзімінің аяқталуына дейін 14 күннен аз уақыт қалса, осы түрдегі оқиғалар орын алады. APNs сертификатының жарамдылық мерзімі аяқталғаннан кейін, қолмен APNs сертификатын жаңартып, оны iOS MDM серверіне орнату керек. APNs сертификатын жарамдылық мерзімі аяқталғанға дейін жаңартуды жоспарлау ұсынылады.	Сақталмайды

Оқиға түрінің көрсетілетін атауы	Оқиға түрі идентификаторы	Оқиға түрі	Сипаттамасы	Әдепкі бойынша сақтау мерзімі
APN сертификатының жарамдылық мерзімі аяқталды	4135	KLSRV_APN_CERTIFICATE_EXPIRED	Осы түрдегі оқиғалар, APNs сертификатының жарамдылық мерзімі бітейін деп жатқан кезде туындайды. Сізге қолмен APNs сертификатын жаңарту және оны iOS MDM серверіне орнату қажет.	Сақталмайды
Аудит: SIEM серверімен байланысты сынау сәтсіз аяқталды	5120	KLAUD_EV_SIEM_TEST_FAILED	Бұл түрдегі оқиғалар, SIEM серверіне қосылуды автоматты түрде тексеру сәтсіз аяқталғанда орын алады.	90 күн
Сертификат өшірілді	4134	KLSRV_CERTIFICATE_REMOVED	Егер әкімші Ұялы құрылғыларды басқару үшін кез келген түрдегі сертификатты (жалпы, пошталық, VPN) жойса, осы түрдегі оқиғалар туындайды. Сертификат жойылғаннан кейін, осы сертификатқа қосылған ұялы құрылғылар Басқару серверіне қосыла алмайды. Бұл оқиға Ұялы құрылғыларды басқаруға қатысты ақауларды зерттеуде пайдалы болуы мүмкін.	90 күн
Сертификат сұралды	4133	KLSRV_CERTIFICATE_REQUESTED	Ұялы құрылғыларды басқару үшін сертификатты автоматты түрде қайта шығару мүмкін болмаса, осы түрдегі оқиғалар туындайды. Төменде оқиғалардың ықтимал себептері және оқиғаға жауап беру бойынша тиісті әрекеттер берілген: • Автоматты түрде қайта шығару, **Мүмкін болса, сертификатты автоматты түрде қайта шығару** параметрі өшірілген сертификат үшін басталды. Бұл жағдай, сертификат жасау кезінде пайда болған қатеге байланысты болуы мүмкін. Сертификатты қолмен қайта шығару қажет болуы мүмкін. • Егер сіз жалпыға ортақ инфрақұрылымымен біріктіруді қолдансаңыз, оның себебі PKI-мен біріктіру және сертификат шығару үшін қолданылатын есептік жазбаның SAM-Account-Name атрибутының болмауына байланысты болуы мүмкін. Есептік жазба сипаттарын қарап шығыңыз.	90 күн

Оқиға түрінің көрсетілетін атауы	Оқиға түрі идентификаторы	Оқиға түрі	Сипаттамасы	Әдепкі бойынша сақтау мерзімі
Құрылғылар атауларының қайшылығы	4102	KLSRV_EVENT_HOSTS_CONFLICT	Осы түрдегі оқиғалар, егер Басқару сервері екі немесе одан да көп басқарылатын құрылғыны бір құрылғы ретінде қарастырған кезде туындайды. Көбінесе, клондалған қатты диск бағдарламаларды басқарылатын құрылғыларда орналастыру үшін және Желілік агентті эталонды құрылғыда бөлектелген дискіні клондау режиміне ауыстырып қоспай қолданылған кезде туындайды. Бұл мәселені болдырмау үшін, осы құрылғының қатты дискісін клондаудың алдында Желілік агентті эталонды құрылғыда дискіні клондау режиміне ауыстырып қосыңыз.	90 күн
Негізгі Басқару серверімен байланыс үзілді	4118	KLSRV_EV_MASTER_SRV_DISCONNECTED	Бұл түрдегі оқиғалар негізгі Басқару серверімен байланыс үзілген кезде пайда болады. Негізгі басқару сервері орнатылған құрылғыдағы операциялық жүйенің оқиғалар журналын оқып, соған сәйкес әрекет етіңіз.	90 күн
Қосалқы Басқару серверімен байланыс үзілді	4116	KLSRV_EV_SLAVE_SRV_DISCONNECTED	Бұл түрдегі оқиғалар қосалқы Басқару серверімен байланыс үзілген кезде пайда болады. Қосалқы басқару сервері орнатылған құрылғыдағы операциялық жүйенің оқиғалар журналын оқып, соған сәйкес әрекет етіңіз.	90 күн
Құрылғы желіде ұзақ уақыт бойы белсенді емес болып қалды	4103	KLSRV_EVENT_HOSTS_NOT_VISIBLE	Осы түрдегі оқиғалар, басқарылатын құрылғы бірнеше уақыт бойы белсенді емес болған кезде туындайды. Көбінесе, басқарылатын құрылғы істен шыққан жағдайда туындайды. Сіз оқиғаға келесі тәсілдермен жауап бере аласыз: • Құрылғыны басқарылатын құрылғылар тізімінен қолмен жойыңыз. Kaspersky Security Center Web Console көмегімен **Құрылғы желіде ұзақ уақыт бойы белсенді емес болып қалды** оқиғасы жасалатын уақыт аралығын көрсетіңіз. • Құрылғы Kaspersky Security Center Web Console веб-консолінің көмегімен автоматты түрде жойылатын уақыт аралығын көрсетіңіз.	90 күн

Оқиға түрінің көрсетілетін атауы	Оқиға түрі идентификаторы	Оқиға түрі	Сипаттамасы	Әдепкі бойынша сақтау мерзімі
Құрылғының күйі: "Ескерту"	4114	KLSRV_HOST_STATUS_WARNING	Осы түрдегі оқиғалар, басқарылатын құрылғыға *Ескерту* күйі тағайындалса туындайды. Құрылғы күйі *Ескерту* болып өзгеретін шарттарды конфигурациялай аласыз.	90 күн
Файлды құрылғыға жүктеп алу сәтсіз аяқталды	4165	KLSRV_FILE_DOWNLOAD_FAILED	Мұндай оқиғалар келесі жағдайларда орын алады: • Сіз файлды корпоративтік контейнерге жүктеуге тырысасыз, бірақ корпоративтік контейнер жасалмаған. • Құрылғыда орын жеткіліксіз. • Файл туралы ақпаратты серверден жүктеу мүмкін болмады. • Файл мазмұнын серверден жүктеу мүмкін болмады. • Қалтаны құрылғыда жасау мүмкін болмады. • Жеке құрылғыда файлға арнайы мүмкіндіктер рұқсаты жоқ. • Корпоративтік контейнерде файлға кіруге арнайы мүмкіндіктер рұқсаты жоқ.	90 күн
FCM хабарын FCM серверіне жіберу сәтсіз аяқталды	4140	KLSRV_GCM_GENERAL_ERROR	Бұл түрдегі оқиғалар Google Firebase Cloud Messaging атты HTTP протоколымен жұмыс істеу кезінде Басқару сервері жағындағы күтпеген қателерден туындайды. Оқиғаның сипаттамасындағы ақпаратты оқып, оларға тиісінше ден қойыңыз. Егер сіз мәселенің шешімін өзіңіз таба алмасаңыз, Kaspersky Техникалық қолдау қызметіне хабарласуды ұсынамыз.	90 күн

Оқиға түрінің көрсетілетін атауы	Оқиға түрі идентификаторы	Оқиға түрі	Сипаттамасы	Әдепкі бойынша сақтау мерзімі
Мобильдік құрылғыға FCM хабарын жіберу сәтсіз аяқталды	4138	KLSRV_GCM_DEVICE_ERROR	Бұл түрдегі оқиғалар Ұялы құрылғыларды басқару Android операциялық жүйесі бар басқарылатын ұялы құрылғыларға қосылу үшін Google Firebase Cloud Messaging (FCM) пайдалануға конфигурацияланған болса, ал FCM сервері Басқару серверінен алынған кейбір сұрауларды өңдей алмаса туындайды. Бұл дегеніміз, кейбір басқарылатын ұялы құрылғылар push хабарландыруын алмайды. Оқиғаның сипаттамасындағы HTTP кодын оқып, соған сәйкес жауап беріңіз. FCM серверінен алынған HTTP кодтары және олармен байланысты қателер туралы қосымша ақпарат Google Firebase қызметінің құжаттамасында бар ("Downstream message error response codes" тарауын қараңыз).	90 күн
Жиі болатын оқиғалар анықталды		KLSRV_EVENT_SPAM_EVENTS_DETECTED	Басқару сервері басқарылатын құрылғыда жиі болатын оқиғаларды тіркейтін болса, осы түрдегі оқиғалар орын алады. Қосымша ақпаратты келесі бөлімдерден қараңыз: Жиі оқиғаларды бұғаттау.	90 күн
Қатқыл диск толуға жақын	4105	KLSRV_NO_SPACE_ON_VOLUMES	Бұл түрдегі оқиғалар, Басқару сервері орнатылған құрылғыда диск кеңістігі таусылуға жақын қалған жағдайда туындайды. Құрылғыдағы диск кеңістігін босатыңыз.	90 күн

Оқиға түрінің көрсетілетін атауы	Оқиға түрі идентификаторы	Оқиға түрі	Сипаттамасы	Әдепкі бойынша сақтау мерзімі
FCM хабарын FCM серверіне жіберу кезінде HTTP қатесі пайда болды	4139	KLSRV_GCM_HTTP_ERROR	Бұл түрдегі оқиғалар Ұялы құрылғыларды басқару Android операциялық жүйесімен басқарылатын мобильді құрылғыларды қосу үшін Google Firebase Cloud Messaging (FCM) пайдалануға конфигурацияланған болса және FCM сервері 200 (OK) емес HTTP коды бар Басқару серверіне салынған сұрауды қайтарса туындайды. Төменде оқиғалардың ықтимал себептері және оқиғаға жауап беру бойынша тиісті әрекеттер берілген: • FCM серверінің жағындағы мәселелер. Оқиғаның сипаттамасындағы HTTP кодын оқып, соған сәйкес жауап беріңіз. FCM серверінен алынған HTTP кодтары және олармен байланысты қателер туралы қосымша ақпарат Google Firebase қызметінің құжаттамасында бар ("Downstream message error response codes" тарауын қараңыз). • Прокси-сервер жағындағы мәселелер (прокси-серверді қолдансаңыз). Оқиғаның сипаттамасындағы HTTP кодын оқып, соған сәйкес жауап беріңіз.	90 күн
Лицензиялық шектен асып кетті	4098	KLSRV_EV_LICENSE_CHECK_100_110	Күніне бір рет Kaspersky Security Center Linux қолданбасы лицензиялық шектеулердің асып кетпегенін тексеріп тұрады. Осы түрдегі оқиғалар, Басқару сервері клиент құрылғыларына орнатылған Kaspersky бағдарламаларының лицензиялық шектеуінің асып кеткенін тіркесе және бір лицензияның қолданылатын лицензиялық бірліктерінің саны лицензия қамтитын бірліктердің жалпы саны 100%-дан 110%-ға дейін құраса туындайды. Осы оқиға туындаса да, клиент құрылғылары қорғалған. Сіз оқиғаға келесі тәсілдермен жауап бере аласыз: • Басқарылатын құрылғылардың тізімін қарап шығыңыз. Қолданылмайтын құрылғыларды жойыңыз. • Көптеген құрылғыларға лицензия беріңіз (Басқару серверіне басқа жарамды белсендіру кодын немесе кілт файлын қосыңыз). Kaspersky Security Center Linux бағдарламасы, лицензиялық шектеуден асып кеткен жағдайда оқиғаларды жасау ережесін айқындайды.	90 күн

Оқиға түрінің көрсетілетін атауы	Оқиға түрі идентификаторы	Оқиға түрі	Сипаттамасы	Әдепкі бойынша сақтау мерзімі
Лицензиялы қолданбалар топтарының біреуі жақында орнату санының шегіне жетеді	4128	KLSRV_INVLICPROD_EXPIRED_SOON	Осы түрдегі оқиғалар лицензияланған қолданбалар тобына кіретін үшінші тарап қолданбаларына арналған лицензиялық кілттердің біреуінің мерзімі аяқталуға жақын болғанда орын алады. Сол себепті топтардың бірі үшін орнату шегі азайтылады. Сіз оқиғаға келесі тәсілдермен жауап бере аласыз: • Егер үшінші тарап бағдарламасы басқарылатын құрылғыларда қолданылмаса, бағдарламаны сол құрылғылардан жойыңыз. • Жақын арада үшінші тарап бағдарламасына арналған орнату саны рұқсат етілген шектен асады деп күтсеңіз, көптеген құрылғыларға үшінші тарап бағдарламасының лицензиясын алу мүмкіндігін алдын ала қарастырыңыз. Лицензиялы қолданбалар топтарыныңының функционалдығы арқылы үшінші тарап қолданбаларының лицензиялық кілттерін басқара аласыз.	90 күн
Kaspersky қолданбасы модульдерінің жаңа жаңартулары тіркелді	4141	KLSRV_SEAMLESS_UPDATE_REGISTERED	Бұл түрдегі оқиғалар, Басқару сервері, орнатуды мақұлдауды қажет ететін басқарылатын құрылғыларда орнатылған Kaspersky бағдарламаларының жаңа жаңартуларын тіркеген жағдайда орын алады. Kaspersky Security Center Web Console арқылы жаңартуларды растаңыз немесе қабылдамаңыз.	90 күн
Басқару серверінің дерекқорында бос орын жоқ	4106	KLSRV_NO_SPACE_IN_DATABASE	Бұл түрдегі оқиғалар Басқару сервері дерекқорында бос орын шектеулі болған жағдайда орын алады. Егер сіз бұл мәселені шешпесеңіз, көп ұзамай Басқару сервері дерекқоры өзінің сыйымдылығына жетеді және Басқару сервері жұмыс істемей қалады. Төменде, қолданылатын ДҚБЖ жүйесіне тәуелді оқиғаның туындау себептері және оқиғаға ден қоюдың тиісті тәсілдері келтірілген. • Басқару серверінің дерекқорында сақталатын оқиғалар санын шектемеңіз. • Басқару серверінің дерекқорында сақталатын оқиғалар тізімін қысқартыңыз. ДҚБЖ таңдау туралы ақпаратты қарап шығыңыз.	90 күн

Оқиға түрінің көрсетілетін атауы	Оқиға түрі идентификаторы	Оқиға түрі	Сипаттамасы	Әдепкі бойынша сақтау мерзімі
Дерекқордағы оқиғалар санының шегінен асып кетті, оқиғаларды жою басталды	4145	KLSRV_EVP_DB_TRUNCATING	Мұндай түрдегі оқиғалар, Басқару сервері дерекқорынан ескі оқиғаларды жою, Басқару сервері дерекқорында сақталатын оқиғалардың максималды санына жеткеннен кейін басталған жағдайда орын алады. Сіз оқиғаға келесі тәсілдермен жауап бере аласыз: • Басқару серверінің дерекқорында сақталатын оқиғалардың максималды санын көрсетіңіз. • Басқару серверінің дерекқорында сақталатын оқиғалар тізімін қысқартыңыз.	Сақталмайды
Дерекқордағы оқиғалар санының шегінен асып кетті, оқиғалар жойылды	4146	KLSRV_EVP_DB_TRUNCATED	Мұндай түрдегі оқиғалар, Басқару сервері дерекқорында сақталатын оқиғалардың максималды санына жеткеннен кейін Басқару сервері дерекқорынан ескі оқиғаларды жойылған жағдайда орын алады. Сіз оқиғаға келесі тәсілдермен жауап бере аласыз: • Басқару серверінің дерекқорында сақталатын оқиғалардың максималды рұқсат етілген санын көрсетіңіз. • Басқару серверінің дерекқорында сақталатын оқиғалар тізімін қысқартыңыз.	Сақталмайды

Басқару серверінің ақпараттық оқиғалары

Төмендегі кестеде **Ақпараттық** маңыздылық деңгейі бар Kaspersky Security Center Басқару серверінің оқиғалары келтірілген.

Бағдарлама жасай алатын әрбір оқиға үшін, бағдарлама саясаты сипаттарындағы **Оқиғаларды конфигурациялау** қойындысында хабарландыру параметрлерін және сақтау параметрлерін көрсетуге болады. Басқару сервері үшін, Басқару серверінің сипаттарындағы оқиғалар тізімін қосымша түрде қарап шығуға және конфигурациялауға болады. Барлық оқиғалар үшін хабарландыру параметрлерін бірден конфигурациялау қажет болса, Басқару сервері сипаттарында жалпы хабарландыру параметрлерін конфигурациялаңыз.

Басқару серверінің ақпараттық оқиғалары

Оқиға түрінің көрсетілетін атауы	Оқиға түрі идентификаторы	Оқиға түрі	Сипаттамасы	Әдепкі бойынша сақтау мерзімі
Мобильдік құрылғыларға арналған басқару сервері сертификаты жаңартылып жатыр	6127	KLSRV_EV_SRV_CERT_RENEWED	Бұл оқиға басқару серверінің сертификаты жаңартылған кезде орын алады.	30 күн
Аудит: пәрмен құрылғыға жіберілді	4170	KLAUD_EV_COMMAND_SENT	Осы типтегі оқиғалар пайдаланушы мобильді құрылғыға пәрмен жіберген кезде орын алады.	30 күн

Оқиға түрінің көрсетілетін атауы	Оқиға түрі идентификаторы	Оқиға түрі	Сипаттамасы	Әдепкі бойынша сақтау мерзімі
Аудит: басқару серверіне қосылу тоқтатылды	4151	KLAUD_EV_SERVERDISCONNECT		30 күн
Аудит: басқару серверіне қосылым орнатылды	4147	KLAUD_EV_SERVERCONNECT	Бұл түрдегі оқиғалар пайдаланушы басқару серверіне Kaspersky Security Center Web Console арқылы қосылғанда орын алады. Бұл оқиғалар Kaspersky Security Center Web Console Server орнатылған құрылғының IP мекенжайын қамтиды.	30 күн
Аудит: шифрлау кілттері импортталды/ экспортталды	5100	KLAUD_EV_DPEKEYSEXPORT	Мысалы, бұл оқиға деректерді тасымалдау кезінде орын алады.	30 күн
Аудит: топ параметрлері өзгертілді	4149	KLAUD_EV_ADMGROUP_CHANGED	Осы түрдегі оқиғалар қауіпсіздік тобы өзгерген кезде орын алады.	30 күн
Аудит: нысан өзгертілді	4148	KLAUD_EV_OBJECTMODIFY	Бұл оқиға келесі нысандардағы өзгерістерді қадағалайды: • Басқару тобы • Қауіпсіздік тобы • Пайдаланушы • Орнату пакеттері • Тапсырма • Саясат • Сервер • Виртуалды сервер	30 күн
Аудит: нысан сипаттары өзгертілді	4152	KLAUD_EV_OBJECTPROPMODIFIED	Бұл оқиға келесі параметрлердегі өзгерістерді қадағалайды: • Пайдаланушы • Лицензия • Сервер • Виртуалды сервер	30 күн
Аудит: нысан күйі өзгертілді	4150	KLAUD_EV_TASK_STATE_CHANGED	Мысалы, тапсырма қатемен аяқталса, бұл оқиға туындайды.	30 күн
Аудит: SIEM серверімен байланысты сынау сәтті аяқталды	5110	KLAUD_EV_SIEM_TEST_SUCCESS	Бұл оқиға SIEM серверінің қосылымы сәтті орнатылған кезде пайда болады.	30 күн
Аудит: пайдаланушы рұқсаттары өзгертілді	4153	KLAUD_EV_OBJECTACLMODIFIED	Бұл оқиға пайдаланушы рұқсаттары өзгертілген кезде орын алады	30 күн
Негізгі Басқару серверімен байланыс орнатылды	4117	KLSRV_EV_MASTER_SRV_CONNECTED		30 күн

Оқиға түрінің көрсетілетін атауы	Оқиға түрі идентификаторы	Оқиға түрі	Сипаттамасы	Әдепкі бойынша сақтау мерзімі
Қосалқы Басқару серверімен байланыс орнатылды	4115	KLSRV_EV_SLAVE_SRV_CONNECTED	Қосымша мәліметтер алу үшін Басқару серверлерінің иерархиясын жасау: қосалқы басқару серверін қосу мақаласын қараңыз.	30 күн
Дерекқорлар жаңартылды	4144	KLSRV_UPD_BASES_UPDATED	Осы түрдегі оқиғалар **Жаңартуларды Басқару серверінің қоймасына жүктеп алу** дерекқорды жаңартуды аяқтаған кезде орын алады.	30 күн
Құрылғы топқа автоматты түрде қосылды	4101	KLSRV_EVENT_HOSTS_NEW_REDIRECTED	Бұл түрдегі оқиғалар құрылғыларды жылжыту ережелеріне сәйкес құрылғылар топқа тағайындалғанда орын алады.	30 күн
Құрылғы ережеге сәйкес автоматты түрде жылжытылды	1074	KLSRV_HOST_MOVED_WITH_RULE_EX	Құрылғылар құрылғыларды жылжыту ережелері көмегімен басқару топтарына жылжытылса, осы түрдегі оқиғалар пайда болады.	30 күн
Құрылғы топтан өшірілді: желіде ұзақ уақыт бойы белсенді емес	4104	KLSRV_INVISIBLE_HOSTS_REMOVED	Бұл түрдегі оқиғалар, құрылғылар әрекетсіздікке байланысты топтан автоматты түрде жойылған кезде орын алады.	30 күн
Осы мобильдік құрылғыда FCM данасының идентификаторы өзгертілді	4137	KLSRV_GCM_DEVICE_REGID_CHANGED	Оқиғаның бұл түрі құрылғыдағы Firebase Cloud Messaging токені өзгерген кезде орын алады. FCM токендерінің ротациясы туралы ақпаратты Firebase сервисінің құжаттамасынан қараңыз.	30 күн
Файл Басқару серверінен жойылды	4163	KLSRV_FILE_REMOVED	Бұл оқиға файл басқару серверінен жойылған кезде орын алады.	30 күн
Файл құрылғыға жүктеп алынды	4164	KLSRV_FILE_DOWNLOADED	Бұл оқиға келесі жағдайларда орын алады: • Файл сеанс кезінде құрылғыға жүктеп алынды. • Файл басқару серверінен жүктеп алынды.	30 күн
Kaspersky-ге талдауға жіберетін файлдар табылды	4131	KLSRV_APS_FILE_APPEARED		30 күн
Файл Басқару серверіне жүктеп салынды	4162	KLSRV_FILE_UPLOADED	Бұл оқиға файл басқару серверіне жүктеп салынған кезде орын алады.	30 күн

Оқиға түрінің көрсетілетін атауы	Оқиға түрі идентификаторы	Оқиға түрі	Сипаттамасы	Әдепкі бойынша сақтау мерзімі
Лицензиялы бағдарламалар топтарының біреуі үшін рұқсат етілген орнатулардың саны (90%-дан) асты	4127	KLSRV_INVLICPROD_FILLED	Лицензиялық қолданбалар тобына кіретін үшінші тарап қолданбаларын орнату саны лицензиялық кілт сипаттарында көрсетілген максималды рұқсат етілген мәннің 90%-ына жетсе, осы түрдегі оқиғалар туындайды. Сіз оқиғаға келесі тәсілдермен жауап бере аласыз: • Егер үшінші тарап бағдарламасы басқарылатын құрылғыларда қолданылмаса, бағдарламаны сол құрылғылардан жойыңыз. • Жақын арада үшінші тарап бағдарламасына арналған орнату саны рұқсат етілген шектен асады деп күтсеңіз, көптеген құрылғыларға үшінші тарап бағдарламасының лицензиясын алу мүмкіндігін алдын ала қарастырыңыз. Лицензиялы қолданбалар топтарыныңының функционалдығы арқылы үшінші тарап қолданбаларының лицензиялық кілттерін басқара аласыз.	30 күн
Жаңа құрылғы анықталды	4100	KLSRV_EVENT_HOSTS_NEW_DETECTED	Бұл түрдегі оқиғалар жаңа желілік құрылғылар табылған кезде орын алады.	30 күн
Лицензиялық кілттің 90%-дан көп бөлігі қолданылып қойған	4097	KLSRV_EV_LICENSE_CHECK_90	Осы түрдегі оқиғалар, Басқару сервері клиент құрылғыларына орнатылған Kaspersky бағдарламаларының лицензиялық шектеуінің асып кеткенін тіркесе және бір лицензияның қолданылатын лицензиялық бірліктерінің саны лицензия қамтитын лицензиялық бірліктердің жалпы санының 90%-нан асса туындайды. Лицензия шектеулері асып кетсе де, клиент құрылғылары қорғалады. Сіз оқиғаға келесі тәсілдермен жауап бере аласыз: • Басқарылатын құрылғылардың тізімін қарап шығыңыз. Қолданылмайтын құрылғыларды жойыңыз. • Көптеген құрылғыларға лицензия беріңіз (Басқару серверіне басқа жарамды белсендіру кодын немесе кілт файлын қосыңыз). Kaspersky Security Center Linux бағдарламасы, лицензиялық шектеуден асып кеткен жағдайда оқиғаларды жасау ережесін айқындайды.	30 күн

Оқиға түрінің көрсетілетін атауы	Оқиға түрі идентификаторы	Оқиға түрі	Сипаттамасы	Әдепкі бойынша сақтау мерзімі
Мобильдік құрылғыларға арналған басқару серверінің резервтік сертификаты жасалды	6126	KLSRV_EV_SRV_CERT_RESERVE_CREATED	Бұл оқиға басқару серверінің сертификаты жасалған кезде орын алады.	30 күн
Жаңартулар белгіленген қалтаға сәтті көшірілді	4122	KLSRV_UPD_REPL_OK	Осы түрдегі оқиғалар Жаңартуларды Басқару серверінің қоймасына жүктеп алу файлдарды көрсетілген қалтаға көшіруді аяқтаған кезде туындайды.	30 күн

Резервтік сертификат жасалды және **Сертификат мерзімін ұзарту** оқиғаларына сәйкес келетін операциялар мобильдік құрылғылар мен UEFI құрылғыларына арналған басқару серверінің сертификаттары үшін орындалғанда ғана, осы оқиғалар басқару сервері арқылы автоматты түрде жарияланады және басқару консолінде көрсетіледі.

Желілік агент оқиғалары

Бұл бөлімде Желілік агент оқиғалары туралы ақпарат бар.

Желілік агенттің функционалдық ақауы оқиғалары

Төмендегі кестеде **Функционалдық ақау** маңыздылық деңгейі бар Kaspersky Security Center Linux Басқару серверінің оқиғалары келтірілген.

Бағдарлама жасай алатын әрбір оқиға үшін, бағдарлама саясаты сипаттарындағы **Оқиғаларды конфигурациялау** қойындысында хабарландыру параметрлерін және сақтау параметрлерін көрсетуге болады. Барлық оқиғалар үшін хабарландыру параметрлерін бірден конфигурациялау қажет болса, Басқару сервері сипаттарында жалпы хабарландыру параметрлерін конфигурациялаңыз.

Желілік агенттің функционалдық ақауы оқиғалары

Оқиға түрінің көрсетілетін атауы	Оқиға түрі идентификаторы	Оқиға түрі	Сипаттамасы	Әдепкі бойынша сақтау мерзімі
Түбірлік сертификаттарды орнату сәтсіз аяқталды	7728	KLNAG_EV_ROOT_CERT_INSTALL_ERR	Оқиға сертификаттарды орнату қатесінің сипаттамасын қамтиды.	30 күн
Үшінші тарап бағдарламалық жасақтамасы жаңартуын орнату сәтсіз болды	7697	KLNAG_EV_3P_PATCH_INSTALL_ERROR	Осындай түрдегі оқиғалар, Осалдықтар мен патчтарды басқару мүмкіндіктері қолданылып жатса және үшінші тарап өндірушілерінің бағдарламалық жасақтамасын жаңарту сәтсіз аяқталған болса туындайды. Үшінші тарап бағдарламасына келтірілген сілтеменің дұрыс екенін тексеріңіз. Оқиғаның сипаттамасын оқыңыз.	30 күн

Оқиға түрінің көрсетілетін атауы	Оқиға түрі идентификаторы	Оқиға түрі	Сипаттамасы	Әдепкі бойынша сақтау мерзімі
Windows Update жаңартуларын орнату сәтсіз аяқталды	7717	KLNAG_EV_WUA_INSTALL_ERROR	Осындай түрдегі оқиғалар, егер Windows Update жаңартулары сәтсіз аяқталған болса туындайды. Оқиғаның сипаттамасын оқыңыз. Microsoft білім қорындағы қатенің сипаттамасын іздеп көріңіз. Егер сіз мәселені өзіңіз шеше алмасаңыз, Microsoft техникалық қолдау қызметіне хабарласыңыз.	30 күн
Түбірлік сертификаттарды өшіру сәтсіз аяқталды	7730	KLNAG_EV_ROOT_CERT_REMOVE_ERR	Оқиға сертификаттарды жою қатесінің сипаттамасын қамтиды.	30 күн
Sudoers файлын сілтемелік мәнге қалпына келтіру сәтсіз аяқталды	7726	KLNAG_EV_SUDOER_RESTORED_ERR	Оқиға sudoers файлын ауыстыру қатесінің сипаттамасын қамтиды.	30 күн
Жаңартуды орнату қатесі	7702	KLNAG_EV_PATCH_INSTALL_ERROR	Осындай түрдегі оқиғалар, Kaspersky Security Center Linux құрамдастары үшін жаңартулар мен патчтарды автоматты түрде орнату сәтсіз аяқталған кезде туындайды. Оқиға, Kaspersky басқарылатын бағдарламаларының жаңартуларына жатпайды. Оқиғаның сипаттамасын оқыңыз. Бұл оқиғаның себебі, Басқару серверіндегі Windows операциялық жүйесінің мәселесі болуы мүмкін. Егер сипаттамада Windows конфигурациясының қандай да бір мәселесі туралы айтылса, бұл мәселені шешіңіз.	30 күн
Пайдаланушыларды басқару: қателер	7723	KLNAG_EV_USR_MNG_ERR	Жалпы ескерту оқиғасы.	30 күн

Желілік агенттің ескертулері оқиғалары

Төмендегі кестеде **Ескерту** маңыздылық деңгейі бар желілік агент оқиғалары келтірілген.

Бағдарлама жасай алатын әрбір оқиға үшін, бағдарлама саясаты сипаттарындағы **Оқиғаларды конфигурациялау** қойындысында хабарландыру параметрлерін және сақтау параметрлерін көрсетуге болады. Барлық оқиғалар үшін хабарландыру параметрлерін бірден конфигурациялау қажет болса, Басқару сервері сипаттарында жалпы хабарландыру параметрлерін конфигурациялаңыз.

Желілік агенттің ескертулері оқиғалары

Оқиға түрінің көрсетілетін атауы	Оқиға түрі идентификаторы	Оқиға түрі	Сипаттамасы	Әдепкі бойынша сақтау мерзімі
KSN проксиі іске қосылды. KSN қолжетімділігін тексеру сәтсіз аяқталды	7718	KSNPROXY_STARTED_CON_CHK_FAILED	Бұл түрдегі оқиғалар конфигурацияланған KSN прокси-сервері үшін сынақ қосылымы сәтсіз болғанда орын алады.	30 күн
Қауіпсіздік мәселесі пайда болды	549	GNRL_EV_APP_INCIDENT_OCCURED	Бұл түрдегі оқиғалар құрылғыда оқыс оқиға анықталған кезде орын алады. Мысалы, бұл оқиға құрылғыдағы дискіде кеңістік аз болған кезде орын алады.	30 күн

Оқиға түрінің көрсетілетін атауы	Оқиға түрі идентификаторы	Оқиға түрі	Сипаттамасы	Әдепкі бойынша сақтау мерзімі
Табылған sudoers файлы сілтемелік мәнге сәйкес келмейді	7724	KLNAG_EV_SUDOER_DIFFERENT	Бұл түрдегі оқиғалар sudoers файлы мен анықтамалық файл арасында сәйкессіздік болған кезде орын алады.	30 күн
Үшінші тарап бағдарламалық жасақтаманың жаңартуын орнату кейінге қалдырылды	7698	KLNAG_EV_3P_PATCH_INSTALL_SLIPPED	Мысалы, бұл оқиға түрі үшінші тарап бағдарламаларының жаңартуларын орнатуға арналған Лицензиялық келісім қабылданбаған кезде орын алады.	30 күн
Үшінші тарап бағдарламалық жасақтаманың жаңартуын орнату ескертумен аяқталды	7696	KLNAG_EV_3P_PATCH_INSTALL_WARNING	Трассирлеу файлдарын жүктеп алыңыз және KLRI_PATCH_RES_DESC өрісінің мәнін тексеріңіз.	30 күн
Пайдаланушыларды басқару: ескертулер	7722	KLNAG_EV_USR_MNG_WRN	Жалпы ескерту оқиғасы.	30 күн
Бағдарламалық модуль жаңартуын орнату кезінде ескерту пайда болды	7701	KLNAG_EV_PATCH_INSTALL_WARNING	Трассирлеу файлдарын жүктеп алыңыз және KLRI_PATCH_RES_DESC өрісінің мәнін тексеріңіз.	30 күн

Желілік агенттің ақпараттық оқиғалары

Төмендегі кестеде **Ақпараттық** маңыздылық деңгейі бар желілік агент оқиғалары көрсетілген.

Бағдарлама жасай алатын әрбір оқиға үшін, бағдарлама саясаты сипаттарындағы **Оқиғаларды конфигурациялау** қойындысында хабарландыру параметрлерін және сақтау параметрлерін көрсетуге болады. Барлық оқиғалар үшін хабарландыру параметрлерін бірден конфигурациялау қажет болса, Басқару сервері сипаттарында жалпы хабарландыру параметрлерін конфигурациялаңыз.

Желілік агенттің ақпараттық оқиғалары

Оқиға түрінің көрсетілетін атауы	Оқиға түрі идентификаторы	Оқиға түрі	Әдепкі бойынша сақтау мерзімі
Бағдарлама орнатылды	7703	KLNAG_EV_INV_APP_INSTALLED	30 күн
Бағдарлама жойылды	7704	KLNAG_EV_INV_APP_UNINSTALLED	30 күн
Сертификат HTTPS Web Server-інің портына алынды	—	WEB_SERVER_CERTIFICATE_RENEWED	30 күн
Құрылғы авторизацияланды	7711	KLNAG_EV_NAC_HOST_AUTHORIZED	30 күн
Жаңа құрылғы анықталды	7710	KLNAG_EV_NAC_DEVICE_DISCOVERED	30 күн
Құрылғы жойылды	7709	KLNAG_EV_DEVICE_REMOVE	30 күн
Бағдарламалық модуль жаңартуын орнату басталды	7700	KLNAG_EV_PATCH_INSTALL_STARTING	30 күн
KSN проксиі іске қосылды. KSN қолжетімділігін тексеру сәтті аяқталды	7719	KSNPROXY_STARTED_CON_CHK_OK	30 күн
KSN проксиі тоқтатылды	7720	KSNPROXY_STOPPED	30 күн
Бақыланатын бағдарлама орнатылды	7705	KLNAG_EV_INV_OBS_APP_INSTALLED	30 күн
Бақыланатын бағдарлама жойылды	7706	KLNAG_EV_INV_OBS_APP_UNINSTALLED	30 күн
Жаңа құрылғы қосылды	7708	KLNAG_EV_DEVICE_ARRIVAL	30 күн
Түбірлік сертификаттар орнатылды	7727	KLNAG_EV_ROOT_CERT_INSTALLED	30 күн
Түбіртік сертификаттар жойылды	7729	KLNAG_EV_ROOT_CERT_REMOVED	30 күн

Оқиға түрінің көрсетілетін атауы	Оқиға түрі идентификаторы	Оқиға түрі	Әдепкі бойынша сақтау мерзімі
Sudoers файлы сілтемелік мәнге сәтті қалпына келтірілді	7725	KLNAG_EV_SUDOER_RESTORED	30 күн
Үшінші тарап бағдарламасы орнатылды	7707	KLNAG_EV_INV_CMPTR_APP_INSTALLED	30 күн
Үшінші тарап бағдарламалық жасақтамасының жаңартуы сәтті орнатылды	7694	KLNAG_EV_3P_PATCH_INSTALLED_SUCCESSFULLY	30 күн
Үшінші тарап бағдарламалық жасақтаманың жаңартуын орнату басталды	7695	KLNAG_EV_3P_PATCH_INSTALL_STARTING	30 күн
Бағдарламалық модульдерінің жаңартуы сәтті орнатылды	7699	KLNAG_EV_PATCH_INSTALLED_SUCCESSFULLY	30 күн
Пайдаланушыларды басқару: ақпарат	7721	KLNAG_EV_USR_MNG_INF	30 күн
Веб-сервер хостта іске қосылды	—	WEB_SERVER_STARTED	30 күн
Веб-сервер хостта тоқтатылды	—	WEB_SERVER_STOPPED	30 күн
Windows компьютерлік бөлісу қызметін пайдалану: бағдарлама іске қосылды	7714	KLUSRLOG_EV_PROCESS_LAUNCHED	30 күн
Windows компьютерлік бөлісу қызметін пайдалану: файл өзгертілді	7713	KLUSRLOG_EV_FILE_MODIFIED	30 күн
Windows компьютерлік бөлісу қызметін пайдалану: файл оқылды	7712	KLUSRLOG_EV_FILE_READ	30 күн
Windows компьютерлік бөлісу қызметін пайдалану: басталды	7715	KLUSRLOG_EV_WDS_BEGIN	30 күн
Windows компьютерлік бөлісу қызметін пайдалану: тоқтатылды	7716	KLUSRLOG_EV_WDS_END	30 күн

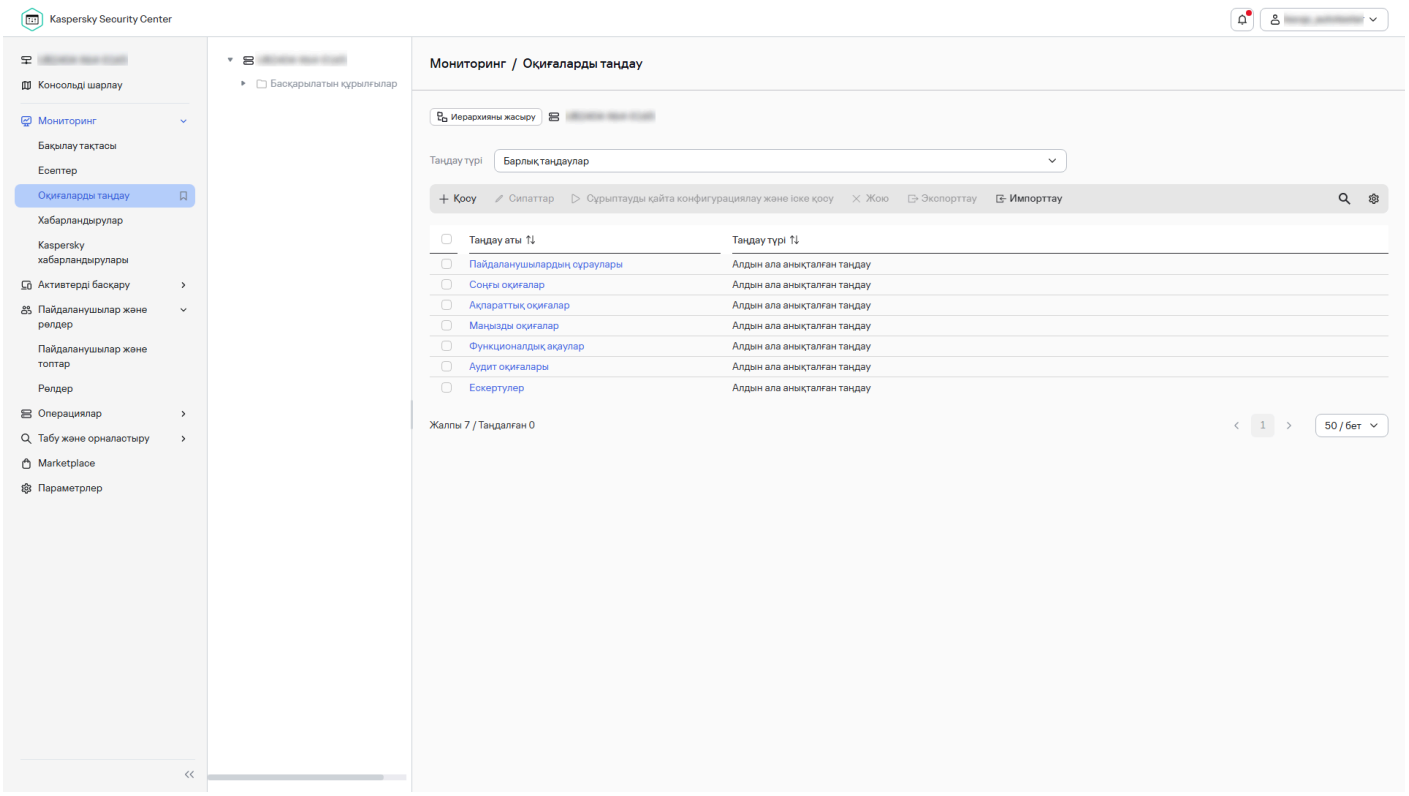
Оқиға таңдауларын пайдалану

Оқиғаларды таңдау, экранда Басқару серверінің дерекқорынан таңдалған аталған оқиғалар жиынтығын көруге арналған. Осы оқиға түрлері келесі санаттар бойынша топтастырылған:

- Маңыздылық деңгейі: **Маңызды оқиғалар**, **Функционалдық ақаулар**, **Ескертулер** және **Ақпараттық оқиғалар**.
- Уақыт: **Соңғы оқиғалар**.
- Түрі: **Пайдаланушылардың сұраулары** және **Аудит оқиғалары**.

Kaspersky Security Center Web Console интерфейсінде конфигурациялауға қолжетімді параметрлер негізінде пайдаланушы тарапынан айқындалған оқиғалар таңдауын жасай аласыз және көре аласыз.

Оқиғаларды таңдау Kaspersky Security Center Web Console бағдарламасының **Мониторинг → Оқиғаларды таңдау** бөлімінде қолжетімді.



Оқиғалар таңдауының тізімі

Әдепкі бойынша, оқиғаларды таңдау соңғы жеті күн ішіндегі ақпаратты қамтиды.

Kaspersky Security Center Linux бағдарламасында әдепкі бойынша таңдаулар жиынтығы бар (алдын ала анықталған):

- Маңыздылық деңгейі әртүрлі оқиғалар:
  - **Критикалық оқиғалар**
  - **Функционалдық ақау**
  - **Ескертулер**
  - **Ақпараттық оқиғалар**
- **Пайдаланушылардың сұраулары** (басқарылатын бағдарлама оқиғалары)
- **Соңғы оқиғалар** (соңғы апта ішінде)
- Аудит оқиғасы.

Сондай-ақ, сіз қосымша оқиғалардың пайдаланушы таңдауларын жасап, конфигурациялай аласыз. Пайдаланушының таңдауларында, сіз оқиғаларды туындаған құрылғылар сипаттары (құрылғылар атауы, IP ауқымдары және басқару топтары) бойынша, оқиғалар түрлері және маңыздылық деңгейлері бойынша, бағдарлама мен құрамдастың атауы бойынша, сондай-ақ уақыт аралығы бойынша сүзгілей аласыз. Сондай-ақ, тапсырма нәтижелерін іздеу аймағына қосуға болады. Сонымен қатар, сөзді немесе бірнеше сөзді енгізуге болатын іздеу өрісін де қолдануға болады. Кез келген енгізілген сөздерді олардың сипаттарының (оқиға атауы, сипаттама, құрамдас атауы сияқты) кез келген жерінде қамтитын барлық оқиғалар көрсетіледі.

Алдын ала анықталған таңдаулар үшін де, пайдаланушы таңдаулары үшін де, көрсетілетін оқиғалардың санын немесе ізделетін жазбалар санын шектеуге болады. Екі нұсқа да Kaspersky Security Center Linux оқиғаларды көрсететін уақытқа әсер етеді. Дерекқор неғұрлым үлкен болса, процесс соғұрлым көп уақытты қажет етеді.

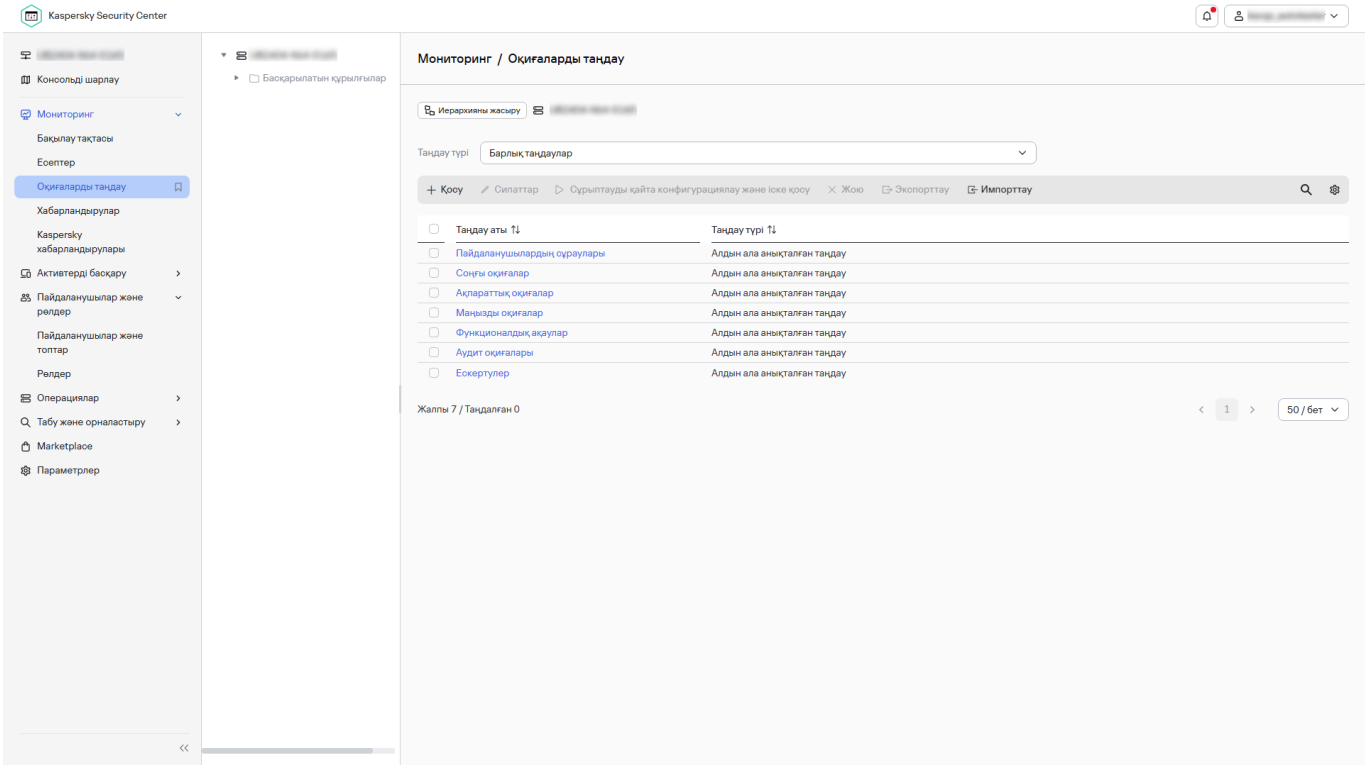
Сіз келесіні орындай аласыз:

- Оқиғаны таңдау параметрлерін өзгерту.
- Оқиғалар таңдауын жасау.
- Таңдалған оқиғалар таңдауы туралы мәліметті көру.
- Оқиғалар таңдауын жою.
- Басқару сервері дерекқорынан оқиғаларды жою.

Оқиғалар таңдауын жасау

Оқиғалар таңдауын жасау үшін:

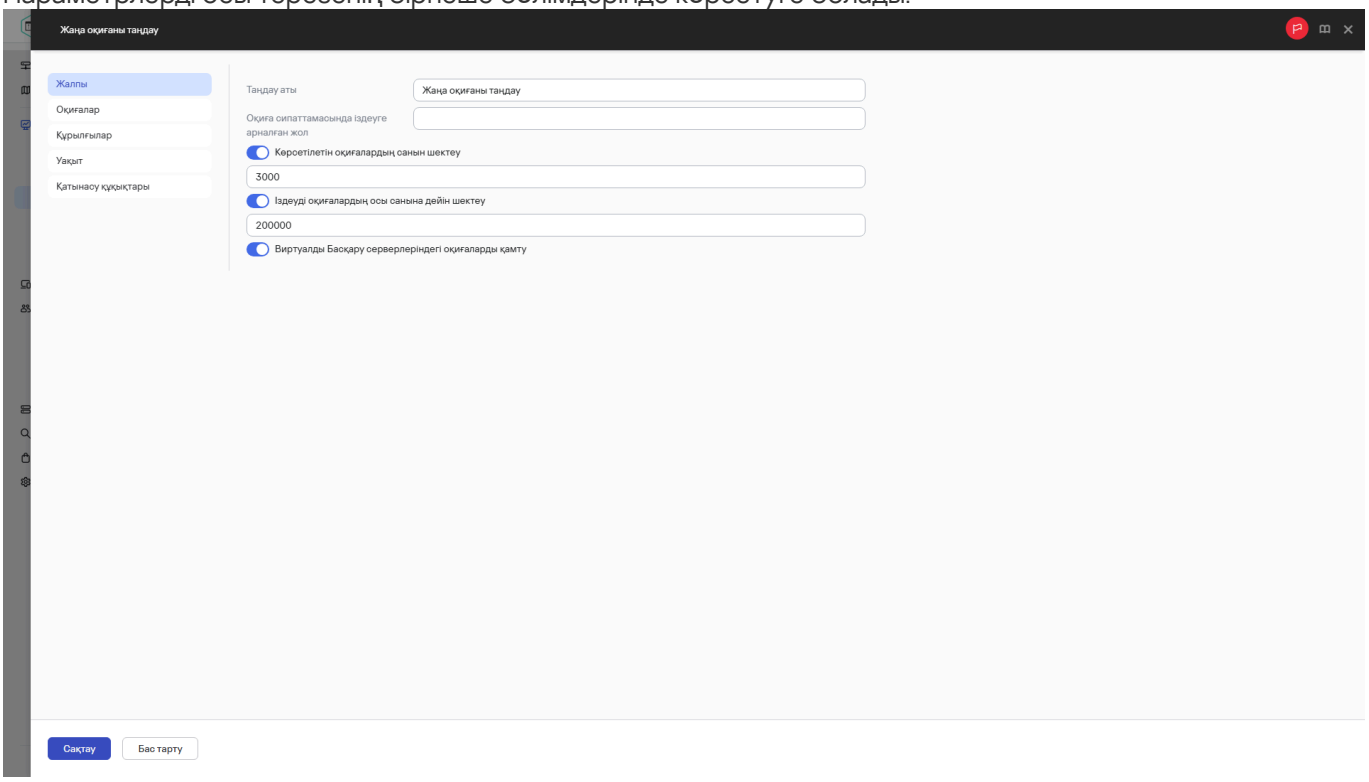
1. Бағдарламаның негізгі терезесінде **Мониторинг** → **Оқиғаларды таңдау** бөліміне өтіңіз.



Оқиғалар таңдауының тізімі

2. **Қосу** түймесін басыңыз.

3. Ашылған **Жаңа оқиғаны таңдау** терезесінде жаңа оқиғалар таңдауы параметрлерін көрсетіңіз. Параметрлерді осы терезенің бірнеше бөлімдерінде көрсетуге болады.



Жаңа оқиға таңдауын жасау

4. Өзгерістерін сақтау үшін **Сақтау** түймесін басыңыз.

   Растау терезесі ашылады.

5. Оқиғаларды таңдаудың нәтижелерін қарау үшін **Таңдау нәтижесіне өту** жалаушасын қойыңыз.

6. Оқиғалар таңдауын жасауды растау үшін **Сақтау** түймесін басыңыз.

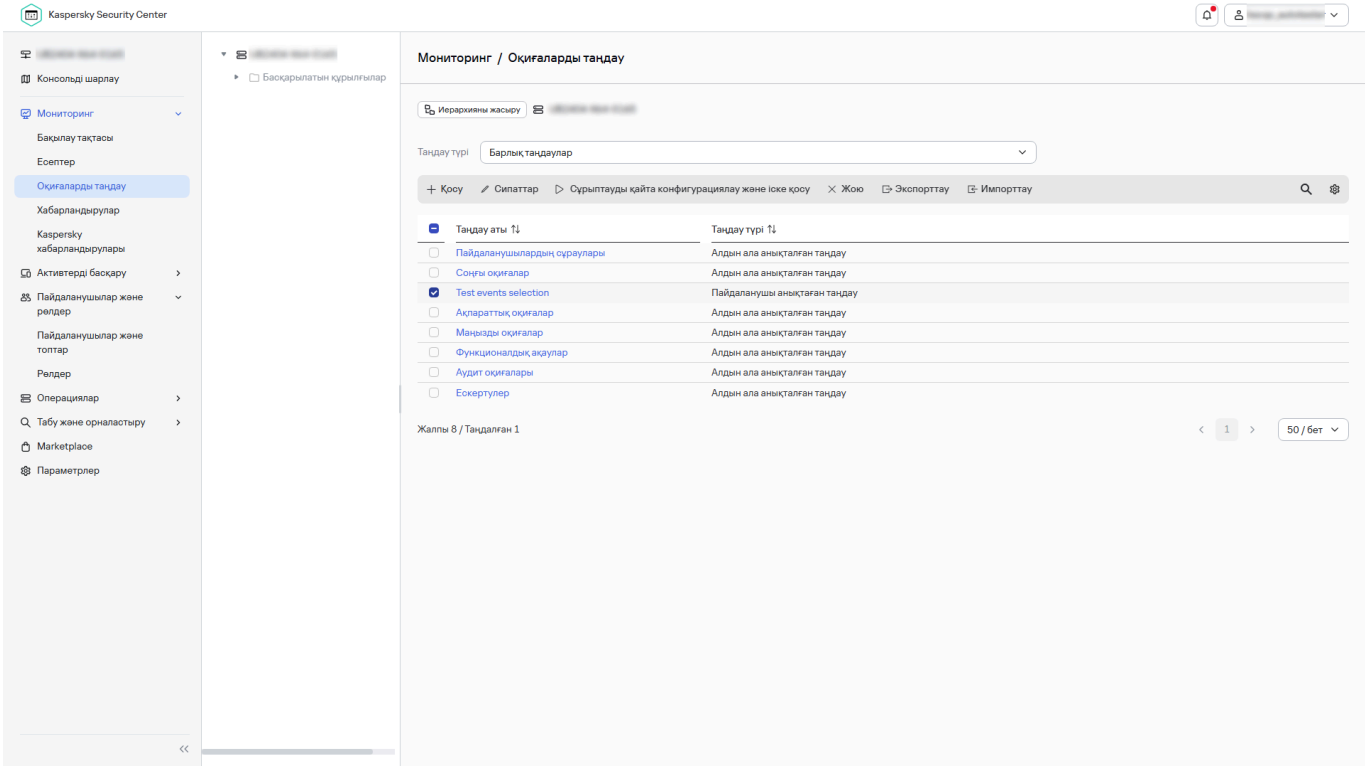
Таңдау нәтижесіне өту жалаушасы қойылған болса, оқиғалар таңдауы нәтижесі экранда көрсетіледі. Әйтпесе, жаңа оқиғалар таңдауы оқиғалар таңдауы тізімінде пайда болады.

Оқиғалар таңдауын өзгерту

Оқиғалар таңдауын өзгерту үшін:

1. Бағдарламаның негізгі терезесінде **Мониторинг** → **Оқиғаларды таңдау** бөліміне өтіңіз.

2. Өзгертуді қажет ететін оқиғалар таңдауына қарама-қарсы жалаушаны қойыңыз.



Оқиғалар таңдауының тізімі

3. **Сипаттар** түймесін басыңыз.

   Оқиғалар таңдауы сипаттары терезесі ашылады.

4. Оқиғалар таңдауы сипаттарын өңдеңіз.

   Алдын ала анықталған оқиғалар таңдауы үшін сипаттарды тек келесі қойыншаларда өңдеуге болады: **Жалпы** (таңдау атауын қоспағанда), **Уақыт** және **Қатынасу құқықтары**.

   Пайдаланушы таңдаулары үшін барлық сипаттарды өңдеуге болады.

5. Өзгерістерін сақтау үшін **Сақтау** түймесін басыңыз.

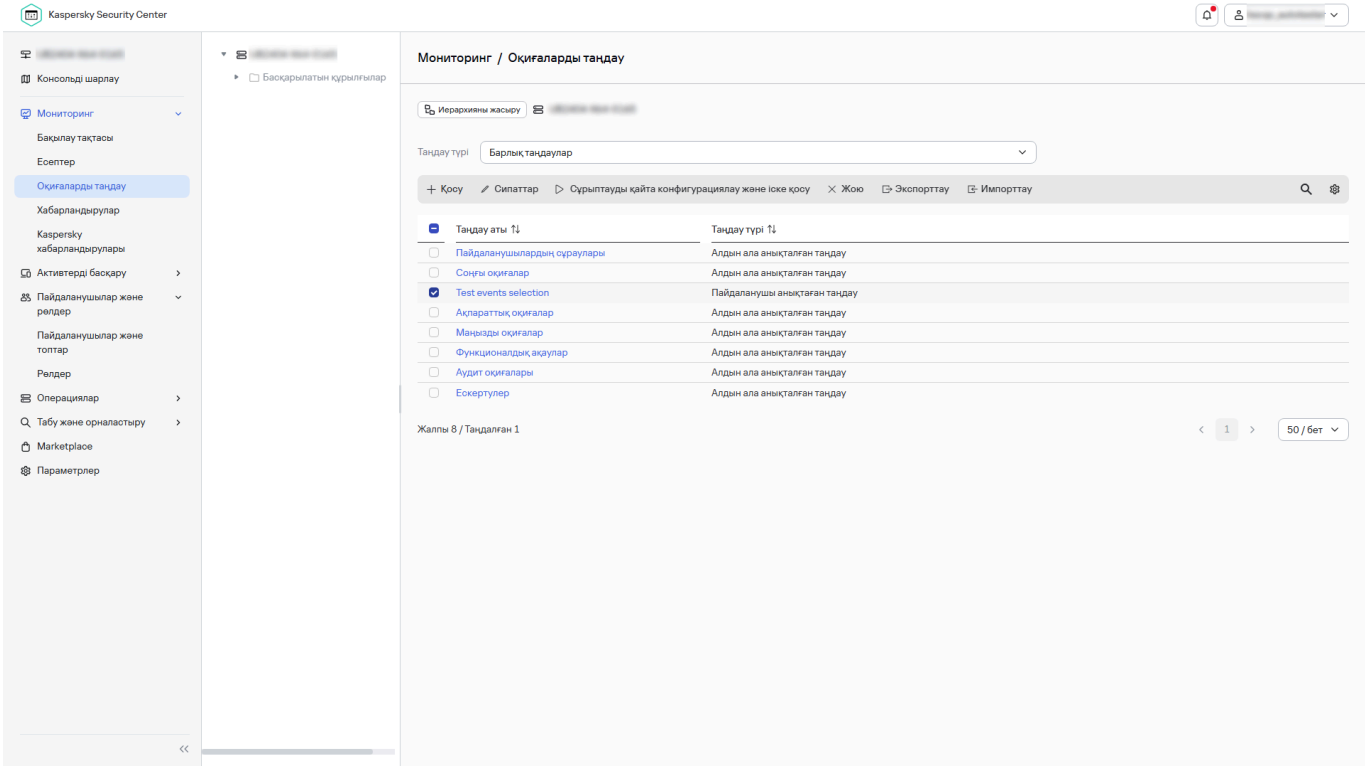
Өзгертілген оқиғалар таңдауы тізімде көрсетіледі.

Оқиғалар таңдауы тізімін қарау

Оқиғалар таңдауын қарап шығу:

1. Бағдарламаның негізгі терезесінде **Мониторинг** → **Оқиғаларды таңдау** бөліміне өтіңіз.

2. Іске қосу қажет оқиғалар таңдауына қарама-қарсы жалаушаны қойыңыз.



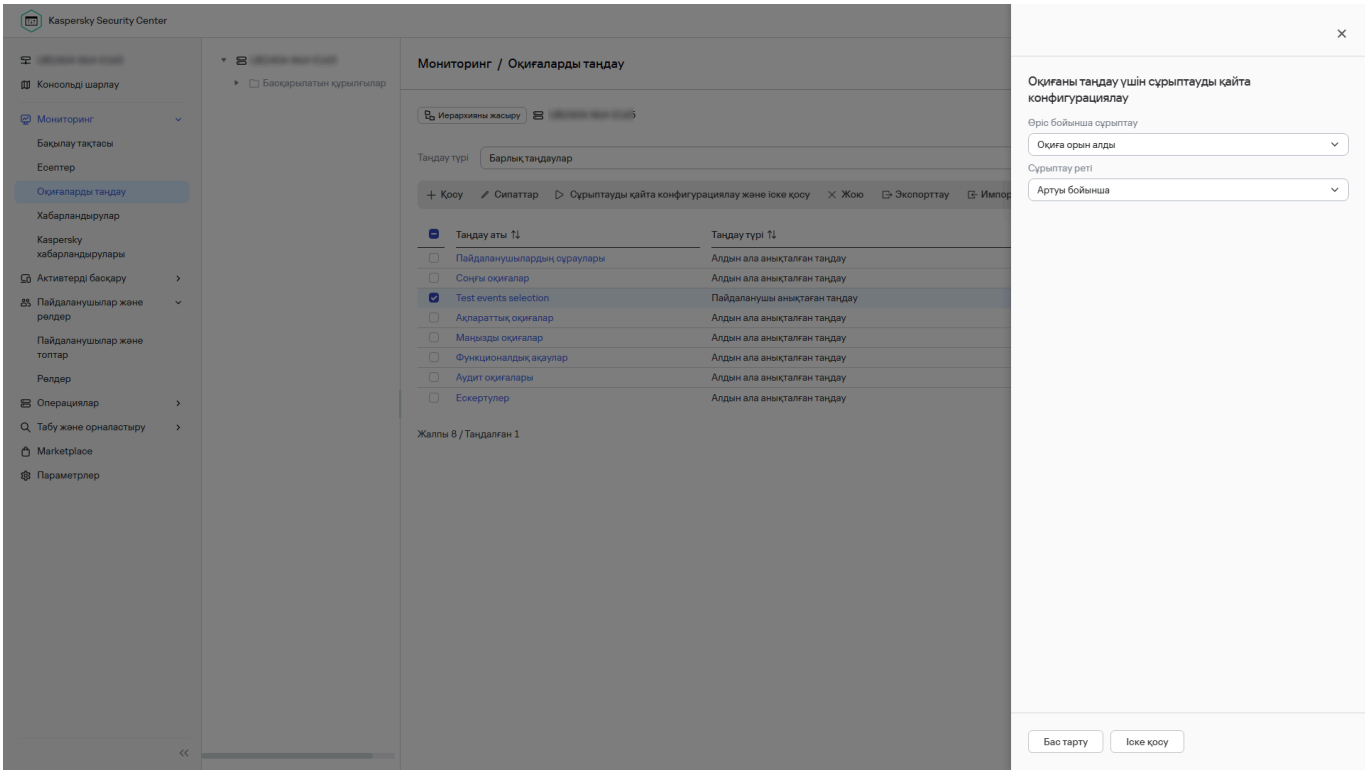
Оқиғалар таңдауының тізімі

3. Келесі әрекеттердің бірін орындаңыз:

- Оқиғалар таңдауы нәтижелері үшін сұрыптауды конфигурациялау үшін:

  a. **Сұрыптауды қайта конфигурациялау және іске қосу** түймесін басыңыз.

  b. Пайда болған **Оқиғаны таңдау үшін сұрыптауды қайта конфигурациялау** терезесінде сұрыптау параметрлерін көрсетіңіз.

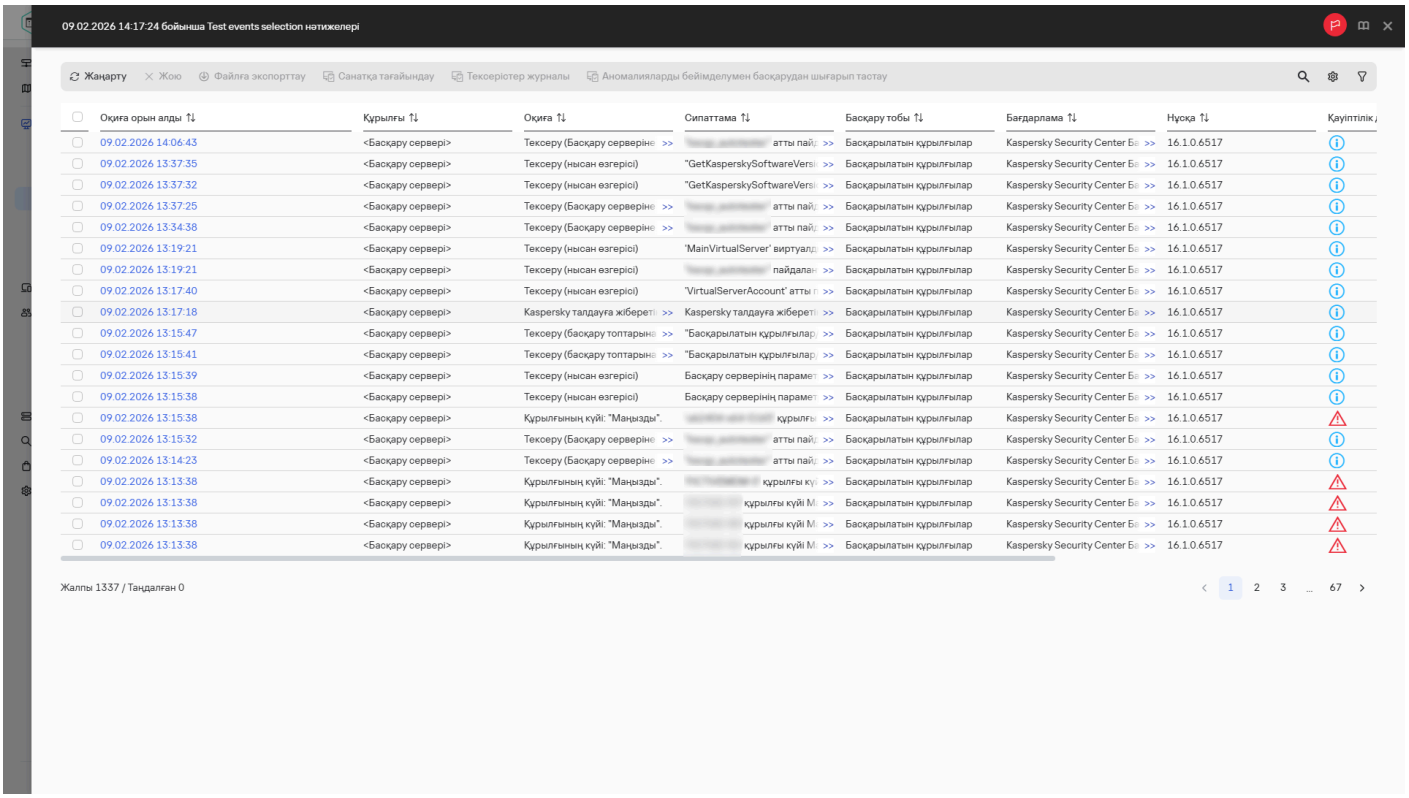


Оқиға таңдауының сұрыптау параметрлерін көрсету

  a. Таңдаудың атауын басыңыз.

- Әйтпесе, оқиғалар тізімін Басқару серверінде сақталғандай етіп көргіңіз келсе, таңдаудың атауын басыңыз.

Оқиғалар таңдауы нәтижесі көрсетіледі.



Оқиғалар таңдауы нәтижесі

Оқиғалар таңдауын экспорттау

Kaspersky Security Center Linux бағдарламасы оқиғалар таңдауын және оның параметрлерін KLO файлына сақтауға мүмкіндік береді. Сақталған оқиға таңдауын Kaspersky Security Center Windows, сондай-ақ Kaspersky Security Center Linux жүйелеріне импорттау үшін KLO файлын пайдалануға болады.

Пайдаланушы анықтаған оқиға таңдауларының кейбіреуін ғана жоюға болатынын ескеріңіз. Kaspersky Security Center Linux жүйесінде әдепкі бойынша орнатылған оқиға таңдауларының жиынын (алдын ала анықталған таңдаулар) файлға сақтау мүмкін емес.

Оқиғалар таңдауын экспорттау үшін:

1. Қолданбаның негізгі терезесінде **Мониторинг → Оқиғаларды таңдау** бөліміне өтіңіз.
2. Экспорттау қажет оқиғалар таңдауына қарама-қарсы жалаушаны белгілеңіз.

   Бірнеше оқиға таңдауын бір уақытта экспорттау мүмкін емес. Бірнеше таңдауды таңдасаңыз, **Экспорттау** түймесі өшірулі болады.
3. **Экспорттау** түймесін басыңыз.
4. Ашылған **Басқаша сақтау** терезесінде оқиғалар таңдауы файлының атын және жолын көрсетіңіз, содан кейін **Сақтау** түймесін басыңыз.

   Басқаша сақтау терезесі Google Chrome, Microsoft Edge немесе Opera қолдансаңыз ғана көрсетіледі. Басқа браузерді қолдансаңыз, оқиғалар таңдауының файлы **Жүктеп алынғандар** қалтасына автоматты түрде сақталады.

Оқиғалар таңдауын импорттау

Kaspersky Security Center Linux жүйесі оқиғалар таңдауын KLO файлынан импорттауға мүмкіндік береді. KLO файлы экспортталған оқиғалар таңдауын және оның параметрлерін қамтиды.

Оқиғалар таңдауын импорттау үшін:

1. Қолданбаның негізгі терезесінде **Мониторинг** → **Оқиғаларды таңдау** бөліміне өтіңіз.
2. Импорттағыңыз келетін оқиғалар таңдауы файлын таңдау үшін **Импорттау** түймесін басыңыз.
3. Ашылған терезеде KLO саясаты файлына апаратын жолды көрсетіңіз және **Ашу** түймесін басыңыз. Назар аударыңыз: оқиғалар таңдауының тек бір файлын таңдауға болады.

   Оқиғалар таңдауын өңдеу басталады.

Импорт нәтижелері бар хабарландыру пайда болады. Оқиғалар таңдауы импортталса, таңдау сипаттарын көру үшін **Импорттау мәліметтерін көру** сілтемесін басуға болады.

Сәтті импорттаудан кейін оқиғалар таңдауы таңдау тізімінде пайда болады. Оқиғалар таңдауының параметрлері де импортталады.

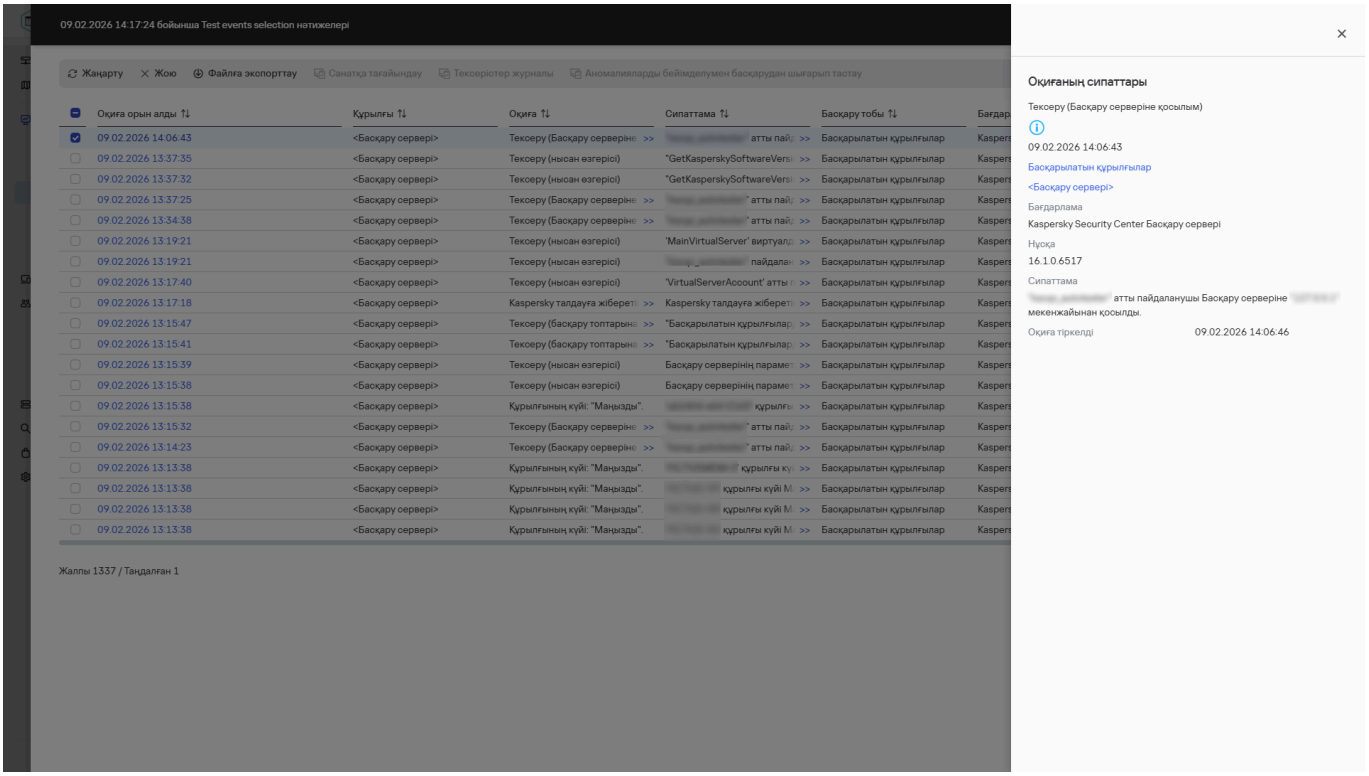
Импортталған жаңа оқиғалар таңдауының атауы бұрыннан бар таңдау атауымен бірдей болса, импортталған таңдау атауы түр **(<реттік нөмір>)**, мысалы: **(1)**, **(2)** жалғауы көмегімен кеңейтіледі.

Оқиға туралы ақпаратты көру

Оқиға туралы ақпаратты көру үшін:

1. Оқиғалар таңдауын іске қосыңыз.
2. Қажетті оқиғаға басыңыз.

Оқиғаның сипаттары терезесі ашылады.



Оқиға сипаттары терезесі

3. Ашылған терезеде келесі әрекеттерді орындауға болады:

   - Таңдалған оқиғаның ақпаратын қарау.
   - Оқиға туындаған құрылғыға өту.
   - Оқиға туындаған құрылғыны қамтитын басқару тобына өту.
   - Тапсырмамен байланысты оқиға үшін тапсырманың сипаттарына өтіңіз.

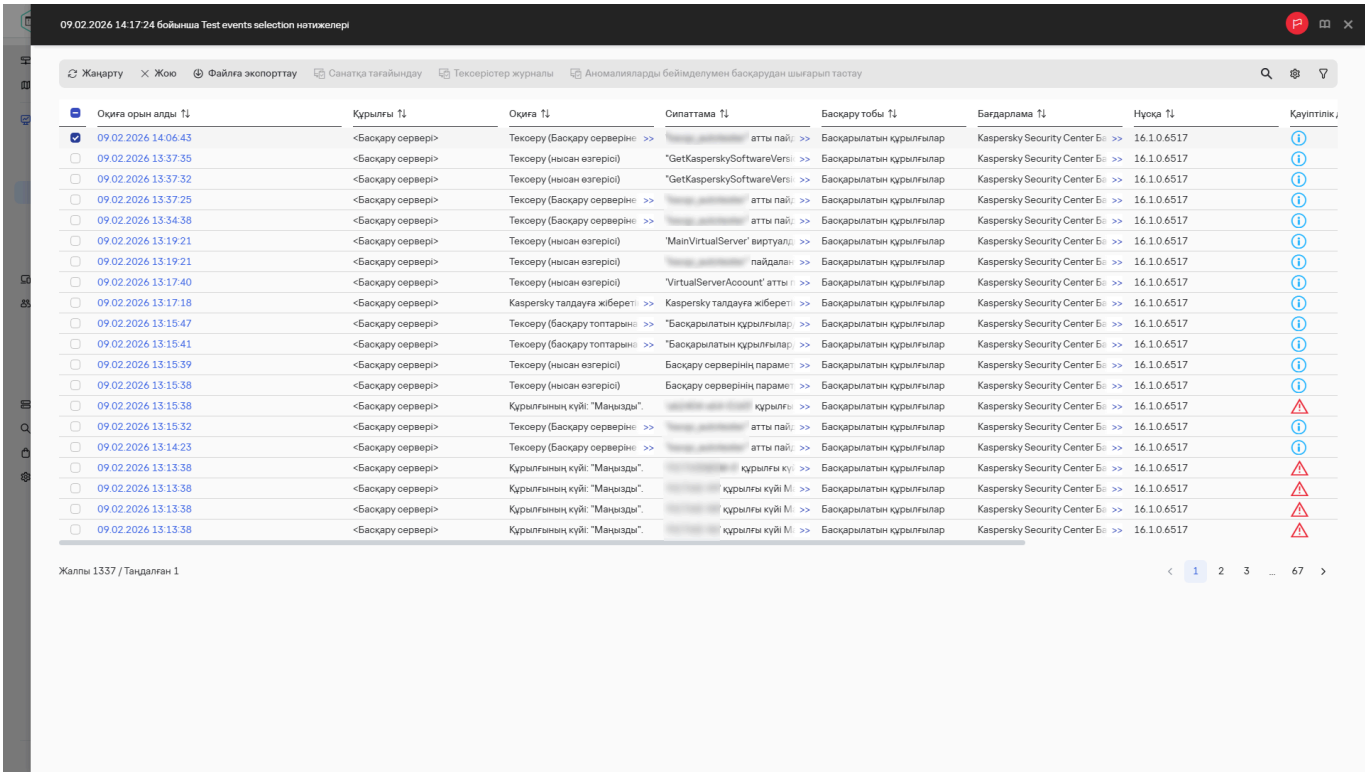
Оқиғаларды файлға экспорттау

Kaspersky Security Center Linux оқиғаларды оқиға таңдауынан TXT файлына сақтауға мүмкіндік береді.

Оқиғаларды файлға экспорттау үшін:

1. Оқиғалар таңдауын іске қосыңыз.
2. Қажетті оқиғаның жанындағы жалаушаны қойыңыз.

Сондай-ақ бірнеше оқиғаны немесе бүкіл оқиғаны таңдауға болады.



Оқиғалар таңдауы нәтижесі

3. **Файлға экспорттау** түймесін басыңыз.

Таңдалған оқиға TXT файлына экспортталады.

Оқиғадан нысан тарихын қарау

Тексеруді басқаруды қолдайтын нысанды жасау оқиғасынан немесе өзгерту оқиғасынан нысанды тексеру тарихына өтуге болады.

Оқиғадан нысанның тарихын көру үшін:

1. Оқиғалар таңдауын іске қосыңыз.
2. Қажетті оқиғаның жанындағы жалаушаны қойыңыз.
3. **Тексерістер журналы** түймесін басыңыз.

Нысанды тексеру тарихы ашылады.

Оқиғаларды жою

Оқиғаларды оқиғалар таңдаудан жою үшін:

1. Оқиғалар таңдауын іске қосыңыз.
2. Келесі оқиғаларды таңдаңыз:
   - Егер сіз бір немесе бірнеше оқиғаны жойғыңыз келсе, оның жанындағы құсбелгілерді қойыңыз.
   - Егер сіз ағымдағы беттегі барлық оқиғаларды жойғыңыз келсе, оқиғалар тізімінің үстіндегі құсбелгіні қойып, **Ағымдағы беттегінің барлығын таңдау** опциясын басыңыз.
   - Егер сіз таңдаудан барлық оқиғаларды жойғыңыз келсе, оқиғалар тізімінің үстіндегі құсбелгіні қойып, **Барлығын таңдау** опциясын басыңыз.
3. **Жою** түймесін басыңыз.
4. Пайда болған терезеде **Жою** түймесін басыңыз.

Құрылғылар оқиғалары тізімінен оқиғаларды жою үшін:

1. Құрылғылар тізімін ашыңыз.
   - Басқарылатын құрылғылар үшін: **Активтерді басқару** → **Активтер (құрылғылар)**.
   - Тағайындалмаған құрылғылар үшін: **Активтерді басқару** → **Тағайындалмаған құрылғылар**.
2. Құрылғылар тізімінде қажетті құрылғының атауы бар сілтемені басып, **Оқиғалар** қойындысына өтіңіз.
3. Келесі оқиғаларды таңдаңыз:
   - Егер сіз бір немесе бірнеше оқиғаны жойғыңыз келсе, оның жанындағы құсбелгілерді қойыңыз.
   - Егер сіз ағымдағы беттегі барлық оқиғаларды жойғыңыз келсе, оқиғалар тізімінің үстіндегі құсбелгіні қойып, **Ағымдағы беттегінің барлығын таңдау** опциясын басыңыз.
   - Егер сіз таңдаудан барлық оқиғаларды жойғыңыз келсе, оқиғалар тізімінің үстіндегі құсбелгіні қойып, **Барлығын таңдау** опциясын басыңыз.
4. **Жою** түймесін басып, әрекетті растаңыз.
5. Пайда болған терезеде **Жою** түймесін басыңыз.

Таңдалған оқиғалар жойылды және оларды қалпына келтіру мүмкін емес.

Оқиға таңдауларын жою

Пайдаланушылардың оқиғалар таңдауын ғана жоюға болады. Алдын ала анықталған оқиғалар таңдауын жоюға болмайды.

Оқиғалар таңдауын жою үшін:

1. Бағдарламаның негізгі терезесінде **Мониторинг** → **Оқиғаларды таңдау** бөліміне өтіңіз.
2. Жойғыңыз келетін оқиғалар таңдауына қарсы жалаушаларды қойыңыз.
3. **Жою** түймесін басыңыз.
4. Пайда болған терезеде **ОК** түймесін басыңыз.

Оқиғалар таңдауы жойылады.

Оқиғаны сақтау мерзімін конфигурациялау

Kaspersky Security Center Linux бағдарламасы, басқарылатын бағдарламаларға орнатылған Kaspersky Басқару сервері мен бағдарламаларының жұмысы барысында орын алған оқиғалар туралы ақпаратты алуға мүмкіндік береді. Оқиғалар туралы ақпарат Басқару серверінің дерекқорында сақталады. Кейбір оқиғаларды әдепкі бойынша көрсетілгеннен әлдеқайда ұзақ немесе қысқа мерзімде сақтау қажет болуы мүмкін. Оқиғаның әдепкі бойынша сақтау мерзімін өзгертуге болады.

Басқару сервері дерекқорында қандай да бір оқиғаларды сақтауға қызығушылық танытпасаңыз, Басқару сервері саясатында, Kaspersky бағдарламасы саясатында немесе Басқару сервері сипаттарында (тек Басқару сервері оқиғалары үшін) тиісті параметрді өшіре аласыз. Бұл дерекқордағы оқиғалар түрлерінің санын азайтады.

Оқиғаны сақтау мерзімі неғұрлым ұзақ болса, дерекқор максималды өлшемге соғұрлым тез жетеді. Алайда, оқиғаны барынша ұзақ сақтау мерзімі мониторинг тапсырмаларын орындауға және есептерді аса ұзақ кезең бойы қарауға мүмкіндік береді.

Басқару сервері дерекқорында оқиғаны сақтау мерзімін белгілеу үшін:

1. Бағдарламаның негізгі терезесінде **Активтерді басқару** → **Саясаттар** бөліміне өтіңіз.
2. Қажетті саясаттың атауын басыңыз.

   Басқарылатын Kaspersky қолданбасының, желілік агенттің немесе басқару серверінің саясатын таңдауға болады. Басқару сервері үшін басқару серверінің атауын басу арқылы оқиғалардың сақтау мерзімін де конфигурациялай аласыз.
3. **Оқиғаларды конфигурациялау** қойыншасын таңдаңыз.

   Байланысты оқиғалар тізімі бар **Маңызды** бөлімі көрсетіледі. Қажет болса, **Функционалдық ақау**, **Ескерту** немесе **Ақпараттық** бөліміне өтуге болады.

4. Оң жақ тақтадағы оқиғалар түрлерінің тізімінде сақтау мерзімін өзгерткіңіз келетін оқиға атауының сілтемесіне өтіңіз.

   Ашылған терезенің **Оқиғаларды тіркеу** бөлімінде **Басқару серверінің дерекқорында сақтау мерзімі (күндер)** ауыстырғыш түймесі қосылады.

5. Қосқыштың астындағы өңдеу өрісінде оқиғаны сақтау күндерінің санын көрсетіңіз.

6. Оқиғаны Басқару сервері дерекқорында сақтағыңыз келмесе, **Басқару серверінің дерекқорында сақтау мерзімі (күндер)** параметрін өшіріңіз.

   Басқару сервері оқиғаларын Басқару сервері сипаттары терезесінде конфигурацияласаңыз және оқиға параметрлері Басқару сервері саясатында бұғатталған болса, оқиғаны сақтау мерзімінің мәнін өзгерте алмайсыз.

7. **OK** түймесін басыңыз, содан кейін оң жақ тақта жабылғаннан кейін, **Сақтау** түймесін басыңыз.

   Саясат сипаттары терезесі жабылады.

Енді Басқару сервері таңдалған түрдегі оқиғаларды қабылдап, сақтаған кезде, олардың сақтау мерзімі өзгертіледі. Басқару сервері бұрын алынған оқиғаларды сақтау мерзімін өзгертпейді.

Жиі болатын оқиғаларды бұғаттау

Бұл бөлімде жиі болатын оқиғаларды бұғаттауды басқару және жиі болатын оқиғаларды бұғаттауды болдырмау туралы ақпарат берілген.

Жиі болатын оқиғаларды бұғаттау туралы

Бір немесе бірнеше басқарылатын құрылғыларда орнатылған Kaspersky Endpoint Security for Linux сияқты басқарылатын бағдарлама Басқару серверіне көптеген бір тіпті оқиғаларды жібере алады. Жиі болатын оқиғаларды қабылдау Басқару сервері дерекқорының шамадан тыс жүктелуіне және басқа оқиғалардың қайта жазылуына әкелуі мүмкін. Басқару сервері барлық алынған оқиғалар саны дерекқор үшін белгіленген шектен асқан кезде ең жиі болатын оқиғаларды бұғаттай бастайды.

Басқару сервері жиі болатын оқиғаларды автоматты түрде бұғаттайды. Сіз жиі болатын оқиғаларды өзіңіз бұғаттай алмайсыз немесе қандай оқиғаларды бұғаттауды таңдай алмайсыз.

Оқиғаның бұғатталғанын білу үшін, хабарландырулар тізімін көруге немесе бұл оқиғаның **Жиі болатын оқиғаларды бұғаттау** бөліміндегі Басқару сервері сипаттарында бар-жоғын көруге болады. Егер оқиға бұғатталған болса, келесі әрекеттерді орындауға болады:

- Дерекқордың қайта жазылуына жол бергіңіз келмесе, оқиғалардың осы түрін алуға тыйым салуды жалғастыра аласыз.
- Егер сіз, мысалы, жиі болатын оқиғаларды Басқару серверіне жіберудің себебін білгіңіз келсе, сіз жиі болатын оқиғалардың құлпын ашып, кез келген жағдайда оқиғалардың осы түрін алуды жалғастыра аласыз.
- Егер сіз жиі болатын оқиғаларды қайтадан бұғатталғанға дейін жалғастырғыңыз келсе, жиі болатын оқиғаларды бұғаттауды болдырмауға болады.

Жиі болатын оқиғаларды бұғаттауды басқару

Басқару сервері жиі болатын оқиғаларды алуды автоматты түрде бұғаттайды, бірақ сіз жиі болатын оқиғалардың құлпын ашып, оларды алуды жалғастыра аласыз. Сондай-ақ, бұрын құлпы ашылған жиі болатын оқиғаларды алуға тыйым салуға болады.

Жиі болатын оқиғады бұғаттуды басқару үшін:

1. Негізгі мәзірдегі басқару серверінің атауын басыңыз.

   Басқару серверінің сипаттары терезесі ашылады.

2. **Жалпы** қойыншасында **Жиі оқиғаларды бұғаттау** бөлімін таңдаңыз.

3. **Жиі оқиғаларды бұғаттау** бөлімінде:

   - Егер сіз жиі болатын оқиғалардың құлпын ашқыңыз келсе:

     a. Құлпын ашқыңыз келетін жиі болатын оқиғаларды таңдап, **Есептен шығару** түймесін басыңыз.

     b. **Сақтау** түймесін басыңыз.

   - Жиі болатын оқиғаларды қабылдауды бұғаттағыңыз келсе:

     a. Бұғаттағыңыз келетін жиі болатын оқиғаларды таңдап, **Құлыптау** түймесін басыңыз.

     b. **Сақтау** түймесін басыңыз.

Басқару сервері құлпы ашылған жиі болатын оқиғаларды қабылдайды және бұғатталған жиі болатын оқиғаларды қабылдамайды.

Жиі болатын оқиғады бұғаттауды болдырмау

Сіз жиі болатын оқиғаларды бұғаттаудан бас тарта аласыз және Басқару сервері осы жиі болатын оқиғаларды қайтадан бұғаттағанға дейін, оқиғаларды алуды бастай аласыз.

Жиі болатын оқиғаларды бұғаттауды болдырмау үшін:

1. Негізгі мәзірдегі басқару серверінің атауын басыңыз.

   Басқару серверінің сипаттары терезесі ашылады.

2. **Жалпы** қойыншасында **Жиі оқиғаларды бұғаттау** бөлімін таңдаңыз.

3. **Жиі болатын оқиғаларды бұғаттау** бөлімінде бұғаттуды болдырмағыңыз келетін жиі болатын оқиға жолын басыңыз.

4. **Бұғаттаудан шығару** түймесін басыңыз.

Жиі болатын оқиға жиі болатын оқиғалар тізімінен жойылады. Басқару сервері осы түрдегі оқиғаларды алып тұрады.

Басқару серверінде оқиғаларды өңдеу және сақтау

Қолданба мен басқарылатын құрылғылар жұмысы кезінде орын алатын оқиғалар туралы ақпарат басқару серверінің дерекқорына сақталады. Әрбір оқиға белгілі бір түрге және маңыздылық деңгейіне қатысты болып келеді (*Критикалық оқиға*, *Функционалдық ақау*, *Ескерту*, *Ақпараттық хабарлар*). Оқиға болған жағдайларға байланысты, бағдарлама бір типті оқиғаларға әртүрлі маңыздылық деңгейлерін бере алады.

Оқиғалардың түрлері мен маңыздылық деңгейлерін Басқару сервері сипаттары терезесінің **Оқиғаны конфигурациялау** бөлімінен көруге болады. **Оқиғаны конфигурациялау** бөлімінде сіз әрбір оқиғаны Басқару сервері тарапынан өңдеу параметрлерін де конфигурациялай аласыз:

- құрылғы мен Басқару серверіндегі операциялық жүйе оқиғалары журналдарында және Басқару серверінде оқиғаларды тіркеу;
- әкімшіні оқиға туралы хабарландыру тәсілі (мысалы, SMS, электрондық пошта хабарламасы).

Басқару сервері сипаттары терезесінің **Оқиғалар қоймасы** бөлімінде Басқару серверінің дерекқорында оқиғаларды сақтау параметрлерін конфигурациялауға болады: оқиғалар туралы жазбалар санын және жазбаларды сақтау уақытын шектеу. Оқиғалардың ең көп санын көрсеткенде, бағдарламалар оқиғалардың көрсетілген санын сақтау үшін диск кеңістігінің долбарлы өлшемін есептейді. Сіз бұл есептеуді дерекқордың толып кетуіне жол бермеу үшін бос диск кеңістігінің жеткілікті ме екенін бағалау үшін пайдалана аласыз. Әдепкі бойынша, Басқару сервері дерекқорының сыйымдылығы 400 000 оқиғаны құрайды. Дерекқордың ұсынылған ең жоғары сыйымдылығы 45 000 000 оқиғаны құрайды.

Бағдарлама дерекқорды 10 минут сайын тексереді. Оқиғалар саны көрсетілген максималды мәннен 10 000 артық болса, бағдарлама оқиғалардың көрсетілген ең көп саны ғана қалуы үшін ең ескі оқиғаларды жояды.

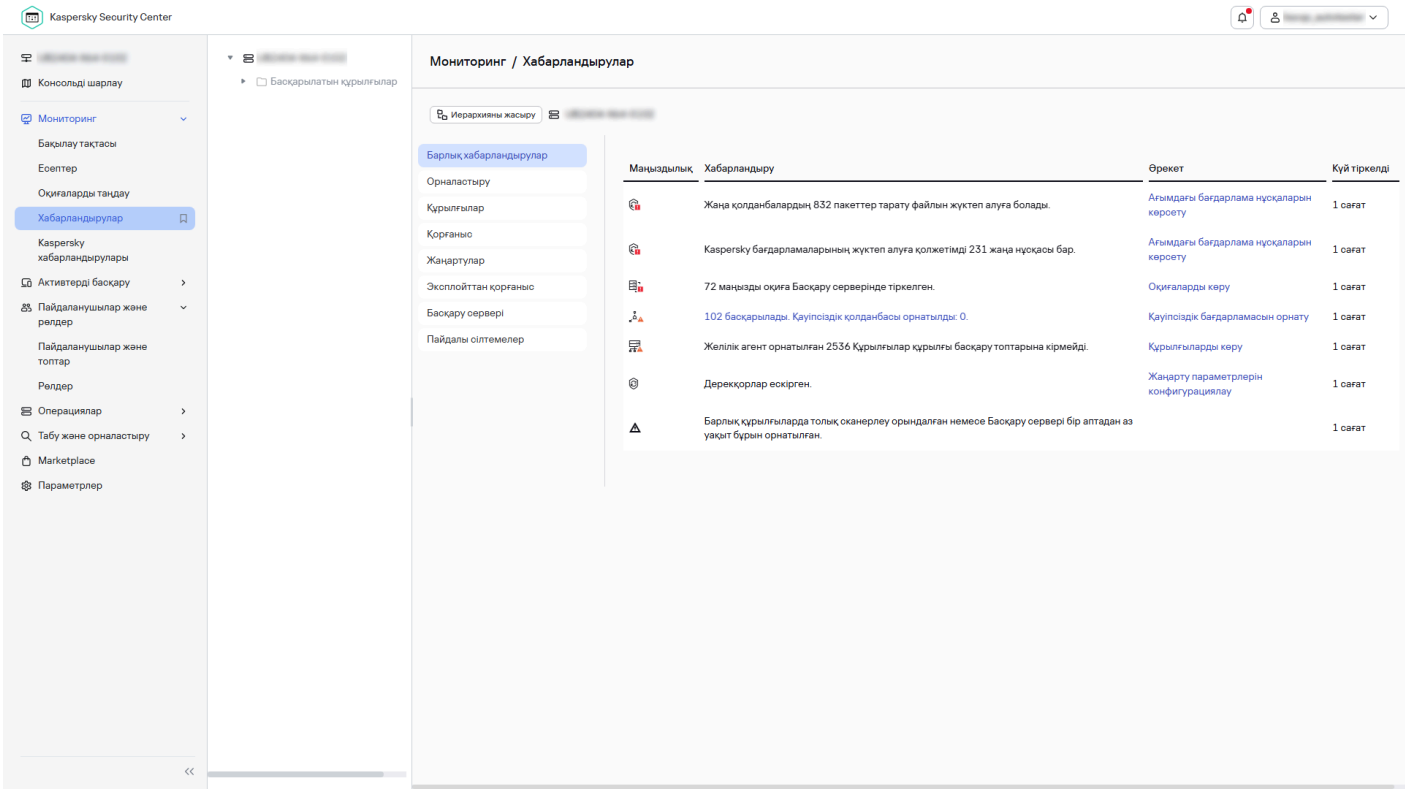
Басқару сервері ескі оқиғаларды жойған кезде, ол жаңа оқиғаларды дерекқорға сақтай алмайды. Осы кезең ішінде қабылданбаған оқиғалар туралы ақпарат операциялық жүйенің оқиғалар журналына жазылады. Жаңа оқиғалар кезекке қойылады, содан соң жою операциясы аяқталғаннан кейін, дерекқорда сақталады. Әдепкі бойынша, оқиға кезегі 20 000 оқиғамен шектеледі. KLEVP_MAX_POSTPONED_CNT жалаушаның мәнін өзгерту арқылы кезек шегін конфигурациялауға болады.

Хабарландырулар және құрылғылар күйлері

Бұл бөлімде хабарландыруларды көру, хабарландыруларды жеткізуді конфигурациялау, құрылғылардың күйін пайдалану және құрылғы күйлерін өзгертуді қосу тәсілі туралы ақпарат бар.

Хабарландыруларды қолдану

Хабарландырулар оқиғалар туралы ескертуге және сіз сәйкес деп санайтын ұсынылған әрекеттерді орындау арқылы осы оқиғаларға жауап беру жылдамдығыңызды арттыруға көмектесу үшін жасалған.



Хабарландырулар тізімі

Таңдалған хабарландыру тәсіліне байланысты келесі хабарландыру түрлері қолжетімді:

- Экрандағы хабарландырулар
- SMS хабарландыруы
- Электрондық пошта арқылы хабарлау
- Орындалатын файлды немесе сценарийді іске қосу арқылы хабарландыру

Экрандағы хабарландырулар

Экрандағы хабарландырулар маңыздылық деңгейлері бойынша топтастырылған оқиғалар туралы ескертеді (*Критикалық хабарландыру*, *Ескерту хабарландыруы*, және *Ақпараттық хабарландыру*).

Экрандағы хабарландырулар екі күйдің біріне ие болуы мүмкін:

- *Қаралды*. Бұл, хабарландыру үшін ұсынылған әрекетті орындағаныңызды немесе осы күйді қолмен хабарлау үшін тағайындағаныңызды білдіреді.
- *Қаралған жоқ*. Бұл, хабарландыру үшін ұсынылған әрекетті орындамағаныңызды немесе осы күйді қолмен хабарлау үшін тағайындамағаныңызды білдіреді.

Әдепкі бойынша, хабарландырулар тізіміне *Қаралған жоқ* мәртебесі бар хабарландырулар кіреді.

Өз ұйымыңыздың желісін экрандағы хабарландыруларды көру және оларға нақты уақыт режимінде жауап беру арқылы басқара аласыз.

Электрондық пошта, SMS бойынша және орындалатын файлды немесе скриптті іске қосу арқылы хабарландыру

Kaspersky Security Center Linux бағдарламасы маңызды деп санайтын оқиғалар туралы хабарландырулар жіберу арқылы ұйымыңыздың желісін басқаруға мүмкіндік береді. Кез келген оқиға үшін электрондық пошта, SMS бойынша немесе орындалатын файлды немесе скриптті іске қосу арқылы хабарландыруларды конфигурациялауға болады.

SMS немесе электрондық пошта бойынша хабарландыру алғаннан кейін, сіз оқиғаға жауап беру туралы шешім қабылдай аласыз. Бұл жауап сіздің ұйымыңыздың желісі үшін ең қолайлы болуы керек. Орындалатын файлды немесе скриптті іске қосу арқылы сіз оқиғаның жауабын алдын ала анықтайсыз. Сондай-ақ, оқиғаға негізгі жауап ретінде орындалатын файлды немесе скриптті іске қосуды қарастыруға болады. Орындалатын файлды іске қосқаннан кейін, оқиғаға жауап беру үшін басқа қадамдар жасауға болады.

Экрандағы хабарландыруларды қарау

Экрандағы хабарландыруларды үш тәсілмен көруге болады:

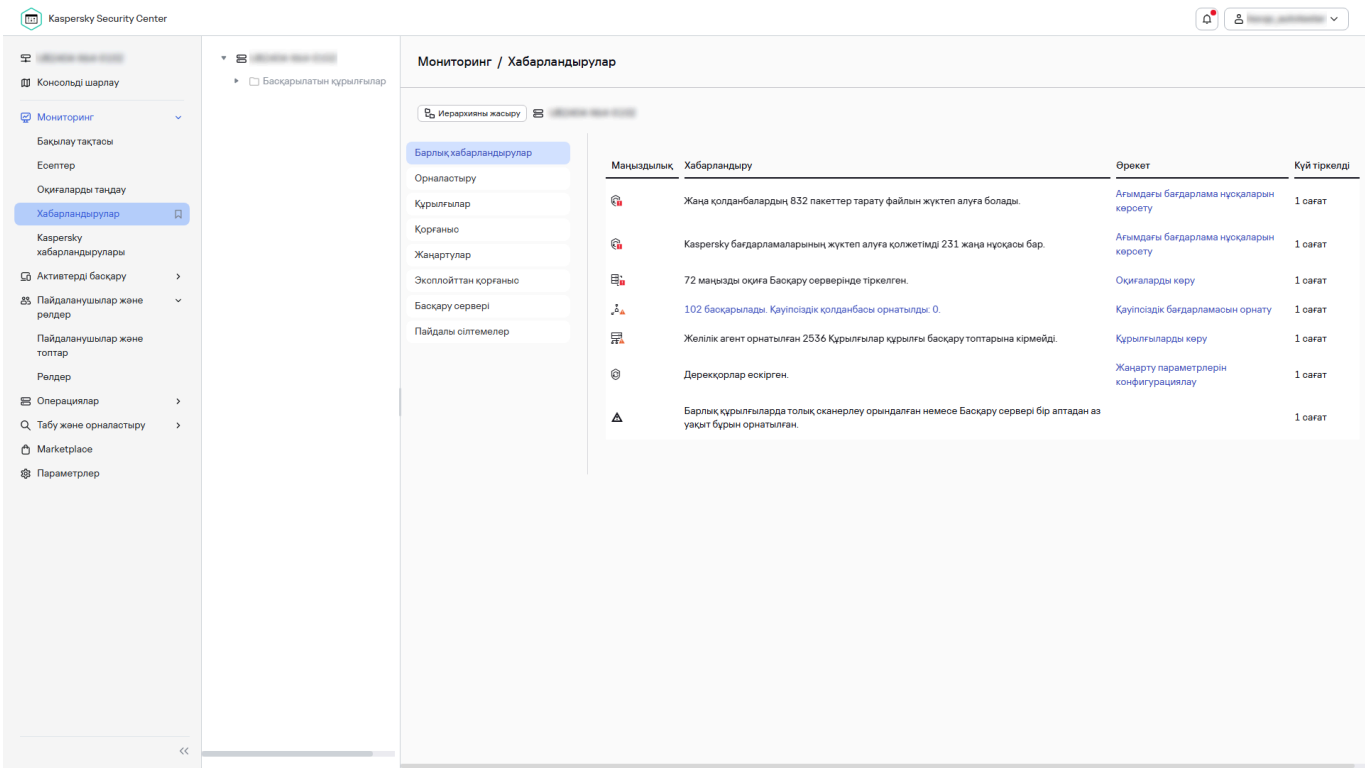
- **Мониторинг → Хабарландырулар** бөлімінде. Мұнда алдын ала анықталған санаттарға қатысты хабарландыруларды көруге болады.
- Қазіргі уақытта қандай бөлімді пайдалансаңыз да ашуға болатын бөлек терезеде. Бұл жағдайда, сіз хабарландыруларды қаралған деп белгілей аласыз.
- **Мониторинг → Бақылау тақтасы** бөліміндегі **Таңдалған қауіптілік деңгейі бойынша хабарландырулар** веб-виджетінде. Бұл веб-виджетте сіз тек *Критикалық* және *Ескерту* маңыздылық деңгейі бар хабарландыруларды ғана қарай аласыз.

Сіз оқиғаға жауап беру сияқты әрекеттерді орындай аласыз.

Алдын ала анықталған санат хабарландыруларын көру үшін:

1. Бағдарламаның негізгі терезесінде **Мониторинг → Хабарландырулар** бөліміне өтіңіз.

Сол жақ тақтада **Барлық хабарландырулар** санаты таңдалған, ал сол жақта барлық хабарландырулар көрсетіледі.



Хабарландырулар тізімі

2. Сол жақ тақтадан келесі санаттардың бірін таңдаңыз:

   - **Орналастыру**
   - **Құрылғылар**
   - **Қорғаныс**
   - **Жаңартулар** (оған жүктеп алуға қолжетімді Kaspersky қолданбалары туралы хабарландырулар, жүктеп алынған антивирустық дерекқор жаңартулары туралы хабарландырулар, сондай-ақ желілік агент жаңартуынан кейін қайта іске қосу керек құрылғылар туралы хабарландырулар (болса))
   - **Эксплойттан қорғаныс**
   - **Басқару сервері** (бұл хабарландыру тек Басқару серверіне қатысты оқиғаларды қамтиды)
   - **Пайдалы сілтемелер** (бұған Kaspersky ресурстарына сілтемелер, мысалы, Kaspersky Техникалық қолдау қызметіне, Kaspersky форумына, лицензияны ұзарту бетіне немесе Вирустық энциклопедияға сілтеме кіреді)

Хабарландырулар тізімінде таңдалған санат көрсетіледі. Тізімде мыналар бар:

- Хабарландыру тақырыбына қатысты белгіше: орналастыру (), қорғаныс (), жаңартулар (), құрылғыларды басқару (), Эксплойттан қорғаныс (), Басқару сервері ().
- Хабарландырудың маңыздылық деңгейі. Келесі маңыздылық деңгейлері бар хабарландырулар көрсетіледі: **Маңызды хабарландырулар** (), **Ескерту хабарландырулары** (), **Ақпараттық хабарландырулар**. Тізімдегі хабарландырулар маңыздылық деңгейі бойынша топтастырылған.
- **Хабарландыру**. Мұнда хабарландыру сипаттамасы бар.

- **Әрекет**. Мұнда орындауға ұсынылатын жылдам әрекетке сілтеме бар. Мысалы, осы сілтеме арқылы қоймаға өтіп, қауіпсіздік бағдарламасын құрылғыларға орната аласыз, құрылғылар тізімін немесе оқиғалар тізімін қарай аласыз. Хабарландыру үшін ұсынылатын әрекетті орындағаннан кейін, бұл хабарландыруға *Қаралды* күйі беріледі.

- **Күй тіркелді**. Мұнда Басқару серверінде хабарландыру тіркелген күннен бастап өткен күндер немесе сағаттар саны бар.

Маңыздылық деңгейі бойынша бөлек терезеде экран хабарландыруларын көру үшін:

1. Kaspersky Security Center Web Console жоғарғы оң жақ бұрышында жалауша () белгішесін басыңыз.

   Жалауша белгішесінің жанында қызыл нүкте болса, демек, қаралмаған хабарландырулар бар.

   Хабарландырулар тізімі бар терезе ашылады. Әдепкі бойынша **Барлық хабарландырулар** қойыншасы таңдалған және маңыздылық деңгейлері бойынша топтастырылған хабарландырулар көрсетіледі: *Критикалық хабарландырулар*, *Ескерту хабарландырулары* және *Ақпараттық хабарландырулар*.

2. **Жүйе** қойыншасын таңдаңыз.

   Критикалық () және *Ескерту* () маңыздылық деңгейлері бар хабарландырулар тізімі көрсетіледі. Хабарландырулар тізіміне мыналар кіреді:

   - Түсті индикатор. Критикалық хабарландырулар қызыл түспен белгіленген. Ескерту хабарландырулары сары түспен белгіленген.
   - Хабарландыру тақырыбына қатысты белгіше: орналастыру (), қорғаныс (), жаңартулар (), құрылғыларды басқару (), Эксплойттан қорғаныс (), Басқару сервері ().
   - Хабарландыру сипаттамасы.
   - Жалауша белгішесі. Сұр жалауша *Қаралған жоқ* күйі берілген хабарландырулар үшін пайдаланылады. Сұр жалаушаны таңдап, хабарландыру үшін *Қаралды* күйін тағайындаған кезде жалаушаның түсі ақ түске өзгереді.
   - Ұсынылатын әрекетке сілтеме. Сілтемені басу арқылы ұсынылған әрекетті орындаған кезде хабарландыруға *Қаралды* күйі беріледі.
   - Басқару серверінде хабарландыру тіркелген күннен бастап өткен күндер саны.

3. **Көбірек** қойыншасын таңдаңыз.

   Ақпараттық хабарландырулар маңыздылық деңгейі бар хабарландырулар тізімі көрсетіледі.

   Тізімнің құрылымы **Жүйе** қойыншасындағы тізім үшін сияқты (сипаттамасы жоғарыда келтірілген). Ол тек түсті индикатордың болмауымен ерекшеленеді.

Хабарландыруларды Басқару серверінде тіркелген күндер бойынша сүзгілеуге болады. Сүзгіні конфигурациялау үшін **Сүзгіні көрсету** жалаушасын қолданыңыз.

Веб-виджетте экран хабарландыруларын көру үшін:

1. **Бақылау тақтасы** бөлімінде **Виджетті қосу не қалпына келтіру** тармағын таңдаңыз.

2. Ашылған терезеде **Басқа** санатын басыңыз, **Таңдалған қауіптілік деңгейі бойынша хабарландырулар** веб-виджетін таңдаңыз және Қосу түймесін басыңыз.

Веб-виджет **Бақылау тақтасы** қойыншасында көрсетіледі. Әдепкі бойынша, веб-виджетте *Критикалық* маңыздылық деңгейі бар хабарландырулар көрсетіледі.

Ескерту хабарландырулары маңыздылық деңгейі бар хабарландыруларды көру үшін веб-виджетте **Параметрлер** түймесін басып, веб-виджет параметрлерін өзгерте аласыз. Не болмаса, басқа веб-виджетті қоса аласыз: *Ескерту хабарландырулары* маңыздылық деңгейі бар **Таңдалған қауіптілік деңгейі бойынша хабарландырулар**.

Веб-виджеттегі хабарландырулар тізімінің көлемі шектеулі және тек екі хабарландыруды қамтиды. Бұл екі хабарландыру соңғы оқиғаларға қатысты.

Веб-виджет хабарландыруларының тізіміне мыналар кіреді:

- Хабарландыру тақырыбына қатысты белгіше: орналастыру (), қорғаныс (), жаңартулар (), құрылғыларды басқару (), Эксплойттан қорғаныс (), Басқару сервері ().
- Ұсынылған әрекетке сілтеме жасалған хабарландырудың сипаттамасы. Сілтемені басу арқылы ұсынылған әрекетті орындаған кезде хабарландыруға *Қаралды* күйі беріледі.
- Басқару серверінде хабарландыру тіркелген күннен бастап өткен күндер немесе сағаттар саны.
- Басқа хабарландыруларға сілтеме. **Мониторинг** бөлімінде **Хабарландырулар** бөліміндегі хабарландыруларды көруге арналған сілтемеден өтіңіз.

Құрылғы күйлері туралы

Kaspersky Security Center Linux бағдарламасы әрбір басқарылатын құрылғыға күй тағайындайды. Нақты күйі, пайдаланушы анықтаған шарттардың орындалғанына байланысты. Кейбір шарттар үшін Kaspersky Security Center Linux құрылғысына күй тағайындау кезінде құрылғының желіде көрінуін ескереді (төмендегі кестені қараңыз). Мысалы, басқарылатын құрылғыға *Критикалық* күйі берілген болса, *Дерекқорлар ескірген* шарты орындалғандықтан, құрылғы үшін көзге көрінетін болғандықтан, құрылғыға *ОК* күйі беріледі. Егер Kaspersky Security Center Linux құрылғыны екі сағат ішінде желіден таппаса, құрылғының көрінуі *Офлайн* мәніне ие болады.

Келесі күйлер бар:

- *Критикалық* немесе *Критикалық/Көзге көрінетін*.
- *Ескерту* немесе *Ескерту/Көзге көрінетін*.
- *ОК* немесе *ОК/Көзге көрінетін*.

Төмендегі кестеде құрылғыға *Критикалық* немесе *Ескерту* күйін және олардың мүмкін мәндерін тағайындау үшін әдепкі бойынша шарттар келтірілген.

Құрылғыға күйлер белгілеу шарттары

Шарт	Шарттың сипаттамасы	Қолжетімді мәндері
Қауіпсіздік бағдарламасы орнатылмаған	Желілік агент құрылғыға орнатылған, бірақ қауіпсіздік бағдарламасы орнатылмаған.	• Қосқыш қосулы. • Қосқыш өшірулі.

Шарт	Шарттың сипаттамасы	Қолжетімді мәндері
Тым көп вирус анықталды	Вирустарды іздеу тапсырмаларының, мысалы, Зиянды БҚ іздеу тапсырмаларының жұмысы нәтижесінде, құрылғыда вирустар табылды және анықталған вирустардың саны көрсетілген мәннен асып түседі.	0-ден артық.
Нақты уақыт режимінде қорғау деңгейі әкімші орнатқан деңгейден өзгеше	Құрылғы желіде көрінеді, бірақ құрылғы күйіне арналған шартта нақты уақыт режимінде қорғау деңгейі әкімші орнатқан деңгейден өзгеше.	• Тоқтатылды. • Кідіртілді. • Орындалуда.
Зиянды БҚ іздеуі ұзақ уақыт орындалмады	Құрылғы желіде көрінеді және құрылғыда қауіпсіздік бағдарламасы орнатылған, бірақ *Зиянды БҚ іздеу* тапсырмасы да, жергілікті тексеру тапсырмасы да көрсетілген уақыттан артық орындалмады. Шарт тек жеті күн бұрын немесе одан бұрын Басқару сервері дерекқорына қосылған құрылғыларға қолданылады.	1-күннен артық.
Дерекқорлар ескірген	Құрылғы желіде көрінеді және құрылғыда қауіпсіздік бағдарламасы орнатылған, бірақ антивирустық дерекқорлар бұл құрылғыда көрсетілген уақыттан артық жаңартылмаған. Шарт тек бір күн бұрын немесе одан бұрын Басқару сервері дерекқорына қосылған құрылғыларға қолданылады.	1-күннен артық.
Қосылмағанына көп болды	Желілік агент құрылғыға орнатылған, бірақ құрылғы Басқару серверіне көрсетілген уақыттан артық қосылмаған, себебі құрылғы өшірулі.	1-күннен артық.
Белсенді қауіптер анықталды	**Белсенді қауіптер** қалтасындағы өңделмеген нысандар саны көрсетілген мәннен асып түседі.	0 данадан артық.
Қайта бастаудан кейінгі қажетті уақыт	Құрылғы желіде көрінеді, бірақ қолданба көрсетілген уақыт аралығынан ұзағырақ уақыт бойы қайта іске қосуды талап етті.	0 минуттан көбірек.
Қайта бастау себебі	Құрылғы желіде көрінеді, бірақ қолданба таңдалған себептердің біріне байланысты құрылғыны қайта іске қосуды талап етеді.	• Белгісіз себеп • Бағдарлама қайта іске қосуға дейін жұмыс істемейді • Жаңартуды аяқтау үшін қайта іске қосу қажет; бағдарлама жұмыс істеуде • Жаңартуды қолдану үшін қайта іске қосу қажет • Сканерлеуді немесе залалсыздандыруды аяқтау үшін қайта жүктеу керек • Қашықтан орнатуды/жоюды аяқтау үшін қайта іске қосу қажет • Дискідегі деректерді шифрлауды аяқтау
Үйлесімсіз бағдарламалар орнатылды	Құрылғы желіде көрінеді, бірақ Желілік агент орындаған бағдарламалық жасақтаманы түгендеу кезінде, құрылғыда үйлесімсіз бағдарламалардың орнатылғаны анықталды.	• Қосқыш өшірулі. • Қосқыш қосулы.
Бағдарламалық жасақтама осалдықтары анықталды	Құрылғы желіде көрінеді және оған Желілік агент орнатылған, бірақ *Осалдықтарды және қажетті жаңартуларды іздеу* тапсырмасын орындау нәтижесінде құрылғыда критикалық деңгейі белгіленген бағдарламаларда осалдықтар анықталды.	• Критикалық. • Жоғары. • Орташа. • Осалдықты жабу мүмкін емес болса, елемеу. • Жаңарту орнатуға белгіленген болса, елемеу.
Лицензия мерзімі өтті	Құрылғы желіде көрінеді, бірақ лицензияның жарамдылық мерзімі өтіп кеткен.	• Қосқыш өшірулі. • Қосқыш қосулы.
Лицензияның қолданылу мерзімі жақында аяқталады	Құрылғы желіде көрінеді, бірақ лицензиялық жарамдылық мерзімі көрсетілген күндер санынан аз уақыттан кейін өтіп кетеді.	0 күннен көп.

Шарт	Шарттың сипаттамасы	Қолжетімді мәндері
Windows Update жаңартуларын іздеу ұзақ уақыт бойы орындалмады	Құрылғы желіде көрінеді, бірақ *Windows Update жаңартуларын синхрондау* тапсырмасы көрсетілген уақыт аралығында орындалмаған.	1-күннен артық.
Жарамсыз шифрлау күйі	Желілік агент құрылғыға орнатылған, бірақ құрылғыны шифрлау нәтижесі көрсетілген мәнге тең.	• Пайдаланушының бас тартуына байланысты саясатқа сәйкес келмейді (тек сыртқы құрылғылар үшін). • Қатеге байланысты саясатқа сай емес. • Саясат қолданылуда – қайта іске қосу қажет. • Шифрлау саясаты белгіленбеген. • Қолдау көрсетілмейді. • Саясат қолданылуда.
Мобильді құрылғы параметрлері саясатқа жауап бермейді	Ұялы құрылғының параметрлері сәйкестік ережелерін тексеру кезінде Kaspersky Endpoint Security for Android саясатында белгіленген параметрлерден ерекшеленеді.	• Қосқыш өшірулі. • Қосқыш қосулы.
Өңделмеген қауіпсіздік мәселелері табылды	Құрылғыда өңделмеген қауіпсіздік мәселелері бар. Қауіпсіздік мәселелері клиенттік құрылғыға орнатылған басқарылатын Kaspersky қолданбалары арқылы автоматты түрде жасалуы немесе әкімші қолмен жасауы мүмкін.	• Қосқыш өшірулі. • Қосқыш қосулы.
Бағдарлама анықтаған құрылғы күйі	Құрылғының күйін басқарылатын бағдарлама анықтайды. Басқарылатын құрылғылар Kaspersky Security Center Linux параметрлеріне қарамастан басқарылатын қолданбалармен анықталған күйге ие болуы мүмкін. Бұл күй Kaspersky Security Center Linux анықтаған күйлердің бірін қайтарғаннан кейін, Басқару сервер басқарылатын құрылғыға басқарылатын құрылғы қайтарған және Басқару сервер тағайындағандардың ең маңызды күйін тағайындайды. Басқарылатын қолданбалар анықтаған күйлердің басқарылатын қолданбалар арқылы берілген сипаттамалары бар. Сипаттамаларды басқарылатын құрылғылар тізімінде, **Күйдің сипаттамасы** бағанында көре аласыз.	• Қосқыш өшірулі. • Қосқыш қосулы.
Құрылғыда бос орын жоқ	Құрылғының бос диск кеңістігі көрсетілген мәннен аз немесе құрылғы Басқару серверімен синхрондала алмайды. Құрылғы Басқару серверімен сәтті синхрондалғанда және құрылғының бос диск кеңістігі көрсетілген мәннен көп немесе тең болса, *Критикалық* немесе *Ескерту* күйлері *ОК* күйіне өзгереді.	0 МБ-тан көбірек.
Құрылғы басқарылмайтын күйге айналды	Құрылғылар табылған кезде құрылғы желіде көрінетін болып анықталады, бірақ Басқару серверімен синхрондаудың үштен артық сәтсіз әрекеті орындалды.	• Қосқыш өшірулі. • Қосқыш қосулы.
Қорғаныс өшірілген	Құрылғы көзге көрінеді, бірақ құрылғыдағы қауіпсіздік бағдарламасы көрсетілген уақыттан артық өшірулі. Бұл жағдайда қауіпсіздік бағдарламасының күйі *Тоқтатылған* немесе *Ақау* болып табылады және келесілерден ерекшеленеді: *Іске қосылуда*, *Орындалуда*, немесе *Кідіртілді*.	0 минуттан көбірек.
Қауіпсіздік бағдарламасы іске қосылмаған	Құрылғы көзге көрінеді және қауіпсіздік бағдарламасы құрылғыда орнатылған, бірақ іске қосылмаған.	• Қосқыш өшірулі. • Қосқыш қосулы.

Kaspersky Security Center Linux бағдарламасы белгіленген шарттарды орындау кезінде басқару тобындағы құрылғы күйін автоматты түрде ауыстырып қосуды конфигурациялауға мүмкіндік береді. Белгіленген шарттарды орындау кезінде, клиент құрылғысына келесі күйлердің бірі беріледі: *Критикалық* немесе *Ескерту*. Белгіленген шарттарды орындамаған жағдайда, клиент құрылғысына *ОК* күйі беріледі.

Бір шарттың әртүрлі мәндеріне әртүрлі күйлер сәйкес келуі мүмкін. Мысалы, әдепкі бойынша **3 күннен артық** мәні бар **Дерекқорлар ескірген** шартын ұстанған кезде клиент құрылғысына *Ескерту* күйі, ал **7 күннен артық** мәні бар шартты ұстанған кезде клиент құрылғысына *Критикалық* күйі беріледі.

Kaspersky Security Center Linux бағдарламасын алдыңғы нұсқасынан жаңартып жатсаңыз, *Критикалық* немесе *Ескерту* күйін тағайындау үшін **Дерекқорлар ескірген** шартының мәні өзгермейді.

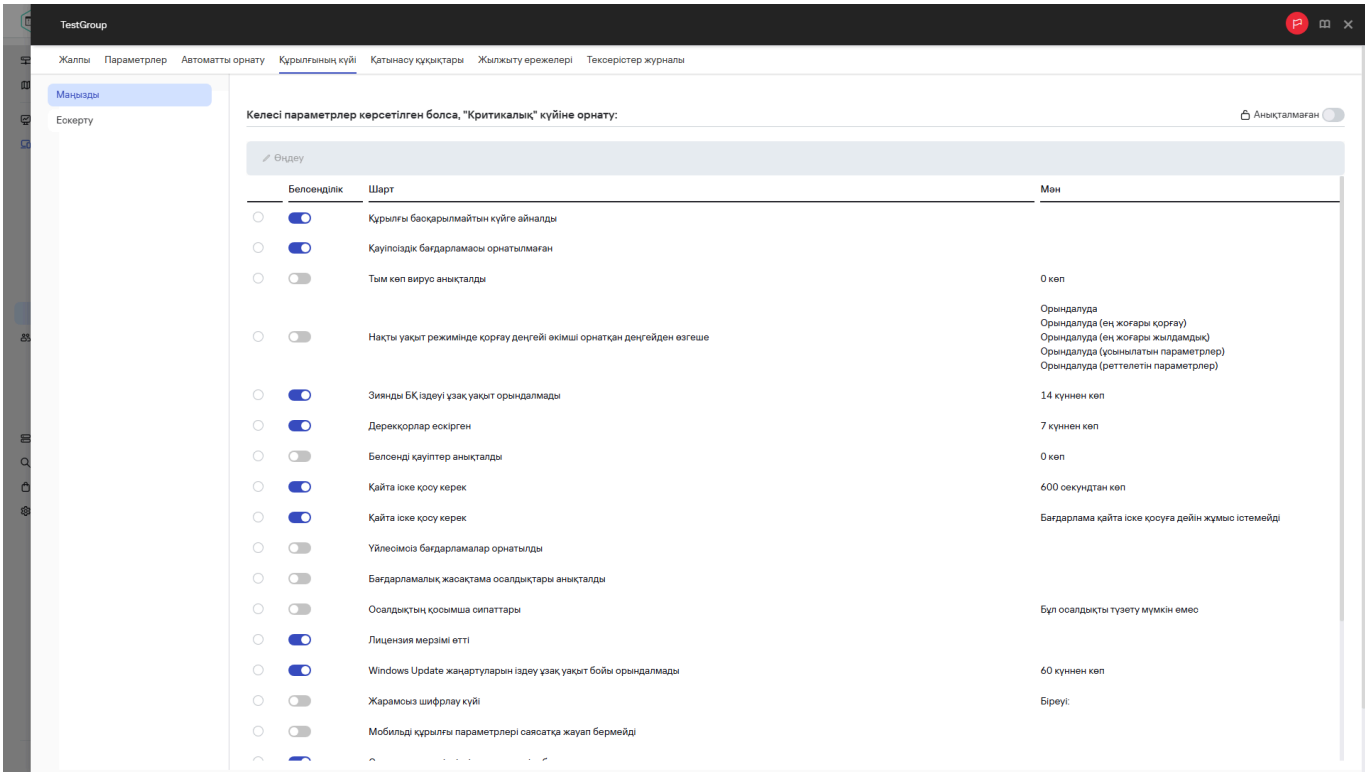
Құрылғылардың күйлерін ауыстыруды конфигурациялау

Құрылғыға *Критикалық* немесе *Ескерту* күйлерін тағайындау шарттарын өзгерте аласыз.

Құрылғының күйін Критикалық деп өзгерту үшін:

1. Бағдарламаның негізгі терезесінде **Активтерді басқару** → **Топтардың иерархиясы** бөліміне өтіңіз.
2. Келесі жолдардың бірімен құрылғы күйлерін өзгерткіңіз келетін басқару тобының сипаттарына өтіңіз:
   - Басқару тобының атауын басыңыз.
   - Беттің жоғарғы жағындағы **Иерархияны көрсету** түймесін басыңыз. Ашылатын навигация панелінде тінтуір курсорын қажетті топ атауының үстіне апарып, параметрлер белгішесін (⚙) басыңыз.

   Басқару тобының сипаттары терезесі ашылады.
3. Сипаттар терезесінен **Құрылғының күйі** қойындысын таңдаңыз.
4. **Маңызды** бөлімін таңдаңыз.
5. **Келесі параметрлер көрсетілген болса, "Критикалық" күйіне орнату** блогында құрылғыны *Критикалық* күйіне ауыстырып қосу үшін шартты қосыңыз.



> Алайда, сіз ата-ана саясатында бұғатталмаған параметрлерді өзгерте аласыз.

6. Тізімдегі шарттың жанына қосқышты орнатыңыз.

7. Тізімнің жоғарғы сол жақ бұрышындағы **Өңдеу** түймесін басыңыз.
8. Таңдалған шарт үшін өзіңізге қажетті мәнді белгілеңіз.

   Мәндерді барлық шарттар үшін бірдей орнату мүмкін емес.
9. **OK** түймесін басыңыз.
10. Өзгерістерін сақтау үшін **Сақтау** түймесін басыңыз.

Белгіленген шарттарды орындамаған жағдайда, басқарылатын құрылғыға *Критикалық* күйі тағайындалады.

Құрылғының күйін Ескерту деп өзгерту үшін:

1. Бағдарламаның негізгі терезесінде **Активтерді басқару** → **Топтардың иерархиясы** бөліміне өтіңіз.
2. Ашылған топтар тізімінде құрылғылардың күйлерін ауыстырып қосуды өзгерткіңіз келетін топтың атауы бар сілтемеден өтіңіз.
3. Пайда болған сипаттар терезесінде **Құрылғының күйі** қойыншасын таңдаңыз.
4. **Ескерту** бөлімін таңдаңыз.
5. **Келесі параметрлер көрсетілген болса, "Ескерту" күйіне орнату** блогында құрылғыны *Ескерту* күйіне ауыстырып қосу үшін шартты қосыңыз.

   Алайда, сіз ата-ана саясатында бұғатталмаған параметрлерді өзгерте аласыз.
6. Тізімдегі шарттың жанына қосқышты орнатыңыз.
7. Тізімнің жоғарғы сол жақ бұрышындағы **Өңдеу** түймесін басыңыз.
8. Таңдалған шарт үшін өзіңізге қажетті мәнді белгілеңіз.

   Мәндерді барлық шарттар үшін бірдей орнату мүмкін емес.
9. **OK** түймесін басыңыз.
10. Өзгерістерін сақтау үшін **Сақтау** түймесін басыңыз.

Белгіленген шарттарды орындамаған жағдайда, басқарылатын құрылғыға *Ескерту* күйі тағайындалады.

Хабарландыруларды жеткізу параметрлерін конфигурациялау

Сіз Kaspersky Security Center Linux бағдарламасында болатын оқиғалар туралы хабарландыруларды конфигурациялай аласыз. Таңдалған хабарландыру тәсіліне байланысты келесі хабарландыру түрлері қолжетімді:

- Электрондық пошта – оқиға болған кезде Kaspersky Security Center Linux бағдарламасы көрсетілген электрондық пошта мекенжайларына хабарландыру жібереді.
- SMS – оқиға болған кезде Kaspersky Security Center Linux бағдарламасы көрсетілген телефон нөмірлеріне хабарландыру жібереді.
- Орындалатын файл – оқиға болған кезде орындалатын файл Басқару серверінде іске қосылады.

Kaspersky Security Center Linux бағдарламасында болған оқиғалар туралы хабарландыруларды жеткізу параметрлерін конфигурациялау үшін:

1. Негізгі мәзірдегі басқару серверінің атауын басыңыз.

   Жалпы қойыншасында Басқару сервері сипаттары терезесі ашылады.

2. **Хабарландыру** бөліміне өтіп, оң жақ тақтадан қажетті хабарландыру тәсілі бар қойыншаны таңдаңыз:

   - **Электрондық пошта**

     Электрондық пошта қойыншасында электрондық пошта арқылы оқиғалар туралы хабарландыруларды конфигурациялауға болады.

     SMTP серверлері өрісінде пошта серверлерінің мекенжайларын нүктелі үтір арқылы көрсетіңіз. Келесі параметр мәндерін пайдалануыңызға болады:

     - IPv4 мекенжайы немесе IPv6 мекенжайы;
     - SMTP сервері DNS атауы.

     SMTP серверінің порты өрісінде SMTP серверіне қосылу портының нөмірін көрсетіңіз. Әдепкі бойынша 25-порт орнатылған.

     DNS MX іздеуін пайдалану параметрін қоссаңыз, SMTP серверінің бірдей DNS атауы үшін IP мекенжайының бірнеше MX жазбасын қолдана аласыз. Бір DNS атауында, алынған электрондық пошталардың әртүрлі басымдықтары бар бірнеше MX жазбалары болуы мүмкін. Басқару сервері MX жазбаларының басымдылығының өсуі ретімен SMTP серверіне электрондық пошта бойынша хабарландырулар жіберуге тырысады.

     > **DNS MX іздеуін пайдалану** параметрін қосып, TLS параметрін қолдануға рұқсат бермесеңіз, онда хабарландыруларды электрондық пошта бойынша жіберу кезінде қосымша қорғаныс шарасы ретінде сіздің серверлік құрылғыңызда DNSSEC параметрлерін қолдану ұсынылады.

     ESMTP аутентификациясын пайдалану параметрі қосулы болса, сіз **Пайдаланушы аты** және **Құпиясөз** өрістерінде ESMTP аутентификациясы параметрлерін көрсете аласыз. Әдепкі бойынша, параметр таңдалмаған және ESMTP аутентификациясы параметрлері қолжетімді емес.

     SMTP сервері үшін TLS қосылым параметрлерін көрсетуіңізге болады:

     - **TLS пайдаланбау**

Электрондық пошта хабарларын шифрлауды өшіргіңіз келсе, осы параметрді таңдауға болады.

- **SMTP сервері қолдау көрсетсе, TLS пайдаланыңыз**

SMTP серверіне қосылу үшін TLS пайдаланғыңыз келсе, бұл параметрді таңдауға болады. Егер SMTP сервері TLS қолдамаса, Басқару сервері SMTP серверін TLS қолданбай қосады.

- **Әрқашан TLS пайдаланыңыз, сервер сертификатының жарамдылығын тексеріңіз**

TLS түпнұсқалық растамасы параметрлерін пайдаланғыңыз келсе, осы параметрді таңдауға болады. Егер SMTP сервері TLS қолдамаса, Басқару сервері SMTP серверіне қосыла алмайды.

Бұл параметрді SMTP серверімен қосылымды қорғау үшін пайдалану ұсынылады. Осы параметрді таңдасаңыз, TLS қосылымы үшін түпнұсқалық растама параметрлерін орната аласыз.

Әрқашан TLS пайдаланыңыз, сервер сертификатының жарамдылығын тексеріңіз мәнін таңдасаңыз, SMTP серверінің түпнұсқалық растамасы үшін сертификатты көрсетіп, кез келген TLS нұсқасы арқылы немесе тек TLS 1.2 не одан кейінгі нұсқалары арқылы қосылуға рұқсат бергіңіз келетінін таңдай аласыз. Сондай-ақ, SMTP серверінде клиенттің түпнұсқалық растамасы үшін сертификатты көрсете аласыз.

Сіз **Сертификаттарды көрсету** сілтемесінен өтіп, TLS қосылымы үшін сертификатты көрсете аласыз:

- SMTP серверінің сертификаты файлын таңдаңыз:

Сіз сенімді сертификаттау орталығынан сертификаттар тізімі бар файлды ала аласыз және оны Басқару серверіне жүктей аласыз. Kaspersky Security Center Linux бағдарламасы SMTP серверінің сертификатына сенімді сертификаттау орталығы да қол қойғанын тексереді. SMTP серверінің сертификаты сенімді сертификаттау орталығынан алынбаса, Kaspersky Security Center Linux бағдарламасы SMTP серверіне қосыла алмайды.

- Клиент сертификаты файлын таңдаңыз:

Сіз кез келген көзден, мысалы, кез келген сенімді сертификаттау орталығынан алынған сертификатты пайдалана аласыз. Сертификаттың келесі түрлерінің бірін пайдаланып, сертификат пен оның жеке кілтін көрсетуіңіз қажет:

- X.509 сертификаты:

Сертификаты бар файлды және жеке кілт файлын көрсетуіңіз қажет. Екі файл да бір-біріне тәуелді емес және файлдарды жүктеу реті маңызды емес. Екі файл да жүктелген кезде жеке кілттің шифрсыздау үшін құпиясөзді көрсету керек. Жеке кілт шифрланбаған болса, құпиясөздің мәні бос болуы мүмкін.

- pkcs12 контейнері:

Сертификат пен сертификаттың жеке кілті бар бір файлды жүктеуіңіз қажет. Файл жүктелген кезде, жеке кілттің шифрсыздау үшін құпиясөзді көрсету керек. Жеке кілт шифрланбаған болса, құпиясөздің мәні бос болуы мүмкін.

Тексеру хабарын жіберу түймесін басу арқылы, хабарлардың дұрыс конфигурацияланғанын тексеруге болады: бағдарлама көрсетілген электрондық пошта мекенжайларына мәтіндік хабарлар жібереді.

Алушылар (электрондық пошта мекенжайлары) өрісінде хабарландырулар жіберілетін электрондық пошта мекенжайларын көрсетіңіз. Бұл өрісте бірнеше мекенжайды нүктелі үтір арқылы көрсетуге болады.

Тақырып өрісінде электрондық пошта тақырыбын көрсетіңіз. Сіз өрісті бос қалдыра аласыз.

Тақырып үлгісі ашылмалы тізімінен өзіңіздің электрондық хат тақырыбы үшін үлгіні таңдаңыз. Айнымалы, таңдалған үлгіге сәйкес, **Тақырып** өрісінде автоматты түрде көрсетіледі. Сіз бірнеше тақырып үлгісін таңдап, электрондық пошта тақырыбын жасай аласыз.

Жіберушінің электрондық пошта мекенжайы: Егер бұл параметр көрсетілмеген болса, онда оның орнына алушының мекенжайы пайдаланылады. Ескерту: Жалған электрондық пошта мекенжайын пайдалану ұсынылмайды терезесінде электрондық пошта жіберушінің мекенжайын көрсетіңіз. Егер сіз өрісті бос қалдырсаңыз, әдепкі бойынша алушының мекенжайы қолданылады. Жоқ мекенжайды пайдалану ұсынылмайды.

Хабарландыру хабары өрісінде, оқиға туындаған кезде бағдарлама жіберетін оқиға туралы хабарландырудың стандартты мәтіні қамтылған. Мәтінде оқиғаның атауы, құрылғының атауы және доменнің атауы сияқты алмастырылатын параметрлер бар. Хабар мәтінін, оқиғаның егжей-тегжейлі деректері бар алмастырылатын параметрлерді қосу арқылы өзгертуге болады.

Хабарландыру мәтінінде пайыз белгішесі (%) болса, хабар жіберілуі үшін, осы пайыз белгішесін қатарынан екі рет көрсету керек. Мысалы, "Орталық процессор жүктемесі 100%%".

Хабарландырулар санының шегін конфигурациялау сілтемесінен өткенде, бағдарлама көрсетілген уақыт аралығында жібере алатын хабарландырулардың ең көп санын көрсетуге болады.

- SMS

SMS қойыншасында ұялы телефонға түрлі оқиғалар туралы SMS хабарландыруларын жіберуді конфигурациялауға болады. SMS хабарлар пошта шлюзі арқылы жіберіледі.

SMTP серверлері өрісінде пошта серверлерінің мекенжайларын нүктелі үтір арқылы көрсетіңіз. Келесі параметр мәндерін пайдалануыңызға болады:

- IPv4 мекенжайы немесе IPv6 мекенжайы;
- SMTP сервері DNS атауы.

SMTP серверінің порты өрісінде SMTP серверіне қосылу портының нөмірін көрсетіңіз. Әдепкі бойынша 25-порт орнатылған.

ESMTP аутентификациясын пайдалану параметрі қосулы болса, сіз **Пайдаланушы аты** және **Құпиясөз** өрістерінде ESMTP аутентификациясы параметрлерін көрсете аласыз. Әдепкі бойынша, параметр таңдалмаған және ESMTP аутентификациясы параметрлері қолжетімді емес.

SMTP сервері үшін TLS қосылым параметрлерін көрсетуіңізге болады:

- **TLS пайдаланбау**

Электрондық пошта хабарларын шифрлауды өшіргіңіз келсе, осы параметрді таңдауға болады.

- **SMTP сервері қолдау көрсетсе, TLS пайдаланыңыз**

SMTP серверіне қосылу үшін TLS пайдаланғыңыз келсе, бұл параметрді таңдауға болады. Егер SMTP сервері TLS қолдамаса, Басқару сервері SMTP серверін TLS қолданбай қосады.

- **Әрқашан TLS пайдаланыңыз, сервер сертификатының жарамдылығын тексеріңіз**

TLS түпнұсқалық растамасы параметрлерін пайдаланғыңыз келсе, осы параметрді таңдауға болады. Егер SMTP сервері TLS қолдамаса, Басқару сервері SMTP серверіне қосыла алмайды.

Бұл параметрді SMTP серверімен қосылымды қорғау үшін пайдалану ұсынылады. Осы параметрді таңдасаңыз, TLS қосылымы үшін түпнұсқалық растама параметрлерін орната аласыз.

Әрқашан TLS пайдаланыңыз, сервер сертификатының жарамдылығын тексеріңіз мәнін таңдасаңыз, SMTP серверінің түпнұсқалық растамасы үшін сертификатты көрсетіп, кез келген TLS нұсқасы арқылы немесе тек TLS 1.2 не одан кейінгі нұсқалары арқылы қосылуға рұқсат бергіңіз келетінін таңдай аласыз. Сондай-ақ, SMTP серверінде клиенттің түпнұсқалық растамасы үшін сертификатты көрсете аласыз.

Сіз **Сертификаттарды көрсету** сілтемесінен өтіп, TLS қосылымы үшін SMTP сервері сертификатын көрсете аласыз. Сіз сенімді сертификаттау орталығынан сертификаттар тізімі бар файлды ала аласыз және оны Басқару серверіне жүктей аласыз. Kaspersky Security Center Linux бағдарламасы SMTP серверінің сертификатына сенімді сертификаттау орталығы да қол қойғанын тексереді. SMTP серверінің сертификаты сенімді сертификаттау орталығынан алынбаса, Kaspersky Security Center Linux бағдарламасы SMTP серверіне қосыла алмайды.

Алушылар (электрондық пошта мекенжайлары) өрісінде хабарландырулар жіберілетін электрондық пошта мекенжайларын көрсетіңіз. Бұл өрісте бірнеше мекенжайды нүктелі үтір арқылы көрсетуге болады. Хабарландырулар, көрсетілген электрондық пошта мекенжайларымен байланысты нөмірлері бар телефондарға жеткізіледі.

Тақырып өрісінде электрондық пошта тақырыбын көрсетіңіз.

Тақырып үлгісі ашылмалы тізімінен өзіңіздің электрондық хат тақырыбы үшін үлгіні таңдаңыз. Айнымалы, таңдалған үлгіге сәйкес, **Тақырып** өрісінде көрсетіледі. Сіз бірнеше тақырып үлгісін таңдап, электрондық пошта тақырыбын жасай аласыз.

Жіберушінің электрондық пошта мекенжайы: Егер бұл параметр көрсетілмеген болса, онда оның орнына алушының мекенжайы пайдаланылады. Ескерту: Жалған электрондық пошта мекенжайын пайдалану ұсынылмайды терезесінде электрондық пошта жіберушінің мекенжайын көрсетіңіз. Егер сіз өрісті бос қалдырсаңыз, әдепкі бойынша алушының мекенжайы қолданылады. Жоқ мекенжайды пайдалану ұсынылмайды.

SMS хабар алушыларының телефон нөмірлері өрісінде SMS алу үшін ұялы телефон нөмірлерін көрсетіңіз.

Хабарландыру хабары өрісінде, оқиға туындаған кезде бағдарлама жіберетін оқиға туралы хабарландыру мәтінін жазыңыз. Мәтінде оқиғаның атауы, құрылғының атауы және доменнің атауы сияқты алмастырылатын параметрлер болуы мүмкін.

> Хабарландыру мәтінінде пайыз белгішесі (%) болса, хабар жіберілуі үшін, осы пайыз белгішесін қатарынан екі рет көрсету керек. Мысалы, "Орталық процессор жүктемесі 100%%".

Хабарлардың дұрыс конфигурацияланғанын тексеру үшін **Тексеру хабарын жіберу** түймесін басыңыз: бағдарлама көрсетілген алушыларға мәтіндік хабарлар жібереді.

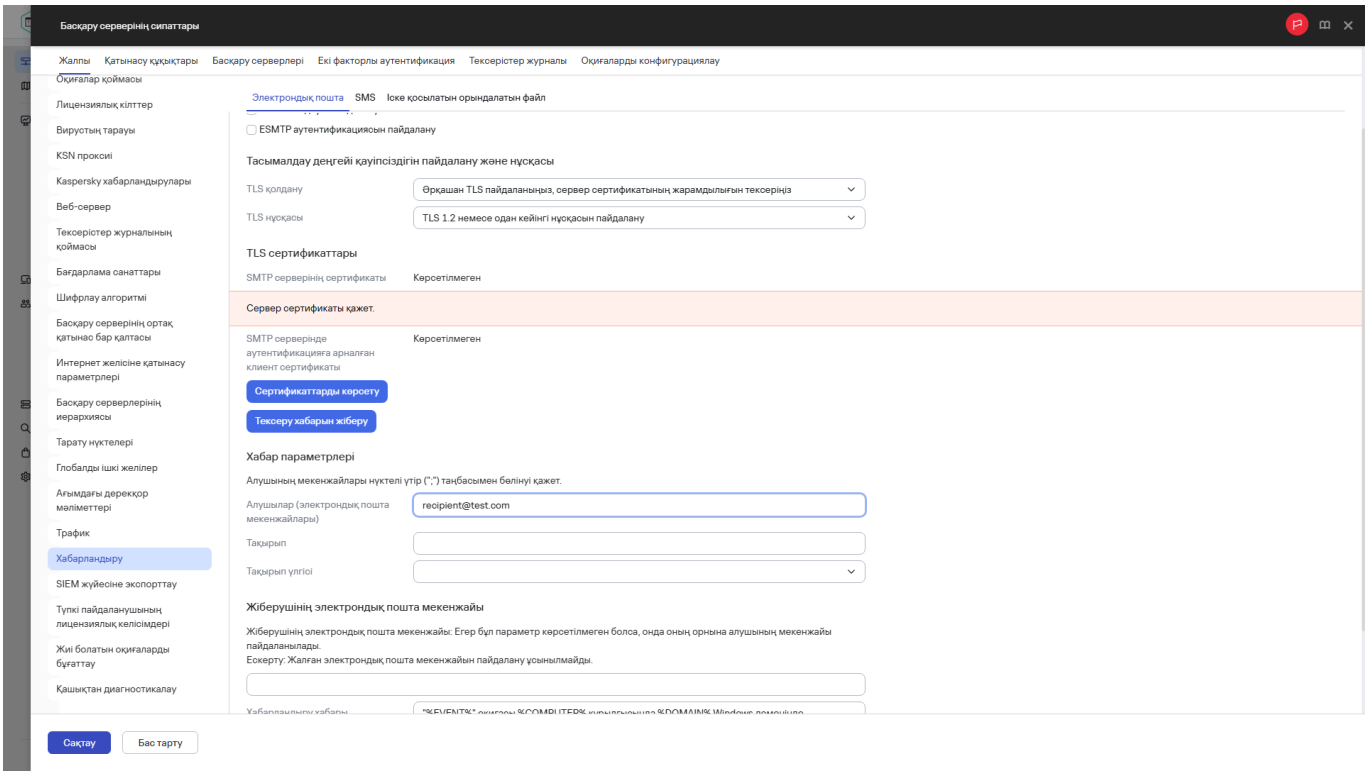
Хабарландырулар санының шегін конфигурациялау сілтемесінен өтіп, бағдарлама көрсетілген уақыт аралығында жібере алатын хабарландырулардың ең көп санын көрсетуге болады.

- **Іске қосылатын орындалатын файл**

  Егер бұл хабарландыру тәсілі таңдалса, енгізу өрісінде оқиға болған кезде қандай бағдарлама іске қосылатынын көрсетуге болады.

  Оқиға пайда болған кезде, орындалатын файл Басқару серверінде іске қосылады өрісінде іске қосылатын файлдың қалтасы мен атауын көрсетіңіз. Файлды көрсетпес бұрын, файлды дайындаңыз және хабарда жіберілетін оқиға туралы мәліметтерді анықтайтын алмастырылатын параметрлерді көрсетіңіз. Көрсетілген қалта мен файл Басқару серверінде болуы керек.

  Хабарландырулар санының шегін конфигурациялау сілтемесінен өткенде, бағдарлама көрсетілген уақыт аралығында жібере алатын хабарландырулардың ең көп санын көрсетуге болады.



Хабарландыру әдісін таңдау

3. Қойыншада хабарландыру параметрлерін конфигурациялаңыз.

4. Өзгерістерді сақтау және Басқару серверінің қасиеттері терезесін жабу үшін **Сақтау** түймесін басыңыз.

   Сақталған хабарландыруларды жеткізу параметрлері Kaspersky Security Center Linux бағдарламасында болатын барлық оқиғаларға қолданылады.

Оқиғаларды конфигурациялау бөлімінде, Басқару сервері параметрлерінде, саясат параметрлерінде немесе бағдарлама параметрлерінде белгіленген оқиғалар үшін хабарландыруларды жеткізу параметрлерінің мәндерін өзгертуге болады.

Хабарландыруларды таратуды тексеру

Оқиға туралы хабарландырулардың таралуын тексеру үшін клиент құрылғыларында Eicar сынақ "вирусын" анықтау туралы хабарландыру қолданылады.

Оқиғалар туралы хабарландырулардың таралуын тексеру үшін:

1. Клиент құрылғысындағы файлдық жүйені нақты уақыт режимінде қорғау тапсырмасын тоқтатыңыз және Eicar сынақ "вирусын" клиент құрылғысына көшіріңіз. Кейін файлдық жүйенің нақты қорғау тапсырмасын қайта іске қосыңыз.

2. Басқару тобына немесе Eicar сынақ "вирусы" бар клиент құрылғысын қамтитын құрылғылар жиынтығына арналған клиент құрылғыларын тексеру тапсырмасын іске қосыңыз.

   Егер сканерлеу тапсырмасы дұрыс конфигурацияланған болса, оны орындау барысында сынақ "вирусы" анықталады. Егер хабарландыру параметрлері дұрыс конфигурацияланған болса, сіз табылған вирус туралы хабарландыру аласыз.

Сынақ "вирусын" анықтау туралы жазбаны ашу үшін:

1. Бағдарламаның негізгі терезесінде **Мониторинг → Оқиғаларды таңдау** бөліміне өтіңіз.
2. **Соңғы оқиғалар** таңдауының атауын басыңыз.

   Ашылған терезеде сынақ "вирусы" туралы хабарлама көрсетіледі.

Eicar сынақ "вирусында" сіздің құрылғыңызға зиян тигізуі мүмкін бағдарламалық код жоқ. Бұл арада, өндіруші компаниялардың қауіпсіздік бағдарламаларының көпшілігі оны вирус ретінде анықтайды. Сынақ "вирусын" EICAR ұйымының ресми сайтынан жүктеп алуға болады.

Орындалатын файл көмегімен оқиғалар туралы хабарлау

Kaspersky Security Center Linux орындалатын файлды іске қосу арқылы әкімшіге клиент құрылғыларындағы оқиғалар туралы хабарлауға мүмкіндік береді. Орындалатын файлда әкімшіге жіберілетін оқиғаның орта айнымалылары бар басқа орындалатын файл болуы керек (төмендегі кестені қараңыз).

Оқиғаны сипаттауға арналған орта айнымалылары

Орта айнымалысы	Орта айнымалысының сипаттамасы
$SEVERITY	Оқиғаның маңыздылық деңгейі. Ықтимал мәндер: • **Ақпараттық** • **Ескерту** • **Сәтсіз аяқталды** • **Маңызды**
$COMPUTER	Оқиға болған құрылғының атауы. Құрылғы атауының максималды ұзындығы - 256 таңба.
$DOMAIN	Оқиға болған құрылғының домен атауы.
$EVENT	Оқиға түрінің атауы. Оқиға түрінің атауының максималды ұзындығы - 50 таңба.
$DESCR	Оқиғаның сипаттамасы. Максималды сипаттама ұзындығы - 1000 таңба.
$RISE_TIME	Оқиғаны құру уақыты.
$KLCSAK_EVENT_TASK_DISPLAY_NAME	Тапсырманың атауы. Тапсырма атауының максималды ұзындығы - 100 таңба.
$KL_PRODUCT	Бағдарлама атауы.
$KL_VERSION	Қолданба нұсқасының нөмірі.
$KLCSAK_EVENT_SEVERITY_NUM	Оқиғаның маңыздылық деңгейінің коды. Ықтимал мәндер: • 1 – **Ақпараттық**. • 2 – **Ескерту**. • 3 – **Сәтсіздік**. • 4 – **Маңызды**.
$HOST_IP	Оқиға болған құрылғының IP мекенжайы.
$HOST_CONN_IP	Оқиға болған құрылғы қосылымының IP мекенжайы.

Мысалы:
Оқиға туралы хабарлау үшін орындалатын файл қолданылады (мысалы, script1.bat), оның ішінде %COMPUTER% алмастырылатын параметрі бар басқа орындалатын файл іске қосылады (мысалы, script2.bat). Оқиға болған кезде әкімші құрылғысында script1.bat файлы іске қосылып, өз кезегінде %COMPUTER% параметрі бар script2.bat файлын іске қосады. Нәтижесінде, әкімші оқиға болған құрылғының атын алады.

Kaspersky хабарландырулары

Бұл бөлімде Kaspersky хабарландыруларын қолдану, конфигурациялау және өшіру тәсілі сипатталған.

Kaspersky хабарландырулары туралы

Kaspersky хабарландырулары бөлімі (**Мониторинг → Kaspersky хабарландырулары**) Kaspersky Security Center нұсқаңыз және басқарылатын құрылғыларға орнатылған басқарылатын бағдарламалар туралы ақпаратты ұсынады. Kaspersky Security Center Linux бағдарламасы бөлімдегі ақпаратты жаңартады, ескірген хабарландыруларды жояды және жаңа ақпаратты қосады.

Kaspersky Security Center Linux тек ағымдағы қосылған Басқару серверіне және осы Басқару серверінің басқарылатын құрылғыларында орнатылған Kaspersky бағдарламаларына қатысты Kaspersky хабарландыруларын ғана көрсетеді. Хабарландырулар Басқару серверінің кез келген түрі (негізгі, қосалқы немесе виртуалды) үшін жеке-жеке көрсетіледі.

Kaspersky хабарландыруларын алу үшін Басқару серверінде интернет қосылымы болуы тиіс.

Хабарландыруларға келесі түрдегі ақпарат кіреді:

- Қауіпсіздікке қатысты хабарландырулар.

  Қауіпсіздікке қатысты хабарландырулар сіздің желіңізде орнатылған Kaspersky бағдарламалары өзекті күйде болуына және толығымен жұмыс істеуге жарамды болуына арналған. Хабарландыруларда Kaspersky бағдарламаларына арналған критикалық жаңартулар, табылған осалдықтарға арналған түзетулер және Kaspersky бағдарламаларындағы басқа мәселелерді шешу тәсілдері туралы ақпарат қамтылуы мүмкін. Әдепкі бойынша, қауіпсіздікке қатысты хабарландырулар қосылды. Хабарландыруларды алып тұрғыңыз келмесе, бұл функцияны өшіре аласыз.

  Сізге желіні қорғау конфигурациясына сәйкес келетін ақпаратты көрсету үшін, Kaspersky Security Center Linux бағдарламасы деректерді Kaspersky бұлтты серверлеріне жібереді және сіздің желіңізде орнатылған Kaspersky бағдарламаларына қатысты хабарландыруларды ғана алады. Серверлерге жіберілуі мүмкін деректер Басқару серверін орнату кезінде қабылдайтын Лицензиялық келісімде сипатталған.

- Жарнамалық хабарландырулар.

  Жарнамалық хабарландырулар Kaspersky бағдарламаларыңыз үшін арнайы ұсыныстар туралы ақпаратты, Kaspersky жарнамалары мен жаңалықтарын қамтиды. Жарнамалық хабарландырулар әдепкі бойынша өшірулі. Сіз жаңартулардың осы түрін Kaspersky Security Network (KSN) бағдарламасын қоссаңыз ғана аласыз. Сіз KSN өшіріп, жарнамалық хабарландыруларды өшіре аласыз.

  Желілік құрылғыларыңыз үшін және күнделікті тапсырмаларды орындау үшін пайдалы болуы мүмкін өзекті ақпаратты ғана көруіңіз үшін, Kaspersky Security Center Linux бағдарламасы деректерді Kaspersky бұлтты серверлеріне жіберіп, тиісті хабарландыруларды алады. Серверлерге жіберілуі мүмкін деректер KSN мәлімдемесінің "Өңделетін деректер" бөлімінде сипатталған.

Ақпарат маңыздылық бойынша келесі санаттарға бөлінген:

1. Критикалық ақпарат
2. Маңызды жаңалық

3. Ескерту

4. Ақпараттық хабар

Kaspersky Хабарландырулар бөлімінде жаңа ақпарат пайда болған кезде, Kaspersky Security Center Web Console бағдарламасы хабарландырулардың маңыздылық деңгейіне сәйкес келетін хабарландыру белгісін көрсетеді. Бұл хабарландыруды Kaspersky Хабарландырулар бөлімінде көру үшін белгіні түртуге болады.

Kaspersky хабарландырулар параметрлерін, соның ішінде көргіңіз келетін хабарландыру санаттарын және хабарландыру белгісін көрсету орнын көрсете аласыз. Хабарландыруларды алып тұрғыңыз келмесе, бұл функцияны өшіре аласыз.

Kaspersky хабарландыру параметрлерін конфигурациялау

Kaspersky хабарландырулары бөлімінде сіз көргіңіз келетін хабарландырулар санаттарын қоса алғанда, Kaspersky хабарландырулары параметрлерін және хабарландыру белгісін қайда көрсету керектігін көрсете аласыз.

Kaspersky хабарландыруларын конфигурациялау үшін:

1. Бағдарламаның негізгі терезесінде **Мониторинг → Kaspersky хабарландырулары** бөліміне өтіңіз.

2. **Параметрлер** сілтемесінен өтіңіз.

   Kaspersky хабарландырулары терезесі ашылады.

3. Келесі параметрлерді белгілеңіз:

   - Көргіңіз келетін хабарландырулардың маңыздылық деңгейін таңдаңыз. Басқа санаттағы хабарландырулар көрсетілмейді.

   - Хабарландыру белгісін көргіңіз келетін орналасуды таңдаңыз. Белгі консольдің барлық бөлімдерінде немесе **Мониторинг** бөлімінде және оның бөлікшелерінде көрсетілуі мүмкін.

4. **ОК** түймесін басыңыз.

   Kaspersky хабарландырулары параметрлері конфигурацияланған.

Kaspersky хабарландыруларын өшіру

Kaspersky хабарландырулары бөлімі (**Мониторинг → Kaspersky хабарландырулары**) Kaspersky Security Center Linux нұсқаңыз және басқарылатын құрылғыларға орнатылған басқарылатын бағдарламалар туралы ақпаратты ұсынады. Kaspersky хабарландыруларын алып тұрғыңыз келмесе, бұл функцияны өшіре аласыз.

Kaspersky хабарландырулары екі түрлі ақпаратты қамтиды: қауіпсіздікке қатысты хабарландырулар және жарнамалық хабарландырулар. Сіз әрбір түрдегі хабарландыруларды бөлек өшіре аласыз.

Қауіпсіздікпен байланысты хабарландыруларды өшіру үшін:

1. Негізгі мәзірдегі басқару серверінің атауын басыңыз.

   Басқару серверінің сипаттары терезесі ашылады.

2. **Жалпы** қойыншасында **Kaspersky хабарландырулары** бөлімін таңдаңыз.
3. Қосқышты **Қауіпсіздікке қатысты хабарландырулар** өшірілген күйіне ауыстырыңыз.
4. **Сақтау** түймесін басыңыз.

   Kaspersky хабарландырулары өшірулі.

Жарнамалық хабарландырулар әдепкі бойынша өшірулі. Сіз Kaspersky Security Network (KSN) қосқан жағдайда ғана жарнамалық хабарландырулар аласыз. KSN өшіру арқылы хабарландырулардың бұл түрін өшіруге болады.

Хабарландыруларды өшіру үшін:

1. Негізгі мәзірдегі басқару серверінің атауын басыңыз.

   Басқару серверінің сипаттары терезесі ашылады.
2. **Жалпы** қойыншасында **KSN прокси параметрлері** бөлімін таңдаңыз.
3. **Kaspersky Security Network пайдалану Қосулы** параметрін өшіріңіз.
4. **Сақтау** түймесін басыңыз.

   Хабарландырулар өшірулі.

Табылған қауіптер туралы ақпаратты қарап шығу

Анықтау туралы ақпаратты көрсетуді қосуға немесе өшіруге болады.

Kaspersky Extended Detection and Response Optimum лицензиясы немесе Kaspersky Security: Бизнеске арналған Кәсіби лицензиясы бойынша Басқару серверін іске қосқаннан кейін, Kaspersky Security Center Web Console негізгі мәзірдің **Мониторинг** бөлімінде **Дабылдар** бөлімшесін автоматты түрде көрсетеді.

*Бас мәзірде **Дабылдар** бөлімінің көрсетілуін қосу немесе өшіру үшін:*

1. Негізгі мәзірдегі **Параметрлер** → **Интерфейс опциялары** бөліміне өтіңіз.
2. **EDR дабылдарын көрсету** параметрін қосыңыз немесе өшіріңіз.
3. **Сақтау** түймесін басыңыз.

EDR дабылдарын көрсету параметрі қосылған кезде, консоль негізгі мәзірдің **Мониторинг** бөлімінде **Дабылдар** бөлімшесін көрсетеді. **Дабылдар** бөлімінде, құрылғыларда табылған қауіптер туралы ақпаратты қарай аласыз.

Сондай-ақ, сіз анықтаулар туралы ақпарат көрсетілетін веб-виджетті қоса аласыз.

Алерт карточкасында анықталған қауіптер туралы толық ақпаратты дұрыс көрсету үшін Kaspersky Endpoint Agent плагинін және Kaspersky Endpoint Security плагинінің үйлесімді нұсқасын (Kaspersky Endpoint Security for Linux 12.1 немесе одан жоғары нұсқасы, Kaspersky Endpoint Security for Mac 12.1 немесе одан жоғары нұсқасы, Kaspersky Endpoint Security for Windows 12.6 немесе одан жоғары нұсқасы) орнату керек.

Анықтауларды күн және өріс мәндері бойынша сүзгілеу үшін **Сүзгі** мәзірін пайдаланыңыз.

Нысан түрі өрісі келесі мәндердің бірін қамтиды:

- белгісіз
- Фишингтік сілтеме
- вирус
- Трояндық бағдарлама
- зиянды құрал
- қашықтан басқаруға арналған трояндық бағдарлама
- құрт
- басқа бағдарлама
- Жарнамалық бағдарлама
- Pornware бағдарлама
- Қауіпті мұрағатталған бағдарлама
- Қауіпті әрекет

Автоматты жауап өрісі келесі мәндердің бірін қамтиды:

- Зиянды нысан анықталды
- Нысан жойылды
- Нысан залалсыздандырылды
- Нысанды залалсыздандыру сәтсіз аяқталды
- Нысан карантинге көшірілді
- Құпиясөзбен қорғалған мұрағат анықталды
- Вирус анықталды

Дабылдарға жауап беруге арналған интеграциялар

Сізде Kaspersky Security: Бизнеске арналған Кәсіби лицензиясы болса, қауіптерге жауап беру үшін интеграцияларды келесі шешімдермен конфигурациялауға болады:

- Kaspersky Automated Security Awareness Platform
- Kaspersky Threat Intelligence Portal Sandbox
- Active Directory

Бұл интеграциялар Басқару серверін Kaspersky Security: Бизнеске арналған Кәсіби лицензиясы бойынша белсендірген жағдайда қолжетімді.
Әрекет ету шараларын орындау үшін Kaspersky Security: Бизнеске арналған Кәсіби лицензиялық кілтін басқарылатын бағдарламаларға тарату керек.
Сынақ лицензиясы бойынша Kaspersky Security: Бизнеске арналған Кәсіби функционалдығын пайдаланған кезде, алдымен қосалқы физикалық басқару серверін қосып, осы қосалқы басқару серверін сынақ лицензиясы бойынша іске қосып, содан кейін осы басқару сервері басқаратын құрылғыларыңызға лицензия кілтін орналастыру керек.

Kaspersky Next EDR Optimum лицензиясын пайдалансаңыз, басқарылатын құрылғыларда Kaspersky Security: Бизнеске арналған Кәсіби лицензиясы бойынша орнатылған қолданбаларды белсендірудің қажеті жоқ. Мұны тек жаңа құрылғылар үшін жасау керек (бар болса).

Kaspersky Security: Бизнеске арналған Кәсіби лицензиясы көптиістілікке қолдау көрсететіндіктен, лицензия кілтін басқарылатын қолданбаларға орталықтан таратуға болады. Лицензияны қосымша және виртуалды басқару серверлеріне автоматты түрде таратуға қолдау көрсетілмейді.

Интеграцияларды конфигурациялау үшін **Жалпы мүмкіндіктер: Қолданба интеграциясы** функционалдық аймағында **Оқу** және **Жазу** құқықтары болуы керек.

Жауап әрекеттерін орындау үшін Active Directory көмегімен интеграцияны конфигурациялау

Active Directory интеграциясы дабыл әсер еткен немесе оған қатысты Active Directory пайдаланушылары үшін жауап әрекеттерін орындауға мүмкіндік береді.

Дабылдарға жауап беру үшін Active Directory интеграциясын конфигурациялау үшін Kaspersky Security Center Linux басқару серверінің 15.4 немесе одан кейінгі нұсқасын пайдалану керек.

Дабылдарға жауап беруге арналған Active Directory интеграциясы және домен контроллері сауалнамасын конфигурациялау кезінде сіз көрсеткен Active Directory домен контроллерін сканерлеу параметрлері (домен контроллерінің мекенжайы мен пайдаланушының тіркелгі деректері) — екі түрлі параметр. Жауап әрекеті орындалатын пайдаланушыда Active Directory есептік жазбасы бар екеніне көз жеткізу қажет болғандықтан, екі интеграцияны да конфигурациялау керек: сканерлеу және жауап беру үшін. Реті маңызды емес.

Интеграция параметрлері мұраланбайды және тек осы параметрлерді конфигурациялайтын басқару серверіне (физикалық немесе виртуалды) қолданылады.

Дабылдарға жауап беруде Active Directory интеграциясын конфигурациялау үшін:

1. Негізгі мәзірдегі басқару серверінің атауын басыңыз.

   Жалпы қойындысы таңдалған басқару сервері сипаттарының терезесі ашылады.

2. Келесі әрекеттердің бірін орындаңыз:

   - **Тарату нүктелері** бөлімін таңдап, қажетті тарату нүктесінің атын басыңыз, содан кейін ашылатын сипаттар терезесінде **Active Directory** бөлімін таңдаңыз.
   - **Active Directory жауабы** бөлімін таңдаңыз.

3. Оң жақ тақтадағы **Active Directory интеграциясы** ауыстырып-қосқышын қосыңыз.

   Кейінірек интеграцияны өшіргіңіз келсе, оны тек **Active Directory интеграциясы** ауыстырып-қосқышын өшіру арқылы барлық қосылым үшін орындауға болады. Бөлек қосылым үшін интеграцияны өшіре алмайсыз. Оның орнына қосылымды жоюға болады.

   > **Active Directory интеграциясы** ауыстырып-қосқышын қосқанда немесе өшіргенде, параметр **Active Directory жауабы** және **Тарату нүктелері** бөлімдері үшін қолданылады.

4. **Қосу** түймесін басып, Active Directory домен контроллерінің қосылымын жасаңыз.

5. Ашылған терезеде қосылымға арналған келесі параметрлерді көрсетіңіз:

   - **Домен контроллерінің мекенжайы**

     Компьютер атауы, мысалы: `server.mycompany.com`.

     Бірнеше мекенжайды көрсетуге болады. Мекенжайлары көрсетілген барлық домен контроллері бір доменге тиесілі болуы керек.

   - **Active Directory домен атауы**

     DNS толық домен аты, мысалы: `mycompany.com`

     Сондай-ақ SAM немесе NetBIOS атауын көрсетуге болады, мысалы: `mycompany`

     Кіші әріптерді пайдаланыңыз. Басқару сервері немесе тарату нүктесі үшін бірнеше қосылым жасасаңыз, әр қосылым үшін әртүрлі атауларды көрсетіңіз.

     > Жауап беру әрекеттерін орындау үшін осы өрісте көрсеткен Active Directory домен атауы ескертуде көрсетілген Active Directory домен атауына сәйкес келуі керек.

   - **Логин**

     Жауап әрекеттері орындалатын әкімші құқықтары бар Active Directory есептік жазбасының атауы.

   - **Құпиясөз**

     Әкімші құқықтары бар Active Directory есептік жазбасының құпиясөзі, ол бойынша жауап әрекеттері орындалады.

6. Қосылым күйін тексергіңіз келсе, **Байланысты тексеру** түймесін басыңыз.

   Қосылым сәтті орнатылса, **Қосылған** күйі көрсетіледі. Әйтпесе күй **Сәтсіз аяқталды** болады және сіз қосыла алмаған домен контроллерлерімен қате туралы хабар көрсетіледі.

Active Directory қызметіне қосылу жолын ескеру қажет: **Linux құрылғысынан немесе Windows құрылғысынан**.

Linux құрылғысынан қосылу

Әдепкісінше Linux құрылғысынан домен контроллеріне қосылу және аутентификациялау кезінде логика келесідей:

1. Басқару сервері немесе тарату нүктесі LDAPS арқылы домен контроллеріне қосылуға әрекеттенуде.

   LDAP сервері сертификатын қатаң тексеру орындалады.

2. Сертифтикатты тексеру үшін домен контроллері сертификатының жалпы бөлігін жүйенің сертификаттар қоймасына орналастырыңыз.

   Жүйе сертификатының органына (CA) ОЖ-ға тәуелді жол сертификаттар тізбегіне кіру үшін пайдаланылады.

   Мысалы:

   - /etc/ssl/certs/ca-certificates.crt — Debian негізіндегі операциялық жүйелерге арналған жол (Debian, Ubuntu, Astra).
   - /etc/pki/ca-trust/extracted/pem/tls-ca-bundle.pem — CentOS немесе Red Hat үшін жол.

3. LDAPS қосылымы сәтсіз болса, қате орын алады және басқа қосылым протоколы пайдаланылмайды.

> LDAPS ақаулары туындаған жағдайда, Kaspersky техникалық қолдау қызметіне хабарласуға болады.

Сертификатты жүйенің сертификаттар қоймасына орнатқыңыз келмесе, домен контроллері сертификатына жолды орнату үшін KLNAG_LDAP_SSL_CACERT жалауын пайдалануға болады. Ол үшін пәрменді іске қосыңыз:

```
klscflag -fset -pv klnagent -n KLNAG_LDAP_SSL_CACERT -t s -v "</path/to/domain-controller/cert>"
```

мұндағы `</path/to/domain-controller/cert>` — домен контроллері сертификатының жалпыға ортақ бөлігіне апаратын жол.

Мысалы, жол `"/var/opt/kaspersky/ldap_cert.crt"` болса, пәрмен — `klscflag -fset -pv klnagent -n KLNAG_LDAP_SSL_CACERT -t s -v "/var/opt/kaspersky/ldap_cert.crt"`

Windows құрылғысынан қосылу

Windows құрылғысынан домен контроллеріне қосылған және аутентификациялаған кезде, қосылым параметрлері домен арқылы анықталады.

Сізге тек мынаны қамтамасыз ету керек:

- LDAPS қосылған және құрылғыда 636 порты қолжетімді.
- Желілік экран немесе прокси-сервер арқылы домен контроллеріне қосылуға рұқсат берілген.

7. **Сақтау** түймесін басыңыз.

Терезе жабылып, қосылым қосылымдар кестесінде көрсетіледі.

Қосылымдар кестесінде келесі әрекеттерді орындауға болады:

- Қосылым параметрлерін өңдеу.

  Ол үшін қажетті қосылымға арналған **Домен контроллерінің мекенжайы** параметрі бар сілтемені басыңыз. Ашылған терезеде қажетті параметрлерді өзгертіп, **Сақтау** түймесін басыңыз.

  Тек **Логин** және **Құпиясөз** параметрлерін өңдей аласыз.

- Қосылымдарды жойыңыз.

  Ол үшін жойғыңыз келетін қосылымның жанындағы құсбелгіні қойып, құралдар тақтасындағы **Өшіру** түймесін басып, қосылымды жоюды растаңыз.

Kaspersky Automated Security Awareness Platform-мен интеграцияны конфигурациялау

Kaspersky Automated Security Awareness Platform (бұдан әрі KASAP деп аталады) интеграциясы KASAP оқыту курстарын дабылдармен байланысты пайдаланушыларға тағайындауға мүмкіндік береді.

Интеграция параметрлері мұраланбайды және тек осы параметрлерді конфигурациялайтын басқару серверіне (физикалық немесе виртуалды) қолданылады.

> Kaspersky Security Center Web Console-де интеграцияны конфигурацияламай тұрып, авторизация токенін жасап, KASAP жүйесінде API сұраулары үшін URL мекенжайын алуыңыз керек.

Kaspersky Automated Security Awareness Platform-мен интеграцияны конфигурациялау үшін:

1. Негізгі мәзірдегі басқару серверінің атауын басыңыз.

   Жалпы қойыншасында Басқару сервері сипаттары терезесі ашылады.

2. **KASAP** бөлімін таңдаңыз.
3. Оң жақ тақтада **KASAP интеграциясы** ауыстырып-қосқышын қосыңыз.
4. KASAP-қа қосылу үшін пайдаланылатын параметрлерді көрсетіңіз:

   - **API токені**: KASAP Open API-ге кіру үшін жасалған токен.
   - **URL**: API токенін жасау кезінде алынған API сұрауларына арналған URL.

- **Прокси-серверді пайдалану**: KASAP жүйесіне қосылу кезінде прокси-серверді пайдалануға мүмкіндік беретін ауыстырып-қосқыш.

  Ауыстырып-қосқыш әдепкісінше өшірулі болады.

5. Қажет болса, **Байланысты тексеру** түймесін басу арқылы көрсеткен параметрлерді тексеріңіз.

   Байланыс күйі көрсетіледі.

6. **Сақтау** түймесін басыңыз.

Kaspersky Automated Security Awareness Platform интеграциясы конфигурацияланған.

KASAP интеграция параметрлері сақталғаннан кейін, **Топтарды көру** түймесін басу арқылы KASAP оқыту топтарының тізімін көруге болады.

Қажет болса, топтар тізімі көрсетілгенде, **Топтарды жаңарту** түймесін басу арқылы оны жаңартуға болады.

Тізімді ашқаннан кейін оны жасыра алмайсыз. **KASAP интеграциясы** ауыстырып-қосқышын өшірсеңіз, KASAP топтарының тізімі көрсетілмейді.

Kaspersky Threat Intelligence Portal Sandbox интеграциясын конфигурациялау

Kaspersky Threat Intelligence Portal (бұдан әрі Kaspersky TIP деп аталады) интеграциясы Kaspersky Sandbox (корпоративтік желіден оқшауланған қауіпсіз орта) көмегімен **Карантин** бөліміне жіберілген файлдарды орындауға мүмкіндік береді.

Интеграция параметрлері мұраланбайды және тек осы параметрлерді конфигурациялайтын басқару серверіне (физикалық немесе виртуалды) қолданылады.

Интеграцияны конфигурациялау алдында Kaspersky TIP жүйесінде API сұраулары үшін авторизация токенін алуыңыз керек.

Kaspersky TIP Sandbox интеграциясын конфигурациялау үшін:

1. Негізгі мәзірдегі басқару серверінің атауын басыңыз.

   Жалпы қойыншасында Басқару сервері сипаттары терезесі ашылады.

2. **Kaspersky TIP** таңдаңыз.

3. Оң жақ тақтада **Біріктіру** ауыстырып-қосқышын қосыңыз.

   Kaspersky TIP жүйесіне қосылу параметрлері көрсетіледі.

   Интеграция параметрлерін конфигурациялап, сақтағаннан кейін, **Біріктіру** ауыстырып-қосқышын өшіріңіз, параметрлер жойылмайды, бірақ жауап әрекетін орындай алмайсыз.

4. **Токен қосу** түймесін басып, ашылған терезеде Kaspersky TIP жүйесінде бұрын алған токенді көрсетіңіз, содан кейін **Қосу** түймесін басыңыз.

   Терезе жабылады және API токені қосылады.

5. Kaspersky TIP қызметіне қосылу кезінде прокси-серверді пайдаланғыңыз келсе, **Прокси-серверді пайдалану** ауыстырып-қосқышын қосыңыз.

   Ауыстырып-қосқыш әдепкісінше өшірулі болады.

6. **Сақтау** түймесін басыңыз.

Kaspersky TIP Sandbox интеграциясы конфигурацияланды.

Енді қауіпті талдау үшін **Карантин** бөліміндегі файлдарды Kaspersky TIP Sandbox жүйесіне жіберуге болады. Файлдың максималды өлшемі – 100 МБ.

Kaspersky Security: Бизнеске арналған Кәсіби лицензиясы көптиістілікке қолдау көрсететіндіктен, файлдар **Карантин** қойылады. Бұл тенант деңгейіндегі бөлініс әкімші әрбір тенантқа қатысты арнайы TIP есептік жазбасын және API токенін пайдаланған кезде Kaspersky TIP Sandbox жүйесіне файлдарды жіберу және нәтижелерді қарау кезінде де қолданылады. Дегенмен барлық тенант үшін **Карантин** бөлімін орталықтандырылған басқару мүмкін емес, себебі карантин тізімі сервер иерархиясына сәйкес нысандарды көрсетпейді.

Дабылдарды атрибуттар бойынша топтау

Дабылдарды біріктіру бір оқиғаға қатысты болуы мүмкін дабылдарды анықтауға көмектеседі, зерттеу процесін жеңілдетеді.

Дабылдарды біріктіру функциясын қосу үшін келесі әрекеттерді орындау керек:

- Негізгі мәзірде **Дабылдар** ішкі бөлімін қосыңыз.
- Kaspersky Security: Бизнеске арналған Кәсіби лицензиясында басқару серверін белсендіріңіз, содан кейін басқарылатын қолданбаларға Kaspersky Security: Бизнеске арналған Кәсіби лицензия кілтін орналастырыңыз.

  Kaspersky Security: Бизнеске арналған Кәсіби функционалдығын сынақ режимінде сынақ лицензия пайдаланған кезде, алдымен қосалқы физикалық басқару серверін қосып, содан кейін бұл лицензияда осы серверді іске қосыңыз.

Kaspersky Next EDR Optimum лицензиясын пайдалансаңыз, басқарылатын құрылғыларда Kaspersky Security: Бизнеске арналған Кәсіби лицензиясы бойынша орнатылған қолданбаларды белсендірудің қажеті жоқ. Мұны тек жаңа құрылғылар үшін жасау керек (бар болса).
Kaspersky Security: Бизнеске арналған Кәсіби лицензиясы көптиістілікке қолдау көрсететіндіктен, лицензия кілтін басқарылатын қолданбаларға орталықтан таратуға болады. Лицензияны қосымша және виртуалды басқару серверлеріне автоматты түрде таратуға қолдау көрсетілмейді.

Дабылдарды құрылғы атауы, есептік жазба немесе хэш атауы (SHA256) бойынша біріктіруге болады.

> Дабылдар атрибут (ол бос болмаса) бойынша біріктіріледі.

Дабылдар кем дегенде бір атрибутты ортақ пайдаланса және топтағы кез келген басқа дабылдан кейін 24 сағат ішінде пайда болса, біріктіріледі.

Дабылдарды атрибуттар бойынша біріктіру үшін:

1. Негізгі мәзірде **Мониторинг** → **Дабылдар** тармағына өтіңіз.

2. Келесі әрекеттердің бірін орындаңыз:

   - **Дабылдарды біріктіру** ауыстырып-қосқышын қосыңыз, содан кейін дабылдарды біріктіру үшін бір немесе бірнеше атрибут таңдаңыз:

     - **Құрылғы атауы**
     - **Есептік жазба**
     - **Файл хэші (SHA256)**

     Құрылғы атауы және **Есептік жазба** атрибуттары әдепкісінше таңдалады.

   - Параметрлер белгішесін (⚙) басыңыз. Ашылған **Кесте параметрлері** тақтасында **Топтау** қойындысына өтіңіз. **Біріктіру тобының идентификаторы** опциясын таңдап, **Қолдану** түймесін басыңыз.

   Біріктіру қосылған кезде, дабылдар ең жаңадан ең ескісіне қарай **Оқиға уақыты** бойынша сұрыпталады. Қосымша сұрыптау опцияларына қолдау көрсетілмейді. Басқа топтау опциясы таңдалса, біріктіру өшеді.

Кестеде атрибуттар бойынша жинақталған дабылдар көрсетіледі. Біріктірілмеген дабылдар кестенің төменгі жағында көрсетіледі.

Әрбір дабыл біріктірілгеннен кейін тек бір топқа тағайындалады.

Cloud Discovery

Kaspersky Security Center Linux қолданбасы Windows операциялық жүйесімен жұмыс істейтін басқарылатын құрылғыларда бұлттық сервистерді пайдалануды бақылауға және қажетсіз бұлттық сервистерге кіруді бұғаттауға мүмкіндік береді. Cloud Discovery пайдаланушылардың браузерлер мен жұмыс үстелі қолданбалары арқылы осы қызметтерге қол жеткізу әрекеттерін бақылайды. Сонымен қатар, ол шифрланбаған қосылымдар арқылы (мысалы, HTTP протоколы бойынша) пайдаланушының бұлттық сервистерге қол жеткізу әрекеттерін бақылайды. Бұл функция бұлттық сервистерді жасырын рұқсатсыз пайдалануды анықтауға және тоқтатуға мүмкіндік береді.

Бұғаттау мүмкіндігі Kaspersky Security Center Linux бағдарламасын Kaspersky Next EDR Optimum немесе Kaspersky кеңейтілген анықтау және әрекет ету сарапшысы лицензиясы арқылы белсендірсеңіз ғана қолжетімді болады.

Бұғаттау мүмкіндігі Kaspersky Endpoint Security 11.2 for Windows және одан жоғары нұсқасын пайдаланған кезде ғана қолжетімді. Қауіпсіздік қолданбасының бұрынғы нұсқалары тек бұлттық сервистерді пайдалануды бақылауға мүмкіндік береді.

Cloud Discovery функциясын қосуға және оны қосу қажет қауіпсіздік саясаттарын немесе профильдерді таңдауға болады. Сондай-ақ, функцияны әрбір қауіпсіздік саясаты немесе профиль үшін бөлек қосуға немесе өшіруге болады. Пайдаланушылардың қолжетімділігін шектегіңіз келетін бұлттық сервистерге қол жеткізуді бұғаттай аласыз.

Қажетсіз бұлттық сервистерге қол жеткізуді бұғаттау үшін келесі шарттар орындалғанын тексеріңіз:

- Сіз Windows жүйесіне арналған Kaspersky Endpoint Security 11.2 немесе одан жоғарырақ нұсқаны пайдаланып жатырсыз. Қауіпсіздік қолданбасының бұрынғы нұсқалары тек бұлттық сервистерді пайдалануды бақылауға мүмкіндік береді.

- Сіз Kaspersky Next лицензиясын сатып алдыңыз, ол қажетсіз бұлттық сервистерге қол жеткізуді бұғаттауға мүмкіндік береді. Қосымша мәліметтер алу үшін Kaspersky Next анықтамасын қараңыз.

Бұлттық қызметтерге қол жеткізудің сәтті және бұғатталған әрекеттері туралы ақпарат Cloud Discovery веб-виджетінде және Cloud Discovery есептерінде көрсетіледі. Веб-виджет әрбір бұлттық сервистің тәуекел деңгейін де көрсетеді. Kaspersky Security Center Linux бұлттық сервистерді пайдалану туралы ақпаратты қауіпсіздік саясаттарымен немесе ол қосылған саясат профильдерімен қорғалған барлық басқарылатын құрылғылардан алады.

Веб-виджетті пайдаланып, Cloud Discovery функциясын қосу

Cloud Discovery функциясы бұлттық сервистерді пайдалану туралы ақпаратты олар қосылған қауіпсіздік саясаттарымен қорғалған барлық басқарылатын құрылғылардан алады. Cloud Discovery функциясы тек Windows жүйесіне арналған Kaspersky Endpoint Security саясаты үшін қосылуы немесе өшірілуі мүмкін.

Cloud Discovery функциясын қосудың екі жолы бар:

- Cloud Discovery веб-виджеті көмегімен.

- Windows жүйесіне арналған Kaspersky Endpoint Security саясатының сипаттарында.

  Windows жүйесіне арналған Kaspersky Endpoint Security саясат сипаттарындағы Cloud Discovery функциясын қосу жолы туралы толық ақпаратты Windows жүйесіне арналған Kaspersky Endpoint Security анықтамасының Cloud Discovery бөлімінен қараңыз.

Cloud Discovery функциясын тек Windows жүйесіне арналған Kaspersky Endpoint Security саясатының параметрлерінде өшіруге болатынын ескеріңіз.

Cloud Discovery функциясын қосу үшін **Жалпы функциялар: Негізгі функционалдылық** функционалды аймағында **Жазу** рұқсатыңыз болуы керек.

Cloud Discovery веб-виджеті көмегімен Cloud Discovery функциясын қосу үшін:

1. Kaspersky Security Center Linux ашыңыз.

2. Бағдарламаның негізгі терезесінде **Мониторинг** → **Бақылау тақтасы** бөліміне өтіңіз.

3. **Cloud Discovery** веб-виджетінде **Қосу** түймесін басыңыз.

Егер сізде Windows жүйесіне арналған Kaspersky Endpoint Security 12.4 нұсқасы орнатылған болса, Windows жүйесіне арналған Kaspersky Endpoint Security саясатының сипаттарында Cloud Discovery функциясын қосыңыз. Қосымша мәліметтер алу үшін Windows жүйесіне арналған Kaspersky Endpoint Security анықтамасының Cloud Discovery бөлімін қараңыз.

Егер сізде Windows жүйесіне арналған Kaspersky Endpoint Security 12.4 нұсқасынан төмен нұсқасы болса, Windows жүйесіне арналған Kaspersky Endpoint Security плагинін 12.5 нұсқасына дейін жаңартыңыз.

4. Ашылған **Cloud Discovery қызметін қосу** терезесінде функцияны қосқыңыз келетін қауіпсіздік саясаттарын таңдап, **Қосу** түймесін басыңыз.

   Келесі саясат параметрлері автоматты түрде қосылады: **Веб-беттермен өзара әрекет жасау үшін веб-трафикке сценарий енгізу**, **Веб-сеанстарды бақылау** және **Шифрланған қосылымдарды тексеру**.

Cloud Discovery функциясы іске қосылды және веб-виджет бақылау тақтасына қосылды.

Cloud Discovery веб-виджетін бақылау тақтасына қосу

Басқарылатын құрылғыларда бұлтты пайдалануды бақылау үшін **Cloud Discovery** веб-виджетін бақылау тақтасына қосуға болады.

Cloud Discovery веб-виджетін бақылау тақтасына қосу үшін **Жалпы функциялар: Негізгі функционалдылық** функционалды аймағында **Жазу** рұқсаты болуы керек.

Cloud Discovery веб-виджетін бақылау тақтасына қосу үшін:

1. Kaspersky Security Center Linux ашыңыз.
2. Бағдарламаның негізгі терезесінде **Мониторинг** → **Бақылау тақтасы** бөліміне өтіңіз.
3. **Виджетті қосу не қалпына келтіру** түймесін басыңыз.
4. Қолжетімді веб-виджеттердің тізімінде **Басқа** санатының жанындағы шеврон белгішесін (›) басыңыз.
5. **Cloud Discovery** веб-виджетін таңдап, **Қосу** түймесін басыңыз.

   Cloud Discovery өшірілсе, веб-виджетті пайдаланып, Cloud Discovery функциясын қосу бөліміндегі нұсқауларды орындаңыз.

Таңдалған веб-виджет бақылау тақтасының соңына қосылады.

Бұлттық сервистерді пайдалану туралы ақпаратты қарау

Cloud Discovery веб-виджеті бұлттық сервистерге қол жеткізу әрекеттері туралы ақпаратты көрсетеді. Веб-виджет әрбір бұлттық сервистің тәуекел деңгейін де көрсетеді. Kaspersky Security Center Linux бұлттық сервистерді пайдалану туралы ақпаратты олар қосылған қауіпсіздік профильдерімен қорғалған барлық басқарылатын құрылғылардан алады.

Көру алдында мыналарға көз жеткізіңіз:

- Cloud Discovery веб-виджеті мониторинг тақтасына қосылған.
- Cloud Discovery функциясы қосылған.
- **Жалпы функциялар: Негізгі функционалдылық** функционалды аймағында **Оқу** құқығыңыз бар.

Cloud Discovery веб-виджетін көру үшін:

1. Kaspersky Security Center Linux ашыңыз.
2. Бағдарламаның негізгі терезесінде **Мониторинг → Бақылау тақтасы** бөліміне өтіңіз.

   Cloud Discovery веб-виджеті бақылау тақтасында көрсетіледі.
3. **Cloud Discovery** веб-виджетінің сол жағында бұлттық сервистер санатын таңдаңыз.

   Веб-виджеттің оң жағындағы кесте пайдаланушылар жиі қатынасуға тырысатын таңдалған санаттағы бес сервиске дейін көрсетеді. Сәтті және бұғатталған қол жеткізу әрекеттері де ескеріледі.
4. Веб-виджеттің оң жағында қажетті қызметті таңдаңыз.

   Төмендегі кестеде осы сервиске жиі кіретін он құрылғыға дейін көрсетіледі. Бұл кестеде есептердің екі түрін жасауға болады: сәтті кіру әрекеттері туралы есеп және бұғатталған кіру әрекеттері туралы есеп.

   Сондай-ақ, осы кестеде белгілі бір құрылғы үшін бұлттық қызметке кіруді бұғаттай аласыз.

Веб-виджетте сұралған деректер көрсетіледі.

Көрсетілген веб-виджетте келесі әрекеттерді орындауға болады:

- Cloud Discovery есептерін көру үшін **Мониторинг → Есептер** тармағына өтіңіз.
- Таңдалған бұлттық қызметкер қол жеткізуді бұғаттаңыз немесе оған рұқсат беріңіз.

Бұғаттау мүмкіндігі Kaspersky Security Center Linux бағдарламасын Kaspersky Next EDR Optimum немесе Kaspersky кеңейтілген анықтау және әрекет ету сарапшысы лицензиясы арқылы белсендірсеңіз ғана қолжетімді болады.

Бұғаттау мүмкіндігі Kaspersky Endpoint Security 11.2 for Windows және одан жоғары нұсқасын пайдаланған кезде ғана қолжетімді. Қауіпсіздік қолданбасының бұрынғы нұсқалары тек бұлттық сервистерді пайдалануды бақылауға мүмкіндік береді.

Бұлттық сервистің тәуекел деңгейі

Cloud Discovery әрбір бұлттық сервис үшін тәуекел деңгейін анықтайды. Тәуекел деңгейі ұйымыңыздың қауіпсіздік талаптарына сәйкес келмейтін қызметтерді анықтауға көмектеседі. Мысалы, белгілі бір қызметке кіруді бұғаттау туралы шешім қабылдаған кезде тәуекел деңгейін ескеруіңізге болады.

Тәуекел деңгейі бағалау болып табылады және бұлттық сервис немесе өндіруші сапасы туралы ештеңе айтпайды. Тәуекел деңгейі – Kaspersky сарапшыларының ұсынысы.

Бұлттық қызметтердің тәуекел деңгейлері Cloud Discovery веб-виджетінде және барлық бақыланатын бұлттық қызметтер тізімінде көрсетіледі.

Қажетсіз бұлттық сервистерге қол жеткізуді бұғаттау

Пайдаланушылардың қолжетімділігін шектегіңіз келетін бұлттық сервистерге қол жеткізуді бұғаттай аласыз. Сондай-ақ, бұрын бұғатталған бұлттық сервистерге қол жеткізуге рұқсат бере аласыз.

Мысалы, белгілі бір қызметке қол жеткізуді бұғаттау туралы шешім қабылдағанда тәуекел деңгейін ескеруге болады.

Қауіпсіздік саясаты немесе саясат профилі үшін бұлттық сервистерге қол жеткізуге тыйым салуға немесе рұқсат беруге болады.

Қажетсіз бұлттық сервистерге қол жеткізуді бұғаттаудың екі жолы бар:

- Cloud Discovery веб-виджеті көмегімен.

  Бұл жағдайда сервистерге қол жеткізуді бір-бірден бұғаттай аласыз.

- Windows жүйесіне арналған Kaspersky Endpoint Security саясатының сипаттарында.

  Бұл жағдайда, сервистерге қол жеткізуді бір-бірден немесе бүкіл санатты бірден бұғаттай аласыз.

  Windows жүйесіне арналған Kaspersky Endpoint Security саясат сипаттарындағы Cloud Discovery функциясын қосу жолы туралы толық ақпаратты Windows жүйесіне арналған Kaspersky Endpoint Security анықтамасының Cloud Discovery бөлімінен қараңыз.

Веб-виджеттің көмегімен бұлттық сервисті бұғаттау немесе оған қол жеткізуге рұқсат беру үшін:

1. Cloud Discovery веб-виджетін ашып, қалаған бұлттық сервисті таңдаңыз.
2. **Қызметті ең көп пайдаланатын 10 құрылғы** тақтасында қызметті бұғаттағыңыз немесе рұқсат еткіңіз келетін қауіпсіздік саясатын немесе саясат профилін табыңыз.
3. **Саясаттағы не профильдегі қол жеткізу күйі** бағанындағы тиісті жолақта келесі әрекеттердің бірін орындаңыз:
   - Қызметті бұғаттау үшін ашылмалы тізімнен **Бұғатталған** тармағын таңдаңыз.
   - Қызметке рұқсат беру үшін ашылмалы тізімнен **Рұқсат етілген** тармағын таңдаңыз.
4. **Сақтау** түймесін басыңыз.

Таңдалған қызметке қол жеткізу, қауіпсіздік саясаты немесе саясат профилі арқылы бұғатталған немесе рұқсат етілген.

Оқиғаларды SIEM жүйелеріне экспорттау

Бұл бөлімде оқиғаларды SIEM жүйелеріне экспорттауды қалай конфигурациялау керектігі сипатталған.

Оқиғаларды SIEM жүйелеріне экспорттауды конфигурациялау

Kaspersky Security Center Linux оқиғаларды SIEM жүйелеріне экспорттауды келесі тәсілдердің бірі арқылы конфигурациялауға мүмкіндік береді: Syslog пішімін пайдаланатын кез келген SIEM жүйесіне экспорттау, LEEF және CEF пішімдерін пайдаланатын Kaspersky SIEM, QRadar, Splunk, ArcSight SIEM жүйелеріне экспорттау немесе оқиғаларды тікелей Kaspersky Security Center дерекқорынан SIEM жүйелеріне экспорттау. Осы сценарий аяқталғаннан кейін, Басқару сервері оқиғаларды автоматты түрде SIEM жүйесіне жібереді.

Алдын ала талаптар

Kaspersky Security Center Linux бағдарламасына оқиғаларды экспорттауды конфигурациялауды бастамас бұрын:

- Оқиғаларды экспорттау әдістері туралы көбірек біліңіз.
- Сізде жүйелік параметрлердің мәндері бар екеніне көз жеткізіңіз.

Сіз осы сценарийдің қадамдарын қалаған тәртіппен орындай аласыз.

Оқиғаларды SIEM жүйесіне экспорттау процесі келесі қадамдардан тұрады:

- **Kaspersky Security Center Linux-тен оқиғаларды алу үшін SIEM жүйесін конфигурациялау**

  Нұсқаулар: Оқиғаларды SIEM жүйесінде экспорттауды конфигурациялау.

- **SIEM жүйесіне экспорттағыңыз келетін оқиғаларды таңдау**

  SIEM жүйесіне экспорттағыңыз келетін оқиғаларды белгілеңіз. Kaspersky басқарылатын барлық бағдарламаларында туындайтын жалпы оқиғаларды белгілеңіз. Кейін белгілі бір басқарылатын бағдарлама үшін экспортталатын оқиғаларды белгілеуге болады.

- **Оқиғаларды SIEM жүйесіне экспорттауды конфигурациялау**

  Оқиғаларды келесі жолдармен экспорттауға болады:

  - TCP, UDP немесе TLS over TCP протоколдарын көрсетіңіз
  - Оқиғаларды тікелей Kaspersky Security Center дерекқорынан экспорттауды пайдалану (жалпыға ортақ көріністер жиынтығы Kaspersky Security Center дерекқорында берілген; осы жалпыға ортақ көріністердің сипаттамасын klakdb.chm құжатынан таба аласыз)

Нәтижелер

Оқиғаларды SIEM жүйесіне экспорттауды конфигурациялағаннан кейін, экспорттағыңыз келетін оқиғаларды таңдаған болсаңыз, экспорт нәтижелерін қарай аласыз.

Алдын ала шарттар

Оқиғаларды Kaspersky Security Center Linux-ге автоматты түрде экспорттауды конфигурациялау кезінде SIEM жүйесінің кейбір параметрлерін көрсету қажет. Kaspersky Security Center Linux конфигурациялауға дайындалу үшін осы параметрлерді ертерек нақтылау ұсынылады.

Оқиғаларды SIEM жүйесіне автоматты түрде экспорттауды конфигурациялау үшін келесі параметрлердің мәндерін білу керек:

- **SIEM жүйелік серверінің мекенжайы**

  Қолданылатын SIEM жүйесі орнатылған сервердің мекенжайы. Бұл мәнді SIEM жүйесінің конфигурацияларында нақтылау керек.

- **SIEM жүйесінің сервер порты**

  Kaspersky Security Center Linux және SIEM жүйесінің сервері арасында қосылым орнатылатын порт нөмірі. Бұл мәнді Kaspersky Security Center Linux конфигурацияларында және SIEM жүйесіндегі қабылдағыштың конфигурацияларында көрсету қажет.

- **Протокол**

  Хабарларды Kaspersky Security Center Linux-тен SIEM жүйесіне жіберу үшін қолданылатын протокол. Бұл мәнді Kaspersky Security Center Linux конфигурацияларында және SIEM жүйесіндегі қабылдағыштың конфигурацияларында көрсету қажет.

Оқиғаларды экспорттау туралы

Kaspersky Security Center Linux бағдарламасы, басқарылатын бағдарламаларға орнатылған Kaspersky Басқару сервері мен бағдарламаларының жұмысы барысында орын алған оқиғалар туралы ақпаратты алуға мүмкіндік береді. Оқиғалар туралы ақпарат Басқару серверінің дерекқорында сақталады.

Сіз қауіпсіздік жүйелерінің мониторингін қамтамасыз ететін және әртүрлі шешімдерден деректерді шоғырландыратын ұйымдастырушылық және техникалық деңгейлерде қауіпсіздік мәселелерімен жұмыс істейтін орталықтандырылған жүйелерде оқиғалар экспортын қолдана аласыз. Оларға желілік аппараттық жасақтама мен қолданбалардың оқиғалары мен қауіпсіздік жүйелерінің ескертулерін нақты уақыт режимінде талдауды қамтамасыз ететін SIEM жүйелері, сондай-ақ қауіпсіздікті басқару орталықтары (Security Operation Center, SOC) қатысты болып келеді.

SIEM жүйелері деректерді көптеген көздерден, сонымен қатар желілерден, қауіпсіздік жүйелерінен, серверлерден, дерекқорлардан және қолданбалардан алады. Сондай-ақ, олар өңделген деректерді біріктіру функциясын қамтамасыз ете отырып, сізге критикалық оқиғаларды жіберіп алуға мүмкіндік бермейді. Бұдан бөлек, бұл жүйелер әкімшілерді дереу шешім қабылдауды талап ететін қауіпсіздік жүйесінің мәселелері туралы хабардар ету үшін дабыл сигналдары мен байланысты оқиғаларды автоматты талдауды орындайды. Хабарландырулар индикаторлар тақтасында көрсетілуі немесе бөгде арналар бойынша, мысалы, электрондық пошта арқылы таратылуы мүмкін.

Оқиғаларды Kaspersky Security Center Linux-тен сыртқы SIEM жүйелеріне экспорттау рәсіміне екі тарап қатысады: оқиғаларды жіберуші – Kaspersky Security Center Linux және оқиғаларды алушы – SIEM жүйесі. Оқиғаларды экспорттау сәтті аяқталуы үшін, қолданылатын SIEM жүйесінде де, Kaspersky Security Center Linux Басқару консолінде де конфигурациялауды орындау керек. Алдымен қай жағын конфигурациялағаныңыз маңызды емес. Kaspersky Security Center Linux жүйесінде оқиғаларды жіберуді конфигурациялауға, содан кейін SIEM жүйесі арқылы оқиғаларды қабылдауды конфигурациялайға немесе керісінше орындауға болады.

Оқиғаларды Kaspersky Security Center Linux-тен жіберу тәсілдері

Оқиғаларды Kaspersky Security Center Linux-тен сыртқы жүйелерге жіберудің үш тәсілі бар:

- Оқиғаларды Syslog протоколы бойынша кез келген SIEM жүйесіне жіберу.

  Syslog протоколын пайдаланып, Kaspersky Security Center Басқару серверінде және басқарылатын құрылғыларға орнатылған Kaspersky бағдарламаларында орын алған кез келген оқиғаларды жіберуге болады. Syslog протоколы – хабарларды тіркеудің стандартты протоколы. Сіз осы протоколды оқиғаларды кез келген SIEM жүйесіне экспорттау үшін қолдана аласыз.

  Бұл үшін SIEM жүйесіне жібергіңіз келетін оқиғаларды белгілеу керек. Сіз оқиғаларды Kaspersky Security Center Web Console көмегімен белгілей аласыз. SIEM жүйесіне тек белгіленген оқиғалар ғана жіберелетін болады. Сіз ештеңе белгілемеген болсаңыз, ешқандай оқиғалар жіберілмейді.

- Оқиғаларды Kaspersky SIEM, QRadar, Splunk және ArcSight жүйелеріне CEF және LEEF протоколдары бойынша жіберу.

  CEF және LEEF протоколдарын жалпы оқиғаларды экспорттау үшін қолдануға болады. Оқиғаларды CEF және LEEF протоколдары бойынша экспорттау кезінде, белгіленген экспортталатын оқиғаларды таңдау мүмкіндігіңіз жоқ. Мұның орнына, барлық жалпы оқиғалардың экспорты орындалады. Kaspersky Security Center Linux оқиғаларын CEF және LEEF форматындағы оқиғаларға түрлендіру үшін siem_conversion_rules.xml file файлын пайдалану қажет. Бұл файлда Kaspersky Security Center Linux оқиға атрибуттарының тізімі және CEF және LEEF форматындағы оқиғалардың сәйкес атрибуттары бар. Сондай-ақ siem_conversion_rules.xml файлында оқиғаларға сәйкес хабарларды жасау ережелері бар. Бұл файл Kaspersky Security Center Linux тарату жиынтығының құрамына кіреді.

  Syslog протоколынан айырмашылығы, CEF және LEEF протоколдары әмбебап болып саналады. CEF және LEEF протоколдары тиісті SIEM жүйелерге (Kaspersky SIEM, QRadar, Splunk және ArcSight) арналған. Сол себепті, SIEM жүйесінде келесі протоколдардың бірі бойынша оқиғаларды экспорттауды таңдау кезінде қажетті талдағыш қолданылады.

- Тікелей Kaspersky Security Center Linux дерекқорынан кез келген SIEM жүйесіне

  Осы оқиғаларды экспорттау тәсілі, оқиғаларды SQL сұрауларының көмегімен дерекқордың көпшілікке қолжетімді көріністерінен тікелей алу үшін қолдануы мүмкін. Сұрау салу нәтижелері .xml файлына сақталады, оны сыртқы жүйеге арналған кіріс деректері ретінде қолдануға болады. Тікелей дерекқордан тек көпшілікке қолжетімді көріністерде қолжетімді оқиғаларды ғана экспорттауға болады.

SIEM жүйесінің оқиғаларды алуы

SIEM жүйесі Kaspersky Security Center Linux-ден алынатын оқиғаларды қабылдауы және дұрыс талдауы тиіс. Бұл үшін SIEM жүйесін конфигурациялауды орындау керек. Конфигурация нақты қолданылатын SIEM жүйесіне байланысты болып келеді. Алайда, барлық SIEM жүйелерінің конфигурацияларында қабылдағыш пен талдағышты конфигурациялау сияқты бірқатар жалпы кезеңдер бар.

Оқиғаларды SIEM жүйесінде экспорттауды конфигурациялау туралы

Оқиғаларды Kaspersky Security Center Linux-тен сыртқы SIEM жүйелеріне экспорттау рәсіміне екі тарап қатысады: оқиғаларды жіберуші – Kaspersky Security Center Linux және оқиғаларды алушы – SIEM жүйесі. Оқиғаларды экспорттау, қолданылатын SIEM жүйесінде және Kaspersky Security Center Linux-де конфигурациялануы керек.

SIEM жүйесінде орындалатын конфигурациялар сіз қолданатын жүйеге байланысты болып келеді. Жалпы жағдайда, алынған хабарларды өрістерге жаю үшін, барлық SIEM жүйелеріне хабар қабылдағышты және қажет болса, хабар талдағышты конфигурациялау керек.

Хабар қабылдағышты конфигурациялау

SIEM жүйесі үшін Kaspersky Security Center Linux жіберетін оқиғаларды қабылдау үшін қабылдағышты конфигурациялау қажет. Жалпы жағдайда, SIEM жүйесінде келесі параметрлерді көрсету керек:

- **Экспорттау протоколы**

  UDP, TCP немесе TLS, TCP арқылы хабарларын жіберу протоколы. Kaspersky Security Center Linux-де оқиғаларды жіберу үшін таңдалған протоколды көрсету керек.

- **Порт**

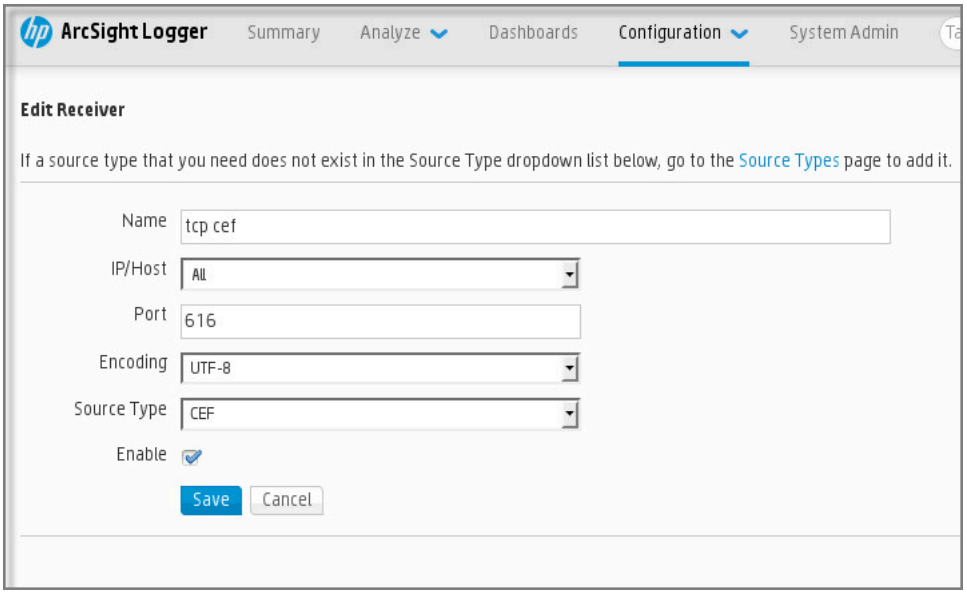
  Kaspersky Security Center Linux-ке қосылуға арналған порт нөмірін көрсетіңіз. Бұл порт оқиғаны SIEM жүйесіне экспорттауды конфигурациялау кезінде Kaspersky Security Center Linux жүйесінде көрсеткен портқа сәйкес келуі керек.

- **Күн пішімі**

  Syslog, CEF немесе LEEF пішімін көрсетіңіз.

Қолданылатын SIEM жүйесіне байланысты, хабар қабылдағыштың қосымша параметрлерін көрсету қажет болуы мүмкін.

Төмендегі суретте, қабылдағышты ArcSight-та конфигурациялау мысалы келтірілген.



Қабылдағышты ArcSight-та конфигурациялау

Хабарлар талдағышы

Экспортталатын оқиғалар SIEM жүйесіне хабарлар түрінде беріледі. Содан соң, оқиғалар туралы ақпарат SIEM жүйесіне тиісінше берілуі үшін, осы хабарларға талдағыш қолданылады. Хабарлар талдағышы SIEM жүйесіне кіріктірілген; ол хабарды хабар идентификаторы, маңыздылық деңгейі, сипаттамасы, параметрлері сияқты өрістерге бөлу үшін қолданылады. Нәтижесінде, SIEM жүйесі Kaspersky Security Center Linux-ден алынған оқиғаларды SIEM жүйесінің дерекқорында сақталатындай етіп өңдеу мүмкіндігіне ие.

CEF және LEEF пішіміндегі оқиғаларды экспорттау туралы

CEF және LEEF пішімдерін SIEM жүйелеріне жалпы оқиғаларды, саясатты өзгерту оқиғаларын және Kaspersky бағдарламалары Басқару серверіне жіберген оқиғаларды экспорттау үшін пайдалануға болады. Экспортталатын оқиғалар жиынтығы алдын ала анықталған, экспортталатын оқиғаларды таңдау мүмкіндігі жоқ. Оқиғаларды SIEM жүйесіне (Kaspersky SIEM, QRadar, ArcSight немесе Splunk) жібермей тұрып, siem_conversion_rules.xml файлында көрсетілген ережелерді пайдалану арқылы Kaspersky Security Center оқиғаларын CEF және LEEF форматындағы оқиғаларға интерпретациялау қажет.

Экспорттау пішімін, сіз қолданатын SIEM жүйесіне байланысты таңдауға болады. Келесі кестеде SIEM жүйелері және оларға сәйкес экспорттау пішімдері келтірілген.

Оқиғаларды SIEM жүйесіне экспорттау пішімдері

SIEM жүйесі	Экспорттау пішімі
Kaspersky SIEM	CEF
ArcSight	CEF

SIEM жүйесі	Экспорттау пішімі
Splunk	CEF
QRadar	LEEF

- LEEF (Log Event Extended Format) — IBM Security QRadar SIEM үшін реттелген оқиға пішімі. QRadar платформасы LEEF оқиғаларын ендіріп, анықтап, өңдей алады. LEEF протоколы үшін UTF-8 кодтамасы қолданылуы керек. LEEF протоколы туралы толығырақ ақпаратты IBM Knowledge Center веб-бетінен қараңыз.

- CEF – бұл әртүрлі желілік құрылғылар мен қолданбалардың қауіпсіздік жүйесі ақпаратының үйлесімділігін жақсартатын "ашық журнал" типті басқару стандарты. CEF протоколы, кәсіпорынды басқару жүйелері талдауға арналған деректерді оңай алуы және біріктіруі үшін оқиғалар журналының жалпы пішімін пайдалануға мүмкіндік береді. CEF протоколы үшін UTF-8 кодтамасы қолданылуы керек.

Автоматты түрде экспорттау кезінде Kaspersky Security Center Linux жалпы оқиғаларды SIEM жүйесіне жібереді. Оқиғаларды автоматты түрде экспорттау қосылғаннан кейін бірден басталады. Бұл бөлімде оқиғаларды автоматты түрде экспорттауды қосу рәсімі сипатталған.

Оқиғаларды CEF немесе LEEF форматына түрлендіру

Оқиғаларды SIEM жүйесіне (Kaspersky SIEM, QRadar, ArcSight немесе Splunk) жібермей тұрып, siem_conversion_rules.xml файлында көрсетілген ережелерді пайдалану арқылы Kaspersky Security Center Linux оқиғаларын CEF және LEEF форматындағы оқиғаларға интерпретациялау қажет. Бұл файл Kaspersky Security Center Linux тарату жиынтығының құрамына кіреді.

siem_conversion_rules.xml файлында оқиғаларды CEF және LEEF форматына түрлендіру үшін алдын ала анықталған интерпретациялау ережелері бар. Оқиғаларды интерпретациялаудың қосымша ережелерін пайдаланғыңыз келсе, оларды файлға қолмен қосуға болады.

siem_conversion_rules.xml файлы келесі бөлімдерді қамтиды:

- `<product name="SP_QRADAR" vendor="IBM">`

  Бұл бөлімде оқиғаларды LEEF форматында жасау ережелері бар, оны QRadar SIEM жүйесіне экспорттауға болады.

- `<product name="SP_ARCSIGHT" vendor="HP">`.

  Бұл бөлімде оқиғаларды CEF форматында жасау ережелері бар, оны ArcSight немесе Splunk SIEM SIEM жүйесіне экспорттауға болады.

- `<product name="Kaspersky SIEM" vendor="Kaspersky">`.

  Бұл бөлімде оқиғаларды CEF форматында жасау ережелері бар, оны KUMA-ға экспорттауға болады.

Әрбір бөлімде `<common>` ішкі бөлімі бар, ол жерде Kaspersky Security Center Linux оқиға атрибуттары және оқиғалардың LEEF форматындағы тиісті атрибуттары орналасқан. Бұл жалпы атрибуттар экспортталатын оқиғалардың барлық түрі үшін пайдаланылады.

Сондай-ақ әрбір бөлімде `<event>` ішкі бөлімдері бар. Әрбір `<event>` ішкі бөлімінде `<common>` бөліміндегіге қосылатын қосымша атрибуттар бар.

siem_conversion_rules.xml файлына жаңа оқиғаны жасау ережесін қолмен қосуға болады.

Жаңа оқиғаны жасау ережесін қосу үшін:

1. Жаңа `<event>` ішкі бөлімін `<product name="SP_QRADAR" vendor="IBM">`, `<product name="SP_QRADAR" vendor="IBM">` не `<product name="Kaspersky SIEM" vendor="Kaspersky">` бөліміне қосыңыз, содан кейін қажет болса, қосымша оқиға атрибуттарын көрсетіңіз.

2. Оқиға тек жалпы төлсипаттардан тұрса, `<event>` ішкі бөлімі бос болады.

siem_conversion_rules.xml

```
<conversion_rules>
    <product name="SP_QRADAR" vendor="IBM">
        <common> <!-- Common Kaspersky Security Center Linux event attributes and corresponding LEEF event
attributes -->
            <param name="KLSPLG_HOST_DISP_NAME" type="STRING_T">
                <attr name="EVC_EV_DISP_HOST_NAME" type="AT_STRING" limit="255"/>
            </param>
            ...
        </common>
        <event id="GNRL_EV_VIRUS_FOUND"> <!-- Generation rule for the GNRL_EV_VIRUS_FOUND event with additional
attributes -->
            <param name="GNRL_EA_PARAM_1" type="STRING_T">
                <attr name="EVC_EV_SHA256" type="AT_STRING" limit="255"/>
            </param>
            ...
        </event>
...
</product>
    <product name="SP_ARCSIGHT" vendor="HP">
        <common> <!-- Common Kaspersky Security Center Linux event attributes and corresponding LEEF event
attributes -->
            <param name="KLSPLG_HOST_DISP_NAME" type="STRING_T">
                <attr name="dhost" type="AT_STRING" limit="1023"/>
            </param>
            ...
        </common>
        <event id="GNRL_EV_VIRUS_FOUND">
            <param name="GNRL_EA_PARAM_1" type="STRING_T">
                <attr name="cs4" type="AT_STRING" limit="255"/>
                <attr name="cs4Label" type="AT_STRING" val="SHA256"/>
            </param>
            ...
</product>
    <product name="Kaspersky SIEM" vendor="Kaspersky">
        <common> <!-- Common Kaspersky Security Center Linux event attributes and corresponding LEEF event
attributes -->
            <param name="KLSPLG_HOST_DISP_NAME" type="STRING_T">
                <attr name="dhost" type="AT_STRING" limit="1023"/>
            </param>
            ...
        </common>
        <event id="GNRL_EV_VIRUS_FOUND">
            <param name="GNRL_EA_PARAM_1" type="STRING_T">
                <attr name="cs4" type="AT_STRING" limit="255"/>
                <attr name="cs4Label" type="AT_STRING" val="SHA256"/>
            </param>
            ...
</product>
</conversion_rules>
```

SIEM жүйелеріне Syslog пішімінде экспортталатын оқиғаларды таңдау

Оқиғаларды автоматты түрде экспорттауды қосқаннан кейін, сыртқы SIEM жүйесіне қандай оқиғалар экспортталатынын таңдау керек.

Оқиғаларды Syslog пішімінде келесі шарттардың біріне негізделген сыртқы жүйеге экспорттауды конфигурациялауға болады:

- Жалпы оқиғаларды таңдау. Егер сіз саясатта, оқиғаның сипаттарында немесе Басқару сервері сипаттарында экспортталатын оқиғаларды таңдасаңыз, онда осы саясатпен басқарылатын барлық бағдарламаларда орын алған таңдалған оқиғалар SIEM жүйесіне жіберіледі. Егер экспортталатын оқиғалар саясатта таңдалған болса, сіз осы саясатпен басқарылатын жеке бағдарлама үшін оларды қайта анықтай алмайсыз.

- Басқарылатын бағдарлама үшін оқиғаларды таңдау. Егер сіз басқарылатын құрылғыларда орнатылған басқарылатын бағдарлама үшін экспортталатын оқиғаларды таңдасаңыз, онда SIEM жүйесіне тек осы бағдарламада орын алған оқиғалар ғана жіберіледі.

Саясатты өзгерту оқиғалары үшін сіз барлық осындай оқиғаларды SIEM жүйесіне экспорттауды тек қосуға немесе өшіруге болады.

Kaspersky бағдарламалары оқиғаларын Syslog пішімінде экспорттау үшін таңдау

Егер сіз басқарылатын құрылғыларда орнатылған белгілі бір басқарылатын бағдарламада болған оқиғаларды экспорттағыңыз келсе, бағдарлама саясатында экспортталатын оқиғаларды таңдаңыз. Бұл жағдайда, белгіленген оқиғалар саясаттың әрекет ету ауқымына кіретін барлық құрылғылардан экспортталады.

Белгілі бір басқарылатын бағдарлама үшін экспортталатын оқиғаларды белгілеу үшін:

1. Бағдарламаның негізгі терезесінде **Активтерді басқару** → **Саясаттар** бөліміне өтіңіз.
2. Оқиғаларды белгілеу қажет бағдарлама саясатын таңдаңыз.

   Саясат сипаттары терезесі ашылады.
3. **Оқиғаларды конфигурациялау** бөліміне өту.
4. SIEM жүйесіне экспорттау қажет оқиғалардың жанында жалаушаларды қойыңыз.
5. **Syslog көмегімен SIEM жүйесіне экспорттауды белгілеу** түймесін басыңыз.

   Сондай-ақ, оқиғаға сілтеме арқылы ашылатын **Оқиғаларды тіркеу** бөлімінде SIEM жүйесіне экспортталатын оқиғаны таңдауға болады.
6. Жалауша (✓), сіз SIEM жүйесіне экспорттау үшін белгілеген оқиға немесе оқиғалар үшін **Syslog** бағанында пайда болады.
7. **Сақтау** түймесін басыңыз.

Белгіленген оқиғалар басқарылатын бағдарламадан SIEM жүйесіне экспорттауға дайын.

Белгілі бір басқарылатын құрылғы үшін SIEM жүйесіне қандай оқиғаларды экспорттау керектігін атап өтуге болады. Егер экспортталатын оқиғалар бұған дейін бағдарлама саясатында таңдалған болса, сіз басқарылатын құрылғы үшін таңдалған оқиғаларды қайта анықтай алмайсыз.

Басқарылатын құрылғыға арналған оқиғаларды таңдау үшін:

1. Бағдарламаның негізгі терезесінде **Активтерді басқару** → **Активтер (құрылғылар)** бөліміне өтіңіз.

   Басқарылатын құрылғылардың тізімі көрсетіледі.

2. Басқарылатын құрылғылар тізімінде қажетті құрылғының атауы бар сілтемеден өтіңіз.

   Таңдалған құрылғы сипаттары терезесі ашылады.

3. **Бағдарламалар** бөліміне өту.

4. Бағдарламалар тізімінде қажетті бағдарламаның атауы бар сілтемеге өтіңіз.

5. **Оқиғаларды конфигурациялау** бөліміне өту.

6. SIEM жүйесіне экспорттау қажет оқиғалардың жанында жалаушаларды қойыңыз.

7. **Syslog көмегімен SIEM жүйесіне экспорттауды белгілеу** түймесін басыңыз.

   Сондай-ақ, оқиғаға сілтеме арқылы ашылатын **Оқиғаларды тіркеу** бөлімінде SIEM жүйесіне экспортталатын оқиғаны таңдауға болады.

8. Жалауша (✓), сіз SIEM жүйесіне экспорттау үшін белгілеген оқиға немесе оқиғалар үшін **Syslog** бағанында пайда болады.

Енді SIEM жүйесіне экспорттауды теңшелген болса, Басқару сервері SIEM жүйесіне таңдалған оқиғаларды жібереді.

Syslog пішімінде экспорттау үшін жалпы оқиғаларды таңдау

Басқару сервері Syslog пішімін пайдаланып, SIEM жүйелеріне экспорттайтын жалпы оқиғаларды белгілей аласыз.

SIEM жүйесіне экспортталатын жалпы оқиғаларды таңдау үшін:

1. Негізгі мәзірде келесі әрекеттердің бірін орындаңыз:

   - Басқару серверінің атауын басыңыз.
   - **Активтерді басқару** → **Саясаттар** бөліміне өтіп, саясат сілтемесін басыңыз.

2. Ашылған терезеде **Оқиғаларды конфигурациялау** қойыншасына өтіңіз.

3. **Syslog көмегімен SIEM жүйесіне экспорттауды белгілеу** түймесін басыңыз.

   Сондай-ақ, оқиғаға сілтеме арқылы ашылатын **Оқиғаларды тіркеу** бөлімінде SIEM жүйесіне экспортталатын оқиғаны таңдауға болады.

4. Жалауша (✓), сіз SIEM жүйесіне экспорттау үшін белгілеген оқиға немесе оқиғалар үшін **Syslog** бағанында пайда болады.

Енді SIEM жүйесіне экспорттауды тоқшелген болса, Басқару сервері SIEM жүйесіне таңдалған оқиғаларды жібереді.

Syslog пішіміндегі оқиғаларды экспорттау туралы

Syslog пішімін қолдана отырып, басқарылатын құрылғыларда орнатылған Kaspersky Басқару сервері мен басқа да бағдарламаларында орын алған оқиғаларды SIEM жүйелеріне экспорттауға болады.

Syslog – бұл хабарларды тіркеудің стандартты протоколы. Бұл протокол, хабарды құрастыратын бағдарламалық жасақтаманы, хабарлар сақталатын жүйені және хабарлар бойынша талдау мен есептілікті орындайтын бағдарламалық жасақтаманы бөлуге мүмкіндік береді. Әрбір хабарға, хабар құрастырылған бағдарламалық жасақтаманың түрін көрсететін құрылғының коды және маңыздылық деңгейі беріледі.

Syslog пішімі Internet Engineering Task Force жариялаған Request for Comments (RFC) құжаттарымен айқындалады. RFC 5424 стандарты оқиғаларды Kaspersky Security Center Linux-тен сыртқы жүйелерге экспорттау үшін қолданылады.

Kaspersky Security Center Linux-де оқиғаларды Syslog пішімінде сыртқы жүйелерге экспорттауды конфигурациялауға болады.

Экспорттау процесі екі қадамнан тұрады:

1. Оқиғаларды автоматты түрде экспорттауды қосу. Бұл қадамда Kaspersky Security Center Linux бағдарламасы, оқиғалар SIEM жүйесіне жіберілетіндей етіп конфигурацияланады. Автоматты түрде экспорттау қосылғаннан кейін, Kaspersky Security Center Linux-тен оқиғаларды жіберу бірден басталады.

2. Сыртқы жүйеге экспортталатын оқиғаларды таңдау. Бұл қадамда қандай оқиғалардың SIEM жүйесіне экспортталтанын таңдау керек.

Оқиғаларды SIEM жүйесіне экспорттау үшін Kaspersky Security Center Linux конфигурациялау

Оқиғаларды SIEM жүйесіне экспорттау үшін Kaspersky Security Center Linux жүйесінде экспорттау процесін конфигурациялау керек.

Оқиғаларды SIEM жүйесіне (Kaspersky SIEM, QRadar, ArcSight немесе Splunk) жібермей тұрып, siem_conversion_rules.xml файлында көрсетілген ережелерді пайдалану арқылы Kaspersky Security Center Linux оқиғаларын CEF және LEEF форматындағы оқиғаларға интерпретациялау қажет.

Kaspersky Security Center Web Console веб-консолінен SIEM жүйелеріне экспорттауды конфигурациялау үшін:

1. Негізгі мәзірдегі басқару серверінің атауын басыңыз.

   Басқару серверінің сипаттары терезесі ашылады.

2. **Жалпы** қойындысында **SIEM жүйесіне экспорттау** бөлімін таңдаңыз.

3. **Параметрлер** сілтемесінен өтіңіз.

   Параметрлерді экспорттау бөлімі ашылады.

4. **Параметрлерді экспорттау** бөлімінде параметрлерді көрсетіңіз:

   - **SIEM жүйелік серверінің мекенжайы**

     Қолданылатын SIEM жүйесі орнатылған сервердің мекенжайы. Бұл мәнді SIEM жүйесінің конфигурацияларында нақтылау керек.

   - **SIEM жүйелік порты**

     Kaspersky Security Center Linux және SIEM жүйесінің сервері арасында қосылым орнатылатын порт нөмірі. Бұл мәнді Kaspersky Security Center Linux конфигурацияларында және SIEM жүйесіндегі қабылдағыштың конфигурацияларында көрсету қажет.

   - **Протокол**

     SIEM жүйесіне хабар жіберу протоколын таңдаңыз. TCP протоколының орнына TCP, UDP немесе TLS таңдауға болады.

     TLS over TCP таңдасаңыз, келесі TLS параметрлерін көрсетіңіз:

     - **Сервердің аутентификация**

       Сервердің аутентификация өрісінде **Сенімді сертификаттар** немесе **SHA сәйкестендіру белгілері** мәндерін таңдауға болады:

       - **Сенімді сертификаттар**. Сертификаттардың толық тізбегін (түбірлік сертификатты қоса) сенімді сертификаттау орталығынан (CA) ала аласыз және оны Kaspersky Security Center Linux бағдарламасына жүктей аласыз. Kaspersky Security Center Linux бағдарламасы SIEM жүйесінің сертификаттар тізіміне сенімді сертификаттау орталығы да қол қойғанын тексереді.

         Сенімді сертификатты қосу үшін **Сертификаттау орталығының файлын таңдау** түймесін басып, сертификатты жүктеп алыңыз.

       - **SHA сәйкестендіру белгілері**. Kaspersky Security Center Linux жүйесінде SIEM жүйесінің бүкіл сертификаттар тізбегінің (соның ішінде түбірлік сертификаттың) SHA1 саусақ іздерін көрсетуге болады. SHA1 сәйкестендіру белгісін қосу үшін, оны **Саусақ іздері** өрісіне енгізіп, **Қосу** түймесін басыңыз.

       > **Клиенттік аутентификация қосу** көмегімен Kaspersky Security Center Linux түпнұсқалық растамасы үшін сертификатты жасай аласыз. Осылайша, сіз Kaspersky Security Center Linux шығарған өздігінен қол қойылған сертификатты қолданасыз. Бұл жағдайда, SIEM жүйесінің серверінің түпнұсқалық растамасы үшін сенімді сертификатты да, SHA сәйкестендіру белгісін де пайдалануға болады.

     - **Тақырып атауын/Тақырыптың баламалы атауын қосу**

       Субъект атауы – сертификат алуға себеп болған домендік атау. SIEM жүйесі серверінің домендік атауы SIEM жүйесінің сервері сертификаты субъектісінің атауына сәйкес келмесе, Kaspersky Security Center Linux бағдарламасы SIEM жүйесінің серверіне қосыла алмайды. Алайда, сертификатта атау өзгерген жағдайда, SIEM жүйесінің сервері өзінің домендік атауын өзгерте алады. Бұл жағдайда, сіз **Тақырып атауын/Тақырыптың баламалы атауын қосу** өрісіндегі субъектілердің аттарын көрсете аласыз. Егер аталған субъектілердің кез келген атауы SIEM жүйесі сертификаты субъектісінің атауына сәйкес келсе, Kaspersky Security Center Linux бағдарламасы SIEM жүйесі серверінің сертификатын тексереді.

- **Клиенттік аутентификация қосу**

  Клиенттің түпнұсқалық растамасы үшін сіз өзіңіздің сертификатыңызды енгізе аласыз немесе оны Kaspersky Security Center Linux бағдарламасында жасай аласыз.

  - **Сертификатты енгізу**. Сіз кез келген көзден, мысалы, кез келген сенімді сертификаттау орталығынан алынған сертификатты пайдалана аласыз. Сертификаттың келесі түрлерінің бірін пайдаланып, сертификат пен оның жеке кілтін көрсетуіңіз қажет:

    - **X.509 сертификаты PEM**. Сертификаты бар файлды **Сертификаты бар файл** өрісіне және жеке кілті бар файлды **Кілті бар файл** өрісіне жүктеп салыңыз. Екі файл да бір-біріне тәуелді емес және файлдарды жүктеу реті маңызды емес. Екі файл да жүктелген кезде, **Құпиясөзді немесе сертификатты растау** өрісінде жеке кілтті шифрсыздау үшін құпиясөзді енгізіңіз. Жеке кілт шифрланбаған болса, құпиясөздің мәні бос болуы мүмкін.

    - **X.509 сертификаты PKCS12**. Сертификат пен оның жеке кілтін қамтитын бір файлды **Сертификаты бар файл** өрісіне жүктеңіз. Файл жүктелгеннен кейін, **Құпиясөзді немесе сертификатты растау** өрісінде жеке кілтті шифрсыздау үшін құпиясөзді көрсетіңіз. Жеке кілт шифрланбаған болса, құпиясөздің мәні бос болуы мүмкін.

  - **Кілт жасау**. Сіз Kaspersky Security Center Linux бағдарламасында өздігінен қол қойылған сертификатты жасай аласыз. Нәтижесінде, Kaspersky Security Center Linux өздігінен қол қойылған сертификатты сақтайды және сіз сертификаттың жария бөлігін немесе SHA1 сәйкестендіру белгісін SIEM жүйесіне жібере аласыз.

- **Деректер пішімі**

  SIEM жүйесінің талаптарына байланысты Kaspersky SIEM, IBM QRadar SIEM, ArcSight, Splunk немесе жүйелік журнал форматтарын таңдай аласыз.

  Егер сіз Жүйе журналының деректер пішімін таңдасаңыз, **Хабардың максималды өлшемі, байт** көрсетуіңіз керек

  SIEM жүйесіне жіберілетін бір хабардың байтындағы максималды өлшемді көрсетіңіз. Әр оқиға бір хабармен беріледі. Егер хабардың нақты ұзындығы көрсетілген мәннен асып кетсе, хабар кесіліп, деректер жоғалуы мүмкін. Хабардың әдепкі өлшемі 2048 байтты құрайды. Бұл өріс **Протокол** өрісінде Syslog пішімін таңдаған болсаңыз ғана қолжетімді.

5. Мұрағатталған оқиғаларды Басқару серверінің дерекқорынан экспорттауға және мұрағатталған оқиғаларды экспорттауды бастағыңыз келетін басталу күнін орнатуға болады:

   a. **Экспорттың басталу күнін орнату** сілтемесінен өтіңіз.

   b. Ашылған бөлімде **Экспорттың басталу күні** өрісінде басталу күнін енгізіңіз.

   c. **OK** түймесін басыңыз.

6. **Оқиғаларды SIEM жүйесіне экспорттау** опциясын қосыңыз.

7. Саясатты өзгерту оқиғаларын SIEM-ге жіберу үшін **Саясат өзгерістеріне арналған кеңейтілген оқиғаларды SIEM жүйесіне экспорттау** параметрін қосыңыз. Әрбір өзгертілген саясат параметрі үшін SIEM-ге бөлек оқиға жіберіледі.

8. SIEM жүйесіне қосылым сәтті конфигурацияланғанына көз жеткізу үшін **Байланысты тексеру** түймесін басыңыз.

   SIEM жүйелік серверімен байланыс орнатылып, сынақ оқиғасы жіберіледі. Қосылым күйі көрсетіледі.

9. **Сақтау** түймесін басыңыз.

SIEM жүйесіне экспорттау теңшелді. Бұдан былай, егер SIEM жүйесінде оқиғаларды қабылдауды конфигурациялаған болсаңыз, Басқару сервері белгіленген оқиғаларды немесе саясатты өзгерту оқиғаларын SIEM жүйесіне экспорттайды. Экспорттауды бастау күнін орнатсаңыз, Басқару сервері Басқару серверінің дерекқорында сақталатын белгіленген оқиғаларды көрсетілген күннен бастап экспорттайды.

Саясат пен саясат профилінің өзгерістерін бақылау

Саясат параметрі өзгертілгенде, саясатты өзгерту оқиғасы жасалады; саясат өзгерістерін бақылау және дабылдарды қалыптастыру үшін оны SIEM жүйесіне экспорттауға болады. Саясатты өзгерту оқиғаларына тек SIEM жүйесі арқылы қол жеткізуге болады.

"Саясатты өзгерту оқиғалары генерацияланғаннан кейін Басқару серверінің дерекқорында сақталмайды және оларды Kaspersky Security Center Web Console жүйесінің **Мониторинг → Оқиғаларды таңдау** бөлімінде көру мүмкін емес. Сондай-ақ, **Оқиғаларды конфигурациялау** қойындысында осы оқиғалар үшін хабарландыру параметрлерін және сақтау параметрлерін көрсете алмайсыз.

Саясат жасалған кезде, саясатты өзгерту оқиғасы әрбір саясат параметрі үшін жасалады. Саясат өзгертілген кезде, саясаттың әрбір өзгертілген параметрі үшін саясатты өзгерту оқиғасы жасалады. Саясатты жою бір оқиғаны тудырады. Мысалы, Kaspersky Security Center саясатын құру шамамен 1000 оқиғаны қалыптастырады, ал Kaspersky Endpoint Security саясатын құру 7000-нан астам оқиғаны қалыптастырады.

Саясатты өзгерту оқиғаларын генерациялау шарттары

Саясатты өзгерту оқиғалары келесі жағдайларда жасалады:

- Келесі қолданбалардың саясаттарын жасау, өзгерту немесе жою:
  - Kaspersky Security Center Желілік агенті
  - Kaspersky Security Center Басқару сервері
  - Kaspersky Endpoint Security for Windows 14.1
  - Kaspersky Endpoint Security for Linux 12.5
  - Kaspersky Endpoint Security for Linux 12.4
  - Kaspersky Endpoint Security for Mac 12.2.1
- Басқару серверінің қасиеттерінде **Саясат өзгерістеріне арналған кеңейтілген оқиғаларды SIEM жүйесіне экспорттау** опциясы қосылған.
- Саясат Kaspersky Security Center Web Console интерфейсі арқылы қолмен өзгертіледі.

Саясатты өзгерту оқиғалары келесі жағдайларда жасалмайды:

- Жалпы саясат параметрлері өзгертіледі.
- Ата-аналық саясаттан мұраға алынған саясат параметрлері өзгертіледі.

- Саясатты реттеу Kaspersky Security Center OpenAPI арқылы өзгертіледі.
- Kaspersky қолданбасының параметрлері қолданбада тікелей өзгертіледі.

Саясатты өзгерту оқиғасының өрістері

Төмендегі кестеде саясатты өзгерту оқиғасы өрістерінің жиынтығы көрсетілген. Бұл өрістердің көрсетілуі шығыс оқиғасының форматына байланысты (мысалы, Syslog, CEF немесе LEEF). Өріс атаулары мен оқиға үлгілерін нақты көру үшін siem_conversion_rules.xml файлын қараңыз. Оқиға параметрлері тек ағылшын тілінде қолжетімді.

Оқиға өрісі	Деректер түрі	Сипаттамасы
`eventType`	string	Оқиғаның түрі. Оқиғаның белгілі бір типі үшін корреляция ережелерін жасауға мүмкіндік береді. Мүмкін мәндер: "Саясат жасалды", "Саясат өзгертілді", "Саясат жойылды".
`srvName`	жол	Басқару серверінің атауы.
`eventTime`	күн-уақыт	Оқиғаның күні мен уақыты (UTC бойынша).
`eventGroupID`	int	Өзгерту оқиғасы тобының идентификаторы.
`objectID`	int	Объектінің ішкі идентификаторы.
`objectName`	string	Саясаттың көрсетілетін атауы.
`objectGroup`	string	Саясатты қамтитын әкімшілік тобының толық жолы және атауы.
`user`	string	Өзгертуді жасаған пайдаланушының аты-жөні.
`operation`	string	Параметрді өзгерту түрі. Мүмкін мәндер: "Қосылды", "Алынып тасталды", "Өзгертілді".
`path`	string	Параметрдің жолы. Соңғы параметрдің ата-аналық түйініне жолды қамтиды. Жол саясаттың бөлімдері мен кіші бөлімдерінің атаулары негізінде жасалады. Жол құрылымы Желілік агент саясатының параметрлері, Жалпы саясат параметрлері және Саясат нұсқаларын салыстыру бөлімдерінде сипатталғандармен бірдей.
`parameter`	string	Соңғы параметрдің атауы.
`oldValue`	string	Соңғы параметрдің ескі мәні.
`newValue`	string	Соңғы параметрдің жаңа мәні.

Оқиғаларды тікелей дерекқордан экспорттау

Kaspersky Security Center Linux интерфейсін пайдаланбай-ақ, оқиғаларды тікелей Kaspersky Security Center Linux дерекқорынан алуға болады. Тікелей жария көріністерге сұраулар жасауға және олардан оқиғалар туралы деректерді алуға немесе бұрыннан бар жария көріністер негізінде өзіндік көріністер жасауға және қажетті деректерді алу үшін оларға жүгінуге болады.

Жария көріністер

Сізге ыңғайлы болу үшін, Kaspersky Security Center Linux дерекқорында көпшілікке арналған көріністер жиынтығы қарастырылған. Жария ұсыныстардың сипаттамасы klakdb.chm құжатында келтірілген.

v_akpub_ev_event жария көрінісі дерекқордағы оқиғалар параметрлеріне сәйкес келетін өрістер жиынтығын қамтиды. klakdb.chm құжатында Kaspersky Security Center Linux-дің басқа нысандарына, мысалы, құрылғыларға, бағдарламаларға, пайдаланушыларға қатысты жария көріністер туралы ақпарат та бар. Сіз бұл ақпаратты сұраулар жасау кезінде пайдалана аласыз.

Бұл бөлімде klsql2 утилитасы арқылы SQL сұрауын жасау нұсқаулары, сондай-ақ осындай сұраудың мысалы берілген.

Сондай-ақ, SQL сұраулары мен дерекқор көріністерін жасау үшін дерекқорлармен жұмыс істеуге арналған кез келген басқа бағдарламаларды пайдалануға болады. Kaspersky Security Center Linux дерекқорына қосылу параметрлерін, мысалы, дананың атауын және дерекқордың атауын қалай қарау керектігі туралы ақпарат тиісті бөлімде берілген.

klsql2 утилитасы арқылы SQL сұрауын жасау

Бұл мақалада klsql2 утилитасын пайдалану, сондай-ақ осы утилита көмегімен SQL сұрауын жасау нұсқаулары берілген. Kaspersky Security Center Linux жүйесінің орнатылған нұсқасына кіретін klsql2 утилитасының нұсқасын пайдаланыңыз.

klsql2 утилитасын пайдалану үшін:

1. Басқару сервері орнатылған каталогке өтіңіз. Әдепкі бойынша жол - /opt/kaspersky/ksc64/sbin.
2. Бұл каталогте .sql кеңейтімі бар бос файл жасаңыз.
3. Жасалған .sql файлын кез келген мәтіндік редакторда ашыңыз.
4. .sql файлында қажетті SQL сұрауын енгізіп, файлды сақтаңыз.
5. Басқару сервері орнатылған құрылғының пәрмен жолында .sql файлынан SQL сұрауын орындау үшін келесі пәрменді теріп, нәтижелерді result.xml файлына сақтаңыз:
   ```
   sudo ./klsql2 -i src.sql -u <пайдаланушы аты> -p <құпиясөз> -o result.xml
   ```
   мұндағы <пайдаланушы аты> және <құпия сөз> дерекқорға рұқсаты бар пайдаланушы есептік жазбасының есептік деректері болып табылады.
6. Қажет болса, дерекқорға қатынасуға рұқсаты бар пайдаланушының есептік жазбасының атауы мен құпиясөзін енгізіңіз.
7. Жаңадан жасалған result.xml файлдарын ашып, SQL сұрау нәтижелерін қараңыз.

.sql файлын өңдей аласыз және кез келген SQL сұрауын жалпыға жария жасай аласыз. Содан кейін, пәрмен жолындағы пәрменді пайдаланып, сұрауды іске қосып, нәтижелерді файлға сақтауға болады.

klsql2 утилитасы арқылы жасалған SQL сұрауының мысалы

Бұл бөлімде klsql2 утилитасы арқылы жасалған SQL сұрауының мысалы көрсетілген.

Келесі мысалдарда құрылғыларда соңғы жеті күнде орын алған оқиғаларды шығарып алу және пайда болған уақытына байланысты ретімен берілген оқиғалар берілген. Ең соңғы оқиғалар бірінші көрсетіледі.

PostgreSQL мысалы:

```
SELECT
  /* оқиға идентификаторы */
  "e"."nId",

  /* оқиға болған уақыт */
  "e"."tmRiseTime",

  /* оқиға түрінің ішкі атауы */
  "e"."strEventType",

  /* оқиғаның көрсетілген атауы */
  "e"."wstrEventTypeDisplayName",

  /* оқиғаның көрсетілген сипаттамасы */
  "e"."wstrDescription",

  /* оқиғаның көрсетілген сипаттамасы */
  "e"."wstrGroupName",

  /* оқиға орын алған құрылғының көрсетілген атауы */
  "h"."wstrDisplayName",
  (
    CAST((("h"."nIp" / 16777216 )& 255 ) AS VARCHAR(4))  || '.'  ||
    CAST((("h"."nIp" / 65536 )& 255 ) AS VARCHAR(4))  || '.'  ||
    CAST((("h"."nIp" / 256 )& 255 ) AS VARCHAR(4))  || '.'  ||

    /* оқиға орын алған құрылғының IP мекенжайы */
    CAST((("h"."nIp" )& 255 ) AS VARCHAR(4))
  )  AS "strIp"
FROM "v_akpub_ev_event"  AS "e"
  INNER JOIN  "v_akpub_host"  AS "h" ON "h"."nId" = "e"."nHostId"
WHERE "e"."tmRiseTime" >= NOW() AT TIME ZONE 'utc'  + make_interval(days => CAST(-7  AS INT))
ORDER BY "e"."tmRiseTime" DESC ;
```

MySQL немесе MariaDB мысалы:

```
SELECT

  /* оқиға идентификаторы */
  `e`.`nId`,

  /* оқиға болған уақыт */
  `e`.`tmRiseTime`,

  /* оқиға түрінің ішкі атауы */
  `e`.`strEventType`,

  /* оқиғаның көрсетілген атауы */
  `e`.`wstrEventTypeDisplayName`,

  /* оқиғаның көрсетілген сипаттамасы */
  `e`.`wstrDescription`,

  /* құрылғы тобының атауы */
  `e`.`wstrGroupName`,

  /* оқиға орын алған құрылғының көрсетілген атауы */
  `h`.`wstrDisplayName`,
  CONCAT(
    LEFT(CAST(((`h`.`nIp`  DIV  1677721) & 255) AS CHAR), 4), '.',
    LEFT(CAST(((`h`.`nIp`  DIV  65536) & 255) AS CHAR), 4), '.',
    LEFT(CAST(((`h`.`nIp`  DIV  256) & 255) AS CHAR), 4), '.',

    /* оқиға орын алған құрылғының IP мекенжайы */
    LEFT(CAST(((`h`.`nIp`) & 255) AS CHAR), 4)
  )  AS `strIp`
FROM `v_akpub_ev_event`  AS `e`
  INNER JOIN  `v_akpub_host`  AS `h` ON `h`.`nId` = `e`.`nHostId`
WHERE `e`.`tmRiseTime` >= ADDDATE( UTC_TIMESTAMP( ) , INTERVAL -7  DAY)
ORDER BY `e`.`tmRiseTime` DESC ;
```

Kaspersky Security Center Linux дерекқорының атауын қарау

Kaspersky Security Center Linux дерекқорына MySQL немесе MariaDB көмегімен қол жеткізу үшін SQL скрипттер редакторынан оған қосылу мүмкіндігін алу үшін дерекқордың атауын білу қажет.

Kaspersky Security Center Linux дерекқорының атауын көру үшін:

1. Негізгі мәзірдегі басқару серверінің атауын басыңыз.

   Басқару серверінің сипаттары терезесі ашылады.

2. **Жалпы** қойындысында **Ағымдағы дерекқор мәліметтері** бөлімін таңдаңыз.

   Дерекқорының атауы **Дерекқор атауы** өрісінде көрсетілген. SQL сұрауларында дерекқорға қосылу және жүгіну үшін осы дерекқор атауын пайдаланыңыз.

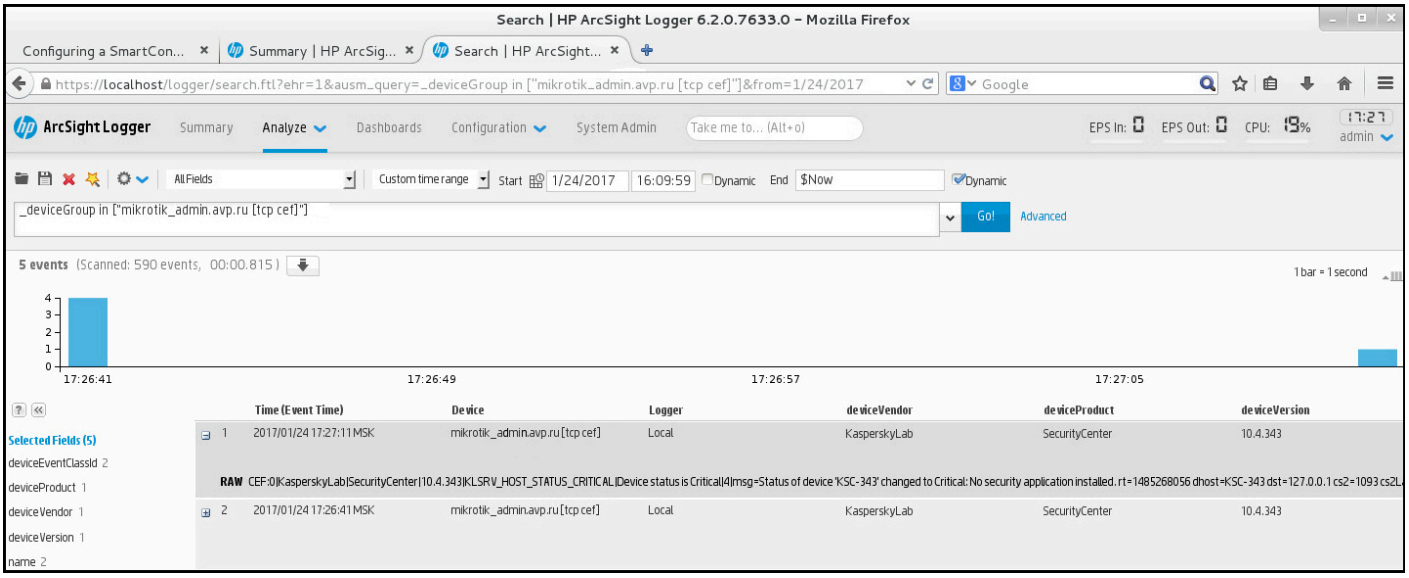
Экспорт нәтижелерін қарау

Экспорттау рәсімі сәтті аяқталғанын білуіңізге болады. Бұл үшін SIEM жүйесі экспортталатын оқиғаларды қамтитын хабарларды алып-алмағанын тексеріңіз.

Kaspersky Security Center Linux-ден жіберілген оқиғаларды SIEM жүйесі алып, дұрыс түсіндірсе, онда екі жақтағы конфигурациялау дұрыс орындалды. Әйтпесе, Kaspersky Security Center Linux және SIEM жүйесінің конфигурациясын тексеріп, қажет болған жағдайда түзетіңіз.

Төменде ArcSight жүйесіне экспортталған оқиғалардың мысалы келтірілген. Мысалы, бірінші оқиға – Басқару серверінің критикалық оқиғасы: *Құрылғының күйі "Критикалық"*.

Экспортталған оқиғалардың көрсетілуі қолданылатын SIEM жүйесіне байланысты.



Оқиғалар мысалы

Нысанды тексерумен жұмыс

Бұл бөлімде нысандарды тексерумен жұмыс істеу туралы ақпарат бар. Kaspersky Security Center Linux жүйесі нысандардың өзгерістерін бақылауға мүмкіндік береді. Нысанның өзгерістерін сақтаған сайын, *тексеру* жасалады. Әр тексерудің өзі нөмірі бар.

Тексерістермен жұмысты қолдайтын нысандар:

- Басқару серверінің қасиеттері
- Саясаттар
- Тапсырмалар
- Басқару топтары
- Пайдаланушы есептік жазбалары
- Орнату пакеттері

Нысандарды тексерумен келесі әрекеттерді орындауыңызға болады:

- таңдалған тексерісті қарау (саясаттар үшін ғана қолжетімді);
- нысанның өзгерістерін таңдалған тексеруге шегіндіру;
- тексерістерді JSON файлы ретінде сақтау (тек саясаттар үшін қолжетімді).

Тексерулермен жұмыс істеуді қолдайтын нысандардың сипаттары терезесінде **Тексерістер журналы** бөлімінде келесі ақпаратпен бірге нысанды тексеру тізімі көрсетіледі:

- **Тексеру** – нысанды тексеру нөмірі.
- **Уақыт** – нысанды өзгерту күні мен уақыты.
- **Пайдаланушы** – нысанды өзгерткен пайдаланушы атауы.
- **Пайдаланушы құрылғысының IP мекенжайы** – нысан өзгертілген құрылғының IP-мекенжайы.
- **Web Console консольдің IP мекенжайы** – нысан өзгертілген Kaspersky Security Center Web Console қолданбасының IP-мекенжайы.
- **Әрекет** – нысанмен орындалған әрекет.
- **Сипаттама** – нысан параметрлерінің өзгерістерін тексеру сипаттамасы.

  Әдепкі бойынша, нысанды тексеру сипаттамасы толтырылмаған. Тексеру сипаттамасын қосу үшін қажетті тексеруді таңдап, **Сипаттаманы өңдеу** түймесін басыңыз. Ашылған терезеде тексеру сипаттамасы мәтінін енгізіңіз.

Саясаттың нұсқасын қарау және сақтау

Kaspersky Security Center Linux қолданбасы белгілі бір кезеңде саясатқа қандай өзгерістер енгізілгенін көруге және осы өзгерістер туралы ақпаратты файлда сақтауға мүмкіндік береді.

Тиісті веб-басқару плагині бұл функцияны қолдайтын болса, саясаттың тексерісін қарау және сақтау қолжетімді болады.

Саясат тексерісін қарау үшін:

1. Қолданбаның негізгі терезесінде **Активтерді басқару** → **Саясаттар** бөліміне өтіңіз.
2. Көргіңіз келетін саясат тексерісін нұқыңыз және **Тексерістер журналы** бөліміне өтіңіз.
3. Саясат тексерістерінің тізімінде көргіңіз келетін тексеріс нөмірін басыңыз.

   Тексеріс өлшемі 10 МБ-тан асса, оны Kaspersky Security Center Web Console веб-консолі арқылы қарау мүмкін емес. Сізге таңдалған тексерісті JSON файлына сақтау ұсынылады.

   Тексеріс өлшемі 10 МБ-тан аз болса, таңдалған саясат тексерісінің параметрлерімен HTML пішіміндегі есеп көрсетіледі. Есеп қалқымалы терезеде пайда болғандықтан, браузеріңізде қалқымалы терезелерге рұқсат етілгеніне көз жеткізіңіз.

Kaspersky Endpoint Security for Windows және Kaspersky Endpoint Security for Mac саясаттары үшін есепте саясат профильдері туралы ақпарат болмайды.

Саясаттың тексерісін JSON файлына сақтау үшін,

Саясат тексерістері тізімінде сақтағыңыз келетін тексерісті таңдап, **Файлға сақтау** түймесін басыңыз.

Тексеріс JSON файлында сақталады.

Қажет болса, саясат түзетулерін салыстыра аласыз. Бұл опция Басқару сервері, Желілік агент, Kaspersky Endpoint Security for Windows (14.0 веб-плагин нұсқасынан бастап) және Kaspersky Endpoint Security for Mac (12.2.1 Patch A веб-плагин нұсқасынан бастап) саясаттары үшін қолжетімді.

Саясат тексерістерін салыстыру

Саясаттың бұрынғы түзетулерін оның ағымдағы түзетуімен салыстыруға, тізімде таңдалған әртүрлі түзетулерді салыстыруға немесе бір саясаттың түзетуін басқа саясаттың түзетуімен салыстыруға болады. Бұл опциялар Басқару сервері, Желілік агент, Kaspersky Endpoint Security for Windows (14.0 веб-плагин нұсқасынан бастап) және Kaspersky Endpoint Security for Mac (12.2.1 Patch A веб-плагин нұсқасынан бастап) саясаттары үшін қолжетімді.

Саясат тексерісін қарау үшін:

1. Бағдарламаның негізгі терезесінде **Активтерді басқару** → **Саясаттар** бөліміне өтіңіз.
2. Нұсқаларын салыстырғыңыз келетін саясатты басыңыз.

   Саясат сипаттары терезесі ашылады.
3. **Тексерістер журналы** қойындысына өтіп, салыстырылатын түзетулердің жанындағы құсбелгілерді таңдаңыз.
4. Құралдар тақтасында **Салыстыру** түймесін басыңыз, содан кейін ашылмалы тізімнен келесі опциялардың бірін таңдаңыз:

   - **Ағымдағы түзетумен**, егер сіз 3-қадамда таңдаған түзетуіңізді сол саясаттың соңғы сақталған түзетуімен салыстырғыңыз келсе.
   - **Таңдалған түзетулер**, егер сіз 3-қадамда құсбелгілерін таңдаған екі түзетуді салыстырғыңыз келсе.

     Құсбелгілерді таңдау реті салыстыру нәтижелеріне әсер етпейді. Әдепкі бойынша, таңдалған нұсқаның бұрынғы нұсқасы ең соңғы нұсқамен салыстырылады. Мысалы, егер сіз 5 және 1 нұсқаларының жанындағы құсбелгілерді таңдасаңыз, 1 нұсқа 5 нұсқамен салыстырылады. Есепте 5 нұсқамен салыстырғанда қосылған, жойылған немесе өзгертілген 1 нұсқадағы параметрлер туралы ақпарат болады.
   - **Басқа саясат нұсқасымен**, егер сіз екі түрлі саясаттың нұсқаларын салыстырғыңыз келсе.

     Ашылған оң жақ тақтада келесі әрекеттердің бірін орындаңыз:

     a. **Қолданба атауы** өрісінде салыстырғыңыз келетін саясатты таңдаңыз: Желілік агент немесе Басқару сервері.

     b. **Саясат атауы** өрісінде 3-қадамда таңдаған нұсқаңызбен салыстырғыңыз келетін саясаттың атауын көрсетіңіз.

     Бар саясатты тексеру тізімі көрсетіледі.

     c. Қажетті нұсқаны таңдап, содан кейін **Салыстыру** түймесін басыңыз.

Түзетулерді салыстыру туралы есеп шолғышыңыздың жаңа қойындысында HTML форматында көрсетіледі.

Егер салыстыру нәтижесі 10 МБ-тан асса, сәйкес диалогтік терезе көрсетіледі. Есепті файл ретінде сақтау үшін **Файлға сақтау** түймесін басуға немесе оператор әрекетін болдырмауға болады.

Есеп Kaspersky Security Center Web Console интерфейс тілінде көрсетіледі. Есептің кейбір бөлімдерін сол бөлімнің жанындағы төмен көрсеткі белгісін (▼) басу арқылы жаюға немесе жоғары көрсеткі белгісін (▲) басу арқылы жинауға болады.

Есеп келесі ақпаратты қамтиды:

- Kaspersky логотипі.
- Есептің атауы.

- Есептің жасалған уақыты мен күні.
- Саясат атауы, Басқару сервері және түзетулері салыстырылған саясатты (саясаттарды) қамтитын Басқару тобы.
- **HTML ретінде сақтау** түймесі. Егер сіз түймені бассаңыз, есеп компьютеріңізге сақталады.
- Салыстырылған түзетулер туралы жалпы ақпаратты көрсететін «**Қорытынды**» бөлімі: саясат (саясаттар) атауы, түзету нөмірі, түзету сақталған уақыты мен күні, түзетуді сақтаған пайдаланушы және түзету сипаттамасы.

  Мұраланған саясаттар үшін пайдаланушы көрсетілмейді.

- Салыстырылған түзетулер арасындағы айырмашылықтар. Айырмашылықтар келесі бөлімдерде көрсетіледі:
  - **Қосылған параметрлер**
  - **Алынған параметрлер**
  - **Өзгертілген параметрлер**
  - **Параметрлер тек 1-ші нысан үшін қолжетімді** (егер сіз екі түрлі саясаттың нұсқаларын салыстырған болсаңыз)
  - **Параметрлер тек 2-ші нысан үшін қолжетімді** (егер сіз екі түрлі саясаттың нұсқаларын салыстырған болсаңыз)

  Егер бөлімде деректер болмаса, көрсетілмейді.

Kaspersky Endpoint Security for Windows және Kaspersky Endpoint Security for Mac саясаттары үшін түзетулерді салыстыру туралы есепте саясат профильдері туралы ақпарат болмайды.

Нысанның өзгерістерін алдыңғы тексеруге шегіндіру

Қажет болса, нысанның өзгерістерін шегіндіруге болады. Мысалы, саясат параметрлерін белгілі бір күндегі күйге кері қайтару қажет болып қалуы мүмкін.

Нысан өзгерістерін шегіндіру үшін:

1. Нысан сипаттары терезесінде **Тексерістер журналы** қойыншасына өтіңіз.
2. Нысанды тексеру тізімінде, өзгерістерін шегіндіру қажет болған тексеруді таңдаңыз.

3. **Шегіндіру** түймесін басыңыз.

4. Операцияны растау үшін **ОК** түймесін басыңыз.

Таңдалған тексеруге шегіндіру орын алады. Нысанды тексеру тізімінде орындалған әрекет туралы жазба көрсетіледі. Тексеру сипаттамасында, нысанды қайтарған тексеру нөмірі туралы ақпарат көрсетіледі.

Шегіндіру операциясы тек саясат пен тапсырмалар үшін қолжетімді.

Белсенді қауіптер

Клиент құрылғыларында табылған кейін өңделетін файлдар туралы ақпарат **Қоймалар** бөліміндегі **Белсенді қауіптер** кіші бөлімінде сақталады.

Кейінге қалдырылған өңдеу мен дезинфекцияны қауіпсіздік бағдарламасы сұрау бойынша немесе белгілі бір оқиғадан кейін орындайды. Файлдарды кешіктіріп зарарсыздандыру файлдарының параметрлерін конфигурациялауға болады.

Кейін өңделетін файлды дезинфекциялау

Кейін өңделетін файлды зарарсыздандыруды іске қосу үшін:

1. Негізгі мәзірде **Қоймалар** → **Белсенді қауіптер** бөліміне өтіңіз.

2. Келесі әрекеттердің бірін орындаңыз:

   - Зарарсыздандырғыңыз келетін файлға қарсы жалаушаны қойыңыз.
   - Зарарсыздандырылатын файлдың атауын басыңыз.

3. **Залалсыздандыру** түймесін басу арқылы файлды Зарарсыздандыруды бастаңыз.

Нәтижесінде, таңдалған файлды зарарсыздандыру әрекеті орындалады.

Файл зарарсыздандырылған болса, клиент құрылғысына орнатылған қауіпсіздік бағдарламасы оны бастапқы қалтаға қалпына келтіреді. Файл туралы жазба **Белсенді қауіптер** бөліміндегі тізімнен жойылады. Файлды зарарсыздандыру мүмкін болмаса, құрылғыда орнатылған қауіпсіздік бағдарламасы файлды құрылғыдан жояды. Файл туралы жазба **Белсенді қауіптер** бөліміндегі тізімнен жойылады.

Орнатылған қауіпсіздік бағдарламасына, оның нұсқасы мен параметрлеріне байланысты файлдарды зарарсыздандыру мен жою мүмкіндіктері әртүрлі болуы мүмкін.

Кейін өңделетін файлды жүктеу

Kaspersky Security Center Linux, клиент құрылғыларында анықталған кейін өңделетін файлдардың көшірмелерін жүктеуге мүмкіндік береді. Бұл қолданба өңдеген немесе жойған файлдарға қатысты. Файлдар Kaspersky Security Center Linux орнатылған құрылғыға, сіз көрсеткен қалтаға жүктеледі.

Залалсыздандыру кезінде жойылған немесе өзгертілген файлдардың көшірмелерін файлдар жадта сақталған болса жүктей аласыз. Басқарылатын құрылғыдағы Linux жүйесіне арналған Kaspersky Endpoint Security.

Кейін өңделетін файлдың көшірмесін жүктеу үшін:

1. Негізгі мәзірде **Қоймалар** → **Белсенді қауіптер** бөліміне өтіңіз.
2. Келесі әрекеттердің бірін орындаңыз:
   - Жүктеп алынатын файлға қарсы жалаушаны қойыңыз.
   - Жүктеп алынатын файлдың атауын басыңыз.
3. **Жүктеп алу** түймесін басу арқылы жүктей бастаңыз.

Нәтижесінде, таңдалған кейін өңделетін файл анықталған клиент құрылғысының қауіпсіздік бағдарламасы файлдың көшірмесін көрсетілген қалтаға жүктейді.

Белсенді қауіптер бөліміндегі файлдарды жою

***Белсенді қауіптерденБелсенді қауіптер** бөлім:*

1. Негізгі мәзірде **Қоймалар** → **Белсенді қауіптер** бөліміне өтіңіз.
2. Келесі әрекеттердің бірін орындаңыз:
   - Жойғыңыз келетін файлға қарсы жалаушаны қойыңыз.
   - Жойылатын файлдың атауын басыңыз.
3. Файлдарды **Жою** түймесін басу арқылы жойыңыз.
4. Пайда болған терезеде **Жою** түймесін басыңыз.

Нәтижесінде, таңдалған файлдарды клиент құрылғыларындағы сақтау орындарына орналастырған қауіпсіздік бағдарламалары файлдарды осы сақтау орындарынан жояды. Файлдар туралы жазбалар **Белсенді қауіптер** бөліміндегі тізімнен жойылады.

Нысандарды жою

Бұл бөлімде нысандарды жою туралы ақпарат берілген.

Сіз келесі нысандарды жоя аласыз:

- Саясаттар
- Тапсырмалар
- Орнату пакеттері
- Виртуалды Басқару серверлері
- Пайдаланушылар
- Қауіпсіздік топтары
- Басқару топтары

Нысанды жою үшін:

1. Kaspersky Security Center Web Console қажетті бөлімін ашып, нысанды таңдаңыз.
2. Құралдар тақтасындағы **Жою** түймесін басыңыз.
3. Пайда болған терезеде таңдауыңызды растау үшін **OK** түймесін басыңыз.

   Таңдалған нысан жойылды.

Сіз нысанды жойған кезде, бұл туралы ақпарат дерекқорға жазылады. Жойылған нысандардың ақпаратын сақтау мерзімі, нысандар тексеруді сақтау мерзімімен бірдей (ұсынылатын мерзімі 90 күн). Сақтау уақыты, тек **Жойылған нысандар** аймағы үшін **Өзгерту** құқығы болған кезде ғана өзгертілуі мүмкін.

Клиенттік құрылғыларды жою туралы

Басқарылатын құрылғы басқару тобынан жойылғанда, бағдарлама құрылғыны Тағайындалмаған құрылғылар тобына жылжытады. Құрылғы жойылғаннан кейін, Kaspersky орнатылған қолданбалары – Желілік агент және Kaspersky Endpoint Security сияқты қауіпсіздік бағдарламасы құрылғыда қалады.

Kaspersky Security Center Linux келесі ережелерге сәйкес Тағайындалмаған құрылғылар тобындағы құрылғыларды өңдейді:

- Құрылғыны жылжыту ережелерін конфигурациялаған болсаңыз және құрылғы жылжыту ережесінің шарттарына сай болса, құрылғы ережеге сәйкес автоматты түрде басқару тобына жылжытылады.
- Құрылғы Тағайындалмаған құрылғылар тобында сақталады және құрылғыны сақтау ережелеріне сәйкес топтан автоматты түрде жойылады.

  Құрылғыны сақтау ережелері, бір немесе бірнеше дискілері толық дискілік шифрлау арқылы шифрланған құрылғыларға әсер етпейді. Мұндай құрылғылар автоматты түрде жойылмайды – оларды тек қолмен жоюға болады. Шифрланған қатты дискісі бар құрылғыны жою қажет болса, алдымен дискінің шифрын шешіп, содан кейін құрылғыны алып тастаңыз.

Шифрланған қатты дискісі бар құрылғыны алып тастаған кезде, дискінің шифрын шешуге қажетті деректер де жойылады. Егер сіз осындай құрылғыларды (**Тағайындалмаған құрылғылар** тобынан немесе **Басқарылатын құрылғылар** тобынан) жойған кезде ашылатын растау терезесінде **Тәуекелді түсінемін және таңдалған құрылғыларды жойғым келеді** құсбелгісін қойсаңыз, бұл сіздің деректердің кейінірек жойылатынын білетініңізді білдіреді.

Бұл жағдайда, дискінің шифрын ашу үшін келесі шарттар орындалуы керек:

- Дискінің шифрын шешуге қажетті деректерді қалпына келтіру үшін құрылғы Басқару серверіне қайта қосылады.
- Құрылғының пайдаланушысы шифрды шешу құпиясөзін есте сақтайды.
- Құрылғыда Kaspersky Endpoint Security for Windows сияқты дискіні шифрлау үшін пайдаланылған қауіпсіздік бағдарламасы орнатылған.

Егер диск Kaspersky Disk Encryption технологиясы арқылы шифрланған болса, FDERT Restore утилитасын пайдаланып деректерді қалпына келтіруге де болады.

VDI жүйесінде шифрланған дискілері бар құрылғы болса, құрылғыны жойғаннан кейін шифрланған дискідегі ақпарат жойылады.

Құрылғыны Тағайындалмаған құрылғылар тобынан қолмен жойған кезде, бағдарлама құрылғыны тізімнен жояды. Құрылғы жойылғаннан кейін, Kaspersky орнатылған бағдарламалары (бар болса) құрылғыда қалады. Содан кейін, құрылғы әлі де Басқару серверіне көрініп тұрса және сіз тұрақты желі сұрауын конфигурациялаған болсаңыз, Kaspersky Security Center Linux желі сауалнамалары кезінде құрылғыны анықтайды және оны Тағайындалмаған құрылғылар тобына қайта қосады. Сондықтан, егер ол Басқару серверіне көрінбейтін болса ғана құрылғыны қолмен алып тастаған жөн.

Файлдарды Карантинге және Файлдардың сақтық көшірмелері жүктеу және одан жою

Бұл бөлімде, файлдарды Карантин мен Файлдардың сақтық көшірмелері Kaspersky Security Center Web Console веб-консоліне жүктеу және одан жою тәсілі туралы ақпарат келтірілген.

Файлдарды Карантиннен және Файлдардың сақтық көшірмелерінен жүктеп алу

Келесі екі шарттың бірі орындалса ғана, файлдарды Карантин мен Файлдардың сақтық көшірмелерінен жүктеп алуға болады: құрылғының сипаттарында **Басқару серверімен байланысты үзбеу** параметрі қосулы болса немесе қосылым шлюзі қолданылса. Әйтпесе, жүктеп алу мүмкін емес.

Файлдың көшірмесін карантиннен немесе Файлдардың сақтық көшірмелері қатты дискіге сақтау үшін:

1. Келесі әрекеттердің бірін орындаңыз:

   - Карантиндегі файлдың көшірмесін сақтағыңыз келсе, басты мәзірде **Операциялар** → **Қоймалар** → **Карантин** бөліміне өтіңіз.

   - Сақтық көшірмелеудегі файлдың көшірмесін сақтағыңыз келсе, басты мәзірде **Операциялар** → **Қоймалар** → **Файлдардың сақтық көшірмелері** бөліміне өтіңіз.

2. Ашылған терезеде жүктегіңіз келетін файлды таңдап, **Жүктеп алу** түймесін басыңыз.

   Жүктеу басталады. Клиент құрылғысында Карантинге салынған файл көшірмесі көрсетілген қалтаға сақталады.

Нысандарды Карантин, Сақтық көшірмелеу файлдары немесе Белсенді қауіптерден жою туралы

Клиент құрылғыларына орнатылған Kaspersky қауіпсіздік қолданбалары нысандарды Карантин, Сақтық көшірмелеу немесе Белсенді қауіптерге салған кезде, олар қосылған нысандар туралы ақпаратты, **Карантин**, **Файлдардың сақтық көшірмелері** немесе **Белсенді қауіптер** бөлімдеріне қосылған нысандар туралы ақпаратты Kaspersky Security Center Linux бағдарламасына береді. Осы бөлімдердің бірін ашқан кезде, қажетті нысанды өшіруге болады.

Файлдардың сақтық көшірмелері немесе **Белсенді қауіптер** бөлімі үшін тізімнен нысанды таңдап, **Өшіру** түймесін басыңыз.

Карантин бөлімінде келесі әрекеттердің бірін орындауға болады:

- Өшірілетін нысан атауының жанындағы құсбелгіні қойып, құралдар тақтасында **Жою** түймесін басыңыз.

- Өшірілетін нысанның атауын басыңыз және ашылатын мәліметтер терезесіндегі құралдар тақтасында **Жою** түймесін басыңыз.

  Бұл жағдайда нысан жойылады, экранда сәйкес хабарландыру көрсетіледі және мәліметтер терезесі жабылады.

Kaspersky Security Center Linux таңдалған нысанды тізімнен өшіреді немесе таңдалған нысанды қоймадан жояды. Орындалуы тиісті әрекет, таңдалған нысанды қоймаға салынған Kaspersky бағдарламасы тарапынан анықталады. Kaspersky бағдарламасы **Жазба қосылды** өрісінде көрсетілген.

Орындалатын әрекет туралы толық ақпаратты Kaspersky қолданбасының құжаттамасынан қараңыз.

Қолданбаны SNMP арқылы басқару

Бұл бөлімде Linux жүйесінде SNMP (Simple Network Management Protocol) арқылы Басқару серверінен ақпаратты қалай алуға болатыны сипатталады.

SNMP – бұл желілік құрылғыларды басқару хаттамасы.

SNMP арқылы жұмыс істеу үшін Kaspersky Security Center Linux операциялық жүйеге кіретін snmpd қызметін және SNMP агентін Басқару серверінің жұмысын бақылау және OID арқылы қосымша қолданбаларға деректерді жіберу үшін пайдаланады. Kaspersky Security Center Linux бұл ақпаратты статистика немесе SNMP тұзақтары түрінде жібере алады, олар қолданба оқиғалары туралы хабарландырулар болып табылады.

SNMP қолданба туралы келесі ақпаратқа қол жеткізуге мүмкіндік береді:

- Жалпы ақпарат
- Қолданба орнатылғаннан бері Kaspersky Security Center Linux статистикасы
- Kaspersky Security Center Linux оқиғалары туралы ақпарат

Тек оқуға рұқсат етіледі.

SNMP тұзақтары және SNMP арқылы жіберілген статистика туралы ақпарат adminkit.mib файлында сақталады. Әдепкі бойынша, adminkit.mib файлы /opt/kaspersky/ksc64/share/snmp/ қалтасында орналасқан.

Әрбір кластер түйініндегі жергілікті snmpd қызметі статистиканы қабылдайтын SNMP сервері ретінде қызмет етеді. Сыртқы SNMP серверімен өзара әрекеттесуге қолдау көрсетілмейді. SNMP тұзақтарын әрбір кластер түйінінде жергілікті snmptrapd қызметін пайдалану арқылы алуға немесе оларды сыртқы серверге қайта бағыттауға болады.

SNMP арқылы операциялар үшін әрбір кластер түйініндегі операциялық жүйеде snmpd қызметін алдын ала конфигурациялаңыз.

Операциялық жүйеде snmpd қызметін конфигурациялау

Конфигурациялау алдында snmpd қызметі операциялық жүйеңізге орнатылғанына көз жеткізіңіз.

Деректерге қол жеткізу үшін пайдаланушы есептік жазбасын жасау

Есептік жазбаны жасамас бұрын, келесі пәрменді орындау арқылы snmpd қызметін тоқтатыңыз:

```
bash
sudo systemctl stop snmpd
```

SNMPv3 арқылы деректерге аутентификация және шифрлау арқылы кіру қауіпсіздігін қамтамасыз ету үшін snmpd қызмет жағында келесі ақпаратпен пайдаланушы есептік жазбасын жасау қажет:

- Пайдаланушы аты (регистрге сезімтал)
- Аутентификация алгоритмі (MD5 немесе SHA – SHA ұсынылады)
- Аутентификация құпиясөзі

- Шифрлау алгоритмі (тек AES қолдауы бар)
- Шифрлау құпиясөзі

Пайдаланушы есептік жазбасын келесі жолдармен жасауға болады:

- Операциялық жүйеде қолжетімді болса, net-snmp-create-v3-user утилитасын пайдалану арқылы.
- snmpd қызметінің конфигурация файлына тиісті директиваны қолмен қосу арқылы.

net-snmp-create-v3-user утилитасын пайдаланып, пайдаланушы есептік жазбасын жасау үшін келесі пәрменді орындаңыз:

```
net-snmp-create-v3-user -ro -a <аутентификация алгоритмі> -x <шифрлау алгоритмі> <пайдаланушы аты>
```

Аутентификация және шифрлау құпиясөздері интерактивті түрде сұралады.

Мысалы:

```
net-snmp-create-v3-user -ro -a SHA -x AES MonitoringUser
```

Пайдаланушы есептік жазбасын қолмен жасау үшін:

1. Келесі пәрменді іске қосу арқылы /var/lib/snmp/snmpd.conf конфигурация файлын жасаңыз:

   ```
   touch /var/lib/snmp/snmpd.conf
   ```

2. Конфигурациялық файлға келесі жолды қосыңыз:

   ```
   createUser <пайдаланушы аты> <аутентификация алгоритмі> "<аутентификация құпиясөзі>" <шифрлау алгоритмі> "
   <шифрлау құпиясөзі>"
   ```

   Мысалы:

   ```
   createUser MonitoringUser SHA "MonitoringAuthSecret" AES "MonitoringPrivSecret"
   ```

SNMP тұзақтарын алу үшін пайдаланушы есептік жазбасын жасау

Аутентификация және шифрлау арқылы SNMPv3 арқылы SNMP тұзақтарын алу үшін, сәйкес қызметтің (әдетте snmptrapd қызметі) контекстінде бақылау жүйесінің жағында есептік жазба жасау қажет.

Есептік жазба келесі ақпаратты қамтуы тиіс:

- Пайдаланушы аты
- Аутентификация алгоритмі
- Аутентификация құпиясөзі

- Шифрлау алгоритмі
- Шифрлау құпиясөзі

Қауіпсіздік мақсатында деректерге қол жеткізу және SNMP тұзақтарын алу үшін бөлек пайдаланушы есептік жазбаларын пайдаланыңыз.

SNMP тұзақтарын алу үшін пайдаланушы есептік жазбасын жасау бойынша нұсқауларды бақылау жүйеңіздің құжаттамасын қараңыз.

snmpd қызметін конфигурациялау

snmpd қызметінің конфигурациясы /etc/snmp/snmpd.conf файлында сақталады. Қажетті ақпаратты бар конфигурация файлына қосуға немесе жаңа конфигурация файлын жасауға және төменде көрсетілген жолдарды берілген ретпен қосуға болады.

Егер сіз жаңа конфигурация файлын жасауды таңдасаңыз, оған тек суперпайдаланушының ғана кіре алатынына көз жеткізіңіз. Қажетті кіру рұқсаттары орнатылмаған болса, оларды көрсетілген ретпен келесі командаларды орындау арқылы конфигурациялаңыз:

```
chown root:root /etc/snmp/snmpd.conf
chmod 600 /etc/snmp/snmpd.conf
```

snmpd қызметін конфигурациялау үшін:

1. Конфигурация файлында snmpd қызметі кіріс сұрауларды тыңдауы керек протоколды, желілік интерфейс мекенжайын және порт нөмірін көрсетіңіз.

   - Егер сіз барлық желі интерфейстеріндегі сұрауларды тыңдағыңыз келсе, конфигурация файлына келесі жолдарды қосыңыз:

     ```
     agentAddress udp:161
     ```

   - Егер сіз тек жергілікті желі интерфейсінде сұрауларды тыңдағыңыз келсе, мысалы, бақылау жүйесі бір машинада орнатылған болса, конфигурация файлына келесі жолдарды қосыңыз:

     ```
     agentAddress udp:127.0.0.1:161
     ```

2. Kaspersky Security Center Linux және snmpd қызметі арасындағы өзара әрекеттесуді конфигурациялаңыз. Сіз UNIX сокетні немесе TCP сокетін пайдалана аласыз.

   - Егер сіз UNIX сокеті пайдалансаңыз:

     a. UNIX сокеті үшін жол мен рұқсаттарды көрсетіңіз. Ол үшін конфигурациялық файлға келесі жолдарды қосыңыз:

     ```
     master agentx
     agentXSocket unix:/var/run/agentx-master.socket
     agentXPerms 770 770 kluser klusers
     ```

     b. {'KLSRV_UNATT_KLSVCUSER'} есептік жазбасы үшін қосымша топ ретінде klusers тобын қосыңыз.

   - Егер сіз TCP сокеті пайдалансаңыз, TCP сокеті үшін порт пен мекенжайды көрсетіңіз. Ол үшін конфигурациялық файлға келесі жолдарды қосыңыз:

     ```
     master agentx
     agentXSocket tcp:127.0.0.1:705,tcp6:[::1]:705
     ```

3. Ең аз жауап беру уақытын кемінде 30 секундқа орнатыңыз. Ол үшін конфигурациялық файлға келесі жолдарды қосыңыз:

   ```
   agentxTimeout 30
   ```

4. Қажет болса, SNMP конфигурацияланған сервердің сипаттамасын, жүйенің орналасқан жерін және әкімшінің байланыс мекенжайын бере аласыз. Ол үшін конфигурациялық файлға келесі жолдарды қосыңыз:

   ```
   sysDescr <server description>
   sysLocation <server location>
   sysContact <contact address of the administrator>
   sysServices 72
   ```

5. SNMP протоколы арқылы бақылау жүйеңізге қолжетімді болғыңыз келетін OID ағашының ауқымын көрсетіңіз. Ол үшін конфигурациялық файлға келесі жолдарды қосыңыз:

   ```
   view monitoring included .1.3.6.1.4.1.23668.1093.1

   view systemonly included .1.3.6.1.4.1.23668.1093.1
   ```

6. Қажет болса, snmpd қызметі сақтайтын операциялық жүйе туралы ақпаратты қамтитын OID ағашының ауқымын қосымша көрсете аласыз. Бұл ауқым сіздің бақылау жүйеңізге қолжетімді болады.

Операциялық жүйе туралы ақпаратқа, мысалы, CPU және RAM пайдалануы, диск бөлімдеріндегі бос орын, желілік интерфейстердің жүктелуі туралы ақпарат; орнатылған бағдарламалық жасақтама тізімі; ашық желілік қосылымдардың тізімі; және іске қосылған процестердің тізімі кіреді. Бұл ақпараттың бір бөлігі құпия болуы мүмкін.

- Егер сіз тек жалпы жүйелік ақпаратқа және жедел жадты, процессорды және диск құрылғыларын пайдалану туралы ақпаратқа қол жеткізуге рұқсат бергіңіз келсе, конфигурация файлына келесі жолдарды қосыңыз:

```
# SNMPv2-MIB - Basic system information
view monitoring included .1.3.6.1.2.1.1
# HOST-RESOURCES-MIB - CPU, Memory, Filesystems
view monitoring included .1.3.6.1.2.1.25.1
view monitoring included .1.3.6.1.2.1.25.2
view monitoring included .1.3.6.1.2.1.25.3
view monitoring included .1.3.6.1.2.1.25.5
# UCD-SNMP-MIB - Memory and CPU usage
view monitoring included .1.3.6.1.4.1.2021.4
view monitoring included .1.3.6.1.4.1.2021.10
view monitoring included .1.3.6.1.4.1.2021.11
# UCD-SNMP-DISKIO-MIB - Block devices I/O statistics
view monitoring included .1.3.6.1.4.1.2021.13
# IF-MIB - Network interfaces I/O statistics
view monitoring included .1.3.6.1.2.1.2
view monitoring included .1.3.6.1.2.1.31
```

- Егер сіз барлық жүйелік ақпаратқа қол жеткізуге рұқсат бергіңіз келсе, конфигурация файлына келесі жолдарды қосыңыз:

```
view monitoring included .1
```

7. Жасалған пайдаланушы есептік жазбасы үшін кіру режимін және ақпарат ауқымын көрсетіңіз. Ол үшін файлға келесі жолдарды қосыңыз:

```
rouser <user name> priv -V monitoring
```

8. SNMP тұзақтарын жіберу үшін бақылау жүйесінің IP мекенжайын және тұзақтарды қабылдау үшін пайдаланушының есептік деректерін көрсетіңіз. Ол үшін файлға келесі жолдарды қосыңыз:

```
trapsess -Ci -v3 -t0.1 -r1 -l authPriv -u <user name for receiving traps> -a <authentication algorithm> -A "
<user password for receiving traps>" -x <encryption algorithm> -X "<encryption password>" udp:<IP address>:162
```

snmpd қызметі конфигурацияланған.

Бірнеше бақылау жүйелерімен интеграциялау үшін әрбір жүйе үшін бөлек пайдаланушы тіркелгісін жасаңыз, әрбір пайдаланушы есептік жазбасы үшін қолжетімді ақпарат ауқымын көрсетіңіз ("view" және "rouser" директивалары) және SNMP тұзақтарын жіберуді конфигурациялаңыз ("trapsess" директивасы).

snmpd қызметін жаңа конфигурациямен іске қосу

Жаңа конфигурацияны қолдану үшін:

1. snmpd қызметін қайта іске қосыңыз:

   ```
   systemctl restart snmpd
   ```

2. snmpd қызметінің күйін тексеріңіз:

   ```
   systemctl status snmpd
   ```

   Күйі `running` болуы керек.

3. Операциялық жүйе іске қосылған кезде қызметтің автоматты түрде іске қосылуына рұқсат ету:

   ```
   systemctl enable snmpd
   ```

4. Егер сіз операциялық жүйеңізде немесе желілік жабдықта брандмауэр пайдалансаңыз, SNMP пакеттерінің өтуіне мүмкіндік беретін ережелерді қосыңыз.

snmpd қызметі жұмыс істеп тұр.

Егер snmpd қызметі конфигурацияланған кезде klcssnmp қызметі жұмыс істеп тұрса, klcssnmp қызметін де қайта іске қосыңыз.

snmpd қызметінің жұмысын тексеру

snmpd қызметін тексеру үшін Kaspersky Security Center Linux жүйесінде SNMP пайдалануын конфигурациялаңыз және snmpwalk утилитасын пайдаланып SNMP деректерін сұраңыз.

Kaspersky Security Center Linux ұсынған SNMP деректерінің ауқымын алу үшін,

келесі пәрменді орындаңыз:

```
snmpwalk -v3 -l authPriv -u <user name> -a <authentication algorithm> -A "<authentication password>" -x
<encryption algorithm> -X "<encryption password>" <IP address> .1.3.6.1.4.1.23668.1093.1
```

Мысалы:

```
snmpwalk -v3 -l authPriv -u MonitoringUser -a SHA -A "MonitoringAuthSecret" -x AES -X "MonitoringPrivSecret"
127.0.0.1 .1.3.6.1.4.1.23668.1093.1
```

SNMP арқылы хабарландыруды қосу және өшіру

Kaspersky Security Center Linux Басқару сервері оқиғалары туралы хабарландыруларды SNMP тұзақтары түрінде жібереді.

Әдепкі бойынша, Kaspersky Security Center Linux оқиғалары үшін SNMP хабарландырулары өшірілген.

Kaspersky Security Center Linux оқиғалары үшін SNMP арқылы хабарландыруды қосу немесе өшіру үшін:

1. Негізгі мәзірдегі басқару серверінің атауын басыңыз.

   Басқару серверінің сипаттары терезесі ашылады.

2. Сипаттар терезесінің **Оқиғаларды конфигурациялау** қойындысында SNMP хабарландыруларын алғыңыз келетін оқиға түрін басыңыз.

3. Ашылған терезеде **SNMP арқылы хабарлау** ауыстырып-қосқышын қосыңыз немесе өшіріңіз.

   Бұл опция тек **SNMP арқылы статистиканы жіберу** опциясы қосылған жағдайда ғана қолжетімді.

Kaspersky Security Center Linux оқиғаларына арналған SNMP хабарландырулары сіздің таңдауыңызға сәйкес қосылады немесе өшіріледі.

Kaspersky Security Center Linux жүйесінде SNMP қосу және өшіру

Әдепкі бойынша, SNMP арқылы статистика жіберу қосылған. SNMP тұзақтарын жіберу үшін snmpd қызметін конфигурациялаңыз.

SNMP арқылы статистика жіберуді қосу немесе өшіру үшін:

1. Негізгі мәзірдегі басқару серверінің атауын басыңыз.

   Басқару серверінің сипаттары терезесі ашылады.

2. **Жалпы** қойыншасында **SNMP** бөлімін таңдаңыз.

3. **SNMP арқылы статистиканы жіберу** ауыстырып-қосқышын қосыңыз немесе өшіріңіз.

4. **Сақтау** түймесін басыңыз.

SNMP арқылы статистика жіберу сіздің таңдауыңызға сәйкес қосылады немесе өшіріледі.

SNMP үшін нысан идентификаторларының мәндері

Төмендегі кестеде үшінші тарап бағдарламаларына Басқару серверінің өнімділігі туралы ақпаратты беру үшін пайдаланылатын нысан идентификаторының (бұдан әрі - OID) мәндері мен сипаттамалары келтірілген.

Нысан идентификаторларының мәндері	Деректердің сандық түрі	OID	Сипаттамасы
deploymentStatus	INTEGER { ok(0), info(1), warning(2), critical(3) }	.1.3.6.1.4.1.23668.1093.1.1.1	Орналастыру күйі. Күй келесі мәндердің біріне ие болуы мүмкін: • **Ақпараттық хабар**. Лицензия бұдан былай N құрылғылар үшін қолданылмайды. • **Ескерту**. Келесілердің бірі: Басқару сервері топтарындағы N құрылғыларда Kaspersky бағдарламалары орнатылған M құрылғылар (N > M). L лицензиясының мерзімі N құрылғыларда M күннен кейін өтіп кетеді. Бағдарламаларды орнату бойынша T тапсырмасы N құрылғыларда аяқталды, M құрылғылар үшін қайта іске қосу қажет. • **Критикалық**. Лицензия мерзімі N құрылғы үшін өтіп кеткен. • **OK**. Жоғары аталғандардың ешқайсысы.
noAntivirusSoftware	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.1.2.1	deploymentStatus көрсетіп тұрғандай, Басқару серверінің топтарында басқарылатын бағдарламалар орнатылмаған құрылғылар тым көп. Басқарылатын бағдарламалары жоқ бірнеше құрылғы анықталған болса, мәні 1-ге, ал басқа жағдайда – 0-ге тең.
remoteInstallTaskFailed	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.1.2.2	deploymentStatus, кейбір құрылғыларда қашықтан орнату тапсырмасын орындау мүмкін болмағанын көрсетеді. Осы құрылғылардың санын hostsRemoteInstallFailed көмегімен алуға болады.
licenceExpiring	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.1.2.3	deploymentStatus, лицензия мерзімі жеті күннен кейін өтіп кететін бірнеше құрылғының бар екенін көрсетеді. Осы құрылғылардың санын hostsLicenseExpiring көмегімен алуға болады.
licenceExpired	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.1.2.4	deploymentStatus, лицензия мерзімі өтіп кеткен бірнеше құрылғының бар екенін көрсетеді. Сіз осы құрылғылардың санын hostsLicenseExpired көмегімен біле аласыз.
hostsInGroups	Counter32	.1.3.6.1.4.1.23668.1093.1.1.3	Басқару серверінің топтарындағы құрылғылар саны.
hostsWithAntivirus	Counter32	.1.3.6.1.4.1.23668.1093.1.1.4	Басқарылатын бағдарламалары орнатылған Басқару сервері топтарындағы құрылғылардың саны.
hostsRemoteInstallFailed	Counter32	.1.3.6.1.4.1.23668.1093.1.1.5	Қашықтан орнату тапсырмасын орындау мүмкін болмаған құрылғылардың саны.
licenceExpiringSerial	OCTET STRING	.1.3.6.1.4.1.23668.1093.1.1.6	Жарамдылық мерзімі жақын арада, 7 күннен кем уақыттан кейін өтіп кететін лицензиялық кілт идентификаторы.
licenceExpiredSerial	OCTET STRING	.1.3.6.1.4.1.23668.1093.1.1.7	Жарамдылық мерзімі өтіп кеткен лицензиялық кілт идентификаторы.
licenceExpiringDays	Unsigned32	.1.3.6.1.4.1.23668.1093.1.1.8	Лицензия мерзімі өтіп кеткенге дейінгі күндер саны. Бұл параметр үшін, лицензия мерзімінің аяқталуына 7 күннен аз уақыт қалса, оның мерзімі аяқталды. Мерзімінің аяқталуына 7 күннен артық уақыт қалса, мән 0-ге тең болады.
hostsLicenceExpiring	Counter32	.1.3.6.1.4.1.23668.1093.1.1.9	Лицензия мерзімі жақында, 7 күннен кем уақыттан кейін өтіп кететін лицензиясы бар құрылғылардың саны.
hostsLicenceExpired	Counter32	.1.3.6.1.4.1.23668.1093.1.1.10	Лицензия мерзімі өтіп кеткен құрылғылар саны.

Нысан идентификаторларының мәндері	Деректердің сандық түрі	OID	Сипаттамасы
updatesStatus	INTEGER { ok(0), info(1), warning(2), critical(3) }	.1.3.6.1.4.1.23668.1093.1.2.1	Антивирустық дерекқорларды жаңарту күйі. Күй келесі мәндердің біріне ие болуы мүмкін: • **Ақпараттық хабар**. Басқару серверіндегі немесе құрылғылардағы антивирустық дерекқорлар бір күннен артық жаңартылмаған; бағдарлама орнатылғаннан бері бір күннен аз уақыт өтті. • **Ескерту**. Басқару серверіндегі немесе құрылғылардағы антивирустық дерекқорлар 3 күннен артық жаңартылмаған. Бұл мәнді топ сипаттарында өзгертуге болады. • **Критикалық**. Басқару серверіндегі немесе құрылғылардағы антивирустық дерекқорлар 7 күннен артық жаңартылмаған. Бұл мәнді топ сипаттарында өзгертуге болады. • **ОК**. Жоғары аталғандардың ешқайсысы.
serverNotUpdated	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.2.2.1	Басқару сервері көптен бері жаңартылмады. Ұзақ болып саналатын уақыт updatesStatus күйінде көрсетіледі.
notUpdatedHosts	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.2.2.2	Кейбір құрылғылардың ұзақ уақыт (әдепкі бойынша **Критикалық** – 7 күн және одан да көп, **Ескерту** – 3 күн) бойы жаңартылмаған. Сіз осы құрылғылардың санын hostsNotUpdated көмегімен біле аласыз.
lastServerUpdateTime	Hex-STRING	.1.3.6.1.4.1.23668.1093.1.2.3	Басқару серверінде антивирустық дерекқорлардың соңғы рет жаңартылған күні.
hostsNotUpdated	Counter32	.1.3.6.1.4.1.23668.1093.1.2.4	Ұзақ уақыт бойы жаңартылмаған антивирустық дерекқорлары бар құрылғылардың саны (әдепкі бойынша **Критикалық** - 7 күн немесе одан көп, **Ескерту** - 3 күн). **Критикалық** жаңарту күйі бар құрылғылар болса, тек сол құрылғылар ескеріледі. Жаңарту күйін updatesStatus көмегімен алуға болады.
protectionStatus	INTEGER { ok(0), warning(2), critical(3) }	.1.3.6.1.4.1.23668.1093.1.3.1	Нақты уақыт режимінде қорғау күйі. Келесілердің бірі: • **Ескерту**. Келесілердің бірі: Басқару серверіне кіретін құрылғыда қауіпсіздіктің бұзылғаны анықталды. Шифрлау қателеріне байланысты, кейбір құрылғылар қорғаныс күйін өзгертті. Толықтай сканерлеу көптен бері орындалмады. • **Критикалық**. Басқару серверінің топтарындағы кейбір құрылғыларда антивирустық қорғаныс жұмыс істемейді. • **ОК**. Жоғары аталғандардың ешқайсысы.
antivirusNotRunning	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.3.2.1	Қауіпсіздік бағдарламасы кейбір құрылғыларда жұмыс істемейді. Сіз осы құрылғылардың санын hostsAntivirusNotRunning көмегімен біле аласыз.
realtimeNotRunning	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.3.2.2	Нақты уақыт режимінде қорғау кейбір құрылғыларда жұмыс істемейді. Сіз осы құрылғылардың санын hostsRealtimeNotRunning көмегімен біле аласыз.
psRealtimeLevelChanged	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.3.2.3	Жұмыс уақытындағы қорғау деңгейі басқару топтарындағы N компьютерлерде әкімші орнатқан деңгейден өзгеше.
notCuredFound	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.3.2.4	Нысандары зарарсыздандырылмаған құрылғылар бар. Сіз осы құрылғылардың санын hostsNotCuredObject көмегімен біле аласыз.
tooManyThreats	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.3.2.5	Кейбір құрылғыларда қауіптер анықталды. Сіз осы құрылғылардың санын hostsTooManyThreats көмегімен біле аласыз.

Нысан идентификаторларының мәндері	Деректердің сандық түрі	OID	Сипаттамасы
virusOutbreak	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.3.2.6	Жүйенің вирустың тарауы күйі. Вирустардың белгілі бір саны белгіленген уақыт ішінде анықталған болса, мәні 1-ге, ал басқа жағдайларда – 0-ге тең болады. Вирустардың саны және уақыты Басқару серверінде Вирустық шабуыл параметрі көмегімен көрсетіледі.
psVulnerabilitiesFound	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.3.2.7	Осалдықтар анықталды.
psEncryptionFaultsFound	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.3.2.8	Құрылғының қорғаныс күйін өзгерткен шифрлау қателері анықталды.
psVulnerableHostsFound	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.3.2.9	Кейбір құрылғыларда осалдықтар анықталды.
psNotScannedLately	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.3.2.10	Ұзақ уақыт бойы толық сканерлеусіз құрылғылар анықталды.
psNagentsNotRunningUntilReboot	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.3.2.11	Желілік агент қайта іске қосылғаннан кейін ғана іске қосылатын құрылғылар анықталды.
hostsAntivirusNotRunning	Counter32	.1.3.6.1.4.1.23668.1093.1.3.3	Қауіпсіздік бағдарламалары іске қосылмаған құрылғылар саны.
hostsRealtimeNotRunning	Counter32	.1.3.6.1.4.1.23668.1093.1.3.4	Нақты уақыт режимінде қорғау іске қосылмаған құрылғылар саны.
hostsRealtimeLevelChanged	Counter32	.1.3.6.1.4.1.23668.1093.1.3.5	Нақты уақыт режимінде қорғау деңгейі жарамсыз болып табылатын құрылғылар саны.
hostsNotCuredObject	Counter32	.1.3.6.1.4.1.23668.1093.1.3.6	Нысандары зарарсыздандырылмаған құрылғылар саны.
hostsTooManyThreats	Counter32	.1.3.6.1.4.1.23668.1093.1.3.7	Қауіптері бар құрылғылар саны.
fullscanStatus	INTEGER { ok(0), info(1), warning(2), critical(3) }	.1.3.6.1.4.1.23668.1093.1.4.1	Антивирустық толықтай сканерлеу күйі келесілердің бірі: • **Ақпараттық хабар**. Бағдарламаны орнатқан сәттен бастап 7 күннен кем уақыт өтті. • **Ескерту**. Толықтай сканерлеу, бағдарлама орнатылған сәттен бастап 7 күннен артық уақыт бойы жүргізілмеді. • **Критикалық**. Толықтай сканерлеу, бағдарлама орнатылған сәттен бастап 14 күннен артық уақыт бойы жүргізілмеді. • **OK**. Жоғары аталғандардың ешқайсысы.
notScannedLately	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.4.2.1	Тексеру белгілі бір уақыт бойы орындалмаған кейбір құрылғылар. Сіз осы құрылғылардың санын hostsNotScannedLately көмегімен біле аласыз. Уақыты fullScanStatus күйінде көрсетіледі.
hostsNotScannedLately	Counter32	.1.3.6.1.4.1.23668.1093.1.4.3	Тексеру белгілі бір уақыт бойы орындалмаған құрылғылар саны. Уақыты fullScanStatus күйінде көрсетіледі.
logicalNetworkStatus	INTEGER { ok(0), warning(1), critical(2) }	.1.3.6.1.4.1.23668.1093.1.5.1	Басқару серверінің логикалық желісінің күйі. Келесілердің бірі: • **Ескерту**. Қатынасу мүмкін емес Ескерту күйі бар құрылғылар бар болса немесе Басқару серверінің ешбір тобына жатпайтын құрылғылар бар болса. • **Критикалық**. Басқару сервері бақылай алмай жатқан құрылғылар болса немесе қатынасу мүмкін емес Критикалық күйі бар құрылғылар болса. • **OK**. Жоғары аталғандардың ешқайсысы.

Нысан идентификаторларының мәндері	Деректердің сандық түрі	OID	Сипаттамасы
notConnectedLongTime	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.5.2.1	Кейбір құрылғылардың ұзақ уақыт бойы Басқару серверіне қосылмаған (**Ескерту** күйі бар құрылғылар үшін 7 күн және одан да көп және **Критикалық** күйі бар құрылғылар үшін 4 күн). Сіз осы құрылғылардың санын hostsNotConnectedLongTime көмегімен біле аласыз.
controlLost	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.5.2.2	Басқару сервері бақылай алмай жатқан құрылғылардың бар. Сіз осы құрылғылардың санын hostsControlLost көмегімен біле аласыз.
hostsFound	Counter32	.1.3.6.1.4.1.23668.1093.1.5.3	Басқару серверінің ешбір тобына кірмейтін Басқару сервері анықтаған құрылғылардың саны.
groupsCount	Counter32	.1.3.6.1.4.1.23668.1093.1.5.4	Басқару сервері топтарының саны.
hostsNotConnectedLongTime	Counter32	.1.3.6.1.4.1.23668.1093.1.5.5	Ұзақ уақыт бойы Басқару серверіне қосылмаған құрылғылардың саны. Ұзақ болып саналатын уақыт notConnectedLongTime күйінде көрсетіледі.
hostsControlLost	Counter32	.1.3.6.1.4.1.23668.1093.1.5.6	Басқару сервері бақыламайтын құрылғылардың саны.
eventsStatus	INTEGER { ok(0), info(1), warning(2), critical(3) }	.1.3.6.1.4.1.23668.1093.1.6.1	Оқиғалар ішкі жүйесінің күйі келесілердің бірі: • **Ескерту**. Келесілердің бірі: Басқару сервері топтарының құрылғылары ұзақ уақыт бойы Windows жаңартуларын іздемеді. Күймен байланысты мәселелер туындаған құрылғылар бар. • **Критикалық**. Келесілердің бірі: Кем дегенде бір құрылғыда "критикалық оқиға" бар. Кемінде бір құрылғыда "Функционалдық ақау" деңгейі бар оқиға орын алды. Кемінде бір құрылғыда тапсырманың сәтсіз аяқталуы оқиғасы бар. Басқару сервері топтарының құрылғылары ұзақ уақыт бойы Windows жаңартуларын іздемеді. Күймен байланысты мәселелер туындаған құрылғылар бар. • **Ақпараттық хабар.** Келесілердің бірі: Барлық құрылғыларда вирустарды толықтай сканерлеудің соңғы аптасынан аз уақыт өтті. Қашықтан орнату тапсырмалары аяқталды және ешбір құрылғы қайта іске қосуды қажет етпейді. Басқару серверінің соңғы жаңартуынан бері бір аптадан аз уақыт өтті. Басқару сервері ұзақ уақыт бойы жаңартылмаған, бірақ қазіргі уақытта жаңарту жүргізілуде. • **ОК**. Жоғары аталғандардың ешқайсысы.
criticalEventOccured	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.6.2.1	eventsStatus, Басқару серверінде критикалық оқиғалардың орын алғанын көрсетеді. Сіз осы оқиғалардың санын criticalEventsCount көмегімен ала аласыз. Кез келген құрылғыда кемінде бір критикалық оқиға болса, мәні 1-ге, ал басқа жағдайда – 0-ге тең.
criticalEventsCount	Counter32	.1.3.6.1.4.1.23668.1093.1.6.3	Басқару серверіндегі критикалық оқиғалардың саны.

Kaspersky Security: Бизнеске арналған Кәсіби лицензиясында Kaspersky Security Center Linux жүйесімен жұмыс істеу

EPP қолданбасы лицензиясының бір бөлігі ретінде Kaspersky Security: Бизнеске арналған Кәсіби лицензиясын және Kaspersky Security Center Linux лицензиясын сатып алсаңыз, бастапқы орнатуды орындағаннан кейін Kaspersky Security: Бизнеске арналған Кәсіби функцияларын пайдалана аласыз.

Kaspersky Security: Бизнеске арналған Кәсіби лицензиясын құрылғыларда Kaspersky қолданбаларын орнатып, белсендіргеннен кейін бұрын сатып алынған лицензияның кеңейтімі ретінде бөлек сатып алсаңыз, Kaspersky Security: Бизнеске арналған Кәсіби лицензиясын сатып алу әдісіне байланысты жаңа белсендіру кодын немесе кілт файлын пайдалану арқылы құрылғыларда Kaspersky Security Center Linux қызметін қайта белсендіру қажет. Содан кейін бастапқы орнатуды орындауға болады.

Сондай-ақ сынақ режимінде Kaspersky Security: Бизнеске арналған Кәсіби функционалдығын пайдалануға болады. Ол үшін алдымен қосалқы физикалық басқару серверін қосып, содан кейін бұл серверді сынақ Kaspersky Security: Бизнеске арналған Кәсіби лицензиясы бойынша белсендіру керек. Kaspersky Security: Бизнеске арналған Кәсіби функционалдығы сынақ лицензиясының мерзімінде қосалқы серверде қолжетімді болады.

Басқару серверін Kaspersky Security: Бизнеске арналған Кәсіби лицензиясы бойынша белсендіріп, тиісті басқару сервері басқаратын құрылғыларға лицензия кілтін орналастырғаннан кейін, келесі әрекеттерді орындауға болады:

- Kaspersky Automated Security Awareness Platform, Kaspersky Threat Intelligence Portal Sandbox және Active Directory интеграцияларын қолданып, қауіптерге жауап беру.
- Дабылдарды атрибуттар бойынша топтау.

Kaspersky Security: Бизнеске арналған Кәсіби лицензиясымен қосылған мүмкіндіктер туралы қосымша ақпаратты Kaspersky Endpoint Detection and Response Optimum анықтамасынан қараңыз.

Дабылдарға жауап беруге арналған интеграциялар

Сізде Kaspersky Security: Бизнеске арналған Кәсіби лицензиясы болса, қауіптерге жауап беру үшін интеграцияларды келесі шешімдермен конфигурациялауға болады:

- Kaspersky Automated Security Awareness Platform
- Kaspersky Threat Intelligence Portal Sandbox
- Active Directory

Бұл интеграциялар Басқару серверін Kaspersky Security: Бизнеске арналған Кәсіби лицензиясы бойынша белсендірген жағдайда қолжетімді.
Әрекет ету шараларын орындау үшін Kaspersky Security: Бизнеске арналған Кәсіби лицензиялық кілтін басқарылатын бағдарламаларға тарату керек.
Сынақ лицензиясы бойынша Kaspersky Security: Бизнеске арналған Кәсіби функционалдығын пайдаланған кезде, алдымен қосалқы физикалық басқару серверін қосып, осы қосалқы басқару серверін сынақ лицензиясы бойынша іске қосып, содан кейін осы басқару сервері басқаратын құрылғыларыңызға лицензия кілтін орналастыру керек.

Kaspersky Next EDR Optimum лицензиясын пайдалансаңыз, басқарылатын құрылғыларда Kaspersky Security: Бизнеске арналған Кәсіби лицензиясы бойынша орнатылған қолданбаларды белсендірудің қажеті жоқ. Мұны тек жаңа құрылғылар үшін жасау керек (бар болса).

Kaspersky Security: Бизнеске арналған Кәсіби лицензиясы көптиістілікке қолдау көрсететіндіктен, лицензия кілтін басқарылатын қолданбаларға орталықтан таратуға болады. Лицензияны қосымша және виртуалды басқару серверлеріне автоматты түрде таратуға қолдау көрсетілмейді.

Интеграцияларды конфигурациялау үшін **Жалпы мүмкіндіктер: Қолданба интеграциясы** функционалдық аймағында **Оқу** және **Жазу** құқықтары болуы керек.

Жауап әрекеттерін орындау үшін Active Directory көмегімен интеграцияны конфигурациялау

Active Directory интеграциясы дабыл әсер еткен немесе оған қатысты Active Directory пайдаланушылары үшін жауап әрекеттерін орындауға мүмкіндік береді.

Дабылдарға жауап беру үшін Active Directory интеграциясын конфигурациялау үшін Kaspersky Security Center Linux басқару серверінің 15.4 немесе одан кейінгі нұсқасын пайдалану керек.

Дабылдарға жауап беруге арналған Active Directory интеграциясы және домен контроллері сауалнамасын конфигурациялау кезінде сіз көрсеткен Active Directory домен контроллерін сканерлеу параметрлері (домен контроллерінің мекенжайы мен пайдаланушының тіркелгі деректері) — екі түрлі параметр. Жауап әрекеті орындалатын пайдаланушыда Active Directory есептік жазбасы бар екеніне көз жеткізу қажет болғандықтан, екі интеграцияны да конфигурациялау керек: сканерлеу және жауап беру үшін. Реті маңызды емес.

Интеграция параметрлері мұраланбайды және тек осы параметрлерді конфигурациялайтын басқару серверіне (физикалық немесе виртуалды) қолданылады.

Дабылдарға жауап беруде Active Directory интеграциясын конфигурациялау үшін:

1. Негізгі мәзірдегі басқару серверінің атауын басыңыз.

   Жалпы қойындысы таңдалған басқару сервері сипаттарының терезесі ашылады.

2. Келесі әрекеттердің бірін орындаңыз:

   - **Тарату нүктелері** бөлімін таңдап, қажетті тарату нүктесінің атын басыңыз, содан кейін ашылатын сипаттар терезесінде **Active Directory** бөлімін таңдаңыз.
   - **Active Directory жауабы** бөлімін таңдаңыз.

3. Оң жақ тақтадағы **Active Directory интеграциясы** ауыстырып-қосқышын қосыңыз.

   Кейінірек интеграцияны өшіргіңіз келсе, оны тек **Active Directory интеграциясы** ауыстырып-қосқышын өшіру арқылы барлық қосылым үшін орындауға болады. Бөлек қосылым үшін интеграцияны өшіре алмайсыз. Оның орнына қосылымды жоюға болады.

   > **Active Directory интеграциясы** ауыстырып-қосқышын қосқанда немесе өшіргенде, параметр **Active Directory жауабы** және **Тарату нүктелері** бөлімдері үшін қолданылады.

4. **Қосу** түймесін басып, Active Directory домен контроллерінің қосылымын жасаңыз.

5. Ашылған терезеде қосылымға арналған келесі параметрлерді көрсетіңіз:

   - **Домен контроллерінің мекенжайы**

     Компьютер атауы, мысалы: `server.mycompany.com`.

     Бірнеше мекенжайды көрсетуге болады. Мекенжайлары көрсетілген барлық домен контроллері бір доменге тиесілі болуы керек.

   - **Active Directory домен атауы**

     DNS толық домен аты, мысалы: `mycompany.com`

     Сондай-ақ SAM немесе NetBIOS атауын көрсетуге болады, мысалы: `mycompany`

     Кіші әріптерді пайдаланыңыз. Басқару сервері немесе тарату нүктесі үшін бірнеше қосылым жасасаңыз, әр қосылым үшін әртүрлі атауларды көрсетіңіз.

     > Жауап беру әрекеттерін орындау үшін осы өрісте көрсеткен Active Directory домен атауы ескертуде көрсетілген Active Directory домен атауына сәйкес келуі керек.

   - **Логин**

     Жауап әрекеттері орындалатын әкімші құқықтары бар Active Directory есептік жазбасының атауы.

   - **Құпиясөз**

     Әкімші құқықтары бар Active Directory есептік жазбасының құпиясөзі, ол бойынша жауап әрекеттері орындалады.

6. Қосылым күйін тексергіңіз келсе, **Байланысты тексеру** түймесін басыңыз.

   Қосылым сәтті орнатылса, **Қосылған** күйі көрсетіледі. Әйтпесе күй **Сәтсіз аяқталды** болады және сіз қосыла алмаған домен контроллерлерімен қате туралы хабар көрсетіледі.

Active Directory қызметіне қосылу жолын ескеру қажет: **Linux құрылғысынан немесе Windows құрылғысынан**.

Linux құрылғысынан қосылу

Әдепкісінше Linux құрылғысынан домен контроллеріне қосылу және аутентификациялау кезінде логика келесідей:

1. Басқару сервері немесе тарату нүктесі LDAPS арқылы домен контроллеріне қосылуға әрекеттенуде.

   LDAP сервері сертификатын қатаң тексеру орындалады.

2. Сертифтикатты тексеру үшін домен контроллері сертификатының жалпы бөлігін жүйенің сертификаттар қоймасына орналастырыңыз.

   Жүйе сертификатының органына (CA) ОЖ-ға тәуелді жол сертификаттар тізбегіне кіру үшін пайдаланылады.

   Мысалы:

   - /etc/ssl/certs/ca-certificates.crt — Debian негізіндегі операциялық жүйелерге арналған жол (Debian, Ubuntu, Astra).
   - /etc/pki/ca-trust/extracted/pem/tls-ca-bundle.pem — CentOS немесе Red Hat үшін жол.

3. LDAPS қосылымы сәтсіз болса, қате орын алады және басқа қосылым протоколы пайдаланылмайды.

   LDAPS ақаулары туындаған жағдайда, Kaspersky техникалық қолдау қызметіне хабарласуға болады.

Сертификатты жүйенің сертификаттар қоймасына орнатқыңыз келмесе, домен контроллері сертификатына жолды орнату үшін KLNAG_LDAP_SSL_CACERT жалауын пайдалануға болады. Ол үшін пәрменді іске қосыңыз:

```
klscflag -fset -pv klnagent -n KLNAG_LDAP_SSL_CACERT -t s -v "</path/to/domain-controller/cert>"
```

мұндағы `</path/to/domain-controller/cert>` — домен контроллері сертификатының жалпыға ортақ бөлігіне апаратын жол.

Мысалы, жол `"/var/opt/kaspersky/ldap_cert.crt"` болса, пәрмен — `klscflag -fset -pv klnagent -n KLNAG_LDAP_SSL_CACERT -t s -v "/var/opt/kaspersky/ldap_cert.crt"`

Windows құрылғысынан қосылу

Windows құрылғысынан домен контроллеріне қосылған және аутентификациялаған кезде, қосылым параметрлері домен арқылы анықталады.

Сізге тек мынаны қамтамасыз ету керек:

- LDAPS қосылған және құрылғыда 636 порты қолжетімді.
- Желілік экран немесе прокси-сервер арқылы домен контроллеріне қосылуға рұқсат берілген.

7. **Сақтау** түймесін басыңыз.

Терезе жабылып, қосылым қосылымдар кестесінде көрсетіледі.

Қосылымдар кестесінде келесі әрекеттерді орындауға болады:

- Қосылым параметрлерін өңдеу.

  Ол үшін қажетті қосылымға арналған **Домен контроллерінің мекенжайы** параметрі бар сілтемені басыңыз. Ашылған терезеде қажетті параметрлерді өзгертіп, **Сақтау** түймесін басыңыз.

  Тек **Логин** және **Құпиясөз** параметрлерін өңдей аласыз.

- Қосылымдарды жойыңыз.

  Ол үшін жойғыңыз келетін қосылымның жанындағы құсбелгіні қойып, құралдар тақтасындағы **Өшіру** түймесін басып, қосылымды жоюды растаңыз.

Kaspersky Automated Security Awareness Platform-мен интеграцияны конфигурациялау

Kaspersky Automated Security Awareness Platform (бұдан әрі KASAP деп аталады) интеграциясы KASAP оқыту курстарын дабылдармен байланысты пайдаланушыларға тағайындауға мүмкіндік береді.

Интеграция параметрлері мұраланбайды және тек осы параметрлерді конфигурациялайтын басқару серверіне (физикалық немесе виртуалды) қолданылады.

> Kaspersky Security Center Web Console-де интеграцияны конфигурацияламай тұрып, авторизация токенін жасап, KASAP жүйесінде API сұраулары үшін URL мекенжайын алуыңыз керек.

Kaspersky Automated Security Awareness Platform-мен интеграцияны конфигурациялау үшін:

1. Негізгі мәзірдегі басқару серверінің атауын басыңыз.

   Жалпы қойыншасында Басқару сервері сипаттары терезесі ашылады.

2. **KASAP** бөлімін таңдаңыз.
3. Оң жақ тақтада **KASAP интеграциясы** ауыстырып-қосқышын қосыңыз.
4. KASAP-қа қосылу үшін пайдаланылатын параметрлерді көрсетіңіз:

   - **API токені**: KASAP Open API-ге кіру үшін жасалған токен.
   - **URL**: API токенін жасау кезінде алынған API сұрауларына арналған URL.

- **Прокси-серверді пайдалану**: KASAP жүйесіне қосылу кезінде прокси-серверді пайдалануға мүмкіндік беретін ауыстырып-қосқыш.

  Ауыстырып-қосқыш әдепкісінше өшірулі болады.

5. Қажет болса, **Байланысты тексеру** түймесін басу арқылы көрсеткен параметрлерді тексеріңіз.

   Байланыс күйі көрсетіледі.

6. **Сақтау** түймесін басыңыз.

Kaspersky Automated Security Awareness Platform интеграциясы конфигурацияланған.

KASAP интеграция параметрлері сақталғаннан кейін, **Топтарды көру** түймесін басу арқылы KASAP оқыту топтарының тізімін көруге болады.

Қажет болса, топтар тізімі көрсетілгенде, **Топтарды жаңарту** түймесін басу арқылы оны жаңартуға болады.

Тізімді ашқаннан кейін оны жасыра алмайсыз. **KASAP интеграциясы** ауыстырып-қосқышын өшірсеңіз, KASAP топтарының тізімі көрсетілмейді.

Kaspersky Threat Intelligence Portal Sandbox интеграциясын конфигурациялау

Kaspersky Threat Intelligence Portal (бұдан әрі Kaspersky TIP деп аталады) интеграциясы Kaspersky Sandbox (корпоративтік желіден оқшауланған қауіпсіз орта) көмегімен **Карантин** бөліміне жіберілген файлдарды орындауға мүмкіндік береді.

Интеграция параметрлері мұраланбайды және тек осы параметрлерді конфигурациялайтын басқару серверіне (физикалық немесе виртуалды) қолданылады.

Интеграцияны конфигурациялау алдында Kaspersky TIP жүйесінде API сұраулары үшін авторизация токенін алуыңыз керек.

Kaspersky TIP Sandbox интеграциясын конфигурациялау үшін:

1. Негізгі мәзірдегі басқару серверінің атауын басыңыз.

   Жалпы қойыншасында Басқару сервері сипаттары терезесі ашылады.

2. **Kaspersky TIP** таңдаңыз.

3. Оң жақ тақтада **Біріктіру** ауыстырып-қосқышын қосыңыз.

   Kaspersky TIP жүйесіне қосылу параметрлері көрсетіледі.

   Интеграция параметрлерін конфигурациялап, сақтағаннан кейін, **Біріктіру** ауыстырып-қосқышын өшіріңіз, параметрлер жойылмайды, бірақ жауап әрекетін орындай алмайсыз.

4. **Токен қосу** түймесін басып, ашылған терезеде Kaspersky TIP жүйесінде бұрын алған токенді көрсетіңіз, содан кейін **Қосу** түймесін басыңыз.

   Терезе жабылады және API токені қосылады.

5. Kaspersky TIP қызметіне қосылу кезінде прокси-серверді пайдаланғыңыз келсе, **Прокси-серверді пайдалану** ауыстырып-қосқышын қосыңыз.

   Ауыстырып-қосқыш әдепкісінше өшірулі болады.

6. **Сақтау** түймесін басыңыз.

Kaspersky TIP Sandbox интеграциясы конфигурацияланды.

Енді қауіпті талдау үшін **Карантин** бөліміндегі файлдарды Kaspersky TIP Sandbox жүйесіне жіберуге болады. Файлдың максималды өлшемі – 100 МБ.

Kaspersky Security: Бизнеске арналған Кәсіби лицензиясы көптиістілікке қолдау көрсететіндіктен, файлдар **Карантин** қойылады. Бұл тенант деңгейіндегі бөлініс әкімші әрбір тенантқа қатысты арнайы TIP есептік жазбасын және API токенін пайдаланған кезде Kaspersky TIP Sandbox жүйесіне файлдарды жіберу және нәтижелерді қарау кезінде де қолданылады. Дегенмен барлық тенант үшін **Карантин** бөлімін орталықтандырылған басқару мүмкін емес, себебі карантин тізімі сервер иерархиясына сәйкес нысандарды көрсетпейді.

Дабылдарды атрибуттар бойынша топтау

Дабылдарды біріктіру бір оқиғаға қатысты болуы мүмкін дабылдарды анықтауға көмектеседі, зерттеу процесін жеңілдетеді.

Дабылдарды біріктіру функциясын қосу үшін келесі әрекеттерді орындау керек:

- Негізгі мәзірде **Дабылдар** ішкі бөлімін қосыңыз.
- Kaspersky Security: Бизнеске арналған Кәсіби лицензиясында басқару серверін белсендіріңіз, содан кейін басқарылатын қолданбаларға Kaspersky Security: Бизнеске арналған Кәсіби лицензия кілтін орналастырыңыз.

  Kaspersky Security: Бизнеске арналған Кәсіби функционалдығын сынақ режимінде сынақ лицензия пайдаланған кезде, алдымен қосалқы физикалық басқару серверін қосып, содан кейін бұл лицензияда осы серверді іске қосыңыз.

Kaspersky Next EDR Optimum лицензиясын пайдалансаңыз, басқарылатын құрылғыларда Kaspersky Security: Бизнеске арналған Кәсіби лицензиясы бойынша орнатылған қолданбаларды белсендірудің қажеті жоқ. Мұны тек жаңа құрылғылар үшін жасау керек (бар болса).
Kaspersky Security: Бизнеске арналған Кәсіби лицензиясы көптиістілікке қолдау көрсететіндіктен, лицензия кілтін басқарылатын қолданбаларға орталықтан таратуға болады. Лицензияны қосымша және виртуалды басқару серверлеріне автоматты түрде таратуға қолдау көрсетілмейді.

Дабылдарды құрылғы атауы, есептік жазба немесе хэш атауы (SHA256) бойынша біріктіруге болады.

Дабылдар атрибут (ол бос болмаса) бойынша біріктіріледі.

Дабылдар кем дегенде бір атрибутты ортақ пайдаланса және топтағы кез келген басқа дабылдан кейін 24 сағат ішінде пайда болса, біріктіріледі.

Дабылдарды атрибуттар бойынша біріктіру үшін:

1. Негізгі мәзірде **Мониторинг** → **Дабылдар** тармағына өтіңіз.

2. Келесі әрекеттердің бірін орындаңыз:

   - **Дабылдарды біріктіру** ауыстырып-қосқышын қосыңыз, содан кейін дабылдарды біріктіру үшін бір немесе бірнеше атрибут таңдаңыз:

     - **Құрылғы атауы**
     - **Есептік жазба**
     - **Файл хэші (SHA256)**

     Құрылғы атауы және **Есептік жазба** атрибуттары әдепкісінше таңдалады.

   - Параметрлер белгішесін (⚙) басыңыз. Ашылған **Кесте параметрлері** тақтасында **Топтау** қойындысына өтіңіз. **Біріктіру тобының идентификаторы** опциясын таңдап, **Қолдану** түймесін басыңыз.

   Біріктіру қосылған кезде, дабылдар ең жаңадан ең ескісіне қарай **Оқиға уақыты** бойынша сұрыпталады. Қосымша сұрыптау опцияларына қолдау көрсетілмейді. Басқа топтау опциясы таңдалса, біріктіру өшеді.

Кестеде атрибуттар бойынша жинақталған дабылдар көрсетіледі. Біріктірілмеген дабылдар кестенің төменгі жағында көрсетіледі.

Әрбір дабыл біріктірілгеннен кейін тек бір топқа тағайындалады.

Kaspersky Security Center Web Console-ін Kaspersky басқа шешімдерімен біріктіру

Бұл бөлімде Kaspersky Security Center Web Console серверінен Kaspersky Managed Detection and Response сияқты Kaspersky басқа бағдарламасына қатынасуды қалай конфигурациялау керектігі сипатталған. Бұл бөлімде SIEM жүйелеріне экспорттауды қалай конфигурациялау керектігі сипатталған.

Фондық қосылым орнату

Kaspersky Security Center Linux Kaspersky басқа бағдарламасымен немесе шешімімен, мысалы, Kaspersky Managed Detection and Response (бұдан әрі – MDR) өзара әрекеттесуін конфигурациялау үшін, Kaspersky Security Center Web Console мен Басқару сервері арасында сервис аралық қосылымды орнату қажет. Есептік жазбада **Жалпы функциялар: Пайдаланушы құқықтары** функционалды аймағының Нысанның ACL тізімдерін өзгерту құқығы болса ғана, бұл қосылымды орнатуға болады.

Тек Kaspersky Managed Detection and Response және Kaspersky Security Center бағдарламасының Windows негізіндегі нұсқасы арасындағы өзара әрекетті конфигурациялауға болады.

Фондық қосылым орнату үшін:

1. Бағдарламаның негізгі терезесінде **Параметрлер** → **Біріктіру** бөліміне өтіңіз.
2. **Web Console прокси-серверінің параметрлері** қойындысын таңдаңыз.
3. **Біріктіру** бөлімінде фондық қосылымды орнату қосқышын **Біріктіру үшін фондық қосылу Қосулы** күйіне ауыстырыңыз.
4. **Фондық қосылымды қосу** бөлімінде **OK** түймесін басыңыз.

Kaspersky Security Center Web Console веб-консолі мен Басқару сервері арасында фондық қосылым орнатылды. Басқару сервері фондық қосылым үшін есептік жазба жасайды және бұл есептік жазба Kaspersky Security Center Linux басқа бағдарламамен немесе Kaspersky шешімімен өзара әрекеттесуін қолдау үшін қызметтік есептік жазба ретінде пайдаланылады. Бұл қызмет есептік жазбасының атауында NWCSvcUser префиксі бар. Басқару сервері қауіпсіздік мақсатында 30 күн сайын қызмет есептік жазбасының құпия сөзін автоматты түрде өзгертеді. Қызмет есептік жазбасын қолмен жою мүмкін емес. Басқару сервері бұл есептік жазбаны сервис аралық байланыс өшірілген кезде автоматты түрде жояды. Басқару сервері әрбір Kaspersky Security Center Web Console және Басқару консолі үшін бір қызмет есептік жазбасын жасайды және барлық қызмет есептік жазбаларын ServiceNwcGroup деп аталатын қауіпсіздік тобына тағайындайды. Басқару сервері бұл қауіпсіздік тобын Kaspersky Security Center Linux орнату процесінде автоматты түрде жасайды. Сіз осы қауіпсіздік тобын қолмен жоя алмайсыз.

Прокси-сервер қосылымын конфигурациялау

Kaspersky Security Center Web Console мен веб-плагиндерге арналған прокси-сервер қосылымын конфигурациялау үшін:

1. Бағдарламаның негізгі терезесінде **Параметрлер** → **Біріктіру** бөліміне өтіңіз.
2. **Web Console прокси-серверінің параметрлері** қойындысын таңдаңыз.
3. **Прокси-серверді пайдалану** опциясын қосыңыз.
4. Прокси-сервер қосылымының параметрлерін көрсетіңіз:
   - **Прокси серверінің мекенжайы**
   - **Порт нөмірі**
   - **Прокси-сервердегі түпнұсқалық растама**
   - **Пайдаланушы аты** (**Прокси-сервер аутентификациясы** опциясын қоссаңыз қажет)
   - **Құпиясөз** (**прокси-сервер аутентификациясы** опциясын қоссаңыз қажет)
5. Прокси-сервердің қосылым параметрлерін сақтау үшін **Сақтау** түймесін басыңыз.

Егер сізде Басқару серверлерінің иерархиясы болса, прокси-сервер Қосылымдарының параметрлері қосалқы Басқару серверлерін басқаратын Web Console веб-консольдеріне таратылмайды. Әрбір Kaspersky Security Center Web Console веб-консолі үшін прокси-сервер қосылымын бөлек конфигурациялау керек.

Клиент құрылғыларын қашықтан диагностикалау

Windows және Linux негізіндегі клиенттік құрылғыларда келесі әрекеттерді қашықтан орындау үшін қашықтағы диагностиканы пайдалануға болады:

- Трассалауды қосу және өшіру, трассалау деңгейін өзгерту және трассалау файлын жүктеу
- Жүйелік ақпарат пен бағдарлама параметрлерін жүктеу
- Оқиғалар журналдарын жүктеу
- Бағдарламадан алынған қоқыс файлын жасау
- Диагностиканы іске қосу және диагностика нәтижелерін жүктеу
- Бағдарламаларды іске қосу, тоқтату және қайта іске қосу

Ақауларды жою үшін клиент құрылғысынан жүктелген оқиғалар журналы мен диагностикалық есептерді пайдалануыңызға болады. Сондай-ақ, Kaspersky Техникалық қолдау қызметіне хабарласатын болсаңыз, онда Kaspersky техникалық қолдау маманы сізден трассалау файлдарын, қоқыс файлдарын, оқиғалар журналын және диагностикалық есептерді Kaspersky талдау мақсатымен клиент құрылғысынан жүктеп алуды сұрауы мүмкін.

Қашықтан диагностикалау терезесін ашу

Windows және Linux негізіндегі клиенттік құрылғыларда қашықтағы диагностиканы орындау үшін алдымен қашықтан диагностикалау терезесін ашу керек.

Қашықтан диагностикалау терезесін ашу үшін:

1. Қашықтан диагностикалау терезесін ашқыңыз келетін құрылғыны таңдау үшін келесі әрекеттердің бірін орындаңыз:
   - Құрылғы басқару тобына тиесілі болса, басты мәзірде **Активтерді басқару** → **Активтер (құрылғылар)** бөліміне өтіңіз.
   - Құрылғы тағайындалмаған құрылғылар тобына жататын болса, басты мәзірде **Активтерді басқару** → **Тағайындалмаған құрылғылар** бөліміне өтіңіз.
2. Қажетті құрылғының атауын басыңыз.
3. Ашылған құрылғының сипаттар терезесінде **Кеңейтілген** бөлімін таңдаңыз.
4. **Кеңейтілген** қойындысында **Қашықтан диагностикалау** түймесін басыңыз.

   Нәтижесінде, клиент құрылғысының **Қашықтан диагностикалау** терезесі ашылады. Басқару сервер мен клиенттік құрылғы арасында байланыс болмаса, қате туралы хабар пайда болады.

Linux жүйесімен жұмыс істейтін клиенттік құрылғы туралы барлық диагностикалық ақпаратты бірден алу қажет болса, сол құрылғыда collect.sh скриптісін іске қосуға болады.

Бағдарламалар үшін трассалауды қосу және өшіру

xperf трассалауын қоса, бағдарламалар үшін трассалауды қосуға және өшіруге болады.

Трассалауды қосу және өшіру

Қашықтағы құрылғыда трассалауды қосу немесе өшіру үшін:

1. Клиент құрылғысын қашықтан диагностикалау утилитасын ашыңыз.
2. Қашықтан диагностикалау терезесінде **Kaspersky бағдарламалары** бөлімін таңдаңыз.

   Бағдарламаларды басқару бөлімінде құрылғыға орнатылған Kaspersky қолданбаларының тізімі көрсетілген.
3. Қолданбалар тізімінде трассалауды қосу немесе өшіру қажет қолданбаны таңдаңыз.

   Қашықтан диагностикалау параметрлері тізімі ашады.
4. Трассалауды қосқыңыз келсе:

   a. **Трассирлеу** бөлімінде **Трассирлеуді қосу** түймесін басыңыз.

   b. Ашылған **Трассирлеу деңгейін өзгерту** терезесінде әдепкі бойынша белгіленген мәндерді өзгертпеу ұсынылады. Қажет болса, Техникалық қолдау қызметінің маманы сізді конфигурациялау процесі арқылы өткізеді. Келесі параметрлер қолжетімді:

   - **Трассирлеу деңгейі**

     Трассалау деңгейі, трассалау файлындағы ақпарат құрамын анықтайды.

   - **Айналдыру негізіндегі трассирлеу**

     Бағдарлама трассалау файлының шамадан тыс ұлғаюына жол бермеу үшін трассалау ақпаратын қайта жазады. Трассалау ақпаратын сақтау үшін пайдаланылатын файлдардың ең көп санын және әр файлдың ең үлкен өлшемін көрсетіңіз. Ең үлкен өлшемдегі трассирлеу файлдарының ең көп саны жазылған болса, ең ескі трассирлеу файлы жойылады, осылайша жаңа трассирлеу файлын жазуға болады.

     Бұл параметр тек Kaspersky Endpoint Security үшін ғана қолжетімді.

   c. **Сақтау** түймесін басыңыз.

Трассалау таңдалған бағдарлама үшін қосулы. Кейбір жағдайларда, қауіпсіздік бағдарламасын трассалауды қосу үшін осы бағдарламаны және оның тапсырмасын қайта іске қосу қажет.

Linux жүйесінде жұмыс істейтін клиенттік құрылғыларда желілік агентті жаңарту компонентін трассалау желілік агент параметрлері арқылы реттеледі. Сондықтан Linux арқылы басқарылатын клиенттік құрылғыларда осы компонент үшін **Трассирлеуді қосу** және **Трассирлеу деңгейін өзгерту** параметрлері өшірілген.

5. Таңдалған қолданба үшін трассалауды қосқыңыз келсе, **Трассирлеуді өшіру** түймесін басыңыз.

   Трассалау таңдалған бағдарлама үшін өшірулі.

Xpref трассалауын қосу

Kaspersky Endpoint Security үшін Техникалық қолдау қызметінің мамандары жүйенің өнімділігі туралы ақпарат алу үшін сізден Xperf трассалауын қосуыңызды сұрауы мүмкін.

Xperf трассалауын қосу, орнату немесе өшіру үшін:

1. Клиент құрылғысын қашықтан диагностикалау утилитасын ашыңыз.

2. Қашықтан диагностикалау терезесінде **Kaspersky бағдарламалары** бөлімін таңдаңыз.

   Бағдарламаларды басқару бөлімінде құрылғыға орнатылған Kaspersky қолданбаларының тізімі көрсетілген.

3. Бағдарламалар тізімінен Kaspersky Endpoint Security for Windows таңдаңыз.

   Kaspersky Endpoint Security for Windows үшін қашықтан диагностикалау параметрлері тізімі көрсетіледі.

4. **Xpref трассирлеу** бөлімінде **Xperf трассирлеуді қосу** түймесін басыңыз.

   Xperf трассалау әлдеқашан қосылған болса, **Xperf трассирлеуді өшіру** түймесі көрсетіледі. Kaspersky Endpoint Security for Windows үшін Xperf трассалауын өшіргіңіз келсе, осы түймені басыңыз.

5. Ашылған **Xperf трассирлеу деңгейін өзгерту** терезесінде, Техникалық қолдау қызметі маманының сұрауына қарай, келесі әрекеттерді орындаңыз:

   a. Трассалау деңгейлерінің бірін таңдаңыз:

   - **Жеңіл деңгей**

     Бұл түрдегі трассирлеу файлы жүйе туралы ақпараттың ықшам өлшемін қамтиды.

     Әдепкі бойынша, осы нұсқа таңдалған.

   - **Күрделі деңгей**

     Бұл түрдегі трассалау файлы *Жеңіл деңгей* типті файлдан да егжей-тегжейлі ақпаратты қамтиды және *жеңіл деңгейлі* трассалау файлындағы ақпарат өнімділікті бағалау үшін жеткіліксіз болса, Техникалық қолдау қызметінің мамандары тарапынан сұралуы мүмкін. *Егжей-тегжейлі деңгейдегі* трассирлеу файлы жабдық, операциялық жүйе туралы ақпаратты, іске қосылған және аяқталған процестер мен бағдарламалардың тізімін, өнімділікті бағалау үшін пайдаланылатын оқиғаларды және Windows жүйесін бағалау құралының оқиғаларын қамтиды.

b. Xperf трассалау деңгейлерінің бірін таңдаңыз:

- **Негізгі түрі**

  Бағдарлама трассалау деректерін Kaspersky Endpoint Security бағдарламасы жұмыс істеп тұрған кезде алады.

  Әдепкі бойынша, осы нұсқа таңдалған.

- **Қайта бастау түрі**

  Бағдарлама, басқарылатын құрылғыда операциялық жүйе іске қосылған кезде трассалау деректерін алады. Осы трассалау түрі, жүйенің өнімділігіне әсер ететін мәселе құрылғыны қосқаннан кейін және Kaspersky Endpoint Security іске қосылмай тұрып пайда болған кезде тиімді болады.

Сондай-ақ, трассалау файлының шамадан тыс ұлғаюына жол бермеу үшін **Айналдыру файлының өлшемі, МБ** параметрін қосу ұсынылуы мүмкін. Трассалау файлының ең үлкен өлшемін көрсетіңіз. Файл ең үлкен өлшемге жеткенде, ең ескі трассирлеу файлы жаңа файлмен алмастырылып, қайта жазылады.

c. Ротация файлының өлшемін анықтаңыз.

d. **Сақтау** түймесін басыңыз.

Xperf трассалау қосылған және конфигурацияланған.

6. Kaspersky Endpoint Security for Windows үшін Xperf трассалауын өшіргіңіз келсе, **Xpref трассирлеу** бөліміндегі **Xperf трассирлеуді өшіру** түймесін басыңыз.

   Xpref трассалау өшірулі болса.

Бағдарламаны трассалау файлын жүктеу

Бағдарламаны трассирлеу файлын жүктеп алу үшін:

1. Клиент құрылғысын қашықтан диагностикалау утилитасын ашыңыз.

2. Қашықтан диагностикалау терезесінде **Kaspersky бағдарламалары** бөлімін таңдаңыз.

   Бағдарламаларды басқару бөлімінде құрылғыға орнатылған Kaspersky қолданбаларының тізімі көрсетілген.

3. Қолданбалар тізімінен трассирлеу файлын іске қосқыңыз келетін қолданбаны таңдаңыз.

4. **Трассирлеу** бөлімінде **Трассирлеу файлдары** түймесін басыңыз.

   Құрылғыны трассирлеу журналдары терезесі ашылып, онда трассалау файлдары тізімі көрсетіледі.

5. Трассалау файлдары тізімінен жүктегіңіз келетін файлды таңдаңыз.

6. Келесі әрекеттердің бірін орындаңыз:

   - **Жүктеп алу** түймесін басып, таңдалған файлды жүктеңіз. Жүктеп салу үшін бір немесе бірнеше файлды таңдауға болады.
   - Таңдалған файлдың бөлігін жүктеңіз:

     a. **Файл бөлігін жүктеп алу** түймесін басыңыз.

     Бірнеше файлды бір уақытта ішінара жүктеу мүмкін емес. Бірнеше трассалау файлын таңдасаңыз, **Файл бөлігін жүктеп алу** түймесі өшіріледі.

     b. Ашылған терезеде, өз талаптарыңызға сай жүктеу үшін файлдың аты мен бөлігін көрсетіңіз.

     Linux арқылы басқарылатын құрылғылар үшін файл бөлігінің атауын өзгерту мүмкін емес.

     c. **Жүктеп алу** түймесін басыңыз.

Таңдалған файл немесе оның бөлігі сіз көрсеткен орналасқан жерге жүктеледі.

Трассалау файлдарын жою

Енді қажет емес трассалау файлдарын жоя беруге болады.

Трассирлеу файлын жою үшін келесі қадамды орындаңыз:

1. Клиент құрылғысын қашықтан диагностикалау утилитасын ашыңыз.
2. Ашылатын қашықтағы диагностика терезесінде **Оқиға журналдары** бөлімін таңдаңыз.
3. Қай трассалау файлдарын жойғыңыз келетініне байланысты **Трассирлеу файлдары** бөлімінде **Windows жаңарту журналдары** немесе **Қашықтан орнату журналдары** түймесін басыңыз.

   Windows жаңарту журналдары сілтемесі тек Windows арқылы басқарылатын клиенттік құрылғылар үшін қолжетімді.

   Құрылғыны трассирлеу журналдары терезесі ашылып, онда трассалау файлдары тізімі көрсетіледі.
4. Трассалау файлдары тізімінен жойғыңыз келетін бір немесе бірнеше файлды таңдаңыз.
5. **Жою** түймесін басыңыз.

Таңдалған трассалау файлдары жойылды.

Бағдарламалар параметрлерін жүктеу

Клиент құрылғысынан бағдарлама параметрлерін жүктеп алу үшін:

1. Клиент құрылғысын қашықтан диагностикалау утилитасын ашыңыз.
2. Қашықтан диагностикалау терезесінде **Kaspersky бағдарламалары** бөлімін таңдаңыз.
3. Клиенттік құрылғыда орнатылған қолданбалардың параметрлері туралы ақпаратты жүктеу үшін **Бағдарлама параметрлері** бөлімінде **Жүктеп алу** түймесін басыңыз.

Ақпараты бар ZIP мұрағаты көрсетілген орынға жүктеледі.

Клиенттік құрылғыдан жүйелік ақпаратын жүктеп алу

Клиенттік құрылғыдан жүйелік ақпаратты жүктеп алу үшін мына қадамдарды орындаңыз:

1. Клиент құрылғысын қашықтан диагностикалау утилитасын ашыңыз.
2. Қашықтан диагностикалау терезесінде **Жүйе туралы ақпарат** бөлімін таңдаңыз.
3. Клиент құрылғысы туралы жүйелік ақпаратты жүктеу үшін **Жүктеп алу** түймесін басыңыз.

   Linux арқылы басқарылатын құрылғы туралы жүйелік ақпаратты алсаңыз, алынған файлға қатемен аяқталған қолданбаларға арналған қоқыс файлы қосылады.

   Мұрағатта қарапайым мәтіндегі құпия деректер (мысалы, кілттер мен құпия сөздер) болуы мүмкін. Мұрағаттағы файлдарды қарап шығып, оларды Kaspersky техникалық қолдау қызметіне жібермес бұрын жоюды ұсынамыз.

Ақпараты бар файл көрсетілген орынға жүктеледі.

Оқиғалар журналдарын жүктеу

Қашықтағы құрылғыдан оқиғалар журналын жүктеу үшін:

1. Клиент құрылғысын қашықтан диагностикалау утилитасын ашыңыз.
2. Қашықтан диагностикалау терезесінің **Оқиға журналдары** бөлімінде **Барлық құрылғы журналдары** бөлімін таңдаңыз.
3. **Барлық құрылғы журналдары** терезесінде бір немесе бірнеше оқиғалар журналын таңдаңыз.

4. Келесі әрекеттердің бірін орындаңыз:

   - **Бүкіл файлды жүктеп алу** түймесін басып, таңдалған оқиғалар журналын жүктеңіз.
   - Таңдалған оқиғалар журналының бөлігін жүктеңіз:

     a. **Файл бөлігін жүктеп алу** түймесін басыңыз.

     Бірнеше оқиғалар журналын бір уақытта ішінара жүктеп алу мүмкін емес. Бірнеше оқиғалар журналын таңдасаңыз, **Файл бөлігін жүктеп алу** түймесі өшіріледі.

     b. Ашылған терезеде өз талаптарыңызға сай жүктеп алу үшін оқиғалар журналының аты мен бөлігін көрсетіңіз.

     Linux арқылы басқарылатын құрылғылар үшін оқиғалар журналы бөлігінің атауын өзгерту қолжетімді емес.

     c. **Жүктеп алу** түймесін басыңыз.

Таңдалған оқиғалар журналы немесе оның бөлігі көрсетілген жерге жүктеп алынады.

Бағдарламаны іске қосу, тоқтату және қайта іске қосу

Сіз клиент құрылғысында бағдарламаларды іске қоса, тоқтата және қайта іске қоса аласыз.

Бағдарламаны іске қосу, тоқтату және қайта қосу үшін:

1. Клиент құрылғысын қашықтан диагностикалау утилитасын ашыңыз.
2. Қашықтан диагностикалау терезесінде **Kaspersky бағдарламалары** бөлімін таңдаңыз.

   Бағдарламаларды басқару бөлімінде құрылғыға орнатылған Kaspersky қолданбаларының тізімі көрсетілген.
3. Бағдарламалар тізімінен іске қосқыңыз, тоқтатқыңыз немесе қайта іске қосқыңыз келетін бағдарламаны таңдаңыз.
4. Келесі түймелердің бірін басып, әрекетті таңдаңыз:

   - **Бағдарламаны тоқтату**

     Бұл түйме, бағдарлама қазіргі сәтте іске қосылған болса ғана қолжетімді.
   - **Бағдарламаны қайта іске қосу**

     Бұл түйме, бағдарлама қазіргі сәтте іске қосылған болса ғана қолжетімді.
   - **Бағдарламаны іске қосу**

     Бұл түйме, бағдарлама қазіргі сәтте іске қосылмаған болса ғана қолжетімді.

   Өзіңіз таңдаған әрекетке байланысты, қажетті бағдарлама клиент құрылғысында іске қосылады, тоқтайды немесе қайта іске қосылады.

Желілік агентті қайта іске қоссаңыз, құрылғының Басқару серверімен ағымдағы қосылымы үзілетіні туралы хабар пайда болады.

Kaspersky Security Center Linux Желілік агент қашықтағы диагностикасын іске қосу және нәтижелерді жүктеп алу

Kaspersky Security Center Linux Желілік агент диагностикасын қашықтағы құрылғыда іске қосу және оның нәтижелерін жүктеп алу үшін:

1. Клиент құрылғысын қашықтан диагностикалау утилитасын ашыңыз.
2. Қашықтан диагностикалау терезесінде **Kaspersky бағдарламалары** бөлімін таңдаңыз.

   Бағдарламаларды басқару бөлімінде құрылғыға орнатылған Kaspersky қолданбаларының тізімі көрсетілген.
3. Қолданбалар тізімінен **Kaspersky Security Center Linux Network Agent** опциясын таңдаңыз.

   Қашықтан диагностикалау параметрлері тізімі ашады.
4. **Диагностикалау есеп** бөлімінде **Диагностиканы іске қосу** түймесін басыңыз.

   Қашықтан диагностикалау процесі іске қосылып, диагностика туралы есеп құрастырылады. Диагностика процесі аяқталғаннан кейін, **Диагностикалау есепті жүктеп алу** түймесі қолжетімді болмайды.
5. Есепті жүктеп алу үшін **Диагностикалау есепті жүктеп алу** түймесін басыңыз.

Есеп көрсетілген орынға жүктеледі.

Бағдарламаны клиент құрылғысында іске қосу

Сізден Kaspersky техникалық қолдау қызметінің маманы сұраса, клиенттік құрылғыда қолданбаны іске қосу қажет болуы мүмкін. Сізге бағдарламаны осы құрылғыға өз бетіңізше орнатудың қажеті жоқ.

Клиенттік құрылғыда арнаулы скриптіні іске қосқыңыз келсе, орындау нәтижелері сақталатын жолды анықтау үшін `KLACDT_SAVE_SETTING` ортасының айнымалысын пайдалануға болады. Мысалы:

- Windows негізіндегі құрылғы үшін:

  ```
  @echo some result > %KLACDT_SAVE_SETTING%\res.log
  ```
- Linux негізіндегі құрылғы үшін:

  ```
  echo some result > $KLACDT_SAVE_SETTING/res.log
  ```

Бағдарламаны клиент құрылғысында іске қосу үшін:

1. Клиент құрылғысын қашықтан диагностикалау утилитасын ашыңыз.
2. Қашықтан диагностикалау терезесінде **Қашықтан жұмыс істейтін бағдарламаны іске қосу** бөлімін таңдаңыз.

3. **Нысан түрі** өрісінде жүктеп салғыңыз келетін нысан түрін таңдаңыз:

   - Орындалатын файлды жүктеп салу үшін **Файлды** таңдаңыз.
   - Клиент құрылғысында іске қосқыңыз келетін қолданбасы бар қалтаны жүктеп салу үшін **Қалтаны** таңдаңыз.

     Осы нысан түрін таңдасаңыз, **Іске қосылатын орындалатын файл атауы** өрісі пайда болады. Бұл өрісте қалтадағы орындалатын файлдың атауын көрсетіңіз. Сондай-ақ файлға қатысты жолды көрсетуге болады.
   - Клиент құрылғысында іске қосу қажет қолданбаны қамтитын ZIP мұрағатын жүктеп салу үшін **Мұрағаттау** опциясын таңдаңыз.

     Осы нысан түрін таңдасаңыз, **Іске қосылатын орындалатын файл атауы** өрісі пайда болады. Бұл өрісте қалтадағы орындалатын файлдың атауын көрсетіңіз. Сондай-ақ файлға қатысты жолды көрсетуге болады.

     > ZIP мұрағатында утилита қалтасы болуы керек. Бұл қалта қашықтағы құрылғыда іске қосу үшін орындалатын файлды қамтиды.

4. Жүйе терезесінде нысанды таңдау немесе жүктеп салу өрісіне сүйреп апару арқылы жүктеп салыңыз.
5. Қажет болса, **Пәрмен жолының аргументтері** өрісінде орындалатын файлды іске қосу кезінде жіберілетін пәрмен желісі аргументтерін көрсетіңіз.
6. Таңдалған қолданбаны клиент құрылғысында іске қосу үшін **Жүктеп салу және іске қосу** түймесін басыңыз.
7. Қолданбаны орындау сәтті аяқталғаннан кейін, **Бағдарламаның орындау нәтижелерін жүктеп алу** түймесін басу арқылы орындау нәтижелерін жүктеп алыңыз.

   > Қолданбаны орындау нәтижелері жаңа диагностиканы іске қосқанша немесе терезені жапқанша сақталады.

Қолданбаны пайдалану арқылы клиент құрылғысын қашықтан диагностикалау аяқталды.

Linux операциялық жүйесі бар клиенттік құрылғыда қашықтағы диагностиканы іске қосу

Kaspersky Security Center Linux жүйесі клиенттік құрылғыдан негізгі диагностикалық ақпаратты жүктеп алуға мүмкіндік береді. Бұған қоса Kaspersky бағдарламасының collect.sh скриптісін пайдаланып, Linux операциялық жүйесімен жұмыс істейтін құрылғы туралы диагностикалық ақпаратты алуға болады. Бұл скрипт диагностикалануы қажет Linux негізіндегі клиент құрылғысында іске қосылады, содан кейін диагностикалық ақпараты, осы құрылғы туралы жүйелік ақпараты бар файлды, қолданбалардың трассалау файлдарын, құрылғы журналдарын және төтенше жағдайда тоқтатылатын қолданбаларға арналған дамп файлын жасайды.

Linux операциялық жүйесімен жұмыс істейтін клиенттік құрылғы туралы барлық диагностикалық ақпаратты дереу алу үшін collect.sh скриптісін пайдалану ұсынылады. Егер диагностикалық ақпаратты Kaspersky Security Center Linux арқылы қашықтан жүктеп алсаңыз, қашықтағы диагностика интерфейсінің барлық бөлімдерін өтуіңіз керек. Оған қоса Linux операциялық жүйесі бар құрылғының диагностикалық ақпараты толық алынбауы мүмкін.

Диагностикалық ақпараты бар жасалған файлды Kaspersky техникалық қолдау қызметіне жіберу қажет болса, файлды жібермес бұрын барлық құпия ақпаратты жойыңыз.

collect.sh скриптісін пайдаланып, Linux операциялық жүйесі бар клиенттік құрылғыдан диагностикалық ақпаратты жүктеп алу үшін:

1. collect.sh скриптісін жүктеп алыңыз, ол collect.tar.gz мұрағатына жинақталған.
2. Жүктелген мұрағатты диагностикалау қажет Linux операциялық жүйесі бар клиент құрылғыға көшіріңіз.
3. collect.tar.gz мұрағатын шығару үшін келесі пәрменді орындаңыз:

   ```
   # tar -xzf collect.tar.gz
   ```

4. Скриптіні орындауға құқықтарын көрсету үшін келесі пәрменді орындаңыз:

   ```
   # chmod +x collect.sh
   ```

5. collect.sh скриптісін әкімші құқықтары бар есептік жазба арқылы іске қосыңыз:

   ```
   # ./collect.sh
   ```

Диагностикалық ақпараты бар файл /tmp/$HOST_NAME-collect.tar.gz қалтасында жасалады және сақталады.

Клиент құрылғыларындағы қолданбалар мен орындалатын файлдарды басқару

Бұл бөлімде клиент құрылғыларындағы қолданбалар мен орындалатын файлдарды басқарумен байланысты Kaspersky Security Center Linux мүмкіндіктері сипатталған.

Орындалатын файлдарды басқару үшін Бағдарламаларды басқару компонентін пайдалану

Пайдаланушы құрылғыларында орындалатын файлдардың орындалуына рұқсат беру немесе тыйым салу үшін Бағдарламаларды бақылау компонентін пайдалануға болады. Бағдарламаларды бақылау компоненті Windows және Linux операциялық жүйелерін қолдайды.

Linux операциялық жүйелері үшін Бағдарламаны басқару құрамдасы Kaspersky Endpoint Security 11.2 for Linux нұсқасынан бастап қолжетімді.

Алдын ала талаптар

- Kaspersky Security Center Linux бағдарламасы сіздің ұйымыңызда орналастырылған.
- Kaspersky Endpoint Security for Linux немесе Kaspersky Endpoint Security for Windows саясаты жасалды және белсенді. Бағдарламаларды бақылау компоненті саясатта қосылған.

Кезеңдер

Бағдарламаны басқару құрамдасын қолдану сценарийі келесі кезеңдерден тұрады:

1. **Клиент құрылғыларында орындалатын файлдар тізімін құрастыру және қарау**

   Бұл кезең сізге басқарылатын құрылғыларда қандай орындалатын файлдардың орнатылғанын анықтауға көмектеседі. Орындалатын файлдар тізімін қарап шығыңыз және оны рұқсат етілген және тыйым салынған орындалатын файлдардың тізімдерімен салыстырыңыз. Орындалатын файлдарды қолданудағы шектеулер ұйымдағы ақпараттық қауіпсіздік саясаттарымен байланысты болуы мүмкін.

   Нұсқаулар: Клиент құрылғыларында сақталған орындалатын файлдардың тізімін алу және қарау.

2. **Ұйымыңызда қолданылатын орындалатын файлдар үшін санаттарды жасау**

   Басқарылатын құрылғыларда сақталған орындалатын файлдардың тізімдерін талдаңыз. Талдау негізінде орындалатын файлдар үшін санаттарды қалыптастырыңыз. Ұйымыңызда қолданылатын орындалатын файлдардың стандартты жиынтығын қамтитын "Жұмыс бағдарламалары" санатын құру ұсынылады. Егер әртүрлі қауіпсіздік топтары өз жұмысында өзіндік орындалатын файлдар жиынтығын қолданса, әр қауіпсіздік тобы үшін бөлек санатты құруға болады.

Бағдарламаларды бақылау ережесінің ешқайсысына сәйкес келмейтін параметрлері бар орындалатын файлдарды іске қосу, келесі құрамдастың таңдалған жұмыс режимі тарапынан реттеледі:

- *Тыйым салу тізімі*. Егер сіз тыйым салу ережелерінде көрсетілгендерден басқа барлық орындалатын файлдардың іске қосылуына рұқсат бергіңіз келсе, режим қолданылады. Әдепкі бойынша осы режим таңдалған.

- *Рұқсат ету тізімі*. Рұқсат ету ережелерінде көрсетілгендерден басқа барлық орындалатын файлдарды іске қосуға тыйым салғыңыз келсе, режим пайдаланылады.

Бағдарламаларды бақылау ережелері орындалатын файлдар санаттарында жүзеге асырылған. Kaspersky Security Center Linux қолданбасында орындалатын файлдар санаттарының үш түрі бар:

- Қолмен толтырылатын санат. Сіз орындалатын файлдарды санатқа қосу үшін файл метадеректері, файл хэші, файл сертификаты, файл жолы сияқты шарттарды анықтайсыз.

- Таңдалған құрылғылардағы орындалатын файлдар кіретін санат. Сіз орындалатын файлдары автоматты түрде санатқа қосылатын құрылғыны көрсетесіз.

- Таңдалған қалталардан алынған орындалатын файлдарды қамтитын санат. Сіз орындалатын файлдар автоматты түрде санатқа кіретін қалтаны көрсетесіз.

3 Kaspersky Endpoint Security саясатындағы Бағдарламаларды басқару конфигурациялау

Алдыңғы кезеңде жасаған санаттарды қолдана отырып, Kaspersky Endpoint Security for Linux саясатындағы Бағдарламаларды басқару құрамдасын конфигурациялаңыз.

Нұсқаулар: Kaspersky Endpoint Security for Windows саясатындағы Бағдарламаларды басқару құрамдасын конфигурациялау

4 Тест режимінде Бағдарламаларды басқару құрамдасын қосу

Бағдарламаларды басқару ережелері пайдаланушылардың жұмысына қажетті орындалатын файлдарды бұғаттамауы үшін, Қолданбаларды бақылау ережелерін тестілеуді қосып, ережелер жасалғаннан кейін олардың жұмысын талдау ұсынылады. Тестілеу қосылған кезде, Kaspersky Endpoint Security for Windows Бағдарламаларды басқару ережелерімен іске қосуға тыйым салынған орындалатын файлдарды бұғаттамайды, оның орнына оларды іске қосу туралы хабарландыруларды Басқару серверіне жібереді.

Бағдарламаларды бақылау ережелерін тестілеу кезінде келесі әрекеттерді орындау ұсынылады:

- Тестілеу кезеңін анықтаңыз. Тестілеу кезеңі бірнеше күннен екі айға дейін өзгеруі мүмкін.

- Бағдарламаны басқару құрамдасының жұмысын тексеру нәтижесінде пайда болатын оқиғаларды зерттеңіз.

Kaspersky Security Center Web Console үшін нұсқаулар: Kaspersky Endpoint Security for Windows саясатында Бағдарламаны басқару құрамдасын конфигурациялау. Осы нұсқаулықты орындаңыз және орнату процесінде **Сынақ режимі** опциясын қосыңыз.

5 Бағдарламаны басқару құрамдасының параметрлерін өзгерту

Қажет болса, Бағдарламаларды басқару құрамдасының параметрлерін өзгертіңіз. Тестілеу нәтижелеріне сүйене отырып, Бағдарламаларды басқару құрамдасының оқиғаларына байланысты орындалатын файлдарды қолмен толықтырылатын санатқа қосуға болады.

Нұсқаулар: Kaspersky Security Center Web Console: Бағдарлама санатына оқиғамен байланысты орындалатын файлдарды қосу.

6. **Жұмыс режимінде Бағдарламаларды бақылау ережелерін қолдану**

   Бағдарламаларды бақылау ережелерін тексергеннен кейін және санаттарды конфигурациялауды аяқтағаннан кейін, сіз жұмыс режимінде Бағдарламаларды басқару ережелерін қолдана аласыз.

   Kaspersky Security Center Web Console үшін нұсқаулар: Kaspersky Endpoint Security for Windows саясатында Бағдарламаны басқару құрамдасын конфигурациялау. Осы нұсқаулықты орындап, конфигурациялау барысында **Сынақ режимі** параметрін өшіріңіз.

7. **Бағдарламаны басқару конфигурациясын тексеру**

   Келесіні орындағаныңызға көз жеткізіңіз:

   - Орындалатын файлдар үшін санаттар жасадық.
   - Санаттарды қолдана отырып, Бағдарлама санаттарын конфигурацияладыңыз.
   - Жұмыс режимінде Бағдарламаларды бақылау ережелерін қолдандыңыз.

Нәтижелер

Сценарий аяқталғаннан кейін, басқарылатын құрылғыларда орындалатын файлдардың іске қосылуы бақыланады. Пайдаланушылар сіздің ұйымыңызда рұқсат етілген орындалатын файлдарды ғана басқара алады және сіздің ұйымыңызда тыйым салынған орындалатын файлдарды іске қоса алмайды.

Бағдарламаларды бақылау құрамдас бөлігінің толық сипаттамасын Kaspersky Endpoint Security for Linux және Kaspersky Endpoint Security for Windows бағдарламасының онлайн анықтамасынан қараңыз.

Клиент құрылғыларында сақталған орындалатын файлдардың тізімін алу және қарау

Клиент құрылғыларында сақталған орындалатын файлдар тізімін келесі жолдардың бірімен алуға болады:

- Kaspersky Endpoint Security саясатында қолданбаларды іске қосу туралы хабарландыруларды қосу.
- Түгендеу тапсырмасын жасау.

Kaspersky Endpoint Security саясатында қолданбаларды іске қосу туралы хабарландыруларды қосу

Бағдарламаларды іске қосу туралы хабарландыруларды қосу үшін:

1. Kaspersky Endpoint Security саясат параметрлерін ашыңыз, содан кейін **Жалпы параметрлер** → **Есептер және қоймалар** тармағына өтіңіз.
2. **Деректерді әкімші серверіне тасымалдау** параметрлер тобында **Іске қосылған қолданбалар туралы ақпарат** құсбелгісін қойып, өзгерістерді сақтаңыз.

Пайдаланушы орындалатын файлдарды іске қосуға әрекет жасағанда, осы файлдар туралы ақпарат клиент құрылғысындағы орындалатын файлдар тізіміне қосылады. Kaspersky Endpoint Security бұл ақпаратты желілік агентке жібереді, содан кейін желілік агент оны басқару серверіне жібереді.

Түгендеу тапсырмасын жасау

Орындалатын файлдарды түгендеу функциясы Kaspersky Endpoint Security for Linux 11.2 және одан да жоғары нұсқасы бағдарламасы үшін қолжетімді.

Орнатылған бағдарламалар туралы ақпаратты алу арқылы дерекқорға түсетін жүктемені азайтуға болады. Дерекқор орнын үнемдеу үшін бағдарламалық жасақтаманың стандартты жиынтығы орнатылған анықтамалық құрылғыларда түгендеу тапсырмасын іске қосыңыз. Құрылғылардың саны 1-3 болғаны дұрыс.

Клиент құрылғыларында орындалатын файлдарды түгендеу тапсырмасын жасау үшін:

1. Бағдарламаның негізгі терезесінде **Тапсырмалар** бөліміне өтіңіз.

   Тапсырмалар тізімі көрсетіледі.
2. **Қосу** түймесін басыңыз.

   Жаңа тапсырма жасау шебері іске қосылады. Содан кейін, шебердің нұсқауларын орындаңыз.
3. **Жаңа тапсырма параметрлері** бетінде, **Бағдарлама** ашылмалы тізімінде, клиент құрылғыларының операциялық жүйесінің түріне байланысты Kaspersky Endpoint Security for Linux немесе Kaspersky Endpoint Security for Windows таңдаңыз.
4. **Тапсырма түрі** ашылмалы тізімінен **Қойма** тармағын таңдаңыз.
5. **Тапсырманы жасауды аяқтау** бетінде **Аяқтау** түймесін басыңыз.

   Жаңа тапсырма жасау шебері өз жұмысын аяқтағаннан кейін, **Қойма** тапсырмасы жасалды және конфигурацияланды. Сіз жасалған тапсырманың параметрлерін өзгерте аласыз. Нәтижесінде, жасалған тапсырма тапсырмалар тізімінде көрсетіледі.

Түгендеу тапсырмасының толық сипаттамасын Kaspersky Endpoint Security for Linux бағдарламасының онлайн анықтамасын және Kaspersky Endpoint Security for Windows қараңыз.

Қойма тапсырмасын орындағаннан кейін, басқарылатын құрылғыларда сақталған орындалатын файлдардың тізімі жасалады және сіз осы тізімді қарай аласыз.

Түгендеу кезінде келесі форматтағы орындалатын файлдарды анықтауға болады (түгендеу тапсырмасы сипаттарында таңдалған опцияға байланысты): MZ, COM, PE, NE, SYS, CMD, BAT, PS1, JS, VBS, REG, MSI, CPL, DLL, JAR, and HTML.

Басқарылатын құрылғыларда сақталған орындалатын файлдардың тізімін көру.

Клиент құрылғыларында сақталатын орындалатын файлдар тізімін көру үшін,

Бағдарламаның негізгі терезесінде **Бағдарламалық жасақтаманы басқару → Үшінші тарап бағдарламалары → Орындалатын файлдар** бөліміне өтіңіз.

Бетте клиент құрылғыларында сақталған орындалатын файлдардың тізімі көрсетіледі.

Қажет болса, басқарылатын құрылғының орындалатын файлын Kaspersky Security Center Web Console ашық құрылғыға жіберуге болады.

Орындалатын файлды жіберу үшін:

1. Бағдарламаның негізгі терезесінде **Бағдарламалық жасақтаманы басқару → Үшінші тарап бағдарламалары → Орындалатын файлдар** бөліміне өтіңіз.
2. Жібергіңіз келетін орындалатын файл сілтемесін басыңыз.
3. Ашылған терезеде **Құрылғылар** бөліміне өтіп, орындалатын файлды жібергіңіз келетін басқарылатын құрылғының жанына жалаушаны қойыңыз.

   Орындалатын файлды жібермей тұрып, Басқару серверімен байланысты үзбеу құсбелгі ұяшығын таңдап, басқарылатын құрылғыда басқару серверіне тікелей қосылым бар екенін тексеріңіз.

4. **Жіберу** түймесін басыңыз.

   Таңдалған орындалатын файл Kaspersky Security Center Web Console ашық құрылғыға одан әрі жіберу үшін жүктеп алынады.

Қолмен толықтырылатын бағдарламалар санатын жасау

Сіз өзіңіздің ұйымыңызда іске қосуға рұқсат бергіңіз немесе тыйым салғыңыз келетін орындалатын файлдарға арналған үлгі ретінде критерийлер жиынтығын көрсете аласыз. Критерийлерге сәйкес орындалатын файлдардың негізінде, сіз бағдарламалар санатын құра аласыз және оны Бағдарламаны басқару құрамдасының конфигурациясында қолдана аласыз.

Қолмен толықтырылатын бағдарламалар санатын жасау үшін:

1. Бағдарламаның негізгі терезесінде **Бағдарламалық жасақтаманы басқару → Үшінші тарап бағдарламалары → Бағдарлама санаттары** бөліміне өтіңіз.

   Бағдарлама санаттары тізімі бар бет ашылады.

2. **Қосу** түймесін басыңыз.

   Жаңа санат шебері іске қосылады. Шебердің жұмысын жалғастыру үшін **Келесі** түймесін басыңыз.

3. Шебердің **Санатты жасау әдісін таңдау** қадамында қолданбаның санат атауын көрсетіп, **Қолмен қосылған мазмұны бар санат. Орындалатын файлдардың деректері санатқа қолмен қосылады** параметрін таңдаңыз.

4. **Шарттар** қадамында, файлдарды жасалып жатқан санатқа қосуға арналған критерийді қосу үшін **Қосу** түймесін басыңыз.

5. **Жағдай шарттары** қадамында келесі әрекеттерді орындаңыз:

   a. Санат жасау үшін ереже түрін таңдаңыз:

   - **KL санатынан**

     Осы нұсқа таңдалған болса, бағдарламаларды пайдаланушы санатына қосу шарты ретінде Kaspersky бағдарламалары санатын қосуға болады. Көрсетілген KL санатына кіретін бағдарламалар бағдарламалардың пайдаланушы санатына қосылатын болады.

   - **Репозиторийден сертификатты таңдау**

     Осы нұсқа таңдалған болса, қоймадағы сертификаттарды көрсетуге болады. Санат шарты көрсетілген сертификатпен қол қойылған орындалатын файлдарға ғана сәйкес келеді.

     Түгендеу тапсырмасын жасап, іске қоссаңыз немесе Kaspersky Endpoint Security саясатында **Іске қосылған қолданбалар** туралы құсбелгісін таңдасаңыз, сертификаттар қоймаға қосылады. Сіз екі әрекетті де орындай аласыз.

     > Сертификаттар туралы ақпаратты тек PE форматындағы (.exe, .dll, .sys) орындалатын файлдардан алуға болады.

   - **Бағдарлама жолын көрсету (қолдау көрсетілетін маскалар)**

     Осы нұсқа таңдалған болса, орындалатын файлдары бағдарламалардың пайдаланушы санаттарына қосылатын клиент құрылғысындағы қалтаны көрсетуге болады.

   - **Алынбалы жетек**

     Осы нұсқа таңдалған болса, бағдарлама іске қосылатын тасушының түрін (кез келген немесе алынбалы диск) көрсетуге болады. Таңдалған типтегі тасушыда іске қосылатын бағдарламалар бағдарламалардың пайдаланушы санатына қосылады.

   - **Хэш, метадеректер немесе сертификат**:

     - **Орындалатын файлдар тізімінен таңдау**

       Осы нұсқа таңдалған болса, санатқа қосылатын бағдарламаларды клиент құрылғысындағы орындалатын файлдар тізімінен таңдауға болады.

- **Бағдарламалар тізімдемесінен таңдау**

  Егер бұл параметр таңдалса, бағдарламалар тізімдемесі көрсетіледі. Тізілімнен қолданбаны таңдағаннан кейін сіз таңдаған қолданбаның метадеректерімен толтырылған параметрлермен терезе ашылады:

  - Файл атауы.
  - Файл нұсқасы. Сіз нұсқаның нақты мәнін көрсете аласыз немесе "5.0-ден артық" сияқты шарт жаза аласыз.
  - Бағдарлама атауы.
  - Бағдарлама нұсқасы. Сіз нұсқаның нақты мәнін көрсете аласыз немесе "5.0-ден артық" сияқты шарт жаза аласыз.
  - Өндіруші.

  Сіз таңдаған қолданбаны іске қосу емес, тек көрсетілген параметрлерге сәйкес келетін орындалатын файлдарды іске қосу бұғатталатынын ескеріңіз. Таңдалған қолданба метадеректері қолданбаны іске қосқан кезде іске қосылатын орындалатын файлдың біріне сәйкес келсе, келесі қадамға өтуіңізге болады. Сәйкес келмесе, орындалатын файлдың метадеректеріне сәйкестендіру үшін мәндерді қолмен өзгерту керек.

- **Қолмен көрсету**

  Егер бұл нұсқа таңдалса, бағдарламаларды пайдаланушы санатына қосу шарты ретінде файл хэшін, метадеректерді немесе сертификатты көрсету керек.

  Файл хэші

  Желіңіздегі құрылғыларға орнатылған қауіпсіздік бағдарламасы нұсқасына байланысты, санат файлдары үшін хеш функциясын Kaspersky Security Center Linux бағдарламасы тарапынан есептеп шығару алгоритмін таңдау керек. Хэш функцияларымен есептелетін хэш мәндері туралы ақпарат басқару сервері дерекқорында сақталады.

  SHA256 – алгоритмінде осалдық табылмаған криптографиялық хеш функциясы және ол қазіргі уақытта ең сенімді криптографиялық функция болып саналады. Kaspersky Endpoint Security for Linux қолданбасы SHA256 есептеуін қолдайды.

  Санат файлдары үшін Kaspersky Security Center Linux бағдарламасы тарапынан хеш функциясын есептеп шығару нұсқаларының бірін таңдаңыз:

  - Егер желіңізде орнатылған қауіпсіздік бағдарламаларының барлық үлгілері Kaspersky Endpoint Security for Linux болса, **SHA256** жалаушаны орнатыңыз.
  - Windows үшін Kaspersky Endpoint Security пайдалансаңыз ғана, **MD5 хэші** жалаушаны орнатыңыз. Kaspersky Endpoint Security for Linux MD5 хэш функциясына қолдау көрсетпейді.

  Метадеректер

  Егер бұл параметр таңдалса, сіз файл атауы, файл нұсқасы және өндіруші сияқты файл метадеректерін көрсете аласыз. Санат шарты тек метадеректері бірдей орындалатын файлдарға сәйкес келеді.

  Сертификат

  Осы нұсқа таңдалған болса, қоймадағы сертификаттарды көрсетуге болады. Санат шарты көрсетілген сертификатпен қол қойылған орындалатын файлдарға ғана сәйкес келеді.

  Түгендеу тапсырмасын жасап, іске қоссаңыз немесе Kaspersky Endpoint Security саясатында **Іске қосылған қолданбалар** туралы құсбелгісін таңдасаңыз, сертификаттар қоймаға қосылады. Сіз екі әрекетті де орындай аласыз.

- **Мұрағат қалтасынан**

  Бұл параметр таңдалған болса, мұрағат қалтасында файлды көрсетуге және пайдаланушы санатына бағдарламаларды қосу үшін қандай шартты пайдаланғыңыз келетінін таңдауға болады. Мұрағат қалтасы ашылады және таңдалған шарттар осы қалтадағы файлдарға қолданылады. Шарт ретінде келесі критерийлердің бірін таңдауға болады:

  - **Файл хэші**

    Хэш функциясының мәнін есептеу үшін пайдаланғыңыз келетін хэш функциясын (MD5 немесе SHA256) таңдауға болады. Мұрағаттық қалтадағыдай хэші бар бағдарламалар бағдарламалардың пайдаланушы санатына қосылатын болады.

    Kaspersky Endpoint Security for Windows пайдалансаңыз ғана MD5 хэш функциясын таңдаңыз. Kaspersky Endpoint Security for Linux MD5 хэш функциясына қолдау көрсетпейді.

  - **Метадеректер**

    Критерий ретінде пайдаланғыңыз келетін метадеректерді таңдаңыз. Осындай метадеректері бар орындалатын файлдар бағдарламалардың пайдаланушы санатына қосылады.

  - **Сертификат**

    Критерий ретінде пайдаланғыңыз келетін сертификат параметрлерін (сертификат субъектісінің атауы, саусақ ізі немесе сертификатты берген) таңдаңыз. Параметрлері бірдей сертификаттармен қол қойылған орындалатын файлдар пайдаланушы санатына қосылады.

  Метадеректер мен **Сертификат** критерийлерін қолдану үшін, файлды немесе мұрағатталған қалтаны жүктеген соң оларды қолмен көрсету қажет.

Бұл параметр таңдалған болса, мұрағат қалтасында файлды көрсетуге және пайдаланушы санатына бағдарламаларды қосу үшін қандай шартты пайдаланғыңыз келетінін таңдауға болады. Мұрағат қалтасы ашылады және таңдалған шарттар осы қалтадағы файлдарға қолданылады. Шарт ретінде келесі критерийлердің бірін таңдауға болады:

- **Файл хэші**

  Хэш функциясының мәнін есептеу үшін пайдаланғыңыз келетін хэш функциясын (MD5 немесе SHA256) таңдауға болады. Мұрағаттық қалтадағыдай хэші бар бағдарламалар бағдарламалардың пайдаланушы санатына қосылатын болады.

  Kaspersky Endpoint Security for Windows пайдалансаңыз ғана MD5 хэш функциясын таңдаңыз. Kaspersky Endpoint Security for Linux MD5 хэш функциясына қолдау көрсетпейді.

- **Метадеректер**

  Критерий ретінде пайдаланғыңыз келетін метадеректерді таңдаңыз. Осындай метадеректері бар орындалатын файлдар бағдарламалардың пайдаланушы санатына қосылады.

- **Сертификат**

  Критерий ретінде пайдаланғыңыз келетін сертификат параметрлерін (сертификат субъектісінің атауы, саусақ ізі немесе сертификатты берген) таңдаңыз. Параметрлері бірдей сертификаттармен қол қойылған орындалатын файлдар пайдаланушы санатына қосылады.

Метадеректер мен **Сертификат** критерийлерін қолдану үшін, файлды немесе мұрағатталған қалтаны жүктеген соң оларды қолмен көрсету қажет.

b. Қажет болса, **Сипаттама** өрісіне түсініктеме қосыңыз. Таңбалар саны 1000-нан аспауы керек.

Кейінірек, қолданба санатының сипаттарындағы **Шарттар** ашу арқылы түсініктемені өңдеуге немесе жоюға болады, содан кейін **Шарттың критерийі** бағанында түсініктемені өңдеу немесе жою қажет шарты бар сілтемені басыңыз.

> **KL санатынан** ережесі түрін таңдаған кезде, осы ереже түріне негізделген барлық жасалатын шарттарға бір түсініктеме қосуға болады. Әрбір шарт үшін түсініктемені өңдеуге немесе жоюға болады.

Таңдалған критерий шарттар тізіміне қосылды.

Жасалатын бағдарлама санаты үшін қанша қажет болса, сонша шарт қосуға болады.

6. **Ерекшеліктер** қадамында, ерекшеліктер аймағына критерий қосу және файлдарды жасалып жатқан санаттан шығару үшін **Қосу** түймесін басыңыз.

   Қажет болса, **Сипаттама** өрісіне түсініктеме қосуға болады. Таңбалар саны 1000-нан аспауы керек.

   Кейінірек, **Ерекшеліктер** тармағын ашу арқылы түсініктемені өңдеуге немесе жоюға болады. қолданба санатының сипаттарындағы қойындысын, содан кейін **Шарттың критерийі** бағанында түсініктемені өңдегіңіз немесе жойғыңыз келетін шарты бар сілтемені басыңыз.

7. **Жағдай шарттары** қадамында, санатты жасау үшін ереже түрін таңдағаныңыздай, тізімнен ереже түрін таңдаңыз.

Шебер аяқталғанда, бағдарлама санаты жасалады және қолданба санаттарының тізімінде көрсетіледі. Бағдарламаны басқару құрамдасын конфигурациялау кезінде бағдарламалар санатын жасауға болады.

Бағдарламаларды бақылау құрамдас бөлігінің толық сипаттамасын Kaspersky Endpoint Security for Linux және Kaspersky Endpoint Security for Windows бағдарламасының онлайн анықтамасынан қараңыз.

Таңдалған құрылғылардан орындалатын файлдарды қамтитын бағдарламалар санатын жасау

Құрылғыдан орындалатын файлдарды, іске қосуға рұқсат бергіңіз немесе тыйым салғыңыз келетін орындалатын файлдардың үлгісі ретінде пайдалануға болады. Таңдалған құрылғылардағы орындалатын файлдардың негізінде, сіз бағдарламалар санатын құра аласыз және оны Бағдарламаны басқару құрамдасын конфигурациялау үшін пайдалана аласыз.

Келесі алдын ала талаптардың орындалғанына көз жеткізіңіз:

- Бағдарламаларды басқару компоненті Kaspersky Endpoint Security саясатында қосылған.
- Басқарылатын құрылғыларда сақталған орындалатын файлдардың тізімі алынған.

Таңдалған құрылғылардан орындалатын файлдарды қамтитын бағдарламалар санатын құру үшін:

1. Бағдарламаның негізгі терезесінде **Бағдарламалық жасақтаманы басқару → Үшінші тарап бағдарламалары → Бағдарлама санаттары** бөліміне өтіңіз.

   Орындалатын файлдар санаттары тізімі бар бет ашылады.

2. **Қосу** түймесін басыңыз.

   Жаңа санат шебері іске қосылады. Шебердің жұмысын жалғастыру үшін **Келесі** түймесін басыңыз.

3. **Санатты жасау әдісін таңдау** қадамында санат атауын көрсетіңіз және **Таңдалған құрылғылардағы орындалатын файлдарды қамтитын санат. Осы орындалатын файлдар автоматты түрде өңделеді және метрикалары санатқа қосылады**.

4. **Қосу** түймесін басыңыз.

5. Ашылған терезеде бағдарламалар санатын құру үшін орындалатын файлдары пайдаланылатын құрылғыны немесе құрылғыларды таңдаңыз.

6. Келесі параметрлерді белгілеңіз:

- **Хеш функциясын есептеп шығару алгоритмі**

  Желіңіздегі құрылғыларға орнатылған қауіпсіздік бағдарламасы нұсқасына байланысты, санат файлдары үшін хеш функциясын Kaspersky Security Center Linux бағдарламасы тарапынан есептеп шығару алгоритмін таңдау керек. Хэш функцияларымен есептелетін хэш мәндері туралы ақпарат басқару сервері дерекқорында сақталады.

  SHA256 – алгоритмінде осалдық табылмаған криптографиялық хеш функциясы және ол қазіргі уақытта ең сенімді криптографиялық функция болып саналады. Kaspersky Endpoint Security for Linux қолданбасы SHA256 есептеуін қолдайды.

  Санат файлдары үшін Kaspersky Security Center Linux бағдарламасы тарапынан хеш функциясын есептеп шығару нұсқаларының бірін таңдаңыз:

  - Егер желіңізде орнатылған қауіпсіздік бағдарламаларының барлық үлгілері Kaspersky Endpoint Security for Linux болса, **SHA256** жалаушаны орнатыңыз.

  Windows үшін Kaspersky Endpoint Security пайдалансаңыз ғана, **MD5 хэші** жалаушаны орнатыңыз. Kaspersky Endpoint Security for Linux MD5 хэш функциясына қолдау көрсетпейді.

  Әдепкі бойынша, **Санаттағы файлдар үшін SHA256 есептеп шығару (Kaspersky Endpoint Security 10 Service Pack 2 for Windows үшін қолдау көрсетіледі)** жалаушасы қойылған.

  Әдепкі бойынша, **Осы санаттағы файлдар үшін MD5 есептеу (Kaspersky Endpoint Security 10 Service Pack 2 for Windows нұсқасынан бұрынғы нұсқалармен қолдау көрсетіледі)** алынып тасталған.

- **Басқару серверінің қоймасымен деректерді синхрондау**

  Басқару сервері көрсетілген қалтада (немесе қалталарда) өзгерістерді мезгіл-мезгіл тексеріп отыруын қаласаңыз, осы параметрді таңдаңыз.

  Әдепкі бойынша, параметр өшірулі.

  Егер сіз осы параметрді қоссаңыз, көрсетілген қалтада (қалталарда) өзгерістерді тексеру үшін кезеңді (сағатпен) көрсетіңіз. Әдепкі бойынша, тексеру кезеңі 24 сағатқа тең келеді.

- **Файл түрі**

  Бұл бөлімде бағдарламалар санатын құру үшін қолданылатын файл түрін көрсетуге болады.

  Барлық файлдар. Жасалып жатқан санат үшін барлық файлдар ескеріледі. Әдепкі бойынша, осы нұсқа таңдалған.

  Тек бағдарлама санаттарынан тыс файлдар. Құрылған санат үшін тек бағдарлама санаттарынан тыс файлдар ескеріледі.

- **Қалталар**

  Бұл бөлімде бағдарламалар санатын құру үшін пайдаланылатын файлдары бар таңдалған құрылғылардың қалталарын көрсетуге болады.

Барлық қалталар. Жасалып жатқан санат үшін барлық қалталар ескеріледі. Әдепкі бойынша, осы нұсқа таңдалған.

Көрсетілген қалта. Жасалып жатқан санат үшін тек көрсетілген қалта ескеріледі. Егер сіз осы параметрді таңдасаңыз, қалта жолын көрсетуіңіз керек.

Шебердің жұмысы аяқталған кезде орындалатын файлдардың санаты жасалады. Ол санаттар тізімінде пайда болады. Бағдарламаны басқару құрамдасын конфигурациялау кезінде санатты жасауға болады.

Таңдалған қалталардан орындалатын файлдарды қамтитын бағдарламалар санатын құру

Таңдалған қалталардың орындалатын файлдарын, ұйымыңызда іске қосуға рұқсат бергіңіз немесе тыйым салғыңыз келетін орындалатын файлдардың эталондық жиынтығы ретінде пайдалануға болады. Таңдалған қалталардағы орындалатын файлдардың негізінде, сіз бағдарламалар санатын құра аласыз және оны Бағдарламаны басқару құрамдасын конфигурациялау үшін пайдалана аласыз.

Таңдалған қалталардан орындалатын файлдарды қамтитын санатты құру үшін:

1. Бағдарламаның негізгі терезесінде **Бағдарламалық жасақтаманы басқару → Үшінші тарап бағдарламалары → Бағдарлама санаттары** бөліміне өтіңіз.

   Санаттар тізімі бар бет ашылады.

2. **Қосу** түймесін басыңыз.

   Жаңа санат шебері іске қосылады. Шебердің жұмысын жалғастыру үшін **Келесі** түймесін басыңыз.

3. **Санатты жасау әдісін таңдау** қадамында санат атауын көрсетіп, **Белгілі бір қалтадағы орындалатын файлдарды қамтитын санат. Көрсетілген қалтаға көшірілген бағдарламалардың орындалатын файлдары автоматты түрде өңделеді және олардың метрикалық көрсеткіштері санатқа қосылады** параметрін таңдаңыз.

4. Орындалатын файлдары санатты құру үшін пайдаланылатын қалтаны көрсетіңіз.

5. Келесі параметрлерді конфигурациялаңыз:

   - **Санатқа динамикалық түрде қосылатын кітапханаларды (DLL) қосу**

     Бағдарламалар санатына динамикалық түрде қосылатын кітапханалар (DLL пішіміндегі файлдар) қосылады және Бағдарламаны басқару құрамдасы жүйеде іске қосылған осындай кітапханалардың әрекеттерін тіркейді. DLL пішіміндегі файлдарды санатқа қосу кезінде Kaspersky Security Center Linux жұмысының өнімділігі төмендеуі мүмкін.

     Әдепкі бойынша, жалауша алынып тасталған.

   - **Санатқа скрипт туралы деректерді қосу**

     Бағдарлама санатына скрипт туралы деректер қосылады және скрипттер Веб-қауіптен қорғаныс құрамдасы тарапынан бұғатталмайды. Скрипт туралы деректерді санатқа қосу кезінде Kaspersky Security Center Linux жұмысының өнімділігі төмендеуі мүмкін.

     Әдепкі бойынша, жалауша алынып тасталған.

- **Хэш функциясын есептеу алгоритмі**: **Осы санаттағы файлдар үшін SHA256 мәнін есептеу (Kaspersky Endpoint Security 10 Service Pack 2 for Windows және одан кейінгі нұсқаларында қолдау көрсетіледі) /Осы санаттағы файлдар үшін MD5 есептеу (Kaspersky Endpoint Security 10 Service Pack 2 for Windows нұсқасынан бұрынғы нұсқалармен қолдау көрсетіледі)**

  Желіңіздегі құрылғыларға орнатылған қауіпсіздік бағдарламасы нұсқасына байланысты, санат файлдары үшін хеш функциясын Kaspersky Security Center Linux бағдарламасы тарапынан есептеп шығару алгоритмін таңдау керек. Хэш функцияларымен есептелетін хэш мәндері туралы ақпарат басқару сервері дерекқорында сақталады.

  SHA256 – алгоритмінде осалдық табылмаған криптографиялық хеш функциясы және ол қазіргі уақытта ең сенімді криптографиялық функция болып саналады. Kaspersky Endpoint Security for Linux қолданбасы SHA256 есептеуін қолдайды.

  Санат файлдары үшін Kaspersky Security Center Linux бағдарламасы тарапынан хеш функциясын есептеп шығару нұсқаларының бірін таңдаңыз:

  - Егер желіңізде орнатылған қауіпсіздік бағдарламаларының барлық үлгілері Kaspersky Endpoint Security for Linux болса, **SHA256** жалаушаны орнатыңыз.

  Windows үшін Kaspersky Endpoint Security пайдалансаңыз ғана, **MD5 хэші** жалаушаны орнатыңыз. Kaspersky Endpoint Security for Linux MD5 хэш функциясына қолдау көрсетпейді.

  Әдепкі бойынша, **Санаттағы файлдар үшін SHA256 есептеп шығару (Kaspersky Endpoint Security 10 Service Pack 2 for Windows үшін қолдау көрсетіледі)** жалаушасы қойылған.

  Әдепкі бойынша, **Осы санаттағы файлдар үшін MD5 есептеу (Kaspersky Endpoint Security 10 Service Pack 2 for Windows нұсқасынан бұрынғы нұсқалармен қолдау көрсетіледі)** алынып тасталған.

- **Қалтада өзгертулер бар-жоғын мәжбүрлеп сканерлеу**

  Егер бұл параметр қосулы болса, бағдарлама санаттарды толықтыру қалтасында өзгертулердің бар-жоғын мезгіл-мезгіл мәжбүрлеп тексереді. Тексерудің сағат түріндегі мерзімділігін жалаушаның жанындағы енгізу өрісінде көрсетуге болады. Әдепкі бойынша, мәжбүрлеп тексеру кезеңі 24 сағатқа тең келеді.

  Осы параметр өшірулі болса, қалтаны мәжбүрлеп тексеру орындалмайды. Сервер қалтадағы файлдарды өзгерту, қосу немесе жою кезінде оларға жүгінеді.

  Әдепкі бойынша, параметр өшірулі.

Шебердің жұмысы аяқталған кезде орындалатын файлдардың санаты жасалады. Ол санаттар тізімінде пайда болады. Бағдарламаны басқару құрамдасын конфигурациялау үшін санатты пайдалануға болады.

Бағдарламаларды бақылау құрамдас бөлігінің толық сипаттамасын Kaspersky Endpoint Security for Linux және Kaspersky Endpoint Security for Windows бағдарламасының онлайн анықтамасынан қараңыз.

Бағдарлама санаттары тізімін қарап шығу

Сіз конфигурацияланған орындалатын файлдар санаттарының тізімін және әр санаттың параметрлерін көре аласыз.

Бағдарлама санаттары тізімін көру үшін,

Бағдарламаның негізгі терезесінде **Бағдарламалық жасақтаманы басқару → Үшінші тарап бағдарламалары → Бағдарлама санаттары** бөліміне өтіңіз.

Санаттар тізімі бар бет ашылады.

Бағдарлама санаты сипаттарын көру үшін,

санаттың атауын басыңыз.

Таңдалған санаттың сипаттар терезесі ашылады. Параметрлер бірнеше қойындыда топтастырылған.

Бағдарлама санатына оқиғамен байланысты орындалатын файлдарды қосу

Бағдарламаны басқару құрамдасы конфигурацияланғаннан кейін, Kaspersky Endpoint Security саясаттарында, оқиғалар тізімінде келесі оқиғалар көрсетілуі мүмкін:

- **Бағдарламаны іске қосуға тыйым салынған** (*Критикалық оқиға*). Егер сіз ережелерді қолдану үшін Бағдарламаны басқаруды конфигурациялаған болсаңыз, бұл оқиға көрсетіледі.
- **Бағдарламаны іске қосуға сынақ режиміне тыйым салынған** (*Ақпараттық* оқиға). Егер сіз сынақ режимінде ережелерді қолдану үшін Бағдарламаны басқаруды конфигурациялаған болсаңыз, бұл оқиға көрсетіледі.
- **Әкімшіге бағдарламаның іске қосылуына тыйым салынғаны туралы хабар** (*Ескертудің* маңыздылық деңгейі бар хабар). Егер сіз ережелерді қолдану үшін Бағдарламаны басқаруды конфигурациялаған болсаңыз, ал пайдаланушы іске қосу үшін бұғатталған бағдарламаға қатынасуды сұраса, бұл оқиға көрсетіледі.

Бағдарламаны басқару құрамдасына қатысты оқиғаларды көру үшін оқиғалар таңдауын жасау ұсынылады.

Бағдарламаны басқару оқиғаларына қатысты орындалатын файлдарды қолданыстағы бағдарламалар санатына немесе жаңа бағдарламалар санатына қосуға болады. Орындалатын файлдарды тек қолмен толтырылатын бағдарламалар санатына қосуға болады.

Бағдарламаны басқару құрамдасының оқиғаларымен байланысты орындалатын файлдарды бағдарламалар санатына қосу үшін:

1. Бағдарламаның негізгі терезесінде **Мониторинг** → **Оқиғаларды таңдау** бөліміне өтіңіз.

   Оқиғалар таңдауы тізімі көрсетіледі.

2. Бағдарламаны басқаруға қатысты оқиғаларды көру үшін оқиғалар таңдауын таңдап, сол оқиғалар таңдауын құруды іске қосыңыз.

   Бағдарламаны басқарумен байланысты оқиғалар таңдауын жасамаған болсаңыз, **Соңғы оқиғалар** сияқты алдын ала анықталған таңдауды таңдап, іске қосуға болады.

   Оқиғалар тізімі көрсетіледі.

3. Бағдарламалар санатына қосқыңыз келетін орындалатын файлдары бар оқиғаларды таңдап, **Санатқа тағайындау** түймесін басыңыз.

   Жаңа санат шебері іске қосылады. Шебердің жұмысын жалғастыру үшін **Келесі** түймесін басыңыз.

4. Шебер бетінде қажетті параметрлерді көрсетіңіз:

- **Оқиғаға қатысты орындалатын файл бойынша әрекет** бөлімінде келесі опциялардың бірін таңдаңыз:
  - **Жаңа бағдарлама санатына қосу**

    Оқиғалармен байланысты орындалатын файлдар негізінде бағдарламалар санатын жасағыңыз келсе, осы параметрді таңдаңыз.

    Әдепкі бойынша, осы нұсқа таңдалған.

    Егер сіз осы параметрді таңдасаңыз, жаңа санаттың атын көрсетіңіз.

  - **Қолданыстағы бағдарлама санатына қосу**

    Бар бағдарламалар санатына оқиғаға қатысты орындалатын файлдарды қосқыңыз келсе, осы параметрді таңдаңыз.

    Әдепкі бойынша нұсқа таңдалмаған.

    Егер сіз осы параметрді таңдаған болсаңыз, орындалатын файлдарды қосқыңыз келетін қолмен толықтырылатын бағдарламалар санатын таңдаңыз.

- **Ереже түрі** бөлімінде келесі нұсқалардың бірін таңдаңыз:
  - **Қамтылатындарға қосу ережелері**
  - **Шығарылатындарға қосу ережелері**
- **Шарт ретінде пайдаланылатын параметр** бөлімінде келесі опциялардың бірін таңдаңыз:
  - **Сертификат мәліметтері (немесе сертификаты жоқ файлдар үшін SHA256 хэштері)**

    Файлдарға сертификат арқылы қол қоюға болады. Бұл арада, бір сертификатпен бірнеше файлға қол қоюға болады. Мысалы, бір бағдарламаның әртүрлі нұсқаларына бір сертификатпен қол қоюға болады немесе бір өндірушінің бірнеше түрлі бағдарламаларына бір сертификатпен қол қоюға болады. Сертификатты таңдаған кезде санатқа бағдарламаның бірнеше нұсқасы немесе бір өндірушінің бірнеше бағдарламасы кіруі мүмкін.

    Әрбір файлдың өзіндік бірегей SHA256 хэш функциясы бар. SHA256 хэш функциясын таңдағанда, санатқа бағдарламаның белгіленген нұсқасы сияқты бір ғана тиісті файл кіреді.

    Санат ережелеріне орындалатын файл сертификатының деректерін немесе сертификаты жоқ файлдар үшін SHA256 хэш функциясын қосу қажет болса, осы нұсқаны таңдаңыз.

    Әдепкі бойынша, осы нұсқа таңдалған.

  - **Сертификат мәліметтері (сертификаты жоқ файлдар өткізіп жіберіледі)**

    Файлдарға сертификат арқылы қол қоюға болады. Бұл арада, бір сертификатпен бірнеше файлға қол қоюға болады. Мысалы, бір бағдарламаның әртүрлі нұсқаларына бір сертификатпен қол қоюға болады немесе бір өндірушінің бірнеше түрлі бағдарламаларына бір сертификатпен қол қоюға болады. Сертификатты таңдаған кезде санатқа бағдарламаның бірнеше нұсқасы немесе бір өндірушінің бірнеше бағдарламасы кіруі мүмкін.

    Санат ережелеріне орындалатын файл сертификатының деректерін қосу қажет болса, осы нұсқаны таңдаңыз. Орындалатын файлдың сертификаты болмаса, ондай файлды өткізіп жіберуге болады. Ол туралы ақпарат санатқа қосылмайды.

  - **Тек SHA256 (хэші жоқ файлдар өткізіп жіберіледі)**

    Әрбір файлдың өзіндік бірегей SHA256 хэш функциясы бар. SHA256 хэш функциясын таңдағанда, санатқа бағдарламаның белгіленген нұсқасы сияқты бір ғана тиісті файл кіреді.

Санат ережелеріне тек орындалатын файлдың SHA256 хеш функциясының деректерін ғана қосу керек болса, осы нұсқаны таңдаңыз.

- **Тек MD5 (үзілген режим, тек Kaspersky Endpoint Security 10 Service Pack 1 нұсқасы үшін)**

  Бұл параметрді Kaspersky Endpoint Security for Windows пайдалансаңыз ғана таңдаңыз. Kaspersky Endpoint Security for Linux MD5 хэш функциясына қолдау көрсетпейді.

  Әрбір файлдың өзіндік бірегей MD5 хэш функциясы бар. MD5 хэш функциясын таңдағанда, санатқа бағдарламаның белгіленген нұсқасы сияқты бір ғана тиісті файл кіреді.

5. **OK** түймесін басыңыз.

Шебердің жұмысы аяқталғаннан кейін, Бағдарламаны басқару оқиғаларымен байланысты орындалатын файлдар қолданыстағы бағдарламалар санатына немесе жаңа бағдарламалар санатына қосылады. Сіз өзгерткен немесе жасаған бағдарламалар санатының параметрлерін көре аласыз.

Бағдарламаларды бақылау құрамдас бөлігінің толық сипаттамасын Kaspersky Endpoint Security for Linux және Kaspersky Endpoint Security for Windows бағдарламасының онлайн анықтамасынан қараңыз.

Kaspersky Endpoint Security for Windows саясатындағы Бағдарламаларды басқару конфигурациялау

Бағдарламаны басқаруға арналған санаттарды жасағаннан кейін, оларды Kaspersky Endpoint Security for Windows саясатындағы Бағдарламаны басқаруды конфигурациялау үшін пайдалануға болады.

Kaspersky Endpoint Security for Windows саясатындағы Бағдарламаны басқару құрамдасын конфигурациялау үшін:

1. Бағдарламаның негізгі терезесінде **Активтерді басқару** → **Саясаттар** бөліміне өтіңіз.

   Саясаттар тізімі бар бет көрсетіледі.

2. **Kaspersky Endpoint Security for Windows** саясатын басыңыз.

   Саясат сипаттары терезесі ашылады.

3. **Бағдарлама параметрлері** → **Қауіпсіздікті бақылау** → **Бағдарламаны басқару** бөліміне өтіңіз.

   Бағдарламаны басқару құрамдасының параметрлері бар **Бағдарламаны басқару** терезесі ашылады.

4. **Бағдарламаны басқару** параметрі әдепкі бойынша қосулы. Параметрді өшіру үшін **Бағдарламаны басқару [Өшірулі]** қосқышын өшіріңіз.

5. **Бағдарламаны басқару параметрлері** блогында Бағдарламаны басқару ережелерін қолдана отырып жұмыс режимін қосыңыз және Kaspersky Endpoint Security for Windows бағдарламасына бағдарламаларын іске қосуды бұғаттауға мүмкіндік беріңіз.

   Бағдарламаны басқару ережесін сынап көргіңіз келсе, **Бағдарламаны басқару ережесі** бөлімінде сынақ режимін қосыңыз. Сынақ режимінде Kaspersky Endpoint Security for Windows бағдарламасы бағдарламалардың іске қосылуын бұғаттамайды, бірақ есепте іске қосылған ережелер туралы ақпаратты жазып алады. Осы ақпаратты қарау үшін **Есепті қарап шығу** сілтемесінен өтіңіз.

6. Пайдаланушылар бағдарламаларды іске қосқан кезде Kaspersky Endpoint Security for Windows бағдарламасы DLL модульдерін жүктеуді бақылағанын қаласаңыз, **DLL модульдерін жүктеуді басқару** параметрін қосыңыз.

   Модуль туралы ақпарат және модульді жүктеген бағдарлама есепте сақталады.

   Kaspersky Endpoint Security for Windows бағдарламасы тек **DLL модульдерін жүктеуді басқару** параметрі қосулы болғаннан кейін жүктелген DLL модульдер мен драйверлерді бақылайды. Kaspersky Endpoint Security for Windows барлық DLL модулі мен драйверін, соның ішінде Kaspersky Endpoint Security for Windows іске қосылғанға дейін жүктелгендерді басқарғанын қаласаңыз, **DLL модульдерін жүктеуді басқару** опциясын таңдағаннан кейін құрылғыны қайта іске қосыңыз.

7. (Қажет болса.) **Хабар үлгілері** блогында, бағдарлама іске қосу үшін бұғатталған кезде көрсетілетін хабар үлгісін және сізге жіберілетін электрондық пошта хабары үлгісін өзгертіңіз.

8. **Бағдарламаны басқару режимі** параметрлер блогында **Тыйым салу тізімі** немесе **Рұқсат ету тізімі** режимін таңдаңыз.

   Әдепкі бойынша **Тыйым салу тізімі** режимі таңдалған.

9. **Ереже тізімдері параметрлері** сілтемесінен өтіңіз.

   Бағдарлама санаттарын қосуға болатын **Тыйым салу және рұқсат ету тізімдері** терезесі ашылады. Әдепкі бойынша, **Тыйым салу тізімі** режимі таңдалған болса, **Тыйым салу тізімі** қойындысы немесе **Рұқсат ету тізімі** режимі таңдалған болса, **Рұқсат ету тізімі** режимі көрсетіледі.

10. **Тыйым салу және рұқсат ету тізімдері** терезесінде **Қосу** түймесін басыңыз.

    Бағдарламаны басқару ережесі терезесі ашылады.

11. **Өтініш, санатты таңдаңыз** сілтемесінен өтіңіз.

    Бағдарлама санаттары терезесі ашылады.

12. Бұрын жасаған бағдарламалар санатын (немесе санаттарын) қосыңыз.

    Өзгерту түймесін басу арқылы санат параметрлерін өзгертуге болады.

    Қосу түймесін басу арқылы санат жасауға болады.

    Жою түймесін басу арқылы санатты жоюға болады.

13. Бағдарлама санаттарының тізімін жасау аяқталғаннан кейін **OK** түймесін басыңыз.

    Бағдарлама санаты терезесі жабылады.

14. **Бағдарламаны басқару** ережесі терезесінде, **Субъектілер және олардың құқықтары** бөлімінде Бағдарламаны басқару ережелерін қолдану үшін пайдаланушылар мен пайдаланушылар топтарының тізімін жасаңыз.

15. Параметрлерді сақтау және **Бағдарламаны басқару ережесі** терезесін жабу үшін **OK** түймесін басыңыз.

16. Параметрлерді сақтау және **Тыйым салу және рұқсат ету тізімдері** терезесін жабу үшін **OK** түймесін басыңыз.

17. Параметрлерді сақтау және **Бағдарламаны басқару** ережесі терезесін жабу үшін **OK** түймесін басыңыз.

18. Kaspersky Endpoint Security for Windows саясаты параметрлері терезесін жабыңыз.

Бағдарламаны басқару құрамдасы конфигурацияланған. Саясатты клиент құрылғыларына таратқаннан кейін, орындалатын файлдардың іске қосылуы бақыланады.

Бағдарламаларды бақылау құрамдас бөлігінің толық сипаттамасын Kaspersky Endpoint Security for Linux және Kaspersky Endpoint Security for Windows бағдарламасының онлайн анықтамасынан қараңыз.

Клиент құрылғыларында орнатылған бағдарламалар тізімін алу және қарау

Kaspersky Security Center Linux бағдарламасы, Linux және Windows операциялық жүйесінің басқаруымен жұмыс істейтін басқарылатын клиент құрылғыларында орнатылған бағдарламалық жасақтаманы түгендейді.

Желілік агент құрылғыда орнатылған бағдарламалар тізімін құрастырып, тізімді Басқару серверіне жібереді. Желілік агентке бағдарламалар тізімін жаңарту үшін шамамен 10-15 минут кетеді.

Windows операциялық жүйесі бар клиент құрылғылары үшін Желілік агент орнатылған бағдарламалар туралы ақпараттың көп бөлігін Windows тізімдемесінен алады. Linux операциялық жүйесі бар клиент құрылғылары үшін орнатылған бағдарламалар туралы ақпаратты Желілік агент пакет диспетчерлерінен алады.

Басқарылатын құрылғыларда орнатылған бағдарламалар тізімін көру үшін,

1. Бағдарламаның негізгі терезесінде **Операциялар** → **Үшінші тарап бағдарламалары** → **Бағдарламалар тізімдемесі** бөліміне өтіңіз.

   Бетте басқарылатын құрылғыларда орнатылған бағдарламалары бар кесте көрсетіледі. Сол бағдарламаның қасиеттерін көру үшін бағдарламаны таңдаңыз, мысалы: өндірушінің аты, нұсқа нөмірі, орындалатын файлдар тізімі, бағдарлама орнатылған құрылғылардың тізімі.

2. Орнатылған бағдарламалары бар кесте деректерін келесідей топтастыруға және сүзуге болады:

   - Кестенің жоғарғы оң жақ бұрышындағы ( ) параметрлері белгішесін нұқыңыз.

     Ашылған **Бағандар параметрлері** мәзірінен кестеде көрсетілетін бағандарды таңдаңыз. Бағдарлама орнатылған клиент құрылғыларының операциялық жүйесінің түрін көру үшін **ОЖ түрі** бағанын таңдаңыз.

   - Кестенің жоғарғы оң жақ бұрышындағы ( ) сүзу белгішесін нұқыңыз, ашылған мәзірде сүзу критерийін көрсетіңіз және қолданыңыз.

     Орнатылған бағдарламалардың сүзілген кестесі көрсетіледі.

Таңдалған басқарылатын құрылғыда орнатылған бағдарламалар тізімін көру үшін,

Бағдарламаның негізгі терезесінде **Активтерді басқару** → **Активтер (құрылғылар)** → **<құрылғы атауы>** → **Кеңейтілген** → **Бағдарламалар тізімдемесі** бөліміне өтіңіз. Бұл мәзірде бағдарламалар тізімін CSV немесе TXT пішіміндегі файлдарға экспорттауға болады.

Бағдарламаларды бақылау құрамдас бөлігінің толық сипаттамасын Kaspersky Endpoint Security for Linux және Kaspersky Endpoint Security for Windows бағдарламасының онлайн анықтамасынан қараңыз.

Үшінші тарап бағдарламалары туралы

Kaspersky Security Center Linux клиент құрылғыларында орнатылған үшінші тарап бағдарламалық жасақтамасын жаңартуға және үшінші тарап бағдарламалық жасақтамасының осалдықтарын түзетуге көмектеседі. Kaspersky Security Center Linux үшінші тарап қолданбаларын тек ағымдағы нұсқадан соңғы нұсқаға дейін жаңарта алады.

Үшінші тарап бағдарламалық жасақтамаларының тізімін өзгертуге болады және ол динамикалық түрде жаңартылады. Kaspersky Security Center Web Console веб-консолінде қолжетімді жаңартулар тізімін қарап шығып, үшінші тарап бағдарламалық жасақтамасын (пайдаланушылардың құрылғыларында орнатылған) Kaspersky Security Center Linux көмегімен жаңарта алатыныңызды тексере аласыз.

Төменде сипатталған процедура тек Kaspersky Security Center Linux бағдарламасымен жаңартуға болатын үшінші тарап бағдарламалық жасақтамаларының тізімін көруге арналған. Ешбір тапсырманы бастамастан тиісті ақпаратқа арнайы мүмкіндіктер арқылы қол жеткізу үшін қадамдар орындалады.

Kaspersky Security Center Linux бағдарламасымен жаңартуға болатын үшінші тарап бағдарламалық жасақтамасының тізімін көру үшін:

1. Бағдарламаның негізгі терезесінде **Тапсырмалар** бөліміне өтіңіз.
2. **Қосу** түймесін басыңыз.

   Жаңа тапсырма жасау шебері іске қосылады. Шебердің жұмысын жалғастыру үшін **Келесі** түймесін басыңыз.
3. Шебердің **Жаңа тапсырма параметрлері** қадамында келесі параметрлерді көрсетіңіз:

   a. **Бағдарлама** ашылмалы тізімінде **Kaspersky Security Center Linux** опциясын таңдаңыз.

   b. **Тапсырма түрі** тізімінде **Қажетті жаңартуларды орнату және осалдықтарды түзету** тапсырма түрін таңдаңыз.
4. Шебердің **Тапсырма ауқымы** қадамында **Басқарылатын құрылғылар** опциясын таңдаңыз.
5. Шебердің **Жаңа нұсқаларды орнатуға арналған ережелерді көрсетіңіз** қадамында **Қосу** түймесін басыңыз.

   Ережені жасау шебері іске қосылады. Шебердің жұмысын жалғастыру үшін **Келесі** түймесін басыңыз.
6. Шебердің **Ереже түрін таңдаңыз** қадамында **Үшінші тарап жаңартуларға арналған ереже** опциясын таңдаңыз.
7. Шебердің **Жалпы шарттар** қадамында **Барлық жаңартуларды орнату (қабылданбаған жаңартулардан басқа)** опциясын таңдап, **Келесі** түймесін басыңыз.

Үшінші тарап бағдарламалық жасақтамасының тізімі көрсетіледі.

Үшінші тарап бағдарламаларының жаңартуларын орнату

Kaspersky Security Center Linux қолданбасы басқарылатын құрылғыларда орнатылған үшінші тарап қолданбаларының жаңартуларын басқаруға және қажетті жаңартуларды орнату арқылы мұндай қолданбалардағы осалдықтарды түзетуге мүмкіндік береді.

Kaspersky Security Center Linux жүйесі *Осалдықтарды және қажетті жаңартуларды іздеу* тапсырмасы арқылы жаңартуларды іздейді. Бұл тапсырма аяқталғаннан кейін, Басқару сервері құрылғыларға орнатылған және тапсырма сипаттарында көрсетілген үшінші тарап қолданбалары үшін қажетті жаңартулар мен табылған осалдықтар тізімдерін алады. Қолжетімді жаңартулар туралы ақпаратты көргеннен кейін, жаңартуларды құрылғыларыңызға орнатуға болады.

Kaspersky Security Center Linux кейбір қолданбаларын жаңарту, қолданбаның алдыңғы нұсқасын жою және жаңа нұсқасын орнату арқылы орындалады.

Пайдаланушының араласуы үшінші тарап бағдарламаларын жаңарту кезінде немесе басқарылатын құрылғыдағы үшінші тарап бағдарламаларында осалдықтарды түзету кезінде қажет болуы мүмкін. Мысалы, пайдаланушыдан үшінші тарап бағдарламасын жабу сұралуы мүмкін.

Қауіпсіздік мақсатында, Осалдықтар мен патчтарды басқару арқылы орнатқан кез келген үшінші тарап бағдарламалық жасақтамасы жаңартулары Kaspersky технологиялары арқылы зиянды БҚ-дың бар-жоғы тұрғысынан автоматты түрде тексеріледі. Бұл технологиялар файлдарды автоматты түрде тексеру үшін қолданылады және антивирустық тексеруді, статикалық талдауды, динамикалық талдауды, "құмсалғыштың" жүріс-тұрысын талдауды және машиналық оқытуды қамтиды.

Kaspersky мамандары Осалдықтар мен патчтарды басқару арқылы орнатуға болатын үшінші тарап бағдарламалық жасақтамасы жаңартуларын қолмен талдамайды. Сонымен қатар Kaspersky мамандары мұндай жаңартулардағы осалдықтарды (белгілі немесе белгісіз) немесе құжатталмаған мүмкіндіктерді іздеумен айналыспайды және жоғарыда аталған талдаудың басқа түрлерін жүргізбейді.

Үшінші тарап жасақтамасын құралын жаңарту метадеректері қоймаға жүктеп алынған кезде, жаңартуларды клиенттік құрылғыларға *Қажетті жаңартуларды орнату және осалдықтарды түзету* тапсырмасын орындау арқылы орнатуға болады.

> *Қажетті жаңартуларды орнату және осалдықтарды түзету* тапсырмасын Осалдықтар мен патчтарды басқару лицензиясы болса ғана жасауға болады.

Бұл тапсырма аяқталғаннан кейін, жаңартулар басқарылатын құрылғыларға автоматты түрде орнатылады. Жаңа жаңартулардың метадеректерін Басқару сервері қоймасына жүктеу кезінде, Kaspersky Security Center Linux қолданбасы жаңартулардың жаңарту ережелерінде көрсетілген өлшемшарттарға сәйкес келетіндігін тексереді. Критерийлерге сәйкес келетін барлық жаңа жаңартулар келесі тапсырма басталған кезде автоматты түрде жүктеледі және орнатылады.

Сценарий: Үшінші тарап бағдарламаларын жаңарту

Бұл бөлімде клиент құрылғыларында орнатылған үшінші тарап қолданбаларын жаңарту сценарийі ұсынылған. Үшінші тарап қолданбалары басқа да бағдарламалық жасақтама өндірушілері ұсынған қолданбаларды қамтиды.

Алдын ала талаптар

Үшінші тарап бағдарламалық жасақтамасының жаңартуларын орнату үшін Басқару сервері интернетке қосылған болуы керек.

Кезеңдер

Өндірушілердің жаңартуы келесі кезеңдерден тұрады:

1. **Қажетті жаңартуларды іздеу**

   Басқарылатын құрылғыларға қажет үшінші тарап бағдарламасының жаңартуларын табу үшін *Осалдықтарды және қажетті жаңартуларды іздеу* тапсырмасын іске қосыңыз. Бұл тапсырма аяқталғаннан кейін, Kaspersky Security Center Linux қолданбасы құрылғыларға орнатылған және тапсырма сипаттарында көрсетілген үшінші тарап қолданбалары үшін қажетті жаңартулар мен табылған осалдықтар тізімдерін алады.

   Осалдықтарды және қажетті жаңартуларды іздеу тапсырмасы Басқару серверін жылдам іске қосу шебері автоматты түрде жасалады. Шеберді іске қоспасаңыз, *Осалдықтарды және қажетті жаңартуларды іздеу* тапсырмасын жасаңыз немесе бастапқы орнату шеберін іске қосыңыз.

   > Windows жүйесімен жұмыс істейтін құрылғылар үшін ғана *Осалдықтарды және қажетті жаңартуларды іздеу* тапсырмасын жасай аласыз. Бұл тапсырманы басқа операциялық жүйелермен жұмыс істейтін құрылғылар үшін жасай алмайсыз.

2. **Табылған жаңартулар тізімін талдау**

   Қолжетімді үшінші тарап бағдарламалық жасақтамасы жаңартулары туралы ақпаратты қарап шығыңыз және қандай жаңартуларды орнатқыңыз келетінін шешіңіз. Әрбір жаңарту туралы толық ақпаратты көру үшін тізімдегі жаңарту атын түртіңіз. Тізімдегі әрбір жаңарту үшін клиент құрылғыларындағы жаңартуларды орнату статистикасын да көруге болады.

3. **Жаңартулар орнатуды конфигурациялау**

   Kaspersky Security Center Linux үшінші тарап қолданбалары жаңартулары тізімін алғаннан кейін, оларды *Қажетті жаңартуларды орнату және осалдықтарды түзету* тапсырмасын жасау арқылы клиенттік құрылғыларға орнатуға болады.

   > *Қажетті жаңартуларды орнату және осалдықтарды түзету* тапсырмасын тек Windows жүйесімен жұмыс істейтін құрылғылар үшін ғана жасауға болады. Бұл тапсырманы басқа операциялық жүйелермен жұмыс істейтін құрылғылар үшін жасай алмайсыз.

   Қажетті жаңартуларды орнату және осалдықтарды түзету тапсырмасы Windows Update жаңартулары қызметі ұсынатын жаңартуларды және басқа өндірушілердің қолданбаларының жаңартуларын қоса алғанда, Microsoft қолданбаларына арналған жаңартуларды орнату үшін қолданылады. *Қажетті жаңартуларды орнату және осалдықтарды түзету* тапсырмасын тек Осалдықтар мен патчтарды басқару лицензиясы болған жағдайда ғана жасауға болатынын ескеріңіз.

   Бағдарламалық жасақтаманың кейбір жаңартуларын орнату үшін сіз бағдарламалық жасақтаманы орнатуға арналған Лицензиялық келісімді қабылдауыңыз қажет. Лицензиялық келісімнен бас тартсаңыз, бағдарламалық жасақтама жаңартулары орнатылмайды.

Жаңартуды орнату тапсырмасын кесте бойынша іске қосуға болады. Тапсырманың кестесін көрсету кезінде, жаңартуды орнату тапсырмасы *Осалдықтарды және қажетті жаңартуларды іздеу* тапсырмасы аяқталғаннан кейін іске қосылатынына көз жеткізіңіз.

4. **Тапсырманың кестесін белгілеу**

Жаңартулар тізімі әрқашан өзекті екеніне көз жеткізу мақсатында, *Осалдықтарды және қажетті жаңартуларды іздеу* тапсырмасын мезгіл-мезгіл автоматты түрде іске қосылуы үшін, оны іске қосу кестесін белгілеңіз. Әдепкі бойынша *Осалдықтарды және қажетті жаңартуларды іздеу* тапсырмасы сағат 18:00:00-де қолмен іске қосылады.

Қажетті жаңартуларды орнату және осалдықтарды түзету тапсырмасын жасаған болсаңыз, оны іске қосуды *Осалдықтарды және қажетті жаңартуларды іздеу* тапсырмасына арналған жиілікпен немесе одан сирек жиілікпен іске қосуды белгілей аласыз.

Тапсырмалар кестесін белгілеу кезінде, осалдықтарды түзету тапсырмасы *Осалдықтарды және қажетті жаңартуларды іздеу* аяқталғаннан кейін іске қосылатынына көз жеткізіңіз.

5. **Үшінші тарап қолданбаларының жаңартуларын мақұлдау және қабылдамау (міндетті емес)**

Қажетті жаңартуларды орнату және осалдықтарды түзету тапсырмасын жасаған болсаңыз, сіз тапсырманың сипаттарында жаңартуларды орнату ережелерін көрсете аласыз.

Әрбір ереже үшін олардың күйіне қарай орнатылатын жаңартуларды таңдауға болады: *Анықталмаған*, *Расталды* немесе *Қабылданбады*. Мысалы, сіз серверлер үшін белгілі бір тапсырма жасай аласыз және тек *Расталды* күйі бар жаңартуларды ғана орнатуға рұқсат беру үшін осы тапсырмаға арналған ережені орната аласыз. Содан кейін, орнатқыңыз келетін жаңартулар үшін *Расталды* күйін қолмен белгілейсіз. Бұл жағдайда, *Анықталмаған* немесе *Қабылданбады* күйі бар жаңартулар тапсырмада көрсетілген серверлерге орнатылмайды.

Жаңартуларды орнатуды басқарған кезде, аздаған жаңартулар үшін *Расталды* күйін қолданған жөн. Бірнеше жаңарту орнату үшін, *Қажетті жаңартуларды орнату және осалдықтарды түзету* тапсырмасында конфигурациялауға болатын ережелерді қолданыңыз. *Расталды* күйін, ережелерде көрсетілген өлшемшарттарға сай келмейтін жаңартулар үшін ғана белгілеу ұсынылады. Жаңартулардың көп санын қолмен растасаңыз, Басқару серверінің өнімділігі төмендеп, бұл Басқару серверінің артық жүктелуіне әкелуі мүмкін.

Әдепкі бойынша, жүктелген бағдарламалық жасақтама жаңартулары *Анықталмаған* күйіне ие. Күйді **Бағдарламалық жасақтама жаңартулары** (**Операциялар → Патчтарды басқару → Бағдарламалық жасақтама жаңартулары**) тізімінде *Расталды* немесе *Қабылданбады* деп өзгерте аласыз.

Қосымша ақпарат алу үшін үшінші тарап бағдарламалық жасақтамасының жаңартуларын мақұлдау және қабылдамау нұсқауларын қараңыз.

6. **Жаңартуларды орнату тапсырмасын іске қосу**

Қажетті жаңартуларды орнату және осалдықтарды түзету тапсырмасын іске қосыңыз. Осы тапсырманы орындағаннан кейін, жаңартулар жүктеледі және басқарылатын құрылғыларға орнатылады. Тапсырма аяқталғаннан кейін, оның тапсырмалар тізімінде *Сәтті аяқталды* күйі бар екеніне көз жеткізіңіз.

7. **Жаңарту орнату нәтижелері туралы есеп жасау (міндетті емес)**

Жаңартуды орнату статистикасын қарау үшін, Үшінші тарап бағдарламалық жасақтамасы жаңартуларын орнату нәтижелерін хабарлау құрастырыңыз.

Нәтижелер

Қажетті жаңартуларды орнату және осалдықтарды түзету тапсырмасын жасаған және конфигурациялаған болсаңыз, жаңартулар басқарылатын құрылғыларға автоматты түрде орындалатын болады. Жаңа жаңартуларды Басқару сервері қоймасына жүктеу кезінде, Kaspersky Security Center Linux бағдарламасы жаңартулардың жаңарту ережелерінде көрсетілген критерийлерге сәйкес келетіндігін тексереді. Критерийлерге сәйкес келетін барлық жаңа жаңартулар келесі тапсырма басталған кезде автоматты түрде орнатылады.

Үшінші тарап бағдарламалық жасақтама жаңартуларын орнату нұсқалары

Қажетті жаңартуларды орнату және осалдықтарды түзету тапсырмасын жасау және іске қосу арқылы басқарылатын құрылғыларға Windows Update жаңартуларын және үшінші тарап бағдарламалық жасақтамасының жаңартуларын орнатуға болады. *Қажетті жаңартуларды орнату және осалдықтарды түзету* тапсырмасын, тек Осалдықтар мен патчтарды басқаруға арналған лицензияңыз болса ғана жасауға болады. Бұл тапсырманы үшінші тарап қолданбалары үшін жаңартуларды орнату үшін пайдалануға болады.

Пайдаланушының араласуы үшінші тарап бағдарламаларын жаңарту кезінде немесе басқарылатын құрылғыдағы үшінші тарап бағдарламаларында осалдықтарды түзету кезінде қажет болуы мүмкін. Мысалы, пайдаланушыдан үшінші тарап бағдарламасын жабу сұралуы мүмкін.

Сондай-ақ, қажетті жаңартуларды келесі жолдармен орнату үшін тапсырма жасауға болады:

- Жаңартулар тізімін ашып, қандай жаңартуларды орнату керектігін көрсетіңіз.

  Нәтижесінде, таңдалған жаңартуларды орнату үшін тапсырма жасалады. Сондай-ақ, таңдалған жаңартуларды қолданыстағы тапсырмаға қосуға болады.

- Жаңартуды орнату шеберін іске қосу.

  Осалдықтар мен патчтарды басқару үшін лицензия болған кезде, жаңартуды орнату шебері қолжетімді болады.

  Шебер жаңартуларды орнату тапсырмасын құруды және конфигурациялауды жеңілдетеді және орнату үшін бірдей жаңартуларды қамтитын артық тапсырмаларды құруды болдырмайды.

Жаңарту тізімін пайдаланып, үшінші тарап бағдарламаларының жаңартуларын орнату

Үшінші тарап бағдарламаларының жаңартуларын орнату үшін:

1. Жаңартулар тізімін келесі тәсілдердің бірімен ашыңыз:

   - **Бағдарламалық жасақтаманы басқару** → **Патчтарды басқару** → **Бағдарламалық жасақтама жаңартулары**.
   - **Активтерді басқару** → **Активтер (құрылғылар)** → <device name> → **Кеңейтілген** → **Қолжетімді жаңартулар**.
   - **Бағдарламалық жасақтаманы басқару** → **Үшінші тарап бағдарламалары** → **Бағдарламалар тізімдемесі** → <қолданба атауы> → **Қолжетімді жаңартулар**.

   Қолжетімді жаңартулар тізімі көрсетіледі.

2. Орнатқыңыз келетін жаңартулардың жанына жалаушаны қойыңыз.

3. **Жаңартуларды орнату** түймесін басыңыз. Бұл түйме көрінбесе, көп нүкте түймесін басып, ашылмалы тізімнен **Жаңартуларды орнату** тармағын таңдаңыз.

   Бағдарламалық жасақтаманың кейбір жаңартуларын орнату үшін сіз Лицензиялық келісімді қабылдауыңыз керек. Лицензиялық келісімнен бас тартсаңыз, бағдарламалық жасақтама жаңартулары орнатылмайды.

4. Келесі нұсқалардың бірін таңдаңыз:

   - **Жаңа тапсырма**

     Жаңа тапсырма жасау шебері іске қосылады. Осалдықтар мен патчтарды басқаруға арналған лицензияңыз болса, әдепкі бойынша *Қажетті жаңартуларды орнату және осалдықтарды түзету* тапсырма түрі таңдалады. Тапсырма жасауды аяқтау үшін шебердің алдағы нұсқауларын орындаңыз.

   - **Жаңартуды орнату (көрсетілген тапсырмаға ереже қосу)**

     Таңдалған жаңартуларды қосқыңыз келетін тапсырманы таңдаңыз. Осалдықтар мен патчтарды басқаруға арналған лицензияңыз болса, *Қажетті жаңартуларды орнату және осалдықтарды түзету* тапсырмасын таңдаңыз. Таңдалған тапсырмаға таңдалған осалдықтарды түзетуге арналған ереже автоматты түрде қосылды. Таңдалған жаңартулар тапсырманың сипаттарына қосылды.

     Тапсырма сипаттары терезесі ашылады. Өзгерістерін сақтау үшін **Сақтау** түймесін басыңыз.

   Тапсырма жасауды таңдаған болсаңыз, ол тапсырмалар тізімінде, **Тапсырмалар** бөлімінде жасалып, көрсетіледі. Егер сіз бар тапсырмаға жаңартуларды қосуды таңдасаңыз, жаңартулар тапсырма сипаттарында сақталады.

Үшінші тарап бағдарламалық жасақтамасының жаңартуларын орнату үшін *Қажетті жаңартуларды орнату және осалдықтарды түзету* тапсырмасын орындау керек. Бұл тапсырманы тапсырмалар тізіміндегі **Іске қосу** түймесін басу немесе орындап жатқан тапсырманың сипаттарында кесте параметрлерін көрсету арқылы іске қосуға болады. Тапсырманың кестесін көрсету кезінде, жаңартуды орнату тапсырмасы *Осалдықтарды және қажетті жаңартуларды іздеу* тапсырмасы аяқталғаннан кейін іске қосылатынына көз жеткізіңіз.

Жаңартуды орнату шебері арқылы үшінші тарап бағдарламаларының жаңартуларын орнату

Осалдықтар мен патчтарды басқару үшін лицензия болған кезде, жаңартуды орнату шебері қолжетімді болады.

Жаңартуды орнату шеберін пайдаланып, үшінші тарап бағдарламалары жаңартуларын орнату тапсырмасын жасау үшін:

1. Бағдарламаның негізгі терезесінде **Бағдарламалық жасақтаманы басқару** → **Патчтарды басқару** → **Бағдарламалық жасақтама жаңартулары** бөліміне өтіңіз.

   Қолжетімді жаңартулар тізімі көрсетіледі.

2. Орнатқыңыз келетін жаңартудың жанына жалаушаны қойыңыз.

3. **Жаңартуларды орнату шеберін іске қосу** түймесін басыңыз.

   Жаңартуды орнату шеберін іске қосылады. **Жаңа нұсқаны орнату тапсырмасын таңдау** бетінде келесі түрдегі барлық қолданыстағы тапсырмалар тізімі көрсетіледі:

   - *Қажетті жаңартуларды орнату және осалдықтарды түзету*
   - *Осалдықтарды түзету*

4. Егер сіз шебердің сіз таңдаған жаңартуды орнататын тапсырмаларды ғана көрсетуін қаласаңыз, **Осы жаңа нұсқаны орнататын тапсырмаларды ғана көрсету** параметрін қосыңыз.

5. Орындағыңыз келетін әрекетті таңдаңыз:

   - Бар тапсырманы іске қосу үшін *Қажетті жаңартуларды орнату және осалдықтарды түзету* тапсырмасының жанындағы құсбелгіні қойып, **Іске қосу** түймесін басыңыз.

     Тапсырма фондық режимде орындалады. Қосымша әрекеттер қажет емес.

   - Қолданыстағы тапсырмаға жаңа ережені қосу үшін:

     a. Тапсырманың аты жанына жалаушаны қойып, **Ереже қосу** түймесін басыңыз.

     Егер сіз бірнеше тапсырма таңдаған болсаңыз, **Ереже қосу** түймесі қолжетімді емес.

     Осалдықтарды түзету тапсырмасы үшін ереже қоса алмайсыз. *Осалдықтарды түзету* тапсырмасын таңдаған болсаңыз, келесі хабарландыру пайда болады: *«Жаңартуларды орнату үшін «Қажетті жаңартуларды орнату және осалдықтарды түзету» тапсырмасын пайдаланыңыз»*.

     b. Шебердің **Жаңартуды орнату ережесін жасау** қадамында жаңа ережені конфигурациялаңыз:

     - **Осы маңыздылық деңгейінің жаңартулары үшін орнату ережесі**

       Кейде бағдарламалық жасақтама жаңартуы пайдаланушының бағдарламалық жасақтамамен жұмысын нашарлатуы мүмкін. Мұндай жағдайларда, сіз тек бағдарламалық жасақтама үшін маңызды жаңартуларды орнатып, басқа жаңартуларды өткізіп жібере аласыз.

Егер бұл параметр қосулы болса, жаңартулар тек Kaspersky орнатқан критикалық деңгейі таңдалған жаңартудың маңыздылық мәніне тең немесе одан асатын осалдықтарды ғана түзетеді (**Орташа**, **Жоғары** немесе **Критикалық**). Таңдалған мәннен төмен критикалық деңгейі бар осалдықтар түзетілмейді.

Егер бұл параметр өшірулі болса, жаңартулар олардың критикалық деңгейіне қарамастан барлық осалдықтарды түзетеді.

Әдепкі бойынша, параметр өшірулі.

Таңдалған жаңартудың маңыздылық деңгейі *Белгісіз* болса, бұл ереже көрсетілмейді.

- **MSRC бойынша осы маңыздылық деңгейінің жаңартулары үшін орнату ережесі**

  Кейде бағдарламалық жасақтама жаңартуы пайдаланушының бағдарламалық жасақтамамен жұмысын нашарлатуы мүмкін. Мұндай жағдайларда, сіз тек бағдарламалық жасақтама үшін маңызды жаңартуларды орнатып, басқа жаңартуларды өткізіп жібере аласыз.

  Егер бұл параметр қосылса (Windows Update жаңартулары үшін ғана қолжетімді), жаңартулар тек Microsoft Security Response Center (MSRC) орнатқан критикалық деңгей тізімде таңдалған мәнге тең келетін немесе одан асатын осалдықтарды ғана түзетеді (**Төмен**, **Орташа**, **Жоғары**, немесе **Критикалық**). Таңдалған мәннен төмен критикалық деңгейі бар осалдықтар түзетілмейді.

  Егер бұл параметр өшірулі болса, жаңартулар олардың критикалық деңгейіне қарамастан барлық осалдықтарды түзетеді.

  Әдепкі бойынша, параметр өшірулі.

  Бұл ереже Microsoft бағдарламалық жасақтамасының жаңартулары үшін ғана пайда болады. Таңдалған жаңартудың маңыздылық деңгейі *Белгісіз* болса, ереже көрсетілмейді.

- **Осы жеткізушінің жаңартуларын орнату ережесі**

  Бұл параметр тек үшінші тарап бағдарламаларын жаңарту үшін қолжетімді. Kaspersky Security Center Linux тек таңдалған жаңартумен бірдей өндірушінің қолданбаларына қатысты жаңартуларды орнатады. Басқа өндірушілердің қабылданбаған жаңартулары мен бағдарлама жаңартулары орнатылмайды.

  Әдепкі бойынша, параметр өшірулі.

  Бұл саясат тек үшінші тарап бағдарламалық жасақтама жаңартулары үшін пайда болады.

- **түрінің жаңартулары үшін орнату ережесі**

- **Таңдалған бағдарламаның жаңартуларын орнату ережесі**

  Бұл саясат тек үшінші тарап бағдарламалық жасақтама жаңартулары үшін пайда болады.

- **Таңдалған жаңартуды орнату ережесі**

- **Таңдалған жаңартуларды мақұлдау**

  Таңдалған жаңарту орнатуға мақұлданған. Егер жаңартуды орнатудың кейбір ережелері тек мақұлданған жаңартуларды орнатуға мүмкіндік берсе, бұл параметр қолжетімді.

  Әдепкі бойынша, параметр өшірулі.

- **Таңдалған жаңартуларды орнату үшін керек бағдарламалардың алдыңғы жаңартуларының барлығын автоматты түрде орнату**

  Таңдалған жаңартуларды орнату үшін, қажет болған жағдайда, бағдарламалардың аралық нұсқаларын орнатуға келіссеңіз, осы параметрді қосыңыз.

Егер бұл параметр өшірулі болса, бағдарламалардың тек таңдалған нұсқалары орнатылады. Бағдарламалардың нұсқаларын дәйекті түрде орнатуға тырыспай, бағдарламаларды тікелей жаңартқыңыз келсе, бұл параметрді өшіріңіз. Егер таңдалған жаңартуларды бағдарламаның алдыңғы нұсқаларын орнатпай-ақ орнату мүмкін болмаса, бағдарламаны жаңарту қатемен аяқталады.

Мысалы, сізде құрылғыда бағдарламаның 3-нұсқасы бар, оны 5-нұсқаға жаңартқыңыз келеді, бірақ 5-нұсқаны тек 4-нұсқаның үстіне орнатуға болады. Егер бұл параметр қосулы болса, алдымен бағдарламалық жасақтаманың 4-нұсқасы, содан кейін 5-нұсқасы орнатылады. Егер бұл параметр өшірулі болса, бағдарламалық жасақтаманы жаңарту сәтсіз болады.

Әдепкі бойынша, параметр қосулы.

c. **Қосу** түймесін басыңыз.

Тапсырма сипаттары терезесі ашылады. Тапсырманың сипаттарына жаңа ереже қосылды. Ережені, сондай-ақ басқа тапсырма параметрлерін көруге немесе өзгертуге болады. Өзгерістерін сақтау үшін **Сақтау** түймесін басыңыз.

- Тапсырма жасау үшін:

  a. **Жаңа тапсырма** түймесін басыңыз.

  b. Шебердің **Жаңартуды орнату ережесін жасау** қадамында жаңа ережені конфигурациялаңыз:

  - **Осы маңыздылық деңгейінің жаңартулары үшін орнату ережесі**

    Кейде бағдарламалық жасақтама жаңартуы пайдаланушының бағдарламалық жасақтамамен жұмысын нашарлатуы мүмкін. Мұндай жағдайларда, сіз тек бағдарламалық жасақтама үшін маңызды жаңартуларды орнатып, басқа жаңартуларды өткізіп жібере аласыз.

    Егер бұл параметр қосулы болса, жаңартулар тек Kaspersky орнатқан критикалық деңгейі таңдалған жаңартудың маңыздылық мәніне тең немесе одан асатын осалдықтарды ғана түзетеді (**Орташа**, **Жоғары** немесе **Критикалық**). Таңдалған мәннен төмен критикалық деңгейі бар осалдықтар түзетілмейді.

    Егер бұл параметр өшірулі болса, жаңартулар олардың критикалық деңгейіне қарамастан барлық осалдықтарды түзетеді.

    Әдепкі бойынша, параметр өшірулі.

    Таңдалған жаңартудың маңыздылық деңгейі *Белгісіз* болса, бұл ереже көрсетілмейді.

  - **MSRC бойынша осы маңыздылық деңгейінің жаңартулары үшін орнату ережесі**

    Кейде бағдарламалық жасақтама жаңартуы пайдаланушының бағдарламалық жасақтамамен жұмысын нашарлатуы мүмкін. Мұндай жағдайларда, сіз тек бағдарламалық жасақтама үшін маңызды жаңартуларды орнатып, басқа жаңартуларды өткізіп жібере аласыз.

    Егер бұл параметр қосылса (Windows Update жаңартулары үшін ғана қолжетімді), жаңартулар тек Microsoft Security Response Center (MSRC) орнатқан критикалық деңгей тізімде таңдалған мәнге тең келетін немесе одан асатын осалдықтарды ғана түзетеді (**Төмен**, **Орташа**, **Жоғары**, немесе **Критикалық**). Таңдалған мәннен төмен критикалық деңгейі бар осалдықтар түзетілмейді.

    Егер бұл параметр өшірулі болса, жаңартулар олардың критикалық деңгейіне қарамастан барлық осалдықтарды түзетеді.

    Әдепкі бойынша, параметр өшірулі.

    Бұл ереже Microsoft бағдарламалық жасақтамасының жаңартулары үшін ғана пайда болады. Таңдалған жаңартудың маңыздылық деңгейі *Белгісіз* болса, ереже көрсетілмейді.

  - **Осы жеткізушінің жаңартуларын орнату ережесі**

Бұл параметр тек үшінші тарап бағдарламаларын жаңарту үшін қолжетімді. Kaspersky Security Center Linux тек таңдалған жаңартумен бірдей өндірушінің қолданбаларына қатысты жаңартуларды орнатады. Басқа өндірушілердің қабылданбаған жаңартулары мен бағдарлама жаңартулары орнатылмайды.

Әдепкі бойынша, параметр өшірулі.

Бұл саясат тек үшінші тарап бағдарламалық жасақтама жаңартулары үшін пайда болады.

- **түрінің жаңартулары үшін орнату ережесі**
- **Таңдалған бағдарламаның жаңартуларын орнату ережесі**

  Бұл саясат тек үшінші тарап бағдарламалық жасақтама жаңартулары үшін пайда болады.

- **Таңдалған жаңартуды орнату ережесі**
- **Таңдалған жаңартуларды мақұлдау**

  Таңдалған жаңарту орнатуға мақұлданған. Егер жаңартуды орнатудың кейбір ережелері тек мақұлданған жаңартуларды орнатуға мүмкіндік берсе, бұл параметр қолжетімді.

  Әдепкі бойынша, параметр өшірулі.

- **Таңдалған жаңартуларды орнату үшін керек бағдарламалардың алдыңғы жаңартуларының барлығын автоматты түрде орнату**

  Таңдалған жаңартуларды орнату үшін, қажет болған жағдайда, бағдарламалардың аралық нұсқаларын орнатуға келіссеңіз, осы параметрді қосыңыз.

  Егер бұл параметр өшірулі болса, бағдарламалардың тек таңдалған нұсқалары орнатылады. Бағдарламалардың нұсқаларын дәйекті түрде орнатуға тырыспай, бағдарламаларды тікелей жаңартқыңыз келсе, бұл параметрді өшіріңіз. Егер таңдалған жаңартуларды бағдарламаның алдыңғы нұсқаларын орнатпай-ақ орнату мүмкін болмаса, бағдарламаны жаңарту қатемен аяқталады.

  Мысалы, сізде құрылғыда бағдарламаның 3-нұсқасы бар, оны 5-нұсқаға жаңартқыңыз келеді, бірақ 5-нұсқаны тек 4-нұсқаның үстіне орнатуға болады. Егер бұл параметр қосулы болса, алдымен бағдарламалық жасақтаманың 4-нұсқасы, содан кейін 5-нұсқасы орнатылады. Егер бұл параметр өшірулі болса, бағдарламалық жасақтаманы жаңарту сәтсіз болады.

  Әдепкі бойынша, параметр қосулы.

c. **Қосу** түймесін басыңыз.

Жаңа тапсырма жасау шеберінде тапсырманы жасауды жалғастырыңыз. Жаңартуды орнату шеберінде қосқан жаңа ереже тапсырма жасау шеберінде көрсетіледі. Шебердің жұмысы аяқталғаннан кейін, *Қажетті жаңартуларды орнату және осалдықтарды түзету* тапсырмасы тапсырмалар тізіміне қосылады.

Осалдықтарды және қажетті жаңартуларды іздеу тапсырмасы параметрлері

Осалдықтарды және қажетті жаңартуларды іздеу тапсырмасы бағдарламаны жылдам іске қосу шебері жұмыс істеп тұрған кезде автоматты түрде жасалады. Қолданбаны жылдам іске қосу шеберін іске қоспаған болсаңыз, тапсырманы қолмен жасай аласыз.

Тапсырманың жалпы параметрлерінен бөлек, *Осалдықтарды және қажетті жаңартуларды іздеу* тапсырмасын жасау кезінде немесе кейінірек, жасалған тапсырманың сипаттарын конфигурациялау кезінде келесі параметрлерді көрсете аласыз:

- **Microsoft тізіміндегі осалдықтар мен жаңартуларды іздеңіз**

  Осалдықтар мен жаңартуларды іздеу кезінде Kaspersky Security Center Linux бағдарламасы ағымдағы сәтте қолжетімді Microsoft жаңартулардың көздерінен Microsoft қолжетімді жаңартулары туралы деректерді қолданады.

  Мысалы, Microsoft жаңартулары мен өзге өнімдердің жаңартулары үшін әртүрлі параметрлері бар әртүрлі тапсырмалар болса, осы параметрді өшіруге болады.

  Әдепкі бойынша, параметр қосулы.

  Қосымша Microsoft Windows жаңартулары туралы ақпарат басқару серверіне жіберілмейді.

- **Деректерді жаңарту үшін жаңарту серверіне қосылу**

  Басқарылатын құрылғыдағы Windows Update агенті Microsoft жаңарту көзіне қосылады. Келесі қызметтер Microsoft жаңарту көздері бола алады:

  - Ұйымыңыздың желісінде орналастырылған Microsoft Windows Server Update Services (WSUS) қызметтері бар Windows Server.
  - Microsoft жаңарту серверлері.

  Егер бұл параметр қосулы болса, басқарылатын құрылғыдағы Windows Update агенті Microsoft жаңарту көзіне қосылып, Microsoft Windows қолжетімді жаңартулары туралы ақпарат алады.

  Егер бұл параметр өшірулі болса, басқарылатын құрылғыдағы Windows Update агенті бұған дейін Microsoft жаңарту көзінен алған Microsoft Windows қолжетімді жаңартулары туралы ақпаратты пайдаланады.

  Microsoft жаңарту көзіне қосылу ресурстарды қажет етуі мүмкін. Егер сіз осы жаңарту көзіне басқа тапсырмада немесе Желілік агент саясатының сипаттарында, **Бағдарламалық жасақтаманың жаңартулары мен осалдықтары** бөлімінде тұрақты қосылым орнатқан болсаңыз, бұл параметрді өшіре аласыз Егер сіз бұл параметрді өшіргіңіз келмесе, Серверге түсетін жүктемені азайту үшін тапсырмалар кестесін 360 минут аралығындағы тапсырманы іске қосу кідірісінің кездейсоқ мәнін пайдалануға болатындай конфигурациялауға болады.

  Әдепкі бойынша, параметр қосулы.

Желілік агент саясаты параметрлерінің келесі мәндерінің тіркесімі жаңартуларды алу режимін анықтайды:

- Басқарылатын құрылғыдағы Windows Update агенті жаңартуларды алу үшін жаңарту серверіне тек **Деректерді жаңарту үшін жаңарту серверіне қосылу** параметрі *Осалдықтарды және қажетті жаңартуларды іздеу* тапсырмасының сипаттарында қосылған және **Windows Update жаңартуларын іздеу режимі** параметрі желілік агент саясатының параметрлерінде **Белсенді** болып белгіленген жағдайда ғана қосылады.

- *Осалдықты сканерлеу* тапсырмасын орындаған кезде Microsoft Windows жаңарту көзіне қосылымды бастау және жаңартуларды жүктеп алу үшін Желілік агент қажет болмаса, **Windows Update жаңартуларын іздеу режимі** параметрін **Пассив** күйіне орнатуға болады, бұл арада **Деректерді жаңарту үшін жаңарту серверіне қосылу** параметрі қосулы күйде қала беруі керек. Бұл, ресурстарды үнемдеуге және осалдықтарды іздеу үшін бұрын алынған Windows жаңартуларын пайдалануға мүмкіндік береді. Microsoft Windows жаңартуларын алуды басқа тәсілмен конфигурациялаған болсаңыз, пассивті режимді пайдалануға болады. Microsoft Windows жаңартуларын басқа жолмен алу үшін конфигурацияланбасаңыз, **Windows Update жаңартуларын іздеу режимі** параметрін **Пассив** күйіне орнатпаңыз, себебі бұл жағдайда жаңартулар туралы ақпарат ешқашан алынбайды.

- **Windows Update жаңартуларын іздеу режимі** опциясы **Өшірулі** күйге орнатылса, **Деректерді жаңарту үшін жаңарту серверіне қосылу** опциясының күйіне (қосулы немесе өшірулі) қарамастан, Kaspersky Security Center Linux жаңартулар туралы ешқандай ақпаратты сұрамайды.

Ұйымыңыздың желісінде WSUS сервері (жергілікті WSUS сервері) пайдаланылса және оны Kaspersky Security Center басқару серверімен бірге пайдаланғыңыз келсе, алдымен Kaspersky Security Center басқару сервері WSUS сервері ретінде пайдаланылмайтынына көз жеткізіңіз, содан кейін келесі әрекеттерді орындаңыз:

1. Windows жүйесімен жұмыс істейтін басқарылатын құрылғыларда Windows жаңарту қызметі үшін жергілікті WSUS серверін көрсетіңіз. Мұны Windows тізілімінде қолмен немесе Windows топтық саясатын пайдалану арқылы жасауға болады.

2. Жергілікті WSUS серверінде жаңартулар үшін қажетті жіктеулерді және жаңартулар таратылатын қолданбаларды көрсетіңіз.

3. WSUS серверіңізді жоғарғы ағын серверімен синхрондаңыз (бұл Microsoft WSUS сервері немесе басқа жергілікті жоғарғы ағынның WSUS сервері болуы мүмкін).

Құрылғыда *Осалдықтарды және қажетті жаңартуларды табу* тапсырмасы іске қосылғаннан кейін, желілік агент құрылғыға қолданылатын Windows жаңартуларына сұрауды бастау үшін Windows жаңарту қызметін пайдаланады. Windows жаңарту қызметі сыртқы WSUS серверінің мекенжайын тізілімнен алады және жаңартуларды тікелей сол сыртқы WSUS серверінен іздейді. Содан кейін Windows жаңарту қызметі бұл тізімді желілік агент арқылы басқару серверіне жібереді. Осылайша басқару серверінің жаңартылған негізі болады.

- **Kaspersky ұсынған үшінші тарап осалдықтары мен жаңартуларын іздеңіз**

  Егер бұл параметр қосулы болса, Kaspersky Security Center Linux қолданбасы Windows тізімдемесінде және **Файлдық жүйеде бағдарламаларды қосымша іздеу жолдарын көрсетіңіз** бөлімінде көрсетілген қалталарда үшінші тарап өндірушілерінің қолданбалары (Kaspersky және Microsoft-тан басқа өндірушілер шығарған қолданбалар) үшін осалдықтар мен қажетті жаңартуларды іздейді. Қолдау көрсетілетін үшінші тарап бағдарламаларының толық тізімін Kaspersky бақылайды.

  Егер бұл параметр өшірулі болса, Kaspersky Security Center Linux қолданбасы үшінші тарап қолданбалары үшін осалдықтар мен қажетті жаңартуларды іздемейді. Мысалы, Microsoft Windows жаңартулары мен өзге өнімдердің жаңартулары үшін әртүрлі параметрлері бар әртүрлі тапсырмалар болса, осы параметрді өшіруге болады.

Әдепкі бойынша, параметр қосулы.

- **Файлдық жүйеде бағдарламаларды қосымша іздеу жолдарын көрсету**

  Kaspersky Security Center Linux қолданбасы осалдықтарды түзетуді және жаңартуларды орнатуды қажет ететін үшінші тарап қолданбаларын іздейтін қалталар. Жүйе айнымалыларын пайдалануға болады.

  Бағдарламалар орнатылған қалталарды көрсетіңіз. Әдепкі бойынша, тізімде көптеген бағдарламалар орнатылған жүйелік қалталар бар.

- **Кеңейтілген диагностикалау параметрін қосу**

  Бұл мүмкіндік қосылса, Kaspersky Security Center Linux қашықтан диагностикалау утилитасындағы желілік агент үшін трассирлеу файлдарын жазу өшірулі болса да, желілік агент трассирлеу файлдарын жазады. Трассалау кезекпен екі файлға жазылады; әр файлдың өлшемі **Кеңейтілген диагностикалау файлдарының ең үлкен өлшемі (МБ)** өрісінде көрсетілген мәннің жартысына тең. Екі файл да толтырылған кезде, Желілік агент деректерді үстінен жаза бастайды. Трассалау файлдары %WINDIR%\Temp қалтасында сақталады. Файлдарға қашықтан диагностикалау утилитасы арқылы қатынасуға, сондай-ақ файлдарды жүктеуге немесе жоюға болады.

  Егер бұл функция өшірілген болса, Желілік агент трассалауды Kaspersky Security Center Linux қашықтан диагностикалау утилитасының параметрлеріне сәйкес жазады. Қосымша трассалау жазылмайды.

  Тапсырма жасау кезінде кеңейтілген диагностиканы қосудың қажеті жоқ. Болашақта сізге бұл функцияны пайдалану қажет болуы мүмкін, мысалы, егер қандай да бір құрылғыда тапсырманы іске қосу сәтсіз аяқталса және келесі тапсырманы іске қосу кезінде қосымша ақпарат алу қажет болса.

  Әдепкі бойынша, параметр өшірулі.

- **Кеңейтілген диагностикалау файлдарының ең үлкен өлшемі (МБ)**

  Әдепкі бойынша, 100 МБ мәні және 1-ден 2048 МБ-қа дейінгі рұқсат етілген мәндер көрсетілген. Kaspersky Техникалық қолдау қызметі мамандары, сіз жіберген кеңейтілген диагностика файлдарында мәселені жою үшін жеткілікті ақпарат болмаса, сізден әдепкі бойынша белгіленген мәнді өзгертуді сұрауы мүмкін.

Тапсырма кестесін конфигурациялау бойынша ұсыныстар

Осалдықтарды және қажетті жаңартуларды іздеу тапсырмасын іске қосу кестесін жоспарлау кезінде, **Өткізіп алынған тапсырмаларды іске қосу** және **Тапсырманы бастау үшін автоматты түрде араластырылған кідірісті пайдалану** параметрлерінің қосулы екеніне көз жеткізіңіз.

Әдепкі бойынша *Осалдықтарды және қажетті жаңартуларды іздеу* тапсырмасы сағат 18:00:00-де қолмен іске қосылады. Егер ұйымның жұмыс регламенті осы уақытта құрылғыларды өшіруді көздесе, онда *Осалдықтарды және қажетті жаңартуларды іздеу* тапсырмасы құрылғыны қосқаннан кейін (келесі күні таңертең) іске қосылады. Мұнда жүріс-тұрыс жағымсыз болуы мүмкін, өйткені осалдықтарды іздеу құрылғының процессоры мен диск ішкі жүйесіне жоғары жүктеме түсіруі мүмкін. Ұйымда қабылданған жұмыс регламентіне сүйене отырып, тапсырманың оңтайлы кестесін конфигурациялау керек.

Осалдықтарды және қажетті жаңартуларды іздеу тапсырмасын жасау

Осалдықтарды және қажетті жаңартуларды іздеу тапсырмасының көмегімен Kaspersky Security Center Linux қолданбасы басқарылатын құрылғыларға орнатылған үшінші тарап қолданбалары үшін табылған осалдықтар мен қажетті жаңартулар тізімдерін алады.

Windows жүйесімен жұмыс істейтін құрылғылар үшін ғана *Осалдықтарды және қажетті жаңартуларды іздеу* тапсырмасын жасай аласыз. Бұл тапсырманы басқа операциялық жүйелермен жұмыс істейтін құрылғылар үшін жасай алмайсыз.

Осалдықтарды және қажетті жаңартуларды іздеу тапсырмасы бастапқы орнату шебері кезінде автоматты түрде жасалады. Бағдарламаны жылдам іске қосу шеберін іске қоспаған болсаңыз, тапсырманы қолмен жасай аласыз.

Осалдықтарды және қажетті жаңартуларды іздеу тапсырмасын жасау үшін:

1. Бағдарламаның негізгі терезесінде **Тапсырмалар** бөліміне өтіңіз.
2. **Қосу** түймесін басыңыз.

   Жаңа тапсырма жасау шебері іске қосылады. Шебердің жұмысын жалғастыру үшін **Келесі** түймесін басыңыз.
3. Kaspersky Security Center бағдарламасы үшін **Осалдықтарды және қажетті жаңартуларды іздеу** тапсырма түрін таңдаңыз.
4. Жасап жатқан тапсырманың атын көрсетіңіз. Тапсырма атауы 100 таңбадан асуы және арнайы таңбаларды ("*<>?\:|) қамтуы мүмкін емес.
5. Тапсырмалар тағайындалатын құрылғыларды таңдаңыз.
6. Жаңартуды қажет ететін осалдықтар мен қолданбаларды тексеру жолдарын көрсетіңіз:

   - **Microsoft тізіміндегі осалдықтар мен жаңартуларды іздеңіз**

     Осалдықтар мен жаңартуларды іздеу кезінде Kaspersky Security Center Linux бағдарламасы ағымдағы сәтте қолжетімді Microsoft жаңартулардың көздерінен Microsoft қолжетімді жаңартулары туралы деректерді қолданады.

     Мысалы, Microsoft жаңартулары мен өзге өнімдердің жаңартулары үшін әртүрлі параметрлері бар әртүрлі тапсырмалар болса, осы параметрді өшіруге болады.

     Әдепкі бойынша, параметр қосулы.

Қосымша Microsoft Windows жаңартулары туралы ақпарат басқару серверіне жіберілмейді.

- **Деректерді жаңарту үшін жаңарту серверіне қосылу**

  Басқарылатын құрылғыдағы Windows Update агенті Microsoft жаңарту көзіне қосылады. Келесі қызметтер Microsoft жаңарту көздері бола алады:

  - Ұйымыңыздың желісінде орналастырылған Microsoft Windows Server Update Services (WSUS) қызметтері бар Windows Server.
  - Microsoft жаңарту серверлері.

  Егер бұл параметр қосулы болса, басқарылатын құрылғыдағы Windows Update агенті Microsoft жаңарту көзіне қосылып, Microsoft Windows қолжетімді жаңартулары туралы ақпарат алады.

  Егер бұл параметр өшірулі болса, басқарылатын құрылғыдағы Windows Update агенті бұған дейін Microsoft жаңарту көзінен алған Microsoft Windows қолжетімді жаңартулары туралы ақпаратты пайдаланады.

  Microsoft жаңарту көзіне қосылу ресурстарды қажет етуі мүмкін. Егер сіз осы жаңарту көзіне басқа тапсырмада немесе Желілік агент саясатының сипаттарында, **Бағдарламалық жасақтаманың жаңартулары мен осалдықтары** бөлімінде тұрақты қосылым орнатқан болсаңыз, бұл параметрді өшіре аласыз Егер сіз бұл параметрді өшіргіңіз келмесе, Серверге түсетін жүктемені азайту үшін тапсырмалар кестесін 360 минут аралығындағы тапсырманы іске қосу кідірісінің кездейсоқ мәнін пайдалануға болатындай конфигурациялауға болады.

  Әдепкі бойынша, параметр қосулы.

  Желілік агент саясаты параметрлерінің келесі мәндерінің тіркесімі жаңартуларды алу режимін анықтайды:

  - Басқарылатын құрылғыдағы Windows Update агенті жаңартуларды алу үшін жаңарту серверіне тек **Деректерді жаңарту үшін жаңарту серверіне қосылу** параметрі *Осалдықтарды және қажетті жаңартуларды іздеу* тапсырмасының сипаттарында қосылған және **Windows Update жаңартуларын іздеу режимі** параметрі желілік агент саясатының параметрлерінде **Белсенді** болып белгіленген жағдайда ғана қосылады.
  - *Осалдықты сканерлеу* тапсырмасын орындаған кезде Microsoft Windows жаңарту көзіне қосылымды бастау және жаңартуларды жүктеп алу үшін Желілік агент қажет болмаса, **Windows Update жаңартуларын іздеу режимі** параметрін **Пассив** күйіне орнатуға болады, бұл арада **Деректерді жаңарту үшін жаңарту серверіне қосылу** параметрі қосулы күйде қала беруі керек. Бұл, ресурстарды үнемдеуге және осалдықтарды іздеу үшін бұрын алынған Windows жаңартуларын пайдалануға мүмкіндік береді. Microsoft Windows жаңартуларын алуды басқа тәсілмен конфигурациялаған болсаңыз, пассивті режимді пайдалануға болады. Microsoft Windows жаңартуларын басқа жолмен алу үшін конфигурацияланбасаңыз, **Windows Update жаңартуларын іздеу режимі** параметрін **Пассив** күйіне орнатпаңыз, себебі бұл жағдайда жаңартулар туралы ақпарат ешқашан алынбайды.
  - **Windows Update жаңартуларын іздеу режимі** опциясы **Өшірулі** күйге орнатылса, **Деректерді жаңарту үшін жаңарту серверіне қосылу** опциясының күйіне (қосулы немесе өшірулі) қарамастан, Kaspersky Security Center Linux жаңартулар туралы ешқандай ақпаратты сұрамайды.

Ұйымыңыздың желісінде WSUS сервері (жергілікті WSUS сервері) пайдаланылса және оны Kaspersky Security Center басқару серверімен бірге пайдаланғыңыз келсе, алдымен Kaspersky Security Center басқару сервері WSUS сервері ретінде пайдаланылмайтынына көз жеткізіңіз, содан кейін келесі әрекеттерді орындаңыз:

1. Windows жүйесімен жұмыс істейтін басқарылатын құрылғыларда Windows жаңарту қызметі үшін жергілікті WSUS серверін көрсетіңіз. Мұны Windows тізілімінде қолмен немесе Windows топтық саясатын пайдалану арқылы жасауға болады.

2. Жергілікті WSUS серверінде жаңартулар үшін қажетті жіктеулерді және жаңартулар таратылатын қолданбаларды көрсетіңіз.

3. WSUS серверіңізді жоғарғы ағын серверімен синхрондаңыз (бұл Microsoft WSUS сервері немесе басқа жергілікті жоғарғы ағынның WSUS сервері болуы мүмкін).

Құрылғыда *Осалдықтарды және қажетті жаңартуларды табу* тапсырмасы іске қосылғаннан кейін, желілік агент құрылғыға қолданылатын Windows жаңартуларына сұрауды бастау үшін Windows жаңарту қызметін пайдаланады. Windows жаңарту қызметі сыртқы WSUS серверінің мекенжайын тізілімнен алады және жаңартуларды тікелей сол сыртқы WSUS серверінен іздейді. Содан кейін Windows жаңарту қызметі бұл тізімді желілік агент арқылы басқару серверіне жібереді. Осылайша басқару серверінің жаңартылған негізі болады.

- **Kaspersky ұсынған үшінші тарап осалдықтары мен жаңартуларын іздеңіз**

  Егер бұл параметр қосулы болса, Kaspersky Security Center Linux қолданбасы Windows тізімдемесінде және **Файлдық жүйеде бағдарламаларды қосымша іздеу жолдарын көрсетіңіз** бөлімінде көрсетілген қалталарда үшінші тарап өндірушілерінің қолданбалары (Kaspersky және Microsoft-тан басқа өндірушілер шығарған қолданбалар) үшін осалдықтар мен қажетті жаңартуларды іздейді. Қолдау көрсетілетін үшінші тарап бағдарламаларының толық тізімін Kaspersky бақылайды.

  Егер бұл параметр өшірулі болса, Kaspersky Security Center Linux қолданбасы үшінші тарап қолданбалары үшін осалдықтар мен қажетті жаңартуларды іздемейді. Мысалы, Microsoft Windows жаңартулары мен өзге өнімдердің жаңартулары үшін әртүрлі параметрлері бар әртүрлі тапсырмалар болса, осы параметрді өшіруге болады.

  Әдепкі бойынша, параметр қосулы.

Тапсырма сипаттары терезесіндегі **Бағдарлама параметрлері** қойындысында тапсырма жасағаннан кейін бұл параметрлерді өшіруге болады.

7. **Файлдық жүйеде бағдарламаларды қосымша іздеу жолдарын көрсету**

   Kaspersky Security Center Linux қолданбасы осалдықтарды түзетуді және жаңартуларды орнатуды қажет ететін үшінші тарап қолданбаларын іздейтін қалталар. Жүйе айнымалыларын пайдалануға болады.

   Бағдарламалар орнатылған қалталарды көрсетіңіз. Әдепкі бойынша, тізімде көптеген бағдарламалар орнатылған жүйелік қалталар бар.

   Тапсырма сипаттары терезесіндегі **Бағдарлама параметрлері** қойындысында тапсырманы жасағаннан кейін көрсетілген жолдарды өзгертуге болады.

8. **Кеңейтілген диагностикалау параметрін қосу** керек болса

   Бұл мүмкіндік қосылса, Kaspersky Security Center Linux қашықтан диагностикалау утилитасындағы желілік агент үшін трассирлеу файлдарын жазу өшірулі болса да, желілік агент трассирлеу файлдарын жазады. Трассалау кезекпен екі файлға жазылады; әр файлдың өлшемі **Кеңейтілген диагностикалау файлдарының ең үлкен өлшемі (МБ)** өрісінде көрсетілген мәннің жартысына тең. Екі файл да толтырылған кезде, Желілік агент деректерді үстінен жаза бастайды. Трассалау файлдары %WINDIR%\Temp қалтасында сақталады. Файлдарға қашықтан диагностикалау утилитасы арқылы қатынасуға, сондай-ақ файлдарды жүктеуге немесе жоюға болады.

   Егер бұл функция өшірілген болса, Желілік агент трассалауды Kaspersky Security Center Linux қашықтан диагностикалау утилитасының параметрлеріне сәйкес жазады. Қосымша трассалау жазылмайды.

   Тапсырма жасау кезінде кеңейтілген диагностиканы қосудың қажеті жоқ. Болашақта сізге бұл функцияны пайдалану қажет болуы мүмкін, мысалы, егер қандай да бір құрылғыда тапсырманы іске қосу сәтсіз аяқталса және келесі тапсырманы іске қосу кезінде қосымша ақпарат алу қажет болса.

   Әдепкі бойынша, параметр өшірулі.

   Тапсырма сипаттары терезесіндегі **Бағдарлама параметрлері** қойындысында тапсырма жасағаннан кейін бұл параметрді өшіруге болады.

9. **Кеңейтілген диагностикалау файлдарының ең үлкен өлшемі (МБ)** көрсетіңіз.

   Әдепкі бойынша, 100 МБ мәні және 1-ден 2048 МБ-қа дейінгі рұқсат етілген мәндер көрсетілген. Kaspersky Техникалық қолдау қызметі мамандары, сіз жіберген кеңейтілген диагностика файлдарында мәселені жою үшін жеткілікті ақпарат болмаса, сізден әдепкі бойынша белгіленген мәнді өзгертуді сұрауы мүмкін.

   Алдыңғы қадамда кеңейтілген диагностиканы қосқан болсаңыз, бұл мәнді көрсетуіңіз керек. Тапсырма сипаттары терезесіндегі **Бағдарлама параметрлері** қойындысында тапсырманы жасағаннан кейін бұл мәнді өзгертуге болады.

10. **Жасап болған соң, тапсырма туралы мәліметтерді ашу** бетінде **Тапсырманы жасауды аяқтау** параметрін қоссаңыз, әдепкі бойынша белгіленген тапсырма параметрлері мәндерін өзгерте аласыз. Егер сіз бұл параметрді қоспасаңыз, тапсырма әдепкі бойынша белгіленген параметр мәндерімен жасалады. Әдепкі бойынша параметр мәндерін кейінірек кез келген уақытта өзгертуге болады.

11. **Аяқтау** түймесін басыңыз.

    Шебер жұмысының нәтижесінде тапсырма жасалды. **Жасап болған соң, тапсырма туралы мәліметтерді ашу** параметрі қосулы болса, тапсырма параметрлерінің терезесі автоматты түрде ашылады. Бұл терезеде тапсырманың жалпы параметрлерін көрсетуге және қажет болса, тапсырма жасаған кезде көрсетілген параметрлерді өзгертуге болады.

    > Тапсырмалар тізіміндегі жасалған тапсырма атауын басу арқылы тапсырма сипаттарының терезесін ашуға да болады.

Тапсырма жасалды және конфигурацияланды. Тапсырманы іске қосу үшін тапсырмалар тізімінен тапсырманы таңдап, **Іске қосу** түймесін басыңыз.

Тапсырма кестесін конфигурациялау бойынша ұсыныстар

Осалдықтарды және қажетті жаңартуларды іздеу тапсырмасын іске қосу кестесін жоспарлау кезінде, **Өткізіп алынған тапсырмаларды іске қосу** және **Тапсырманы бастау үшін автоматты түрде араластырылған кідірісті пайдалану** параметрлерінің қосулы екеніне көз жеткізіңіз.

Әдепкі бойынша *Осалдықтарды және қажетті жаңартуларды іздеу* тапсырмасы сағат 18:00:00-де қолмен іске қосылады.

Сондай-ақ, *Осалдықтарды және қажетті жаңартуларды іздеу* тапсырмасын белгілі бір уақытта іске қосу үшін конфигурациялауға болады. Мысалы, тапсырма сипаттары терезесінің **Кесте** қойындысындағы **Тапсырманы бастау** ашылмалы тізімінен **N сағат сайын** кестесі бойынша іске қосуды таңдауға болады. Егер ұйым жұмысының регламенті осы уақытта құрылғыларды сөндіруді қарастырса, онда *Осалдықтарды және қажетті жаңартуларды іздеу* тапсырмасы құрылғыны қосқаннан кейін іске қосылады. Мұнда жүріс-тұрыс жағымсыз болуы мүмкін, өйткені осалдықтарды іздеу құрылғының процессоры мен диск ішкі жүйесіне жоғары жүктеме түсіруі мүмкін. Ұйымда қабылданған жұмыс регламентіне сүйене отырып, тапсырманың оңтайлы кестесін конфигурациялау керек.

Кесте бойынша іске қосу параметрлерінің толық сипаттамасын тапсырманың жалпы параметрлерінен қараңыз.

Үшінші тарап бағдарламаларының қолжетімді жаңартулары туралы ақпаратты қарау

Клиент құрылғыларында орнатылған Microsoft бағдарламалық жасақтамасын қоса, үшінші тарап бағдарламалары үшін қолжетімді жаңартулар тізімін көруге болады.

Клиент құрылғыларында орнатылған үшінші тарап қолданбалары үшін қолжетімді жаңартулар тізімін көру үшін,

Бағдарламаның негізгі терезесінде **Бағдарламалық жасақтаманы басқару** → **Патчтарды басқару** → **Бағдарламалық жасақтама жаңартулары** бөліміне өтіңіз.

Қолжетімді жаңартулар тізімі көрсетіледі.

Бағдарлама жаңартулары тізімін қарау үшін сүзгіні көрсете аласыз. **Сүзгі** белгішесін басыңыз (⚙) сүзгіні басқаруға арналған қолданба жаңартуларының тізімінде. Сонымен қатар, қолданбалардың осалдықтары тізімінің үстіндегі **Алдын ала орнатылған сүзгілер** ашылмалы тізімінде алдын ала орнатылған сүзгілердің бірін таңдай аласыз.

Жаңарту сипаттарын көру үшін:

1. Қажетті бағдарламалық жасақтама жаңартуының атын түртіңіз.
2. Қойындылар бойынша топтастырылған келесі ақпаратты көрсететін жаңарту сипаттары терезесі ашылады:
   - **Жалпы**

     Бұл қойынды таңдалған жаңарту туралы жалпы мәліметтерді көрсетеді:

     - Жаңартуды мақұлдау күйі (ашылмалы тізімнен жаңа күйді таңдау арқылы қолмен өзгертуге болады).
     - Жаңартуды тіркеу күні мен уақыты.
     - Жаңартудың жасалған күні мен уақыты.
     - Жаңартудың маңыздылық деңгейі.
     - Жаңартуға қойылатын орнату талаптары.

- Жаңарту кіретін бағдарламалар тобы.
- Жаңарту қолданылатын бағдарлама.
- Жаңартудың нұсқасының нөмірі.

- **Атрибуттар**

  Бұл қойынды таңдалған жаңарту туралы қосымша ақпарат алу үшін пайдалануға болатын атрибуттар жиынтығын көрсетеді. Бұл жиынтық жаңартуды кім шығарғанына байланысты өзгереді: Microsoft немесе үшінші тарап өндірушісі.

  Қойынды Microsoft жаңартуы туралы келесі ақпаратты көрсетеді:

  - Microsoft Security Response Center (MSRC) талаптарына сәйкес жаңарту маңыздылығы деңгейі.
  - Жаңартуды сипаттайтын Microsoft білім базасындағы мақалаға сілтеме.
  - Жаңартуды сипаттайтын Microsoft Security Bulletin бюллетеніндегі мақалаға сілтеме.
  - Жаңарту идентификаторы (ID).

  Қойынды үшінші тарап өндірушісін жаңарту үшін келесі ақпаратты көрсетеді:

  - Жаңарту патч немесе толық дистрибутив болып табылады ма.
  - Жаңартудың локализация тілі.
  - Жаңарту автоматты түрде немесе қолмен орнатылады ма.
  - Жаңарту қолданылғаннан кейін кері қайтарып алынды ма.
  - Жаңартуды жүктеп алу сілтемесі.

- **Құрылғылар**

  Бұл қойынды таңдалған жаңарту орнатылған құрылғылардың тізімін көрсетеді.

- **Жабылатын осалдықтар**

  Бұл қойынды таңдалған жаңарту түзете алатын осалдықтардың тізімін көрсетеді.

- **Жаңартулардың қиылысу**

  Бұл қойындыда, бір бағдарлама үшін жарияланған түрлі жаңартулар арасындағы ықтимал қиылысулар көрсетіледі, яғни таңдалған жаңарту басқа жаңартуларды алмастыра алады ма немесе, керісінше, оны басқа жаңартулармен алмастыруға болады ма (Microsoft жаңартулары үшін ғана қолжетімді).

- **Жаңартуды орнату тапсырмалары**

  Бұл қойынды таңдалған жаңартуды орнатуды қамтитын тапсырмалар тізімін көрсетеді. Қойындыда жаңартуды қашықтан орнату тапсырмасын да жасауға болады.

Жаңартуды орнату статистикасын көру үшін:

1. Қажетті жаңартудың жанына жалаушаны қойыңыз.

2. **Жаңартуды орнату күйлерінің статистикасы** түймесін басыңыз.

   Диаграмма жаңарту күйлері туралы ақпаратты көрсетеді. Күйді басқан кезде, таңдалған күйі бар құрылғылар тізімі ашылады.

Сіз үшінші тарап бағдарламалары, соның ішінде таңдалған Windows басқарылатын құрылғысында орнатылған Microsoft бағдарламалық жасақтамасы үшін қолжетімді жаңартулар туралы ақпаратты көре аласыз.

Таңдалған басқарылатын құрылғы орнатылған үшінші тарап қолданбалары үшін қолжетімді жаңартулар тізімін көру үшін:

1. Бағдарламаның негізгі терезесінде **Активтерді басқару** → **Активтер (құрылғылар)** бөліміне өтіңіз.

   Басқарылатын құрылғылардың тізімі көрсетіледі.

2. Басқарылатын құрылғылар тізімінде үшінші тарап бағдарламаларының жаңартуларын көргіңіз келетін құрылғының атауы бар сілтемеден өтіңіз.

   Таңдалған құрылғы сипаттары терезесі ашылады.

3. Таңдалған құрылғы сипаттары терезесінде **Кеңейтілген** қойындысын таңдаңыз.

4. Сол жақ тақтадан **Қолжетімді жаңартулар** бөлімін таңдаңыз. Тек орнатылған жаңартуларды қарағыңыз келсе, **Орнатылған жаңартуларды көрсету** параметрін қосыңыз.

Таңдалған құрылғы үшін қолжетімді үшінші тарап бағдарламалық жасақтамасы жаңартуларының тізімі көрсетіледі.

Қолжетімді жаңартулар тізімін файлға экспорттау

Microsoft қолданбасын қоса, үшінші тарап қолданбалары үшін жаңартулар тізімін CSV немесе TXT пішіміндегі файлға экспорттауға болады. Сіз бұл файлдарды, мысалы, ақпараттық қауіпсіздік жөніндегі басшыңызға жіберу немесе статистика мақсатында сақтау үшін пайдалана аласыз.

Үшінші тарап бағдарламалары үшін қолжетімді жаңартулар тізімін барлық басқарылатын құрылғыларда орнатылған мәтіндік файлға экспорттау үшін:

1. Бағдарламаның негізгі терезесінде **Операциялар** → **Патчтарды басқару** → **Бағдарламалық жасақтама жаңартулары** бөліміне өтіңіз.

   Қолжетімді жаңартулар тізімі көрсетіледі.

   Қолданба жаңартуларының толық тізімін экспорттау кезінде тек ағымдағы бетте көрсетілетін жаңартулар экспортталады.

Белгілі бір жаңартуларды ғана экспорттағыңыз келсе, тізімдегі қажетті жаңартулардың жанындағы құсбелгілерді қойыңыз.

2. Экспорттағыңыз келетін пішімге байланысты, **TXT файлына экспорттау** немесе **CSV файлына экспорттау** түймесін басыңыз. Осы түймелердің біреуі көрінбесе, көп нүктелі түймені басып, ашылмалы тізімнен қажетті нұсқаны таңдаңыз.

Үшінші тарап қолданбалары, соның ішінде Microsoft қолданбалары үшін қолжетімді жаңартулар тізімі бар файл ағымдағы құрылғыңызға жүктеледі.

Үшінші тарап бағдарламалары үшін қолжетімді жаңартулар тізімін таңдалған басқарылатын құрылғыда орнатылған мәтіндік файлға экспорттау үшін:

1. Таңдалған басқарылатын құрылғыда қолжетімді үшінші тарап бағдарламалық жасақтама жаңартуларының тізімін ашыңыз.

   Қолжетімді жаңартулар тізімі көрсетіледі.

   Қолданба жаңартуларының толық тізімін экспорттау кезінде тек ағымдағы бетте көрсетілетін жаңартулар экспортталады.

   Белгілі бір жаңартуларды ғана экспорттағыңыз келсе, тізімдегі қажетті жаңартулардың жанындағы құсбелгілерді қойыңыз.

   Егер сіз тек орнатылған жаңартуларды экспорттағыңыз келсе, **Орнатылған жаңартуларды көрсету** жалаушасын қойыңыз.

2. Экспорттағыңыз келетін пішімге байланысты, **TXT файлына экспорттау** немесе **CSV файлына экспорттау** түймесін басыңыз. Осы түймелердің біреуі көрінбесе, көп нүктелі түймені басып, ашылмалы тізімнен қажетті нұсқаны таңдаңыз.

Таңдалған басқарылатын құрылғыларда орнатылған Microsoft қолданбаларын қоса, үшінші тарап қолданбалары үшін қолжетімді жаңартулар тізімі бар файл ағымдағы құрылғыңызға жүктеледі.

Үшінші тарап бағдарламаларының жаңартуларын мақұлдау және қабылдамау

Қажетті жаңартуларды орнату және осалдықтарды түзету тапсырмасын конфигурациялау кезінде, сіз орнату үшін орнатылатын жаңартулар белгілі бір күйге ие болуы керек ереже жасай аласыз. Мысалы, жаңарту ережесі келесілерді орнатуға мүмкіндік береді:

- тек мақұлданған жаңартулар;
- тек мақұлданған жаңартулар мен белгісіз жаңартулар;
- жаңарту күйіне қарамастан барлық жаңартулар.

Орнату қажет болған жаңартуларды растай аласыз немесе орнатылмауы тиісті жаңартулардан бас тарта аласыз.

Жаңартуларды орнатуды басқарған кезде, аздаған жаңартулар үшін *Расталды* күйін қолданған жөн. Бірнеше жаңарту орнату үшін, *Қажетті жаңартуларды орнату және осалдықтарды түзету* тапсырмасының сипаттарында конфигурациялауға болатын ережелерді қолданыңыз. *Расталды* күйін, ережелерде көрсетілген өлшемшарттарға сай келмейтін жаңартулар үшін ғана белгілеу ұсынылады. Жаңартулардың көп санын қолмен мақұлдасаңыз, Басқару серверінің өнімділігі төмендеп, бұл Басқару серверінің артық жүктелуіне әкелуі мүмкін.

Бір немесе бірнеше жаңартуды растау немесе болдырмау үшін:

1. Бағдарламаның негізгі терезесінде **Бағдарламалық жасақтаманы басқару → Патчтарды басқару → Бағдарламалық жасақтама жаңартулары** бөліміне өтіңіз.

   Қолжетімді жаңартулар тізімі көрсетіледі.

2. Растау немесе қабылдамау қажет болған жаңартуларды таңдаңыз.

3. Таңдалған жаңартуды мақұлдау үшін **Бекіту** түймесін басыңыз немесе таңдалған жаңартуды қабылдамау үшін **Қабылдамау** түймесін басыңыз. Осы түймелердің біреуі көрінбесе, көп нүктелі түймені басып, ашылмалы тізімнен қажетті нұсқаны таңдаңыз.

   Әдепкі жаңарту күйі *Анықталмаған*.

Таңдалған жаңартуларда сіз көрсеткен күйлер бар.

Сондай-ақ, қажетті жаңарту сипаттарындағы күйді өзгертуге болады.

Жаңартуды мақұлдау немесе қабылдамау үшін:

1. Бағдарламаның негізгі терезесінде **Бағдарламалық жасақтаманы басқару → Патчтарды басқару → Бағдарламалық жасақтама жаңартулары** бөліміне өтіңіз.

   Қолжетімді жаңартулар тізімі көрсетіледі.

2. Мақұлдау немесе қабылдамау қажет жаңартуды таңдаңыз.

   Жаңарту сипаттары терезесі ашылады.

3. **Жалпы** бөлімінде **Жаңартуды растау күйі** ашылмалы тізімінен жаңарту күйін таңдаңыз. *Расталды*, *Қабылданбады* немесе *Анықталмаған* күйін таңдауға болады.

4. Өзгерістерін сақтау үшін **Сақтау** түймесін басыңыз.

Таңдалған жаңартуларда сіз көрсеткен күйлер бар.

Үшінші тарап бағдарламалық жасақтамасының жаңартулары үшін *Қабылданбады* күйін белгілеп жатсаңыз, бұл жаңартулар орнатылуы жоспарланған, бірақ әлі орнатылмаған құрылғыларға орнатылмайды. Жаңартулар әлдеқашан орнатылған құрылғыларда қала береді. Қажет болса, оларды жергілікті түрде қолмен жоюға болады.

Қажетті жаңартуларды орнату және осалдықтарды түзету тапсырмасын жасау

Қажетті жаңартуларды орнату және осалдықтарды түзету тапсырмасы, Осалдықтар мен патчтарды басқару лицензия болған кезде қолжетімді.

Қажетті жаңартуларды орнату және осалдықтарды түзету тапсырмасы басқарылатын құрылғыларда орнатылған үшінші тарап қолданбаларындағы осалдықтарды жаңарту және түзету үшін пайдаланылады. Бұл тапсырма тапсырма параметрлерінде көрсетілген ережелерге сәйкес бірнеше жаңартуларды орнатуға және бірнеше осалдықтарды түзетуге мүмкіндік береді.

Қажетті жаңартуларды орнату және осалдықтарды түзету тапсырмасының көмегімен жаңартуларды орнату немесе осалдықтарды түзету үшін, сіз келесі әрекеттердің бірін орындай аласыз:

- Жаңартуды орнату шеберін немесе осалдықтарды түзету шеберін іске қосыңыз.
- *Қажетті жаңартуларды орнату және осалдықтарды түзету* тапсырмасын жасаңыз.
- Қолданыстағы *Қажетті жаңартуларды орнату және осалдықтарды түзету* тапсырмасына жаңартуды орнату ережесін қосыңыз.

Қажетті жаңартуларды орнату және осалдықтарды түзету тапсырмасын жасау үшін:

1. Бағдарламаның негізгі терезесінде **Тапсырмалар** бөліміне өтіңіз.
2. **Қосу** түймесін басыңыз.

   Жаңа тапсырма жасау шебері іске қосылады. Шебердің жұмысын жалғастыру үшін **Келесі** түймесін басыңыз.
3. **Бағдарлама** ашылмалы тізімінде Kaspersky Security Center Linux опциясын таңдаңыз.
4. **Тапсырма түрі** тізімінде **Қажетті жаңартуларды орнату және осалдықтарды түзету** тапсырма түрін таңдаңыз.

   Тапсырма көрсетілмесе, тіркелгіңізде **Жүйені басқару**: **Осалдықтар мен патчтарды басқару** функционалды аймағына арналған **Оқу**, **жазу** және **орындау** құқықтары бар екенін тексеріңіз. Сіз осы қатынас құқықтарынсыз *Қажетті жаңартуларды орнату және осалдықтарды түзету* тапсырмасын жасай алмайсыз және конфигурациялай алмайсыз.
5. **Тапсырманың атауы** өрісіне жаңа тапсырманың атын енгізіңіз.

   Тапсырма атауы 100 таңбадан асуы және арнайы таңбаларды ("*<>?\:|) қамтуы мүмкін емес.
6. Тапсырмалар тағайындалатын құрылғыларды таңдаңыз.
7. Шебердің **Жаңа нұсқаларды орнатуға арналған ережелерді көрсетіңіз** қадамында жаңартуды орнату ережелерін қосыңыз.

   Бұл ережелер клиент құрылғыларына жаңартуларды орнату кезінде қолданылады. Егер ережелер көрсетілмесе, тапсырма орындалмайды. Ережелермен жұмыс істеу туралы қосымша ақпаратты Жаңартуларды орнату ережелері бөлімінен қараңыз.

   Бұл ережелер клиент құрылғыларына жаңартуларды орнатуға қолданылады. Ешбір ережені көрсетпесеңіз, тапсырма орындалмайды.
8. Келесі параметрлерді белгілеңіз:

   - **Орнатуды құрылғыны қайта жүктеу немесе өшіру сәтінде бастау**

     Егер жалауша қойылса, құрылғыны қайта іске қоспас немесе өшірмес бұрын жаңартуды орнату орындалады. Әйтпесе, жаңартуларды орнату кесте бойынша жүзеге асырылады.

     Жаңартуларды орнату құрылғылардың жұмысына әсер етуі мүмкін болса, осы жалаушаны қойыңыз.

     Әдепкі бойынша, параметр өшірулі.

   - **Қажетті жалпы жүйелік құрамдастарды орнату**

     Егер жалауша қойылса, жаңартуды орнатпас бұрын, бағдарлама автоматты түрде осы жаңартуды орнатуға қажетті барлық жалпыжүйелік құрамдастарды (алғышарттар) орнатады. Мысалы, мұндай алғышарттар операциялық жүйенің жаңартулары болуы мүмкін.

Егер бұл параметр өшірулі болса, алғышарттарды қолмен орнату керек.

Әдепкі бойынша, параметр өшірулі.

- **Жаңартулар кезінде бағдарламаның жаңа нұсқаларын орнатуға рұқсат ету**

  Бұл опция қосылған болса, бағдарламалық жасақтама қолданбасының жаңа нұсқасын орнатуға әкелсе, жаңартуларға рұқсат беріледі.

  Бұл параметр өшірулі болса, бағдарлама жаңартылмайды. Бағдарламалардың жаңа нұсқаларын кейінірек қолмен немесе басқа тапсырманы қолдана отырып, орнатуға болады. Мысалы, егер сіздің компанияңыздың инфрақұрылымы бағдарламаның жаңа нұсқасын қолдамаса немесе сынақ инфрақұрылымындағы жаңартуды тексеру қажет болса, бұл параметрді пайдалануға болады.

  Әдепкі бойынша, параметр қосулы.

  > Бағдарламаның жаңа нұсқасын орнатқаннан кейін, клиент құрылғыларында орнатылған және жаңартылатын бағдарламаның жұмысына байланысты басқа бағдарламалардың жұмысы бұзылуы мүмкін.

- **Жаңартуларды құрылғыға орнатпастан жүктеп алу**

  Егер жалауша қойылса, бағдарлама жаңартуларды құрылғыға жүктейді, бірақ оларды автоматты түрде орнатпайды. Содан кейін, жүктелген жаңартуларды қолмен орнатуға болады.

  Microsoft жаңартулары Windows қызметтік қалтасына жүктеледі. Үшінші тарап бағдарламаларының жаңартулары (Kaspersky мен Microsoft корпорациясынан басқа өндірушілер шығарған бағдарламалар) **Жаңартуларды келесі жерге жүктеп алу** өрісінде көрсетілген қалтаға жүктеледі.

  Егер бұл параметр өшірулі болса, жаңартулар құрылғыға автоматты түрде орнатылады.

  Әдепкі бойынша, параметр өшірулі.

  - **Жаңартуларды келесі жерге жүктеп алу**

    Бұл қалта, үшінші тарап бағдарламаларының (Kaspersky мен Microsoft корпорациясынан басқа өндірушілер шығарған бағдарламалар) жаңартуларын жүктеу үшін қолданылады.

- **Кеңейтілген диагностикалау параметрін қосу**

  Бұл мүмкіндік қосылса, Kaspersky Security Center Linux қашықтан диагностикалау утилитасындағы желілік агент үшін трассирлеу файлдарын жазу өшірулі болса да, желілік агент трассирлеу файлдарын жазады. Трассалау кезекпен екі файлға жазылады; әр файлдың өлшемі **Кеңейтілген диагностикалау файлдарының ең үлкен өлшемі (МБ)** өрісінде көрсетілген мәннің жартысына тең. Екі файл да толтырылған кезде, Желілік агент деректерді үстінен жаза бастайды. Трассалау файлдары %WINDIR%\Temp қалтасында сақталады. Файлдарға қашықтан диагностикалау утилитасы арқылы қатынасуға, сондай-ақ файлдарды жүктеуге немесе жоюға болады.

  Егер бұл функция өшірілген болса, Желілік агент трассалауды Kaspersky Security Center Linux қашықтан диагностикалау утилитасының параметрлеріне сәйкес жазады. Қосымша трассалау жазылмайды.

  Тапсырма жасау кезінде кеңейтілген диагностиканы қосудың қажеті жоқ. Болашақта сізге бұл функцияны пайдалану қажет болуы мүмкін, мысалы, егер қандай да бір құрылғыда тапсырманы іске қосу сәтсіз аяқталса және келесі тапсырманы іске қосу кезінде қосымша ақпарат алу қажет болса.

  Әдепкі бойынша, параметр өшірулі.

  - **Кеңейтілген диагностикалау файлдарының ең үлкен өлшемі (МБ)**

    Әдепкі бойынша, 100 МБ мәні және 1-ден 2048 МБ-қа дейінгі рұқсат етілген мәндер көрсетілген. Kaspersky Техникалық қолдау қызметі мамандары, сіз жіберген кеңейтілген диагностика файлдарында мәселені жою үшін жеткілікті ақпарат болмаса, сізден әдепкі бойынша белгіленген мәнді өзгертуді сұрауы мүмкін.

Шебердің келесі қадамына өтіңіз.

9. Операциялық жүйені қайта іске қосу параметрлерін көрсетіңіз:

   - **Құрылғыны қайта іске қоспау**

     Операция аяқталғаннан кейін, клиент құрылғылары автоматты түрде қайта жүктелмейді. Операцияны аяқтау үшін құрылғыны қайта қосу қажет (мысалы, қолмен немесе құрылғыны басқару тапсырмасы арқылы). Қайта жүктеу қажеттілігі туралы ақпарат тапсырманы орындау нәтижелерінде және құрылғы күйінде сақталады. Бұл нұсқа, үздіксіз жұмыс өте маңызды болып саналатын серверлердегі және басқа құрылғылардағы тапсырмалар үшін жарамды.

   - **Құрылғыны қайта іске қосу**

     Бұл жағдайда, операцияны аяқтау үшін қайта жүктеу қажет болса, қайта жүктеу әрқашан автоматты түрде орындалады. Бұл нұсқа, мезгіл-мезгіл үзілістерге (өшіру, қайта жүктеу) рұқсат етілген құрылғылардағы тапсырмалар үшін жарамды.

   - **Пайдаланушыдан әрекетті орындауды сұрау**

     Клиент құрылғысының экранында құрылғыны қолмен қайта жүктеу керек деген хабар пайда болады. Бұл нұсқа үшін қосымша параметрлерді конфигурациялауға болады: пайдаланушыға арналған хабар мәтіні, хабардың жиілігі, сондай-ақ қайта жүктеу мәжбүрлі түрде орындалатын уақыт (пайдаланушының растауынсыз). Бұл нұсқа жұмыс станциялары үшін оңтайлы болып табылады, сондықтан пайдаланушылар қайта жүктеудің ең қолайлы уақытын таңдай алады.

     Әдепкі бойынша, осы нұсқа таңдалған.

   - **Сұрауды қайталау жиілігі (мин)**

     Егер бұл нұсқа таңдалса, белгілі бір жиіліктегі бағдарлама пайдаланушыға операциялық жүйені қайта жүктеуді ұсынады.

     Әдепкі бойынша, параметр қосулы. Әдепкі бойынша аралық 5 минутты құрайды. Рұқсат етілген мәндер: 1-ден 1440 минутқа дейін.

     Егер параметр өшірулі болса, қайта жүктеу ұсынысы тек бір рет көрсетіледі.

   - **Келесі уақыттан кейін қайта іске қосу (мин)**

     Пайдаланушыға операциялық жүйені қайта жүктеуді ұсынғаннан кейін, бағдарлама көрсетілген уақыттан кейін мәжбүрлеп қайта жүктеуді орындайды.

     Әдепкі бойынша, параметр қосулы. Әдепкі бойынша уақыт аралығы 30 минутты құрайды. Рұқсат етілген мәндер: 1-ден 1440 минутқа дейін.

   - **Бұғатталған сеанстарда бағдарламаларды келесі уақыттан кейін мәжбүрлеп жабу (мин)**

     Пайдаланушының құрылғысы бұғатталған кезде бағдарламаларды мәжбүрлеп аяқтау (белсенді емес кезеңнен кейін автоматты түрде немесе қолмен).

     Егер параметр қосулы болса, бұғатталған құрылғыдағы бағдарламалардың жұмысы енгізу өрісінде көрсетілген уақыт өткеннен кейін тоқтатылады.

     Егер параметр өшірулі болса, бұғатталған құрылғыдағы бағдарламалардың жұмысы тоқтамайды.

     Әдепкі бойынша, параметр өшірулі.

10. **Тапсырманы жасауды аяқтау** қадамында **Жасап болған соң, тапсырма туралы мәліметтерді ашу** параметрін қоссаңыз, тапсырма параметрлерінің орнатылған әдепкі мәндерін өзгертуге болады.

    Егер сіз бұл параметрді қоспасаңыз, тапсырма әдепкі бойынша белгіленген параметр мәндерімен жасалады. Орнатылған әдепкі параметрлер мәндерін кейінірек өзгертуге болады.

11. **Аяқтау** түймесін басыңыз.

    Шебер жұмысының нәтижесінде Жаңа тапсырма жасау шебері. **Жасап болған соң, тапсырма туралы мәліметтерді ашу** параметрі қосулы болса, тапсырма параметрлерінің терезесі автоматты түрде ашылады. Бұл терезеде тапсырманың жалпы параметрлерін көрсетуге және қажет болса, тапсырма жасаған кезде көрсетілген параметрлерді өзгертуге болады.

    > Тапсырмалар тізіміндегі жасалған тапсырма атауын басу арқылы тапсырма сипаттарының терезесін ашуға да болады.

    Тапсырма жасалып, орнатылып, тапсырмалар тізімінде көрсетіледі.

12. Тапсырманы іске қосу үшін тапсырмалар тізімінен тапсырманы таңдап, **Іске қосу** түймесін басыңыз.

    Сондай-ақ тапсырма сипаттары терезесіндегі **Кесте** қойындысында тапсырманы іске қосу кестесін жасауға да болады.

    Кесте бойынша іске қосу параметрлерінің толық сипаттамасын тапсырманың жалпы параметрлерінен қараңыз.

Тапсырманы орындағаннан кейін қажетті жаңартулар орнатылып, осалдықтар түзетілді.

Ұйымыңыздың желісінде WSUS сервері (жергілікті WSUS сервері) пайдаланылса және оны Басқару серверімен бірге пайдаланғыңыз келсе, алдымен Басқару сервері WSUS сервері ретінде пайдаланылмайтынына көз жеткізіңіз, содан кейін келесі әрекеттерді орындаңыз:

a. Windows жүйесімен жұмыс істейтін басқарылатын құрылғыларда Windows жаңарту қызметі үшін жергілікті WSUS серверін көрсетіңіз. Мұны Windows тізілімінде қолмен немесе Windows топтық саясатын пайдалану арқылы жасауға болады.

b. Жергілікті WSUS серверінде жаңартулар үшін қажетті жіктеулерді және жаңартулар таратылатын қолданбаларды көрсетіңіз.

c. WSUS серверіңізді жоғарғы ағын серверімен синхрондаңыз (бұл Microsoft WSUS сервері немесе басқа жергілікті жоғарғы ағынның WSUS сервері болуы мүмкін).

Құрылғыда *Қажетті жаңартуларды орнату және осалдықтарды түзету* тапсырмасы іске қосылғаннан кейін, желілік агент Windows жаңартуларын орнату үшін Windows жаңарту қызметін пайдаланады. Windows жаңарту қызметі тізілімнен сыртқы WSUS серверінің мекенжайын алады және жаңартуларды сол сыртқы серверден тікелей жүктеп алады.

Жаңартуларды орнату үшін ережелер қосу

> Бұл функционалдық, Осалдықтар мен патчтарды басқаруға арналған лицензия болған кезде қолжетімді.

Бағдарламалық жасақтама жаңартуларын орнату немесе *Қажетті жаңартуларды орнату және осалдықтарды түзету* тапсырмасын қолдана отырып, бағдарламалардағы осалдықтарды түзету кезінде жаңартуларды орнату ережелерін көрсету қажет. Бұл ережелер орнатылатын жаңартуларды және түзетілетін осалдықтарды анықтайды.

Нақты параметрлер барлық Windows Update жаңартулары үшін немесе үшінші тарап қолданбалық жасақтамасының жаңартулары үшін ереже қосатыныңызға байланысты (яғни Kaspersky немесе Microsoft шығармаған қолданбалар). Windows Update жаңартулары немесе үшінші тарап қолданбаларының жаңартулары үшін ереже қосқанда, жаңартуларды орнатқыңыз келетін қолданбалар мен қолданбалардың нұсқаларын таңдауға болады. Барлық жаңартулар үшін ереже қосқанда, сіз орнатылатын жаңартуларды және жаңартуларды орнату арқылы түзеткіңіз келетін осалдықтарды таңдай аласыз.

Жаңартуларды орнату ережесін келесі жолдармен қосуға болады:

- Қажетті жаңартуларды орнату және осалдықтарды түзету кезінде ереже қосу.
- Әрекеттегі *Қажетті жаңартуларды орнату және осалдықтарды түзету* тапсырманың сипаттар терезесінің **Бағдарлама параметрлері** қойындысына ереже қосу.
- Жаңартуды орнату шебері немесе осалдықтарды түзету шебері көмегімен.

Барлық жаңартулар үшін ережелер қосу

Барлық жаңартуларге ережені қосу үшін:

1. **Қосу** түймесін басыңыз.

   Ережені жасау шебері іске қосылады. Шебердің жұмысын жалғастыру үшін **Келесі** түймесін басыңыз.

2. Шеберің **Ереже түрін таңдаңыз** қадамында **Барлық жаңартуларға арналған ереже** тармағын таңдаңыз.

3. Шебердің **Жалпы критерийлер** қадамында келесі параметрлерді көрсетіңіз:

   - **Орнатылатын жаңартулар жиынтығы**

     Клиент құрылғыларына орнатылатын жаңартуларды таңдаңыз:

     - **Тек бекітілген жаңартуларды орнату**. Бұл жағдайда, тек расталған жаңартуларды орнатылады.
     - **Барлық жаңартуларды орнату (қабылданбаған жаңартулардан басқа)**. Бұл жағдайда, *Расталды* немесе *Анықталмаған* күйлері бар жаңартулар орнатылады.
     - **Барлық жаңартуларды орнату (қабылданбаған жаңартуларды қоса)**. Бұл жағдайда, барлық жаңартулар олардың растау мәртебесіне қарамастан орнатылады. Бұл нұсқаны мұқият таңдаңыз. Мысалы, сынақ инфрақұрылымында кейбір қабылданбаған жаңартулардың орнатылуын тексергіңіз келсе, осы параметрді пайдаланыңыз.

   - **Қауіптілік деңгейі келесіге тең не одан жоғарырақ осалдықтарды түзету**

     Кейде бағдарламалық жасақтама жаңартуы пайдаланушының бағдарламалық жасақтамамен жұмысын нашарлатуы мүмкін. Мұндай жағдайларда, сіз тек бағдарламалық жасақтама үшін маңызды жаңартуларды орнатып, басқа жаңартуларды өткізіп жібере аласыз.

     Егер бұл параметр қосылса, жаңартулар тек Kaspersky орнатқан критикалық деңгей тізімде таңдалған мәнге тең келетін немесе одан асатын осалдықтарды ғана түзетеді (**Орташа**, **Жоғары**, немесе **Критикалық**). Таңдалған мәннен төмен критикалық деңгейі бар осалдықтар түзетілмейді.

     Егер бұл параметр өшірулі болса, жаңартулар олардың критикалық деңгейіне қарамастан барлық осалдықтарды түзетеді.

     Әдепкі бойынша, параметр өшірулі.

Шебердің келесі қадамына өтіңіз.

4. Орнатылатын жаңартуларды таңдау:

   - **Барлық жарамды жаңартуларды орнату**

     Бұл жағдайда, шебердің **Жалпы критерийлер** қадамында көрсетілген өлшемшарттарға сәйкес келетін қолданбалық жасақтаманың барлық жаңартулары орнатылады. Әдепкі бойынша таңдалған.

   - **Тек тізімдегі жаңартуларды орнату**

     Бұл жағдайда, тізімде қолмен таңдайтын бағдарламалық жасақтаманың жаңартулары ғана орнатылады. Бұл тізімде барлық қолжетімді бағдарламалық жасақтама жаңартулары бар.

     Мысалы, келесі жағдайларда жаңартуларды орнатуға болады: тек критикалық маңызды бағдарламаларды жаңарту үшін немесе тек қажетті бағдарламаларды жаңарту үшін сынақ ортасында жаңартуларды орнатуды тексеру.

     - **Таңдалған жаңартуларды орнату үшін керек бағдарламалардың алдыңғы жаңартуларының барлығын автоматты түрде орнату**

       Таңдалған жаңартуларды орнату үшін, қажет болған жағдайда, бағдарламалардың аралық нұсқаларын орнатуға келіссеңіз, осы параметрді қосыңыз.

       Егер бұл параметр өшірулі болса, бағдарламалардың тек таңдалған нұсқалары орнатылады. Бағдарламалардың нұсқаларын дәйекті түрде орнатуға тырыспай, бағдарламаларды тікелей жаңартқыңыз келсе, бұл параметрді өшіріңіз. Егер таңдалған жаңартуларды бағдарламаның алдыңғы нұсқаларын орнатпай-ақ орнату мүмкін болмаса, бағдарламаны жаңарту қатемен аяқталады.

       Мысалы, сізде құрылғыда бағдарламаның 3-нұсқасы бар, оны 5-нұсқаға жаңартқыңыз келеді, бірақ 5-нұсқаны тек 4-нұсқаның үстіне орнатуға болады. Егер бұл параметр қосулы болса, алдымен бағдарламалық жасақтаманың 4-нұсқасы, содан кейін 5-нұсқасы орнатылады. Егер бұл параметр өшірулі болса, бағдарламалық жасақтаманы жаңарту сәтсіз болады.

       Әдепкі бойынша, параметр қосулы.

   Шебердің келесі қадамына өтіңіз.

5. Көрсетілген жаңартуды орнатумен түзетілетін осалдықтарды таңдаңыз:

   - **Қалған критерийлерге сай барлық осалдықтарды жабу**

     Бұл жағдайда шебердің **Жалпы критерийлер** қадамында көрсетілген өлшемшарттарға сәйкес келетін қолданбалардағы барлық осалдықтар түзетіледі. Әдепкі бойынша таңдалған.

   - **Тек тізімдегі осалдықтарды жабу**

     Тізімнен қолмен таңдалған осалдықтарды ғана түзетіңіз. Бұл тізімде барлық анықталған осалдықтар бар.

     Мысалы, келесі жағдайларда осалдықтарды белгілеуге болады: сынақ ортасындағы осалдықтардың түзетілуін тексеру, тек маңызды бағдарламалардағы осалдықтарды түзету немесе тек қажетті бағдарламалардағы осалдықтарды түзету үшін.

   Шебердің келесі қадамына өтіңіз.

6. Қосып жатқан ереженің атауын енгізіңіз. Бұл атауды жасалған тапсырманың сипаттар терезесіндегі **Бағдарлама параметрлері** қойындысында кейін өзгертуге болады.

Ереже жасалады, конфигурацияланады және Жаңа тапсырма жасау шебері ережелер кестесінде көрсетіледі.

Windows Update жаңартуларына ережені қосу

Windows Update жаңартуларына ережені қосу үшін:

1. **Қосу** түймесін басыңыз.

   Ережені жасау шебері іске қосылады. Шебердің жұмысын жалғастыру үшін **Келесі** түймесін басыңыз.

2. **Windows Update жаңартуларына арналған ереже** таңдаңыз.

   Шебердің келесі қадамына өтіңіз.

3. Шебердің **Жалпы критерийлер** қадамында келесі параметрлерді көрсетіңіз:

   - **Орнатылатын жаңартулар жиынтығы**

     Клиент құрылғыларына орнатылатын жаңартуларды таңдаңыз:

     - **Тек бекітілген жаңартуларды орнату**. Бұл жағдайда, тек расталған жаңартуларды орнатылады.
     - **Барлық жаңартуларды орнату (қабылданбаған жаңартулардан басқа)**. Бұл жағдайда, *Расталды* немесе *Анықталмаған* күйлері бар жаңартулар орнатылады.
     - **Барлық жаңартуларды орнату (қабылданбаған жаңартуларды қоса)**. Бұл жағдайда, барлық жаңартулар олардың растау мәртебесіне қарамастан орнатылады. Бұл нұсқаны мұқият таңдаңыз. Мысалы, сынақ инфрақұрылымында кейбір қабылданбаған жаңартулардың орнатылуын тексергіңіз келсе, осы параметрді пайдаланыңыз.

   - **Қауіптілік деңгейі келесіге тең не одан жоғарырақ осалдықтарды түзету**

     Кейде бағдарламалық жасақтама жаңартуы пайдаланушының бағдарламалық жасақтамамен жұмысын нашарлатуы мүмкін. Мұндай жағдайларда, сіз тек бағдарламалық жасақтама үшін маңызды жаңартуларды орнатып, басқа жаңартуларды өткізіп жібере аласыз.

     Егер бұл параметр қосылса, жаңартулар тек Kaspersky орнатқан критикалық деңгей тізімде таңдалған мәнге тең келетін немесе одан асатын осалдықтарды ғана түзетеді (**Орташа**, **Жоғары**, немесе **Критикалық**). Таңдалған мәннен төмен критикалық деңгейі бар осалдықтар түзетілмейді.

     Егер бұл параметр өшірулі болса, жаңартулар олардың критикалық деңгейіне қарамастан барлық осалдықтарды түзетеді.

     Әдепкі бойынша, параметр өшірулі.

   - **MSRC бойынша қауіптілік деңгейі келесіге тең не одан жоғарырақ осалдықтарды түзету**

     Кейде бағдарламалық жасақтама жаңартуы пайдаланушының бағдарламалық жасақтамамен жұмысын нашарлатуы мүмкін. Мұндай жағдайларда, сіз тек бағдарламалық жасақтама үшін маңызды жаңартуларды орнатып, басқа жаңартуларды өткізіп жібере аласыз.

     Егер бұл параметр қосылса, жаңартулар тек Microsoft Security Response Center (MSRC) орнатқан критикалық деңгей тізімде таңдалған мәнге тең келетін немесе одан асатын осалдықтарды ғана түзетеді (**Төмен**, **Орташа**, **Жоғары**, немесе **Критикалық**). Таңдалған мәннен төмен критикалық деңгейі бар осалдықтар түзетілмейді.

     Егер бұл параметр өшірулі болса, жаңартулар олардың критикалық деңгейіне қарамастан барлық осалдықтарды түзетеді.

     Әдепкі бойынша, параметр өшірулі.

4. **Бағдарламалар** терезесінде жаңартуларды орнатқыңыз келетін бағдарламалар мен бағдарламалардың нұсқаларын таңдаңыз. Әдепкі бойынша барлық бағдарламалар таңдалған.

5. **Жаңартулардың санаттары** терезесінде орнату үшін жаңарту санаттарын таңдаңыз. Бұл санаттар Microsoft Update каталогымен бірдей. Әдепкі бойынша барлық санаттар таңдалған.

6. **Атауы** терезесінде қосылатын ереженің атауын көрсетіңіз. Ереже атауын кейінірек, **Параметрлер** бөлімінде, жасалған тапсырманың сипаттары терезесінде өзгертуге болады.

Ереже жасау шебері өз жұмысын аяқтағаннан кейін, ереже қосылады және тапсырма жасау шеберінің ережелер тізімінде немесе тапсырманың сипаттарында көрсетіледі.

Үшінші тарап қолданбасын жаңарту ережелерін қосу

Үшінші тарап бағдарламаларын жаңарту ережесін қосу үшін:

1. **Қосу** түймесін басыңыз.

   Ережені жасау шебері іске қосылады. Шебердің жұмысын жалғастыру үшін **Келесі** түймесін басыңыз.

2. **Ереже түрін таңдаңыз** шебері қадамында **Үшінші тарап жаңартуларға арналған ереже** тармағын таңдаңыз.

3. Шебердің **Жалпы критерийлер** қадамында келесі параметрлерді көрсетіңіз:

   - **Орнатылатын жаңартулар жиынтығы**

     Клиент құрылғыларына орнатылатын жаңартуларды таңдаңыз:

     - **Тек бекітілген жаңартуларды орнату**. Бұл жағдайда, тек расталған жаңартуларды орнатылады.

     - **Барлық жаңартуларды орнату (қабылданбаған жаңартулардан басқа)**. Бұл жағдайда, *Расталды* немесе *Анықталмаған* күйлері бар жаңартулар орнатылады.

     - **Барлық жаңартуларды орнату (қабылданбаған жаңартуларды қоса)**. Бұл жағдайда, барлық жаңартулар олардың растау мәртебесіне қарамастан орнатылады. Бұл нұсқаны мұқият таңдаңыз. Мысалы, сынақ инфрақұрылымында кейбір қабылданбаған жаңартулардың орнатылуын тексергіңіз келсе, осы параметрді пайдаланыңыз.

   - **Қауіптілік деңгейі келесіге тең не одан жоғарырақ осалдықтарды түзету**

     Кейде бағдарламалық жасақтама жаңартуы пайдаланушының бағдарламалық жасақтамамен жұмысын нашарлатуы мүмкін. Мұндай жағдайларда, сіз тек бағдарламалық жасақтама үшін маңызды жаңартуларды орнатып, басқа жаңартуларды өткізіп жібере аласыз.

     Егер бұл параметр қосылса, жаңартулар тек Kaspersky орнатқан критикалық деңгей тізімде таңдалған мәнге тең келетін немесе одан асатын осалдықтарды ғана түзетеді (**Орташа**, **Жоғары**, немесе **Критикалық**). Таңдалған мәннен төмен критикалық деңгейі бар осалдықтар түзетілмейді.

     Егер бұл параметр өшірулі болса, жаңартулар олардың критикалық деңгейіне қарамастан барлық осалдықтарды түзетеді.

     Әдепкі бойынша, параметр өшірулі.

   Шебердің келесі қадамына өтіңіз.

4. Жаңартуларды орнатқыңыз келетін қолданбалар мен қолданба нұсқаларын таңдаңыз.

   Әдепкі бойынша барлық бағдарламалар таңдалған.

Шебердің келесі қадамына өтіңіз.

5. Қосып жатқан ереженің атауын енгізіңіз. Бұл атауды жасалған тапсырманың сипаттар терезесіндегі **Бағдарлама параметрлері** қойындысында кейін өзгертуге болады.

Ереже жасалады, конфигурацияланады және Жаңа тапсырма жасау шебері ережелер кестесінде көрсетіледі.

Тапсырма жасалғаннан кейін көрсетілген Қажетті жаңартуларды орнату және осалдықтарды жабу тапсырмасының параметрлері

Тапсырманы жасағаннан кейін, *Қажетті жаңартуларды орнату және осалдықтарды түзету* тапсырма сипаттары терезесінің **Бағдарлама параметрлері** қойындысында келесі параметрлерді көрсетуге болады:

- **Тексеру үшін орнату** бөлімінде:
  - **Сканерлемеу**. Жаңартуларды тексеріп орнатқыңыз келмесе, осы нұсқаны таңдаңыз.
  - **Таңдалған құрылғыларда сканерлеуді іске қосу**. Белгілі бір құрылғыларда жаңартуларды орнатуды тексергіңіз келсе, осы нұсқаны таңдаңыз. **Қосу** түймесін басып, жаңартуларды тексеріп орнату қажет құрылғыларды таңдаңыз.
  - **Көрсетілген топтағы құрылғыларда сканерлеуді іске қосу**. Құрылғылар тобында жаңартуларды орнатуды тексергіңіз келсе, осы нұсқаны таңдаңыз. **Сынақ топты белгілеңіз** өрісінде тексеріп орнату қажет құрылғылар тобын көрсетіңіз.
  - **Құрылғылардың көрсетілген пайызында сканерлеуді іске қосу**. Құрылғылардың белгілі бір санында жаңартуларды орнатуды тексергіңіз келсе, осы нұсқаны таңдаңыз. **Құрылғылардың жалпы санынан сынақ құрылғылардың пайызы** өрісінде жаңартуларды тексеріп орнату қажет құрылғылар пайызын көрсетіңіз.

  Сканерлемеу тармағынан басқа кез келген параметрді таңдағаннан кейін, **Орнатуды жалғастыру туралы шешімді қабылдау уақытының мөлшері, сағ** өрісінде жаңартуларды сынап орнатудан бастап барлық құрылғыларға жаңартуларды орнатудың басталуына дейін өту керек сағаттардың санын көрсетіңіз.
- **Орнатылатын жаңартулар** бөлімінде тапсырмада белгіленген жаңартулар тізімін көруге болады. Таңдалған тапсырманың параметрлеріне сәйкес келетін жаңартулар ғана көрсетіледі.

Тапсырманың толық сипаттамасын тапсырманың жалпы параметрлерінен қараңыз.

Үшінші тарап бағдарламаларын автоматты түрде жаңарту

Кейбір үшінші тарап бағдарламалары автоматты түрде жаңартылуы мүмкін. Қолданба өндірушісі қолданбаның автоматты түрде жаңарту функциясын қолдайтынын анықтайды. Егер басқарылатын құрылғыда орнатылған үшінші тарап бағдарламасы автоматты түрде жаңартуды қолдаса, бағдарлама сипаттарында автоматты түрде жаңарту параметрін көрсетуге болады. Автоматты жаңарту параметрін өзгерткеннен кейін, Желілік агенттер бағдарлама орнатылған әрбір басқарылатын құрылғыда жаңа параметрді қолданады.

Автоматты жаңарту параметрі басқа нысандарға және Осалдықтар мен патчтарды басқару мүмкіндіктеріне тәуелді емес. Мысалы, бұл параметр жаңартуды мақұлдау күйіне немесе *Қажетті жаңартуларды орнату және осалдықтарды түзету* және *Осалдықтарды түзету* сияқты жаңартуды орнату тапсырмаларына тәуелсіз.

Үшінші тарап бағдарламасына арналған автоматты жаңарту параметрін конфигурациялау үшін:

1. Бағдарламаның негізгі терезесінде **Бағдарламалық жасақтаманы басқару → Үшінші тарап бағдарламалары → Бағдарламалар тізімдемесі** бөліміне өтіңіз.

2. Автоматты жаңарту параметрін өзгерткіңіз келетін бағдарламаның атын басыңыз.

   Іздеуді жеңілдету үшін тізімді **Автоматты жаңартулар күйі** және **Автоматты жаңартуларды басқару** бағандары арқылы сүзуге болады.

   Бағдарлама сипаттары терезесі ашылады.

3. **Жалпы** бөлімінде келесі функция үшін мәнді таңдаңыз:

   Автоматты жаңартулар күйі.

   Келесі нұсқалардың бірін таңдаңыз:

   - **Анықталмаған**

     Автоматты жаңарту функциясы өшірулі. Kaspersky Security Center Linux бағдарламасы үшінші тарап қолданбасының жаңартуларын келесі тапсырмалар көмегімен орнатады: *Қажетті жаңартуларды орнату және осалдықтарды түзету* және *Осалдықтарды түзету*.

   - **Рұқсат етілген**

     Өндіруші бағдарлама үшін жаңартуды шығарғаннан кейін, бұл жаңарту автоматты түрде басқарылатын құрылғыларға орнатылады. Қосымша әрекеттер керек емес.

   - **Бұғатталған**

     Бағдарлама жаңартулары автоматты түрде орнатылмайды. Kaspersky Security Center Linux бағдарламасы үшінші тарап қолданбасының жаңартуларын келесі тапсырмалар көмегімен орнатады: *Қажетті жаңартуларды орнату және осалдықтарды түзету* және *Осалдықтарды түзету*.

4. Өзгерістерін сақтау үшін **Сақтау** түймесін басыңыз.

Автоматты жаңарту конфигурациясы таңдалған бағдарламаға қолданылады.

Үшінші тарап бағдарламаларында осалдықтарды түзету

Бұл бөлімде, басқарылатын құрылғыларда орнатылған қолданбаларда осалдықтарды түзетумен байланысты Kaspersky Security Center Linux мүмкіндіктері сипатталған.

Бағдарламалық жасақтама осалдықтарын анықтау және түзету туралы

Kaspersky Security Center Linux қолданбасы Microsoft Windows операциялық жүйелерінің басқаруымен жұмыс істейтін басқарылатын құрылғылардағы қолданбаларда осалдықтарды анықтайды және түзетеді. Осалдықтар операциялық жүйелерде және Microsoft бағдарламалық жасақтамасын қоса, үшінші тарап бағдарламаларында кездеседі.

Жаңарту функционалдығы (антивирустық қолтаңба жаңартуларын және код дерекқоры жаңартуларын қоса) және KSN функционалдығы АҚШ аймағындағы бағдарламада қолжетімді болмауы мүмкін.

Бағдарламалық жасақтама осалдықтарын анықтау

Осалдықтарды анықтау үшін Kaspersky Security Center Linux қолданбасы белгілі осалдықтар туралы дерекқордағы белгілерге негізделген қолданбаның белгілі осалдықтарын іздейді. Дерекқорды Kaspersky мамандары жасап, өзекті күйде ұстайды. Онда осалдықтардың сипаттамасы, осалдықтарды анықтау күні және осалдықтардың қауіптілік деңгейі сияқты осалдықтар туралы ақпарат бар. Қолданбаның осалдықтары туралы ақпаратты Kaspersky сайтында алуға болады.

Kaspersky Security Center Linux жүйесінде қолданбалардағы осалдықтарды іздеу үшін *Осалдықтарды және қажетті жаңартуларды іздеу* тапсырмасы пайдаланылады.

Бағдарламаларда осалдықты түзету

Қолданбаларда осалдықтарды түзету үшін, Kaspersky Security Center Linux қолданбасы қолданбалық жасақтама өндірушілері шығарған қолданбалық жасақтама жаңартуларын қолданады. Бағдарламалық жасақтаманы жаңарту метадеректері *Жаңартуларды Басқару серверінің қоймасына жүктеп алу* тапсырмасын орындау нәтижесінде Басқару сервері қоймасына жүктеледі. Бұл тапсырма Kaspersky қолданбалары мен үшінші тарап қолданбалары үшін жаңарту метадеректерін жүктеуге арналған. Бұл тапсырма Kaspersky Security Center Linux қолданбаны жылдам іске қосу шеберінде автоматты түрде жасалады. *Жаңартуларды Басқару серверінің қоймасына жүктеп алу* тапсырмасын қолмен жасауға да болады.

Осалдықтарды түзетуге арналған бағдарламалық жасақтаманың жаңартулары толық дистрибутивтер немесе патчтар түрінде ұсынылуы мүмкін. Бағдарламалық жасақтаманың осалдықтарын түзететін бағдарламалық жасақтама жаңартулары *түзетулер* деп аталады. *Ұсынылған түзетулер* – бұл Kaspersky мамандары орнатуға ұсынатын түзетулер. *Пайдаланушылық түзетулер* – бұл пайдаланушылар орнату үшін қолмен көрсетілетін түзетулер. Пайдаланушылық түзетулерді орнату үшін осы түзетуді қамтитын орнату пакетін жасау керек.

Kaspersky Security Center Linux лицензиясы Осалдықтар мен патчтарды басқару мүмкіндіктерін көздесе, *Қажетті жаңартуларды орнату және осалдықтарды түзету* тапсырмасын пайдаланыңыз. Бұл тапсырма ұсынылған түзетулерді орнату арқылы бірнеше осалдықтарды автоматты түрде түзетеді. Бұл тапсырма үшін бірнеше осалдықтарды түзету үшін белгілі бір ережелерді қолмен конфигурациялауға болады.

Kaspersky Security Center Linux лицензиясы Осалдықтар мен патчтарды басқару мүмкіндіктерін көздемесе, *Осалдықтарды түзету* тапсырмасын пайдаланыңыз. Бұл тапсырманың көмегімен Microsoft қолданбалары үшін ұсынылған түзетулерді және үшінші тарап қолданбалары үшін пайдаланушылық түзетулерді орнату арқылы осалдықтарды түзетуге болады.

Қауіпсіздік мақсатында, Осалдықтар мен патчтарды басқару арқылы орнатқан кез келген үшінші тарап бағдарламалық жасақтамасы жаңартулары Kaspersky технологиялары арқылы зиянды БҚ-дың бар-жоғы тұрғысынан автоматты түрде тексеріледі. Бұл технологиялар файлдарды автоматты түрде тексеру үшін қолданылады және антивирустық тексеруді, статикалық талдауды, динамикалық талдауды, "құмсалғыштың" жүріс-тұрысын талдауды және машиналық оқытуды қамтиды.

Kaspersky мамандары Осалдықтар мен патчтарды басқару арқылы орнатуға болатын үшінші тарап бағдарламалық жасақтамасы жаңартуларын қолмен талдамайды. Сонымен қатар Kaspersky мамандары мұндай жаңартулардағы осалдықтарды (белгілі немесе белгісіз) немесе құжатталмаған мүмкіндіктерді іздеумен айналыспайды және жоғарыда аталған талдаудың басқа түрлерін жүргізбейді.

> Пайдаланушының араласуы үшінші тарап бағдарламаларын жаңарту кезінде немесе басқарылатын құрылғыдағы үшінші тарап бағдарламаларында осалдықтарды түзету кезінде қажет болуы мүмкін. Мысалы, пайдаланушыдан үшінші тарап бағдарламасын жабу сұралуы мүмкін.

Бағдарламалық жасақтаманың кейбір осалдықтарын түзету үшін, қажет болса, бағдарламалық жасақтаманы орнатуға арналған лицензиялық келісімді қабылдау керек. Егер сіз Лицензиялық келісімнен бас тартсаңыз, бағдарламалық жасақтаманың осалдығы түзетілмейді.

Сценарий: Үшінші тарап бағдарламаларындағы осалдықтарды анықтау және түзету

Бұл бөлімде, Windows басқаруымен жұмыс істейтін құрылғылардағы осалдықтарды анықтау және түзету сценарийі келтірілген. Операциялық жүйелердегі, үшінші тарап бағдарламаларындағы, соның ішінде Microsoft бағдарламаларындағы осалдықтарды анықтауға және түзетуге болады.

Алдын ала талаптар

- Kaspersky Security Center Linux бағдарламасы сіздің ұйымыңызда орналастырылған.
- Ұйымыңыздың желісінде Windows басқаруымен жұмыс істейтін басқарылатын құрылғылар бар.
- Басқару серверін интернетке қосу келесі тапсырмаларды орындау үшін қажет:
  - Microsoft бағдарламалық жасақтама осалдықтарының ұсынылған түзетулер тізімін жасау. Тізімді Kaspersky мамандары қалыптастырады және үнемі жаңартып отырады.
  - Microsoft қолданбаларынан басқа үшінші тарап қолданбаларындағы осалдықтарды түзету.

Кезеңдер

Осалдықтарды анықтау және түзету келесі кезеңдерден тұрады:

1. **Басқарылатын құрылғыларда орнатылған бағдарламалық жасақтамадағы осалдықтарды іздеу**

   Басқарылатын құрылғыларда орнатылған қолданбалардағы осалдықтарды табу үшін *Осалдықтарды және қажетті жаңартуларды іздеу* тапсырмасын іске қосыңыз. Бұл тапсырма аяқталғаннан кейін, Kaspersky Security Center Linux қолданбасы құрылғыларға орнатылған және тапсырма сипаттарында көрсетілген үшінші тарап қолданбалары үшін қажетті жаңартулар мен табылған осалдықтар тізімін алады.

   Осалдықтарды және қажетті жаңартуларды іздеу тапсырмасы Kaspersky Security Center Linux қолданбаны жылдам іске қосу шеберінде автоматты түрде жасалады. Бағдарламаны жылдам іске қосу шеберін іске қоспаған болсаңыз, оны қазір іске қосыңыз немесе тапсырманы қолмен жасаңыз.

   > Windows жүйесімен жұмыс істейтін құрылғылар үшін ғана *Осалдықтарды және қажетті жаңартуларды іздеу* тапсырмасын жасай аласыз. Бұл тапсырманы басқа операциялық жүйелермен жұмыс істейтін құрылғылар үшін жасай алмайсыз.

2. **Қолданбаларда анықталған осалдықтар тізімін қарау**

   Бағдарламалық жасақтама осалдықтары тізімін қарап шығыңыз және қандай осалдықтарды жою керектігін шешіңіз. Әрбір осалдық туралы толық ақпаратты көру үшін тізімдегі осалдық атауын басыңыз. Тізімдегі әрбір осалдық үшін басқарылатын құрылғылардағы осалдық статистикасын да көруге болады.

3. **Осалдықты түзетуді конфигурациялау**

   Қолданбаларда осалдықтарды тапқаннан кейін, оларды басқарылатын құрылғыларда *Қажетті жаңартуларды орнату және осалдықтарды түзету* тапсырмасы немесе *Осалдықтарды түзету* тапсырмасы арқылы түзетуге болады.

   Қажетті жаңартуларды орнату және осалдықтарды түзету тапсырмасы басқарылатын құрылғыларда орнатылған үшінші тарап қолданбаларындағы, соның ішінде Microsoft қолданбаларындағы осалдықтарды жаңарту және түзету үшін пайдаланылады. Бұл тапсырма бірнеше жаңартуларды орнатуға және белгіленген ережелерге сәйкес бірнеше осалдықтарды түзетуге мүмкіндік береді. Назар аударыңыз, Осалдықтар мен патчтарды басқаруға арналған лицензияңыз болса ғана осы тапсырманы жасауға болады. Бағдарламалық жасақтама осалдықтарын түзету үшін, *Қажетті жаңартуларды орнату және осалдықтарды түзету* тапсырмасы ұсынылған бағдарламалар жаңартуын қолданады.

   Осалдықтарды түзету тапсырмасы Осалдықтар мен патчтарды басқару үшін лицензияны қажет етпейді. Бұл тапсырманы пайдалану мақсатында, тапсырма параметрлерінде көрсетілген үшінші тарап қолданбаларындағы осалдықтарды түзету үшін пайдаланушылық түзетулерді қолмен көрсету қажет. *Осалдықтарды түзету* тапсырмасы үшінші тарап қолданбалары үшін ұсынылған Microsoft қолданбаларының түзетулері мен пайдаланушылық түзетулерді пайдаланады.

   > *Қажетті жаңартуларды орнату және осалдықтарды түзету* тапсырмасын және *Осалдықтарды түзету* тапсырмасын тек Windows жүйесі бар құрылғылар үшін жасауға болады. Бұл тапсырмаларды басқа операциялық жүйелермен жұмыс істейтін құрылғылар үшін жасай алмайсыз.

   Сіз осы тапсырмалардың бірін автоматты түрде жасайтын осалдықтарды түзету шеберін іске қоса аласыз немесе сол тапсырмалардың бірін қолмен жасай аласыз.

Қажетті жаңартуларды орнату және осалдықтарды түзету тапсырмасын жасаған және конфигурациялаған болсаңыз, жаңартулар басқарылатын құрылғыларға автоматты түрде түзетілетін болады. Жасалған тапсырманы іске қосу кезінде тапсырма қолжетімді қолданбалық жасақтама жаңартуларының тізімін тапсырма параметрлерінде көрсетілген ережелермен салыстырады. Көрсетілген ережелердегі өлшемшарттарға сәйкес келетін барлық бағдарламалық жасақтама жаңартулары Басқару сервері қоймасына жүктеледі және қолданбалардағы осалдықтарды түзету үшін орнатылады.

Осалдықтарды түзету тапсырмасын жасаған болсаңыз, Microsoft қолданбаларындағы осалдықтар ғана түзетіледі.

4 Тапсырманың кестесін белгілеу

Осалдықтарды және қажетті жаңартуларды іздеу тапсырмасын осалдықтардың тізімін жаңартып отыру үшін мерзімді негізде автоматты түрде іске қосу үшін жоспарлаңыз. Ұсынылатын кезең – аптасына бір рет.

Қажетті жаңартуларды орнату және осалдықтарды түзету тапсырмасын жасаған болсаңыз, оны іске қосуды *Осалдықтарды және қажетті жаңартуларды іздеу* тапсырмасына арналған жиілікпен немесе одан сирек жиілікпен іске қосуды белгілей аласыз. *Осалдықтарды түзету* тапсырмасының кестесін белгілеген кезде, тапсырманы іске қоспас бұрын Microsoft бағдарламаларының түзетулерін таңдау немесе үшінші тарап бағдарламалары үшін арнайы түзетулерді көрсету керек.

Тапсырмалар кестесін белгілеу кезінде, осалдықтарды түзету тапсырмасы *Осалдықтарды және қажетті жаңартуларды іздеу* аяқталғаннан кейін іске қосылатынына көз жеткізіңіз.

5 Бағдарламалық жасақтама осалдықтарын елемеу (қажет болса)

Барлық басқарылатын құрылғыдағы немесе тек таңдалған басқарылатын құрылғылардағы кейбір бағдарламалық жасақтама осалдықтарын елемеуге болады.

6 Осалдықтарды түзету тапсырмасын іске қосу

Қажетті жаңартуларды орнату және осалдықтарды түзету немесе *Осалдықтарды түзету* тапсырмасын бастаңыз. Тапсырма аяқталғаннан кейін, оның тапсырмалар тізімінде *Сәтті аяқталды* күйі бар екеніне көз жеткізіңіз.

7 Қолданбалардың осалдықтарын түзету нәтижелері туралы есеп жасау (қажет болса)

Жабық осалдықтар туралы статистиканы көру үшін осалдықтар туралы есепті жасаңыз. Осы есепте түзетілмеген қолданбалардың осалдықтары туралы ақпарат көрсетіледі. Ол ұйымыңыз пайдаланатын Microsoft бағдарламалық жасақтамасын оса алғанда, үшінші тарап бағдарламалық жасақтамасындағы осалдықтарды анықтауға және түзетуге көмектеседі.

8 Үшінші тарап қолданбаларындағы осалдықтарды анықтау және түзету параметрлерін тексеру

Келесіні орындағаныңызға көз жеткізіңіз:

- басқарылатын құрылғылардағы қолданбалардың осалдықтары тізімін тауып, қарап шықтыңыз;
- қажеттілігіне қарай, қолданбаның кейбір осалдықтарын елемедіңіз;
- осалдықты түзету тапсырмасын конфигурациялағаныңызға;
- қолданбалардағы осалдықтарды іздеуге және түзетуге арналған тапсырмаларды дәйекті түрде іске қосылатындай етіп іске қосуды жоспарлады;
- осалдықтарды түзету міндеті іске қосылғанын тексерді.

Үшінші тарап бағдарламаларында осалдықтарды түзету

Үшінші тарап қолданбаларындағы осалдықтарды табу үшін *Осалдықтарды және қажетті жаңартуларды іздеу* тапсырмасын жасап, іске қосуға және қолданбаның осалдықтарының тізімін алуға болады. Қолданбаларда осалдықтар тізімін алғаннан кейін, Windows операциялық жүйелері бар басқарылатын құрылғылардағы осалдықтарды түзете аласыз.

Тапсырма жасау және Осалдықтарды түзету тапсырмасын немесе Қажетті жаңартуларды орнату және осалдықтарды түзету тапсырмасын іске қосу арқылы операциялық жүйедегі және Microsoft қолданбаларын қоса алғанда, үшінші тарап қолданбаларындағы осалдықтарды түзетуге болады.

Пайдаланушының араласуы үшінші тарап бағдарламаларын жаңарту кезінде немесе басқарылатын құрылғыдағы үшінші тарап бағдарламаларында осалдықтарды түзету кезінде қажет болуы мүмкін. Мысалы, пайдаланушыдан үшінші тарап бағдарламасын жабу сұралуы мүмкін.

Сондай-ақ, бағдарламалардағы осалдықтарды түзету үшін тапсырманы келесі жолдармен жасауға болады:

- Осалдықтар тізімін ашып, қандай осалдықтарды түзету керектігін көрсетіңіз.

  Нәтижесінде, бағдарламалардағы осалдықтарды түзету тапсырмасы туындайды. Таңдалған осалдықтарды қолданыстағы тапсырмаға қосуға болады.

- Осалдықтарды түзету шеберін іске қосыңыз.

  Осалдықтар мен патчтарды басқару үшін лицензия болған кезде, осалдықтарды түзету шебері қолжетімді болады.

  Шебер осалдықтарды түзету тапсырмасын құруды және конфигурациялауды жеңілдетеді, сонымен қатар артық тапсырмаларды құруды болдырмайды.

Бағдарламалардағы осалдықтарды осалдықтар тізімімен түзету

Қолданбаның осалдықтарын осалдықтар тізімін пайдаланып түзету үшін:

1. Төмендегі әрекеттердің бірін орындау арқылы өзгерту үшін осалдықтар тізімін ашыңыз:

   - Бағдарламаның негізгі терезесінде **Бағдарламалық жасақтаманы басқару** → **Патчтарды басқару** → **Бағдарламалық жасақтама осалдықтары** бөліміне өтіңіз.

   - Қолданбаның негізгі терезесінде **Активтерді басқару** → **Активтер (құрылғылар)** → <құрылғының атауы> → **Кеңейтілген** → **Бағдарламалық жасақтама осалдықтары** бөліміне өтіңіз.

   - Қолданбаның негізгі терезесінде **Бағдарламалық жасақтаманы басқару** → **Үшінші тарап бағдарламалары** → **Бағдарламалар тізімдемесі** → <қолданбаның атауы> → **Осалдықтар** бөліміне өтіңіз.

   Басқарылатын құрылғыларда орнатылған үшінші тарап қолданбаларындағы осалдықтар тізімі бар бет ашылады.

2. Осалдықтар тізімінде түзеткіңіз келетін осалдықтардың жанындағы құсбелгілерді таңдап, **Осалдықты түзету** түймесін басыңыз.

   Таңдалған осалдықтардың бірін түзету үшін ұсынылған бағдарламалық жасақтамасының жаңартуы болмаса, ақпараттық хабар көрсетіледі.

   Бағдарламалық жасақтаманың кейбір осалдықтарын түзету үшін, қажет болса, бағдарламалық жасақтаманы орнатуға арналған лицензиялық келісімді қабылдау керек. Егер сіз Лицензиялық келісімнен бас тартсаңыз, бағдарламалық жасақтаманың осалдығы түзетілмейді.

3. Келесі нұсқалардың бірін таңдаңыз:

   - **Жаңа тапсырма**

     Жаңа тапсырма жасау шебері іске қосылады. Осалдықтар мен патчтарды басқару лицензиясы болса, Қажетті жаңартуларды орнату және осалдықтарды түзету тапсырма түрі әдепкі бойынша таңдалады. Лицензияңыз болмаса, әдепкі бойынша Осалдықтарды түзету тапсырма түрі таңдалады. Тапсырма жасауды аяқтау үшін шебердің алдағы нұсқауларын орындаңыз.

   - **Осалдықты түзету (көрсетілген тапсырмаға ереже қосу)**

     Осалдықтардың таңдаулылар тізіміне қосқыңыз келетін тапсырманы таңдаңыз. Осалдықтар мен патчтарды басқару лицензиясы болса, Қажетті жаңартуларды орнату және осалдықтарды түзету тапсырмасын таңдаңыз. Таңдалған тапсырмаға таңдалған осалдықтарды түзетуге арналған жаңа ереже автоматты түрде қосылады. Лицензияңыз болмаса, әдепкі бойынша Осалдықтарды түзету тапсырма түрі таңдалған. Таңдалған осалдықтар тапсырма сипаттарына қосылған.

     Тапсырма сипаттары терезесі ашылады. Өзгерістерін сақтау үшін **Сақтау** түймесін басыңыз.

   Тапсырма жасауды таңдаған болсаңыз, ол тапсырмалар тізімінде, **Тапсырмалар** бөлімінде жасалып, көрсетіледі. Егер сіз бар тапсырмаға осалдықтарды қосуды таңдасаңыз, осалдықтар тапсырма сипаттарында сақталады.

Үшінші тарап қолданбаларындағы осалдықтарды жабу үшін Қажетті жаңартуларды орнату және осалдықтарды түзету тапсырмасын немесе Осалдықтарды түзету тапсырмасын іске қосыңыз. Егер сіз Осалдықтарды түзету тапсырмасын жасаған болсаңыз, тапсырма сипаттарында тізімделген бағдарламалық жасақтама жаңартуларын қолмен көрсету керек.

Осалдықтарды түзету шебері арқылы бағдарламалардағы осалдықтарды түзету

> Осалдықтар мен патчтарды басқару үшін лицензия болған кезде, осалдықтарды түзету шебері қолжетімді болады.

Осалдықтарды түзету шебері арқылы бағдарламалардағы осалдықтарды түзету үшін:

1. Бағдарламаның негізгі терезесінде **Бағдарламалық жасақтаманы басқару → Патчтарды басқару → Бағдарламалық жасақтама осалдықтары** бөліміне өтіңіз.

   Басқарылатын құрылғыларда орнатылған үшінші тарап қолданбаларындағы осалдықтар тізімі бар бет ашылады.

2. Түзетуді қажет ететін осалдыққа қарсы жалауша қойыңыз.

3. **Осалдықтарды түзету шеберін іске қосу** түймесін басыңыз.

Егер сіз бірнеше осалдықты таңдасаңыз, түйме қолжетімді емес.

Осалдықтарды түзету шебері ашылады. Бар тапсырмалар тізімі көрсетіледі. Тізімде келесі тапсырма түрлері болуы мүмкін:

- Қажетті жаңартуларды орнату және осалдықтарды түзету
- Осалдықтарды түзету

Жаңа жаңартуларды орнату үшін Осалдықтарды түзету тапсырмасын өзгерте алмайсыз. Жаңа жаңартуларды орнату үшін тек Қажетті жаңартуларды орнату және осалдықтарды түзету тапсырмасын пайдалануға болады.

4. Егер сіз шебердің таңдалған осалдықты түзететін тапсырмаларды ғана көрсетуін қаласаңыз, **Осы осалдықты түзететін тапсырмаларды ғана көрсету** параметрін қосыңыз.
5. Келесі әрекеттердің бірін орындаңыз:
   - Тапсырманы іске қосу үшін, тапсырманың аты жанында жалаушаны қойып, **Іске қосу** түймесін басыңыз.

     Қосымша әрекеттер қажет емес. Шеберді жаба беруіңізге болады. Тапсырма фондық режимде орындалады.
   - Бар тапсырмаға Қажетті жаңартуларды орнату және осалдықтарды түзету ережесін қосу үшін:
     a. Тапсырманың аты жанына жалаушаны қойып, **Ереже қосу** түймесін басыңыз.

     Егер сіз бірнеше тапсырма таңдаған болсаңыз, **Ереже қосу** түймесі қолжетімді емес.

     Осалдықтарды түзету тапсырмасы үшін ереже қоса алмайсыз. Осалдықтарды түзету тапсырмасын таңдаған болсаңыз, келесі хабарландыру пайда болады: «Жаңартуларды орнату үшін «Қажетті жаңартуларды орнату және осалдықтарды түзету» тапсырмасын пайдаланыңыз».

     b. Ашылған бетте жаңа ережені орнатыңыз:

     - **Осы қауіптілік деңгейіндегі осалдықтарды түзету ережесі**

       Кейде бағдарламалық жасақтама жаңартуы пайдаланушының бағдарламалық жасақтамамен жұмысын нашарлатуы мүмкін. Мұндай жағдайларда, сіз тек бағдарламалық жасақтама үшін маңызды жаңартуларды орнатып, басқа жаңартуларды өткізіп жібере аласыз.

       Егер бұл параметр қосулы болса, жаңартулар тек Kaspersky орнатқан критикалық деңгейі таңдалған жаңартудың маңыздылық мәніне тең немесе одан асатын осалдықтарды ғана түзетеді (**Орташа**, **Жоғары** немесе **Критикалық**). Таңдалған мәннен төмен критикалық деңгейі бар осалдықтар түзетілмейді.

       Егер бұл параметр өшірулі болса, жаңартулар олардың критикалық деңгейіне қарамастан барлық осалдықтарды түзетеді.

       Әдепкі бойынша, параметр өшірулі.

     - **Таңдалған осалдыққа арналған нұсқауларға сәйкес анықталған жаңарту түріндегі жаңартулармен осалдықтарды түзету ережесі**

       Бұл ереже Microsoft қолданбаларындағы осалдықтар үшін ғана пайда болады.

- **Таңдалған жеткізуші бойынша бағдарламаларда осалдықтарды түзету ережесі**

  Бұл ереже тек үшінші тарап қолданбаларының осалдықтары үшін пайда болады.

- **Таңдалған бағдарламаның барлық нұсқаларында осалдықты түзету ережесі**

  Бұл ереже тек үшінші тарап қолданбаларының осалдықтары үшін пайда болады.

- **Таңдалған осалдықты түзету ережесі**

- **Осы осалдықты түзететін жаңартуларды растау**

  Таңдалған жаңарту орнатуға мақұлданған. Егер жаңартуды орнатудың кейбір ережелері тек мақұлданған жаңартуларды орнатуға мүмкіндік берсе, бұл параметр қолжетімді.

  Әдепкі бойынша, параметр өшірулі.

c. **Қосу** түймесін басыңыз.

Тапсырма сипаттары терезесі ашылады. Тапсырманың сипаттарына жаңа ереже қосылды. Ережені, сондай-ақ басқа тапсырма параметрлерін көруге немесе өзгертуге болады. Өзгерістерін сақтау үшін **Сақтау** түймесін басыңыз.

- Тапсырма жасау үшін:

a. **Жаңа тапсырма** түймесін басыңыз.

b. Ашылған бетте жаңа ережені орнатыңыз:

- **Осы қауіптілік деңгейіндегі осалдықтарды түзету ережесі**

  Кейде бағдарламалық жасақтама жаңартуы пайдаланушының бағдарламалық жасақтамамен жұмысын нашарлатуы мүмкін. Мұндай жағдайларда, сіз тек бағдарламалық жасақтама үшін маңызды жаңартуларды орнатып, басқа жаңартуларды өткізіп жібере аласыз.

  Егер бұл параметр қосулы болса, жаңартулар тек Kaspersky орнатқан критикалық деңгейі таңдалған жаңартудың маңыздылық мәніне тең немесе одан асатын осалдықтарды ғана түзетеді (**Орташа**, **Жоғары** немесе **Критикалық**). Таңдалған мәннен төмен критикалық деңгейі бар осалдықтар түзетілмейді.

  Егер бұл параметр өшірулі болса, жаңартулар олардың критикалық деңгейіне қарамастан барлық осалдықтарды түзетеді.

  Әдепкі бойынша, параметр өшірулі.

- **Таңдалған осалдыққа арналған нұсқауларға сәйкес анықталған жаңарту түріндегі жаңартулармен осалдықтарды түзету ережесі**

  Бұл ереже Microsoft қолданбаларындағы осалдықтар үшін ғана пайда болады.

- **Таңдалған жеткізуші бойынша бағдарламаларда осалдықтарды түзету ережесі**

  Бұл ереже тек үшінші тарап қолданбаларының осалдықтары үшін пайда болады.

- **Таңдалған бағдарламаның барлық нұсқаларында осалдықты түзету ережесі**

  Бұл ереже тек үшінші тарап қолданбаларының осалдықтары үшін пайда болады.

- **Таңдалған осалдықты түзету ережесі**

- **Осы осалдықты түзететін жаңартуларды растау**

Таңдалған жаңарту орнатуға мақұлданған. Егер жаңартуды орнатудың кейбір ережелері тек мақұлданған жаңартуларды орнатуға мүмкіндік берсе, бұл параметр қолжетімді.

Әдепкі бойынша, параметр өшірулі.

c. **Қосу** түймесін басыңыз.

d. Жаңа тапсырма жасау шеберінде Жаңа тапсырма жасау шебері.

Осалдықты түзету шеберіне қосылған жаңа ереже шебердің **Жаңа нұсқаларды орнатуға арналған ережелерді көрсетіңіз** қадамында пайда болады. Шебердің жұмысы аяқталғаннан кейін, Қажетті жаңартуларды орнату және осалдықтарды түзету тапсырмасы тапсырмалар тізіміне қосылады.

Осалдықтарды түзету тапсырмасын жасау

Осалдықтарды түзету тапсырмасы басқарылатын құрылғылардағы қолданбаларда осалдықтарды жабуға мүмкіндік береді. Microsoft бағдарламалық жасақтамасын қоса алғанда, үшінші тарап бағдарламалары осалдықтарын түзете аласыз.

Windows жүйесімен жұмыс істейтін құрылғылар үшін ғана *Осалдықтарды түзету* тапсырмасын жасай аласыз. Бұл тапсырманы басқа операциялық жүйелермен жұмыс істейтін құрылғылар үшін жасай алмайсыз.

Осалдықтар мен патчтарды басқару лицензиясы болса, жаңа *Осалдықтарды түзету* тапсырмаларын жасауға болады.

Жаңа осалдықтарды түзету үшін, сіз оларды бұрыннан бар *Осалдықтарды түзету* тапсырмасына қоса аласыз. *Осалдықтарды түзетуҚажетті жаңартуларды орнату және осалдықтарды түзету тапсырмасының орнына Қажетті жаңартуларды орнату және осалдықтарды түзетуОсалдықтарды түзету* тапсырмасын пайдалану ұсынылады. *Қажетті жаңартуларды орнату және осалдықтарды түзету* тапсырмасы автоматты түрде бірнеше жаңартуды орнатуға және белгіленген ережелерге сәйкес бірнеше осалдықты түзетуге мүмкіндік береді.

Пайдаланушының араласуы үшінші тарап бағдарламаларын жаңарту кезінде немесе басқарылатын құрылғыдағы үшінші тарап бағдарламаларында осалдықтарды түзету кезінде қажет болуы мүмкін. Мысалы, пайдаланушыдан үшінші тарап бағдарламасын жабу сұралуы мүмкін.

Осалдықтарды түзету тапсырмасын жасау үшін:

1. Бағдарламаның негізгі терезесінде **Тапсырмалар** бөліміне өтіңіз.

   Бұл тапсырманы **Тапсырмалар** қойындысындағы құрылғы сипаттары терезесінде де жасауға болады.

2. **Қосу** түймесін басыңыз.

   Жаңа тапсырма жасау шебері іске қосылады. Шебердің жұмысын жалғастыру үшін **Келесі** түймесін басыңыз.

3. **Бағдарлама** ашылмалы тізімінде Kaspersky Security Center таңдаңыз.

4. **Тапсырма түрі** тізімінде **Осалдықтарды түзету** тапсырма түрін таңдаңыз.

5. **Тапсырманың атауы** өрісіне жаңа тапсырманың атын енгізіңіз.

   Тапсырма атауы 100 таңбадан асуы және арнайы таңбаларды ("*<>?\:|) қамтуы мүмкін емес.

6. Тапсырмалар тағайындалатын құрылғыларды таңдаңыз.

   Шебердің келесі қадамына өтіңіз.

7. **Қосу** түймесін басыңыз.

   Осалдықтар тізімі ашылады.

8. Осалдықтар тізімінде түзеткіңіз келетін осалдықтардың жанындағы құсбелгілерді таңдап, **OK** түймесін басыңыз.

   Microsoft бағдарламалық жасақтамасының осалдықтары үшін әдетте ұсынылған түзетулер бар. Олар үшін қосымша әрекеттер қажет емес.

   Үшінші тарап бағдарламалары осалдықтары үшін алдымен түзеткіңіз келетін әрбір осалдық үшін пайдаланушы түзетуін көрсету керек. Содан соң, сіз осы осалдықтарды *Осалдықтарды түзету* тапсырмасына қоса аласыз.

   Шебердің келесі қадамына өтіңіз.

9. Операциялық жүйені қайта іске қосу параметрлерін көрсетіңіз:

   - **Құрылғыны қайта іске қоспау**

     Операция аяқталғаннан кейін, клиент құрылғылары автоматты түрде қайта жүктелмейді. Операцияны аяқтау үшін құрылғыны қайта қосу қажет (мысалы, қолмен немесе құрылғыны басқару тапсырмасы арқылы). Қайта жүктеу қажеттілігі туралы ақпарат тапсырманы орындау нәтижелерінде және құрылғы күйінде сақталады. Бұл нұсқа, үздіксіз жұмыс өте маңызды болып саналатын серверлердегі және басқа құрылғылардағы тапсырмалар үшін жарамды.

   - **Құрылғыны қайта іске қосу**

     Бұл жағдайда, операцияны аяқтау үшін қайта жүктеу қажет болса, қайта жүктеу әрқашан автоматты түрде орындалады. Бұл нұсқа, мезгіл-мезгіл үзілістерге (өшіру, қайта жүктеу) рұқсат етілген құрылғылардағы тапсырмалар үшін жарамды.

   - **Пайдаланушыдан әрекетті орындауды сұрау**

     Клиент құрылғысының экранында құрылғыны қолмен қайта жүктеу керек деген хабар пайда болады. Бұл нұсқа үшін қосымша параметрлерді конфигурациялауға болады: пайдаланушыға арналған хабар мәтіні, хабардың жиілігі, сондай-ақ қайта жүктеу мәжбүрлі түрде орындалатын уақыт (пайдаланушының растауынсыз). Бұл нұсқа жұмыс станциялары үшін оңтайлы болып табылады, сондықтан пайдаланушылар қайта жүктеудің ең қолайлы уақытын таңдай алады.

     Әдепкі бойынша, осы нұсқа таңдалған.

   - **Сұрауды қайталау жиілігі (мин)**

     Егер бұл нұсқа таңдалса, белгілі бір жиіліктегі бағдарлама пайдаланушыға операциялық жүйені қайта жүктеуді ұсынады.

     Әдепкі бойынша, параметр қосулы. Әдепкі бойынша аралық 5 минутты құрайды. Рұқсат етілген мәндер: 1-ден 1440 минутқа дейін.

     Егер параметр өшірулі болса, қайта жүктеу ұсынысы тек бір рет көрсетіледі.

   - **Келесі уақыттан кейін қайта іске қосу (мин)**

     Пайдаланушыға операциялық жүйені қайта жүктеуді ұсынғаннан кейін, бағдарлама көрсетілген уақыттан кейін мәжбүрлеп қайта жүктеуді орындайды.

Әдепкі бойынша, параметр қосулы. Әдепкі бойынша уақыт аралығы 30 минутты құрайды. Рұқсат етілген мәндер: 1-ден 1440 минутқа дейін.

- **Бұғатталған сеанстардағы бағдарламалардың мәжбүрлі жабылуы**

  Іске қосылған қолданбалар клиент құрылғысын қайта жүктеуге мүмкіндік бермеуі мүмкін. Мысалы, егер мәтіндік редакторда құжатпен жұмыс жасалса және өзгертулер сақталмаса, бағдарлама құрылғыны қайта жүктеуге мүмкіндік бермейді.

  Егер бұл параметр қосулы болса, құрылғыны қайта іске қоспас бұрын бұғатталған құрылғылардағы мұндай бағдарламалар мәжбүрлі түрде жабылады. Нәтижесінде, пайдаланушылар сақталмаған жұмысын жоғалтуы мүмкін.

  Егер бұл параметр өшірулі болса, бұғатталған құрылғы қайта жүктелмейді. Бұл құрылғыдағы тапсырманың күйі құрылғыны қайта іске қосу қажеттілігін көрсетеді. Пайдаланушылар бұғатталған құрылғыларда жұмыс істейтін барлық бағдарламаларды қолмен жауып, сол құрылғыларды қайта іске қосуы керек.

  Әдепкі бойынша, параметр өшірулі.

Шебердің келесі қадамына өтіңіз.

10. Есептік жазба параметрлерін белгілеңіз:

    - **Әдепкі есептік жазба**

      Тапсырма, сол тапсырманы орындайтын бағдарлама орнатылған және іске қосылған сол есептік жазбамен іске қосылады.

      Әдепкі бойынша, осы нұсқа таңдалған.

    - **Есептік жазбаны көрсету**

      Есептік жазба және **Құпиясөз** өрістерінде тапсырма іске қосылуы тиісті есептік жазба деректерін көрсетіңіз. Есептік жазбада тапсырманы орындау үшін қажетті құқықтар болуы керек.

    - **Есептік жазба**

      Тапсырманы іске қосатын есептік жазба.

    - **Құпиясөз**

      Тапсырманы іске қосатын есептік жазбаның құпиясөзі.

11. **Тапсырманы жасауды аяқтау** қадамында **Жасап болған соң, тапсырма туралы мәліметтерді ашу** параметрін қоссаңыз, тапсырма параметрлерінің орнатылған әдепкі мәндерін өзгертуге болады.

    Егер сіз бұл параметрді қоспасаңыз, тапсырма әдепкі бойынша белгіленген параметр мәндерімен жасалады. Орнатылған әдепкі параметрлер мәндерін кейінірек өзгертуге болады.

12. **Аяқтау** түймесін басыңыз.

    Шебер жұмысының нәтижесінде тапсырма жасалды. **Жасап болған соң, тапсырма туралы мәліметтерді ашу** параметрі қосулы болса, тапсырма параметрлерінің терезесі автоматты түрде ашылады. Бұл терезеде тапсырманың жалпы параметрлерін көрсетуге және қажет болса, тапсырма жасағаннан кезде көрсетілген параметрлерді өзгертуге болады.

> Тапсырмалар тізіміндегі жасалған тапсырма атауын басу арқылы тапсырма сипаттарының терезесін ашуға да болады.

Тапсырма жасалады, теңшеледі және тапсырмалар тізімінде, **Тапсырмалар** бөлімінде көрсетіледі.

13. Тапсырманы іске қосу үшін тапсырмалар тізімінен тапсырманы таңдап, **Іске қосу** түймесін басыңыз.

    Сондай-ақ тапсырма сипаттары терезесіндегі **Кесте** қойындысында тапсырманы іске қосу кестесін жасауға да болады.

    Кесте бойынша іске қосу параметрлерінің толық сипаттамасын тапсырманың жалпы параметрлерінен қараңыз.

Тапсырманы орындағаннан кейін таңдалған осалдықтар жабылады.

Үшінші тарап бағдарламаларындағы осалдықтарға арналған пайдаланушы түзетулері

Осалдықтарды түзету тапсырмасын пайдалану үшін, тапсырма параметрлерінде тізімделген үшінші тарап бағдарламаларындағы осалдықтарды түзету үшін бағдарламалық жасақтама жаңартуларын қолмен көрсету керек. *Осалдықтарды түзету* тапсырмасы басқа үшінші тарап қолданбалары үшін ұсынылған Microsoft қолданбаларының түзетулері мен пайдаланушылық түзетулерді пайдаланады.

Пайдаланушы түзетулері – әкімші осалдықтарды түзету мақсатымен орнату үшін қолмен көрсететін бағдарламалық жасақтама жаңартулары.

Үшінші тарап бағдарламаларындағы осалдықтарға арналған пайдаланушылық түзетулерді таңдау үшін:

1. Бағдарламаның негізгі терезесінде **Бағдарламалық жасақтаманы басқару** → **Патчтарды басқару** → **Бағдарламалық жасақтама осалдықтары** бөліміне өтіңіз.

   Басқарылатын құрылғыларда орнатылған үшінші тарап қолданбаларындағы осалдықтар тізімі бар бет ашылады.

2. Бағдарламалық жасақтама осалдықтары тізімінде пайдаланушылық түзетуді көрсеткіңіз келетін осалдық атауы бар сілтемеге өтіңіз.

   Таңдалған осалдықтың сипаттар терезесі ашылады.

3. Сол жақ тақтадан **Пайдаланушылық және басқа түзетулер** бөлімін таңдаңыз.

   Таңдалған бағдарламалық жасақтама осалдықтары үшін пайдаланушылық түзетулердің тізімі көрсетіледі.

4. **Қосу** түймесін басыңыз.

   Қолжетімді орнату пакеттері тізімі көрсетіледі. Көрсетілген орнату пакеттері тізімі **Бағдарламалық жасақтаманы басқару** → **Орнату пакеттері** қалтасындағы тізімге сай келеді.

   Егер сіз таңдалған осалдықты түзету үшін пайдаланушылық түзетуді қамтитын орнату пакетін жасамаған болсаңыз, **Жаңа** түймесін басу және орнату пакетін жасау шеберін іске қосу арқылы пакетті қазір жасауға болады.

5. Таңдалған осалдық үшін пайдаланушылық түзетуді (немесе пайдаланушылық түзетулерді) қамтитын орнату пакетін (немесе пакеттерін) таңдаңыз.

6. **Сақтау** түймесін басыңыз.

Бағдарламалық жасақтама осалдықтарына арналған пайдаланушылық түзетулерді қамтитын орнату пакеттері көрсетілген. *Осалдықтарды түзету* тапсырмасын іске қосқан кезде орнату пакеті орнатылады және қолданбадағы осалдық түзетіледі.

Барлық басқарылатын құрылғыларда анықталған бағдарламалардағы осалдықтар туралы ақпаратты қарау

Басқарылатын құрылғылардағы бағдарламалық жасақтаманы осалдықтарға сканерлегеннен кейін, қолданбаларда анықталған осалдықтар тізімін көруге болады. Басқару сервері иерархиясы үшін тапсырманы іске қоссаңыз, осалдықтары анықталған басқарылатын құрылғылар тізімін тек таңдалған Басқару сервері үшін көре аласыз.

Сондай-ақ, осалдықтар туралы есепті жасауға және көруге болады.

Барлық басқарылатын құрылғыларда анықталған бағдарламалардағы осалдықтар тізімін қарау үшін,

Бағдарламаның негізгі терезесінде **Операциялар** → **Патчтарды басқару** → **Бағдарламалық жасақтама осалдықтары** бөліміне өтіңіз.

Клиент құрылғысында табылған қолданбалардың осалдықтары тізімі көрсетіледі.

Қолданбаның осалдықтарының тізімін конфигурациялау үшін,

Қолданбаның осалдықтары тізімінің жоғарғы оң жақ бұрышында **Сүзгі** белгішесін ( ) басыңыз және қажетті сүзгіні таңдаңыз. Сонымен қатар, қолданбалардың осалдықтары тізімінің үстіндегі **Алдын ала орнатылған сүзгілер** ашылмалы тізімінде алдын ала орнатылған сүзгілердің бірін таңдай аласыз.

Тізімдегі кез келген осалдық туралы толық ақпаратты ала аласыз.

Қолданбалардың осалдықтары туралы ақпаратты алу үшін,

бағдарламалық жасақтама осалдықтары тізімінде осалдықтың атауы көрсетілген сілтемеден өтіңіз.

Бағдарламалық жасақтама осалдықтары сипаттары терезесі ашылады.

Таңдалған басқарылатын құрылғыларда анықталған бағдарламалардағы осалдықтар туралы ақпаратты қарау

Сіз осалдықтар туралы ақпаратты таңдалған Windows басқарылатын құрылғысында табылған бағдарламалардан көре аласыз.

Таңдалған басқарылатын құрылғыда анықталған бағдарламалық жасақтама осалдықтары тізімін көру үшін:

1. Бағдарламаның негізгі терезесінде **Активтерді басқару** → **Активтер (құрылғылар)** бөліміне өтіңіз.

   Басқарылатын құрылғылардың тізімі көрсетіледі.

2. Басқарылатын құрылғылар тізімінде, бағдарламаларда анықталған осалдықтарды көргіңіз келетін құрылғының атауы бар сілтемеден өтіңіз.

   Таңдалған құрылғы сипаттары терезесі ашылады.

3. Таңдалған құрылғы сипаттары терезесінде **Кеңейтілген** қойындысын таңдаңыз.

4. Сол жақ тақтадан **Бағдарламалық жасақтама осалдықтары** бөлімін таңдаңыз.

   Таңдалған басқарылатын құрылғыда табылған бағдарламалық жасақтама осалдықтары тізімі көрсетіледі.

Таңдалған бағдарламалық жасақтама осалдықтары сипаттарын көру үшін,

бағдарламалардағы осалдықтар тізіміндегі осалдық атауы бар сілтемеге өтіңіз.

Таңдалған бағдарламалық жасақтама осалдықтары сипаттары терезесі ашылады.

Басқарылатын құрылғылардағы осалдықтардың статистикасын қарау

Басқарылатын құрылғылардағы бағдарламалардағы әрбір осалдықтың статистикалық ақпаратын көруге болады. Статистика диаграммалар түрінде ұсынылған. Диаграмма келесі күйлері бар құрылғылардың санын көрсетеді:

- *Еленбеген: <құрылғылар саны>*. Егер сіз осалдық сипаттарында осалдықты елемеу параметрін қолмен орнатсаңыз, осы күй тағайындалады.
- *Түзетілген: <құрылғылар саны>*. Егер осалдықты түзету тапсырмасы сәтті аяқталса, осы күй белгіленеді.
- *Түзетуге жоспарланған: <құрылғылар саны>* Егер сіз осалдықтарды түзету тапсырмасын жасаған болсаңыз, бірақ тапсырма әлі аяқталмаған болса, осы күй белгіленеді.
- *Патч қолданылған: <құрылғылардың саны>*. Егер сіз осалдықты түзету үшін бағдарламалық жасақтаманы жаңартуды қолмен таңдаған болсаңыз, осы күй тағайындалады, бірақ бұл жаңарту осалдықты түзетпеді.
- *Түзету қажет: <құрылғылар саны>*. Осалдық кейбір басқарылатын құрылғыларда ғана жабылған болса, бірақ басқа басқарылатын құрылғыларда осалдықты түзету қажет болса, осы күй тағайындалады.

Басқарылатын құрылғылардағы осалдық статистикасын көру үшін:

1. Бағдарламаның негізгі терезесінде **Операциялар → Патчтарды басқару → Бағдарламалық жасақтама осалдықтары** бөліміне өтіңіз.

   Басқарылатын құрылғыларда табылған қолданбалардағы осалдықтар тізімі бар бет көрсетіледі.

2. Қажетті осалдықтың жанына жалаушаны қойыңыз.

3. **Құрылғылардағы осалдық статистикасы** түймесін басыңыз.

   Құрылғылардағы осалдық статистикасы түймесі, бірнеше осалдықты таңдаған болсаңыз, қолжетімді болмайды.

Осалдық күйінің диаграммасы көрсетіледі. Күйді басу арқылы, осалдықтың таңдалған күйі бар құрылғылардың тізімі ашылады.

Бағдарламалардағы осалдықтар тізімін мәтіндік файлға экспорттау

Көрсетілген осалдықтар тізімін CSV немесе TXT пішіміндегі файлға жүктеп алуға болады. Бұл файлдарды қауіпсіздік маманына жіберуге немесе статистикалық мақсаттар үшін сақтауға болады.

Барлық басқарылатын құрылғыларда анықталған бағдарламалардағы осалдықтар тізімін мәтіндік файлға экспорттау үшін:

1. Бағдарламаның негізгі терезесінде **Операциялар → Патчтарды басқару → Бағдарламалық жасақтама осалдықтары** бөліміне өтіңіз.

   Басқарылатын құрылғыларда табылған қолданбалардың осалдықтары тізімі көрсетіледі.

   Әдепкі бойынша, ағымдағы бетте көрсетілетін осалдықтар ғана экспортталады.

   Белгілі бір осалдықтарды ғана экспорттағыңыз келсе, сол осалдықтардың жанындағы құсбелгілерді қойыңыз.

2. Экспорттағыңыз келетін пішімге байланысты, **TXT файлына экспорттау** немесе **CSV файлына экспорттау** түймесін басыңыз. Осы түймелердің біреуі көрінбесе, көп нүктелі түймені басып, ашылмалы тізімнен қажетті нұсқаны таңдаңыз.

Қолданбаның осалдықтарының тізімі бар файл құрылғыңызға жүктеледі.

Таңдалған басқарылатын құрылғыда анықталған бағдарламалық жасақтама осалдықтары тізімін көру үшін:

1. Бағдарламаның негізгі терезесінде **Активтерді басқару → Активтер (құрылғылар)** бөліміне өтіңіз.

   Басқарылатын құрылғылардың тізімі көрсетіледі.

2. Басқарылатын құрылғылар тізімінде, бағдарламаларда анықталған осалдықтарды көргіңіз келетін құрылғының атауы бар сілтемеден өтіңіз.

   Таңдалған құрылғы сипаттары терезесі ашылады.

3. Таңдалған құрылғы сипаттары терезесінде **Кеңейтілген** қойындысын таңдаңыз.

4. Сол жақ тақтадан **Бағдарламалық жасақтама осалдықтары** бөлімін таңдаңыз.

Таңдалған басқарылатын құрылғыда табылған бағдарламалық жасақтама осалдықтары тізімі көрсетіледі.

Әдепкі бойынша, ағымдағы бетте көрсетілетін осалдықтар ғана экспортталады.

Белгілі бір осалдықтарды ғана экспорттағыңыз келсе, сол осалдықтардың жанындағы құсбелгілерді қойыңыз.

1. Экспорттағыңыз келетін пішімге байланысты, **TXT файлына экспорттау** немесе **CSV файлына экспорттау** түймесін басыңыз. Осы түймелердің біреуі көрінбесе, көп нүктелі түймені басып, ашылмалы тізімнен қажетті нұсқаны таңдаңыз.

Қолданбаның осалдықтарының тізімі бар файл құрылғыңызға жүктеледі.

Бағдарламалардағы осалдықтарды елемеу

Бағдарламалық жасақтама осалдықтарын елемеуіңіз және оларды түзетпеуіңіз мүмкін. Бағдарламалардағы осалдықтарды елемеу себептері, мысалы, келесідей болуы мүмкін:

- Сіз бағдарламадағы осалдықты ұйымыңыз үшін критикалық деп санамайсыз.
- Бағдарламалық жасақтама осалдықтарын түзету, осалдықты түзетуді қажет ететін бағдарламаның деректерін зақымдауы мүмкін екенін түсінесіз.
- Бағдарламалық жасақтама осалдықтары сіздің ұйымыңыздың желісіне қауіп төндірмейтініне сенімдісіз, өйткені сіз басқарылатын құрылғыларды қорғау үшін басқа шараларды қолданасыз.

Барлық басқарылатын құрылғылардағы немесе тек таңдалған басқарылатын құрылғылардағы бағдарламалардағы осалдықты елемеуге болады.

Барлық басқарылатын құрылғылардағы бағдарламалық жасақтама осалдықтарын өткізіп жіберу үшін:

1. Бағдарламаның негізгі терезесінде **Операциялар → Патчтарды басқару → Бағдарламалық жасақтама осалдықтары** бөліміне өтіңіз.

   Басқарылатын құрылғыларда табылған қолданбалардың осалдықтары тізімі көрсетіледі.

2. Бағдарламалық жасақтама осалдықтары тізімінде өткізіп жібергіңіз келетін бағдарламалық жасақтама осалдықтары атауын басыңыз.

   Бағдарламалық жасақтама осалдықтары сипаттары терезесі ашылады.

3. **Жалпы** қойындысында **Осалдықты елемеу** параметрін қосыңыз.

4. **Сақтау** түймесін басыңыз.

   Бағдарламалық жасақтама осалдықтары сипаттары терезесі жабылады.

Бағдарламалық жасақтама осалдықтары барлық басқарылатын құрылғыларда өткізіп жіберіледі.

Барлық басқарылатын құрылғылардағы қолданбалардың осалдықтарын өткізіп жіберу үшін:

1. Қолданбаның негізгі терезесінде **Активтерді басқару → Активтер (құрылғылар)** бөліміне өтіңіз.

   Басқарылатын құрылғылардың тізімі көрсетіледі.

2. Басқарылатын құрылғылар тізімінде бағдарламалық жасақтама осалдықтарын жіберіп алғыңыз келетін құрылғы атауымен сілтемеге өтіңіз.

   Құрылғы сипаттары терезесі ашылады.

3. Құрылғы сипаттары терезесінде **Кеңейтілген** бөлімін таңдаңыз.

4. Сол жақ тақтадан **Бағдарламалық жасақтама осалдықтары** бөлімін таңдаңыз.

   Құрылғыда табылған бағдарламалық жасақтама осалдықтары тізімі көрсетіледі.

5. Бағдарламалық жасақтама осалдықтары тізімінен таңдалған құрылғыда өткізіп жібергіңіз келетін осалдықты таңдаңыз.

   Бағдарламалық жасақтама осалдықтары сипаттары терезесі ашылады.

6. Қолданбалардың осалдықтары сипаттары терезесінде, **Жалпы** қойындысында **Осалдықты елемеу** параметрін қосыңыз.

7. **Сақтау** түймесін басыңыз.

   Бағдарламалық жасақтама осалдықтары сипаттары терезесі жабылады.

8. Құрылғының сипаттар терезесін жабыңыз.

Бағдарламалық жасақтама осалдықтары таңдалған құрылғыда өткізіп жіберіледі.

Өткізіп жіберілген бағдарламалық жасақтама осалдықтары *Осалдықтарды түзету* және *Қажетті жаңартуларды орнату және осалдықтарды түзету* тапсырмаларының жұмысы аяқталғаннан кейін жабылмайды. Бағдарламалардағы жетіспейтін осалдықтарды осалдықтар тізімінен сүзгі арқылы алып тастауға болады.

Kaspersky дерекқорынан үшінші тарап бағдарламасы үшін орнату пакетін жасау

Kaspersky Security Center Web Console сервері орнату пакеттері көмегімен үшінші тарап қолданбаларын қашықтан орнатуды орындауға мүмкіндік береді. Осындай үшінші тарап бағдарламалары тиісті Kaspersky дерекқорына қосылған. Дерекқор *Жаңартуларды Басқару серверінің қоймасына жүктеп алу* тапсырмасын бірінші рет іске қосу кезінде автоматты түрде жасалады.

Осалдықтар мен патчтарды басқару лицензиясы болған жағдайда ғана Kaspersky дерекқорынан үшінші тарап қолданбасы үшін орнату пакетін жасауға болады.

Kaspersky дерекқорынан үшінші тарап бағдарламасына арналған орнату пакетін жасау үшін:

1. Бағдарламаның негізгі терезесінде **Бағдарламалық жасақтаманы басқару** → **Орнату пакеттері** бөліміне өтіңіз.

2. **Қосу** түймесін басыңыз.

   Орнату пакетін жасау шебері іске қосылады. Шебердің жұмысын жалғастыру үшін **Келесі** түймесін басыңыз.

3. **Орнату пакетін жасау үшін Kaspersky дерекқорынан бағдарламаны таңдау** параметрін таңдаңыз.

   Бұл параметр Осалдықтар мен патчтарды басқару лицензиясы болған жағдайда қолжетімді.

   Шебердің келесі қадамына өтіңіз.

4. Орнату пакетін жасағыңыз келетін қолданбаны таңдаңыз.

   Шебердің келесі қадамына өтіңіз.

5. Ашылмалы тізімнен қажетті локализация тілін таңдап, Келесі түймесін басыңыз.

   Бұл қадам, бағдарлама бірнеше тілді ұсынса ғана көрсетіледі.

6. Орнату үшін лицензиялық келісімді қабылдау сұралса, шебердің **Лицензиялық келісімдер және Құпиялылық саясаттары** қадамында мына қадамдарды орындаңыз:

   a. Жеткізушінің веб-сайтындағы Лицензиялық келісімді оқу немесе лицензияны қажет ететін жаңартуларды көру үшін **Көрсету** сілтемесін басыңыз.

   b. **Мен осы соңғы пайдаланушы лицензиясы келісімінің шарттары мен талаптарын толықтай оқып шығып, түсінгенімді растаймын және қабылдаймын** жалаушасын орнатыңыз.

   c. Тізімде көрсетілген барлық Лицензиялық келісімдер мен құпиялылық саясаттарын қабылдау үшін **Барлығын қабылдау** түймесін басыңыз.

7. Шебердің **Жаңа орнату пакетінің атауы** қадамында, **Пакет атауы** өрісінде орнату пакетінің атауын көрсетіңіз және **Келесі** түймесін басыңыз.

   Құрылған орнату пакеті Басқару серверіне жүктелген. Орнату пакетін жасау шебері орнату пакетінің сәтті жасалғанын көрсететін хабарды көрсетеді.

8. **Аяқтау** түймесін басыңыз.

Жасалған орнату пакеті орнату пакеттерінің тізімінде көрсетіледі. Сіз *Бағдарламаны қашықтан орнату* тапсырмасын жасау немесе қайта конфигурациялау кезінде осы пакетті таңдай аласыз.

Осалдықтар мен патчтарды басқару лицензиясы болған жағдайда ғана Kaspersky дерекқорындағы үшінші тарап қолданбаларын орнату пакетін пайдаланып, *Бағдарламаны қашықтан орнату* тапсырмасын жасауға және қайта конфигурациялауға болады.

Kaspersky дерекқорынан үшінші тарап бағдарламасына арналған орнату пакетінің параметрлерін қарау және өзгерту

Егер сіз бұрын Kaspersky дерекқорында атап көрсетілген үшінші тарап бағдарламаларының қандай да бір орнату пакеттерін жасаған болсаңыз, онда сіз осы пакеттердің параметрлерін қарап, өзгерте аласыз.

Kaspersky дерекқорынан үшінші тарап қолданбасының орнату пакетінің параметрлерін өзгерту жүйелік Осалдықтар мен патчтарды басқаруға арналған лицензия болған жағдайда ғана қолжетімді.

Kaspersky дерекқорынан үшінші тарап бағдарламасына арналған орнату пакетінің параметрлерін қарау және өзгерту үшін:

1. Бағдарламаның негізгі терезесінде **Бағдарламалық жасақтаманы басқару** → **Орнату пакеттері** бөліміне өтіңіз.

2. Ашылған орнату пакеттері тізімінде тиісті пакеттің атын басыңыз.

   Сипаттар терезесі ашылады.

3. Қажет болса, параметрлерді өзгертіңіз.

4. **Сақтау** түймесін басыңыз.

Өзгерістер сақталды.

Kaspersky дерекқорынан үшінші тарап бағдарламасына арналған орнату пакетінің параметрлері

Үшінші тарап қолданбасының орнату пакетінің параметрлері келесі қойындыларда топтастырылған:

Төменде тізімделген параметрлердің барлығы әдепкі бойынша көрсетілмейді. **Сүзгі** түймесін басу және тізімнен сәйкес бағаналарын таңдау арқылы қажетті бағандарды қосуға болады.

- **Жалпы** қойыншасы:
  - Қолмен өзгертуге болатын орнату пакетінің атауын қамтитын енгізу өрісі.
  - **Бағдарлама**

    Орнату пакеті жасалған үшінші тарап бағдарламасының атауы.
  - **Нұсқа**

    Орнату пакеті жасалған үшінші тарап бағдарламасының нұсқа нөмірі.
  - **Өлшемі**

    Үшінші тарап бағдарламасына арналған орнату пакетінің өлшемі (килобайт түрінде).
  - **Жасалған күні**

    Үшінші тарап бағдарламасы үшін орнату пакетін жасау күні мен уақыты.
  - **Жолы**

    Үшінші тарап бағдарламасына арналған орнату пакеті орналасқан желілік қалтаға апаратын толық жол.
- **Орнату реті** қойыншасы:
  - **Қажетті жалпы жүйелік құрамдастарды орнату**

    Егер жалауша қойылса, жаңартуды орнатпас бұрын, бағдарлама автоматты түрде осы жаңартуды орнатуға қажетті барлық жалпыжүйелік құрамдастарды (алғышарттар) орнатады. Мысалы, мұндай алғышарттар операциялық жүйенің жаңартулары болуы мүмкін.

    Егер бұл параметр өшірулі болса, алғышарттарды қолмен орнату керек.

    Әдепкі бойынша, параметр өшірулі.

- Жаңарту сипаттарын көрсететін және келесі бағандарды қамтитын кесте:

  - **Атауы**

    Жаңарту атауы.

  - **Сипаттама**

    Жаңарту сипаттамасы.

  - **Көзі**

    Жаңарту көзі, яғни Microsoft немесе басқа үшінші тарап өндірушісі жаңартуды шығарды ма.

  - **Түрі**

    Жаңарту түрі, яғни жаңарту драйверге немесе бағдарламаға арналған ба.

  - **Санат**

    Microsoft жаңартулары үшін көрсетілетін Windows Server Жаңарту қызметтері (WSUS) санаттары (Критикалық жаңартулары, Анықтамалық жаңартулар, Драйверлер, Қосымша құрамдастардың пакеттері, Қауіпсіздік жаңартулары, Қызметтік пакеттер, Құралдар, Жинақтаушы жаңарту пакеттері, Жаңартулар немесе Алдыңғы нұсқалардың жаңартулары).

  - **MSRC бойынша маңыздылық деңгейі**

    Microsoft Security Response Center (MSRC) анықтаған жаңартудың маңыздылық деңгейі.

  - **Маңыздылық деңгейі**

    Kaspersky анықтаған жаңартудың маңыздылық деңгейі.

  - **Патчтың маңыздылық деңгейі**

    Kaspersky бағдарламаларына арналған болса, патчтың маңыздылық деңгейі.

  - **Мақала**

    Жаңарту сипаттамасы бар Білім базасындағы мақаланың идентификаторы.

  - **Бюллетень**

    Жаңарту сипаттамасы бар қауіпсіздік бюллетені идентификаторы.

  - **Орнатуға белгіленбеген (жаңа нұсқа)**

    Орнатуға белгіленбеген күйі жаңартылғаны/жаңартылмағаны көрсетіледі.

  - **Орнатуға белгіленген**

    Орнатуға белгіленген күйі жаңартылғаны/жаңартылмағаны көрсетіледі.

  - **Орнату**

    Орнатылуда күйі жаңартылғаны/жаңартылмағаны көрсетіледі.

  - **Орнатылған**

    Орнатылған күйі жаңартылғаны/жаңартылмағаны көрсетіледі.

- **Сәтсіз аяқталды**

  Сәтсіз аяқталды күйі жаңартылғаны/жаңартылмағаны көрсетіледі.

- **Қайта іске қосу керек**

  Қайта іске қосу керек күйі жаңартылғаны/жаңартылмағаны көрсетіледі.

- **Тіркелген**

  Жаңарту тіркелген күн мен уақыт көрсетіледі.

- **Интерактивті түрде орнатылады**

  Жаңартуды орнату кезінде пайдаланушы тәжірибесі қажет пе екені көрсетіледі.

- **Жаңартуды растау күйі**

  Жаңартуды орнатудың расталғаны/расталмағаны көрсетеді.

- **Тексеру**

  Жаңартудың ағымдағы шығарылымының нөмірі көрсетіледі.

- **Жаңарту идентификаторы**

  Жаңарту идентификаторы көрсетіледі.

- **Бағдарламаның нұсқасы**

  Бағдарлама жаңартылуы тиісті нұсқаның нөмірі көрсетіледі.

- **Ауыстырылып жатқан**

  Осы жаңартуды ауыстыра алатын басқа да жаңартулар көрсетіледі.

- **Ауыстыратын**

  Осы жаңартумен ауыстыруға болатын басқа да жаңартулар көрсетіледі.

- **Лицензиялық келісімнің шарттарын қабылдау керек**

  Лицензиялық келісімнің шарттарымен келісімді жаңарту керек пе екені көрсетіледі.

- **Сипаттамасының URL мекенжайы**

  Жаңарту өндірушісінің аты көрсетіледі.

- **Бағдарламалар тобы**

  Жаңарту қатысты болып табылатын бағдарламалар тобының аты көрсетіледі.

- **Бағдарлама**

  Жаңарту қатысты болып табылатын бағдарламаның аты көрсетіледі.

- **Локализация тілі**

  Жаңартудың локализация тілі көрсетіледі.

- **Орнатуға белгіленбеген (жаңа нұсқа)**

  Орнатуға белгіленбеген (жаңа нұсқа) күйі жаңартылғаны/жаңартылмағаны көрсетіледі.

- **Алғышарттарды орнатуды қажет етеді**

  Алғышарттарды орнатуды қажет етеді күйі жаңартылғаны/жаңартылмағаны көрсетіледі.

- **Жүктеп алу режимі**

  Жаңартуларды жүктеп алу режимі көрсетіледі.

- **Патч болып табылады**

  Жаңартудың патч болып табылады ма екені көрсетіледі.

- **Орнатылмаған**

  Орнатылмаған күйі жаңартылғаны/жаңартылмағаны көрсетіледі.

- **Жасалған күні**

- Орнату кезінде пәрмен жолының параметрлері ретінде пайдаланылатын орнату пакетінің параметрлерін, олардың аттарын, сипаттамаларын және мәндерін көрсететін **Параметрлер** қойындысы. Егер пакетте мұндай параметрлер болмаса, тиісті хабар көрсетіледі. Осы параметрлердің мәндерін өзгертуге болады.

- Орнату пакетінің нұсқаларын көрсететін және келесі бағандарды қамтитын **Тексерістер журналы** қойындысы:

  - **Тексеру** – орнату пакетінің нұсқа нөмірін көрсетеді.

  - **Уақыт** – орнату пакетінің параметрлерін өзгерту күні мен уақыты.

  - **Пайдаланушы** – орнату пакетінің параметрлерін өзгерткен пайдаланушының аты.

  - **Пайдаланушы құрылғысының IP мекенжайы** – нысан өзгертілген құрылғының IP-мекенжайы.

  - **Web Console консольдің IP мекенжайы** – нысан өзгертілген Kaspersky Security Center Web Console қолданбасының IP-мекенжайы.

  - **Әрекет** – осы тексерісте орнату пакетімен орындалған әрекеттер.

  - **Сипаттама** – орнату пакеті параметрлерінің өзгерістерін тексеру сипаттамасы.

    Әдепкі бойынша, тексеру сипаттамасы толтырылмаған. Тексеру сипаттамасын қосу үшін қажетті тексеруді таңдап, **Сипаттаманы өңдеу** түймесін басыңыз. Ашылған терезеде тексеру сипаттамасы мәтінін енгізіңіз.

Оқшауланған желіде осалдықтарды түзету

Бұл бөлімде Басқару серверлеріне қосылған және интернетке қатынасу мүмкіндігі жоқ басқарылатын құрылғылардағы үшінші тарап бағдарламаларындағы осалдықтарды түзету үшін қолдануға болатын әрекеттер сипатталған.

Оқшауланған желідегі үшінші тарап бағдарламаларының осалдықтарын түзету

Жаңартуларды орнатуға және оқшауланған желідегі басқарылатын құрылғыларда орнатылған үшінші тарап бағдарламаларының осалдықтарын түзетуге болады. Мұндай желілерге, интернетке қатынаса алмайтын Басқару серверлері мен оларға қосылған басқарылатын құрылғылар жатады. Мұндай желідегі осалдықтарды түзету үшін интернетке қосылған Басқару сервері қажет. Интернетке кіру мүмкіндігі бар Басқару серверін пайдалану арқылы патчтарды (қажетті жаңартуларды) жүктеп алуға және оларды оқшауланған Басқару серверлеріне тасымалдауға болады.

Сіз бағдарламалық жасақтама өндірушілері шығарған үшінші тарап бағдарламалық жасақтамасының жаңартуларын жүктей аласыз, бірақ Microsoft бағдарламалық жасақтамасының жаңартуларын Kaspersky Security Center көмегімен оқшауланған Басқару серверлерінде жүктей алмайсыз.

Оқшауланған желіде осалдықтарды түзету процесі туралы толығырақ білу үшін осы процестің сипаттамасы және схемасымен танысыңыз.

Алдын ала талаптар

Бастамас бұрын келесі әрекеттерді орындаңыз:

1. Интернетке қосылу және түзетулерді жүктеу үшін бір құрылғыны бөлектеңіз. Бұл құрылғы интернетке қатынасу мүмкіндігі бар Басқару сервері болып саналады.
2. Келесі құрылғыларда Kaspersky Security Center Linux бағдарламасының кемінде 15.1 нұсқасын орнатыңыз:
   - Интернетке қатынасу мүмкіндігі бар Басқару сервері ретінде әрекет ететін бөлектелген құрылғы.
   - Интернеттен оқшауланған Басқару серверлері (бұдан әрі – оқшауланған Басқару серверлері) рөлін атқаратын оқшауланған құрылғылар.
3. Әрбір Басқару серверінде жаңартулар мен түзетулерді жүктеп алу және сақтау үшін дискіде жеткілікті орын бар екеніне көз жеткізіңіз.

Кезеңдер

Оқшауланған Басқару серверлеріне қатысты басқарылатын құрылғыларда жаңартуларды орнату және үшінші тарап қолданбаларының осалдықтарын түзету келесі қадамдардан тұрады:

1. **Интернетке қатынасу арқылы Басқару серверін конфигурациялау**

   Үшінші тарап бағдарламалық жасақтамасының қажетті жаңартуларына сұрауларды өңдеу және жүктеп алу үшін интернетке қатынасу рұқсаты бар Басқару серверін дайындаңыз.

2 **Оқшауланған Басқару серверлерін конфигурациялау**

Оқшауланған Басқару серверлері үнемі қажетті жаңартулар тізімдерін құрастырып, интернетке қатынаса алатын Басқару сервері жүктейтін патчтарды өңдей алуы үшін осы оқшауланған Басқару серверлерін дайындаңыз. Конфигурациялаудан кейін, оқшауланған Басқару серверлері интернеттен патчтарды жүктеуге тырыспайды. Мұның орнына, олар патчтар арқылы жаңартуларды алады.

3 **Оқшауланған Басқару серверлеріне патчтарды беру және жаңартуларды орнату**

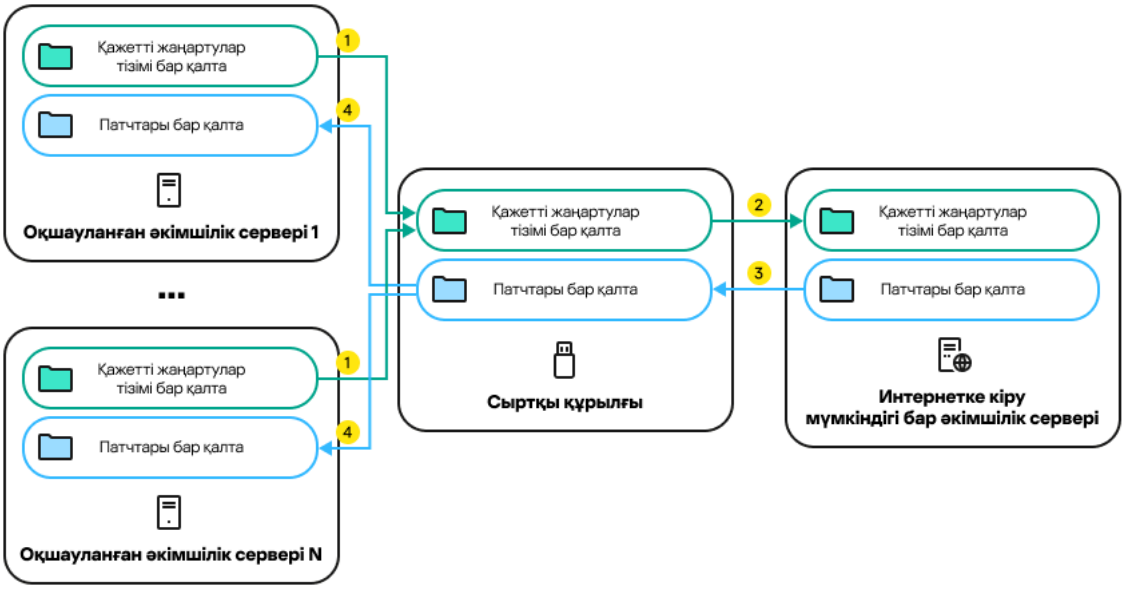
Басқару серверлерінің конфигурациясы аяқталғанда, жаңартулар мен патчтардың тізімдерін Интернетке кіру мүмкіндігі бар Басқару серверінен оқшауланған Басқару серверлеріне тасымалдауға болады. Әрі қарай, түзетулерден алынған жаңартулар *Қажетті жаңартуларды орнату және осалдықтарды түзету* тапсырмасы арқылы басқарылатын құрылғыларға орнатылады.

Нәтижелер

Осылайша, үшінші тарап қолданбаларының жаңартулары оқшауланған Басқару серверлеріне беріледі және қосылған басқарылатын құрылғыларға Kaspersky Security Center Linux көмегімен орнатылады. Өзіңізге қажетті жиілікпен, мысалы, күніне бір немесе бірнеше рет жаңартуларды алып тұру үшін Басқару серверлерін бір рет конфигурациялау жеткілікті.

Оқшауланған желідегі үшінші тарап бағдарламаларының осалдықтарын түзету туралы

Оқшауланған желідегі үшінші тарап қолданбаларындағы осалдықтарды түзету процесі төмендегі суретте көрсетілген. Сіз бұл процесті мезгіл-мезгіл қайталай аласыз.



Интернетке қатынасу мүмкіндігі бар Басқару сервері мен оқшауланған Басқару серверлері арасында патчтар мен қажетті жаңартулар тізімін беру процесі

Интернет желісінен оқшауланған әрбір Басқару сервері (бұдан әрі – оқшауланған Басқару сервері) осы Басқару серверіне қосылған басқарылатын құрылғыларға орнатылуы қажет жаңартулар тізімін қалыптастырады. Бұл жаңартулар тізімі екілік файлдардың жинағы ретінде белгілі бір қалтада сақталады, олардың әрқайсысында қажетті жаңартуды қамтитын патч сәйкестендіргіші бар. Сондықтан, тізімдегі әрбір файл белгілі бір патчқа сәйкес келеді.

Бұл қажетті жаңартулар тізімі оқшауланған Әкімшілік серверінен сыртқы құрылғы арқылы интернетке қатынасу мүмкіндігі бар бөлінген Басқару серверіне тасымалданады. Осыдан кейін, тағайындалған Басқару сервері интернеттен патчтарды жүктейді және оларды тағайындалған қалтаға салады.

Барлық патчтар жүктеліп, көрсетілген қалтаға орналастырылған кезде, олар қажетті жаңартулар тізімі алынған әрбір оқшауланған Басқару серверіне қайта тасымалданады. Патчтар әрбір оқшауланған Басқару серверінде олар үшін арнайы жасалған қалтада сақталады.

Нәтижесінде, *Қажетті жаңартуларды орнату және осалдықтарды түзету* тапсырмасы патчтарды іске қосады және оқшауланған Басқару серверлерінің басқарылатын құрылғыларына жаңартуларды орнатады.

Оқшауланған желідегі осалдықтарды түзету үшін интернетке қатынасу мүмкіндігі бар Басқару серверін конфигурациялау

Оқшауланған желіде осалдықтарды түзетуге және патчтарды беруге дайындалу үшін алдымен интернетке қатынасу арқылы Басқару серверін конфигурациялаңыз, содан кейін оқшауланған Басқару серверлерін конфигурациялаңыз.

Интернетке қатынасу мүмкіндігі бар Басқару серверін конфигурациялау үшін:

1. Басқару сервері орнатылған дискіде екі қалта жасаңыз:

   - қажетті жаңартулар тізіміне арналған қалта;
   - патчтарға арналған қалта.

   Бұл қалталарды қалауыңызша атауға болады.

2. KLAdmins тобына операциялық жүйені басқарудың стандартты құралдарын қолдана отырып, жасалған қалталарға **Өзгерту** құқығын беріңіз.

3. klscflag утилитасын пайдаланып, Басқару сервері сипаттарындағы қалтаға апаратын жолдарды көрсетіңіз.

   Пәрмен жолын іске қосыңыз және ағымдағы каталогты klscflag утилитасы бар каталогке өзгертіңіз. Klscflag утилитасы Басқару сервер орнатылған каталогте орналасқан. Әдепкі бойынша жол - /opt/kaspersky/ksc64/sbin.

4. Пәрмен жолында келесі пәрменді орындаңыз:

   - Түзетулерге арналған қалта жолын көрсету үшін:
     `klscflag -fset -pv klserver -n VAPM_DATA_EXPORT_PATH -t s -v "<қалта жолы>"`
   - Қажетті жаңартулар тізімі үшін қалта жолын белгілеу үшін:
     `klscflag -fset -pv klserver -n VAPM_REQ_IMPORT_PATH -t s -v "<қалта жолы>"`

   Мысалы: `klscflag -fset -pv klserver -n VAPM_DATA_EXPORT_PATH -t s -v "/ПатчтарғаАрналғанҚалта"`

5. Қажет болса, klscflag утилитасын пайдаланып, Басқару сервері жаңа түзету сұрауларын қаншалықты жиі тексеруі керек екенін көрсетіңіз:
   `klscflag -fset -pv klserver -n VAPM_DATA_EXPORT_PERIOD_SEC -t d -v <секундтардағы мән>`

   Әдепкі бойынша, 120 секунд мәні көрсетілген.

Мысалы: `klscflag -fset -pv klserver -n VAPM_DATA_EXPORT_PERIOD_SEC -t d -v 120`

6. Басқарылатын құрылғыларда орнатылған үшінші тарап бағдарламаларының патчтары туралы ақпаратты алу үшін *Осалдықтарды және қажетті жаңартуларды іздеу* тапсырмасын жасаңыз және тапсырманы орындау кестесін конфигурациялаңыз.

7. Осалдықтарды түзету мақсатымен пайдаланылатын үшінші тарап бағдарламаларына арналған патчтарды көрсету үшін *Осалдықтарды түзету* тапсырмасын жасаңыз және тапсырмалар кестесін конфигурациялаңыз.

   Тапсырма кестесінде көрсетілгеннен ертерек орындалуын қаласаңыз, тапсырмаларды қолмен іске қосыңыз. Тапсырмаларды іске қосу реті маңызды. *Осалдықтарды түзету* тапсырмасы *Осалдықтарды және қажетті жаңартуларды іздеу* тапсырмасы аяқталғаннан кейін іске қосылуы керек.

8. Басқару сервері қызметін қайта іске қосыңыз.

Интернетке қатынасу мүмкіндігі бар Басқару сервері жаңартуларды жүктеуге және оқшауланған Басқару серверлеріне жіберуге дайын. Осалдықтарды түзетуді бастамас бұрын, оқшауланған Басқару серверлерін конфигурациялаңыз.

Оқшауланған желідегі осалдықтарды түзету үшін оқшауланған Басқару серверлерін конфигурациялау

Интернетке қатынасу мүмкіндігі бар Басқару серверін конфигурациялау аяқталғаннан кейін, оқшауланған Басқару серверлеріне қосылған басқарылатын құрылғыларда осалдықтарды түзете алу және жаңартуларды орната алу үшін желіңіздегі әрбір оқшауланған Басқару серверін дайындаңыз.

Оқшауланған Басқару серверлерін конфигурациялау үшін, Басқару серверінің әрқайсысы үшін келесі әрекеттерді орындаңыз:

1. Осалдықтар мен патчтарды басқару үшін лицензиялық кілтті белсендіріңіз.

2. Басқару сервері орнатылған дискіде екі қалта жасаңыз:

   - қажетті жаңартулар тізіміне арналған қалта;
   - патчтарға арналған қалта.

   Бұл қалталарды қалауыңызша атауға болады.

3. KLAdmins тобына операциялық жүйені басқарудың стандартты құралдарын қолдана отырып, жасалған қалталарға **Өзгерту** құқығын беріңіз.

4. klscflag утилитасын пайдаланып, Басқару сервері сипаттарындағы қалтаға апаратын жолдарды көрсетіңіз.

   Пәрмен жолын іске қосыңыз және ағымдағы каталогты klscflag утилитасы бар каталогке өзгертіңіз. Klscflag утилитасы Басқару сервер орнатылған каталогте орналасқан. Әдепкі бойынша жол - /opt/kaspersky/ksc64/sbin.

5. Пәрмен жолында келесі пәрменді орындаңыз:

   - Түзетулерге арналған қалта жолын көрсету үшін:
     `klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_PATH -t s -v "<қалта жолы>"`

- Қажетті жаңартулар тізімі үшін қалта жолын белгілеу үшін:
  `klscflag -fset -pv klserver -n VAPM_REQ_EXPORT_PATH -t s -v "<қалта жолы>"`

Мысалы: `klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_PATH -t s -v "/FolderForPatches"`

6. Қажет болса, klscflag утилитасын пайдаланып, қашықтағы Басқару сервері жаңа патчтарды қаншалықты жиі тексеруі керек екенін көрсетіңіз:
   `klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_PERIOD_SEC -t d -v <секундтардағы мән>`

   Әдепкі бойынша, 120 секунд мәні көрсетілген.

   Мысалы: `klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_PERIOD_SEC -t d -v 120`

7. Қажет болса, патчтардың SHA256 хэштерін есептеу үшін klscflag утилитасын пайдаланыңыз:
   `klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_VERIFY_HASH -t d -v 1`

   Осы пәрменді орындап болған соң, сіз патчтарды оқшауланған Басқару серверіне ауыстырған кезде өзгертілмегеніне және қажетті жаңартуларды қамтитын дұрыс патчтарды алғаныңызға көз жеткізе аласыз.

   Әдепкі бойынша, Kaspersky Security Center Linux қолданбасы SHA256 патч хэштерін есептемейді. Егер сіз осы параметрді қоссаңыз, патчтарды оқшауланған Басқару сервері алғаннан кейін, Kaspersky Security Center Linux бағдарламасы олардың хэштерін есептейді және алынған мәндерді Басқару серверінің дерекқорында сақталған хэштермен салыстырады. Егер есептелген хэш дерекқордағы хэшке сәйкес келмесе, қате пайда болып, дұрыс емес патчтарды ауыстыру қажет болады.

8. Басқарылатын құрылғыларда орнатылған үшінші тарап бағдарламаларының патчтары туралы ақпаратты алу үшін *Осалдықтарды және қажетті жаңартуларды іздеу* тапсырмасын жасаңыз және тапсырманы орындау кестесін конфигурациялаңыз.

9. Осалдықтарды түзету мақсатымен пайдаланылатын үшінші тарап бағдарламаларына арналған патчтарды көрсету үшін *Осалдықтарды түзету* тапсырмасын жасаңыз және тапсырмалар кестесін конфигурациялаңыз.

   Тапсырма кестесінде көрсетілгеннен ертерек орындалуын қаласаңыз, тапсырмаларды қолмен іске қосыңыз. Тапсырмаларды іске қосу реті маңызды. *Осалдықтарды түзету* тапсырмасы *Осалдықтарды және қажетті жаңартуларды іздеу* тапсырмасы аяқталғаннан кейін іске қосылуы керек.

10. Басқару сервері қызметін қайта іске қосыңыз.

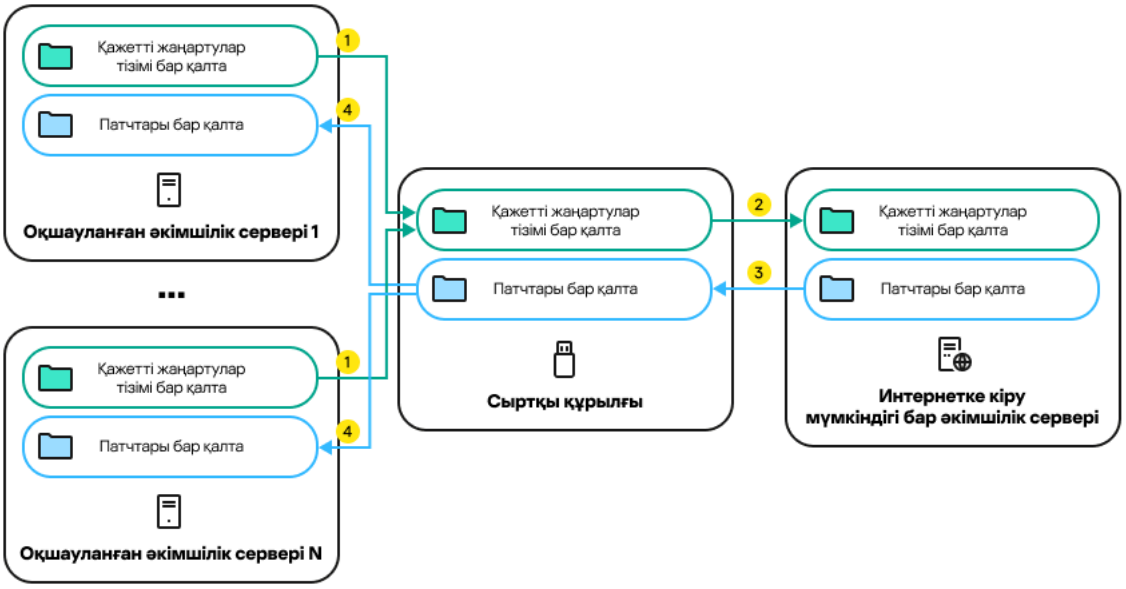
Барлық Басқару серверлерін орнатқаннан кейін, сіз түзетулер мен қажетті жаңартулар тізімдерін жылжыта аласыз және оқшауланған желідегі басқарылатын құрылғылардағы үшінші тарап қолданбаларының осалдықтарын түзете аласыз.

Оқшауланған желіде түзетулерді беру және жаңартуларды орнату

Басқару серверлерін конфигурациялау аяқталғаннан кейін, сіз патчтарды қажетті жаңартулармен бірге интернетке қатынасу мүмкіндігі бар Басқару серверінен оқшауланған Басқару серверлеріне ауыстыра аласыз. Жаңартуларды қажет жиілікпен, мысалы күніне бір немесе бірнеше рет беруге және орнатуға болады.

Сыртқы диск сияқты алынбалы диск Басқару серверлері арасында патчтарды және қажетті жаңартулар тізімін тасымалдау үшін қажет. Сыртқы дискіде патчтарды жүктеу және сақтау үшін жеткілікті орын бар екеніне көз жеткізіңіз.

Патчтар мен қажетті жаңартулар тізімін беру процесі төмендегі суретте көрсетілген:



Интернетке қатынасу мүмкіндігі бар Басқару сервері мен оқшауланған Басқару серверлері арасында патчтар мен қажетті жаңартулар тізімін беру процесі

Оқшауланған Басқару серверлеріне қосылған басқарылатын құрылғыларда жаңартуларды орнату және осалдықтарды түзету үшін:

1. *Қажетті жаңартуларды орнату және осалдықтарды түзету* тапсырмасы әлі іске қосылмаса, оны іске қосыңыз.

2. Сыртқы дискіні кез келген оқшауланған Басқару серверіне қосыңыз.

3. Сыртқы дискіде екі қалта жасаңыз: біреуі – қажетті жаңартулар тізіміне, екіншісі – патчтарға арналған. Бұл қалталарды қалауыңызша атауға болады.

   Егер сіз бұл қалталарды бұрын жасаған болсаңыз, оларды тазалаңыз.

4. Әрбір оқшауланған Басқару серверінен қажетті жаңартулар тізімін көшіріп, осы тізімді сыртқы дискідегі қажетті жаңартулар тізіміне арналған қалтаға салыңыз.

   Нәтижесінде, сіз барлық оқшауланған Басқару серверлерінен алынған барлық тізімдерді бір қалтаға біріктіресіз. Бұл қалтада барлық оқшауланған Басқару серверлеріне қажет патч идентификаторлары бар екілік файлдар болуы керек.

5. Сыртқы дискіні интернетке қатынасу мүмкіндігі бар Басқару серверіне қосыңыз.

6. Қажетті жаңартулар тізімін сыртқы дискіден көшіріп, осы тізімді интернетке қатынасу мүмкіндігі бар Басқару серверіндегі қажетті жаңартулар тізіміне арналған қалтаға салыңыз.

   Барлық қажетті патчтар автоматты түрде интернеттен Басқару серверіндегі патчтар қалтасына жүктеледі. Бұған бірнеше сағат кетуі мүмкін.

7. Барлық қажетті патчтардың жүктелгеніне көз жеткізіңіз. Ол үшін келесі әрекеттердің бірін орындауға болады:

   - Интернетке қатынасу мүмкіндігі бар Басқару серверіндегі патчтар үшін қалтаны тексеріңіз. Қажетті жаңартулар тізімінде көрсетілген барлық түзетулер қажетті қалтаға жүктелуі керек. Егер аздаған түзету қажет болса, бұл ыңғайлырақ.

   - Shell-скрипт сияқты арнайы скриптті дайындаңыз. Егер сіз көп патч алсаңыз, онда барлық түзетулердің жүктелгенін өзіңізге тексеру қиын болады. Мұндай жағдайларда, тексеруді автоматтандырған дұрыс.

8. Патчтарды интернетке қатынасу мүмкіндігі Басқару серверінен көшіріп, сыртқы дискідегі тиісті қалтаға салыңыз.

9. Патчтарды әр оқшауланған Басқару серверіне тасымалдаңыз. Патчтарды өздеріне арналған арнайы қалтаға салыңыз.

Нәтижесінде, әрбір оқшауланған Басқару сервері ағымдағы Басқару серверіне қосылған басқарылатын құрылғылар үшін қажетті жаңартулардың ағымдағы тізімін жасайды. Қажетті жаңартулардың тізімін алғаннан кейін Басқару сервері интернеттен патчтарды жүктейді. Осы патчтар оқшауланған Басқару серверлерінде пайда болған кезде, *Қажетті жаңартуларды орнату және осалдықтарды түзету* тапсырмасы патчтарды өңдейді. Осылайша, басқарылатын құрылғыларға жаңартулар орнатылады және үшінші тарап қолданбаларындағы осалдықтар түзетіледі.

Қажетті жаңартуларды орнату және осалдықтарды түзету тапсырмасын орындаған кезде Басқару серверінің құрылғысына артық жүктеме түсірмеңіз және *Басқару сервері деректерінің сақтық көшірмесін жасау* тапсырмасын іске қоспаңыз (бұл да артық жүктелуге себеп болады). Нәтижесінде, *Қажетті жаңартуларды орнату және осалдықтарды түзету* тапсырмасы үзіледі, ал жаңартулар орнатылмайды. Бұл жағдайда, сіз бұл тапсырманы қолмен қайта бастауыңыз немесе тапсырманың конфигурацияланған кесте бойынша басталуын күтуіңіз керек.

Оқшауланған желіде патчтарды жіберу және жаңартуларды орнату мүмкіндігін өшіру

Оқшауланған Басқару серверлеріне түзетулерді жіберуді өшіруге болады, мысалы, егер сіз оқшауланған желіден бір немесе бірнеше Басқару серверін шығаруды шешсеңіз. Осылайша, сіз түзетулер санын және оларды жүктеу уақытын қысқарта аласыз.

Оқшауланған Басқару серверлеріне патчтарды тасымалдауды өшіру үшін:

1. Егер сіз барлық Басқару серверлерін оқшаулаудан шығарғыңыз келсе, интернетке қатынасу мүмкіндігі бар Басқару серверінің сипаттарында патч болжалды қалталарына апаратын жолдарды және қажетті жаңартулар тізімін жойыңыз. Егер сіз таңдалған Басқару серверлерінің оқшауланған желіде болуын қаласаңыз, бұл қадамды өткізіп жіберіңіз.

   Пәрмен жолын іске қосыңыз және ағымдағы каталогты klscflag утилитасы бар каталогке өзгертіңіз. Klscflag утилитасы Басқару сервер орнатылған каталогте орналасқан. Әдепкі бойынша жол - /opt/kaspersky/ksc64/sbin.

   Пәрмен жолында келесі пәрменді орындаңыз:

   - Патч қалтасына апаратын жолды жою үшін:
     ```
     klscflag -fset -pv klserver -n VAPM_DATA_EXPORT_PATH -t s -v ""
     ```

- Қажетті жаңартулар тізімі бар қалтаға апаратын жолды жою үшін:
  ```
  klscflag -fset -pv klserver -n VAPM_REQ_IMPORT_PATH -t s -v ""
  ```

2. Қалтаға апаратын жолдарды жойған болсаңыз, Интернетке кіру мүмкіндігі бар Басқару сервері қызметін қайта іске қосыңыз.

3. Оқшауланғыңыз келетін әрбір оқшауланған Басқару серверінің сипаттарында патч қалталарына апаратын жолдарды және қажетті жаңартулар тізімін жойыңыз.

   root құқықтары бар есептік жазбадағы пәрмендер желісінде келесі пәрменді іске қосыңыз:

   - Патч қалтасына апаратын жолды жою үшін:
     ```
     klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_PATH -t s -v ""
     ```

   - Қажетті жаңартулар тізімі бар қалтаға апаратын жолды жою үшін:
     ```
     klscflag -fset -pv klserver -n VAPM_REQ_EXPORT_PATH -t s -v ""
     ```

4. Қалталарға апаратын жолдар жойылған әрбір Басқару сервері қызметін қайта іске қосыңыз.

Басқару серверін Интернетке кіру мүмкіндігімен қайта конфигурациялаған болсаңыз, патчтар енді Kaspersky Security Center Linux арқылы тасымалданбайды.

Егер сіз тек белгілі бір Басқару серверлерін қайта конфигурациялап, оларды оқшауланған желіден жойсаңыз, олар енді Kaspersky Security Center Linux арқылы патчтарды алмайды. Оқшауланған желіде қалған Басқару серверлері ғана патчтарды алуды жалғастырады.

Егер сіз болашақта ажыратылған оқшауланған Басқару серверлеріндегі осалдықтарды түзетуді бастағыңыз келсе, онда сіз осы Басқару серверлері мен интернетке қатынасу мүмкіндігі бар Басқару серверін тағы бір рет конфигурациялауыңыз керек.

API анықтамалық нұсқаулығы

Kaspersky Security Center OpenAPI анықтамалық нұсқаулығы келесі мәселелерді шешуге арналған:

- Автоматтандыру және конфигурациялау. Қолмен орындағыңыз келмейтін тапсырмаларды автоматтандыруға болады. Мысалы, әкімші ретінде сіз Kaspersky Security Center OpenAPI интерфейсін басқару топтарының құрылымын әзірлеуді жеңілдететін және оны өзекті күйде ұстайтын сценарийлерді құру және іске қосу үшін пайдалана аласыз.

- Пайдаланушы әзірлемесі. OpenAPI көмегімен клиенттік бағдарламаны жасауға болады.

OpenAPI анықтамалық нұсқаулығынан қажетті ақпаратты табу үшін экранның оң жағындағы іздеу өрісін пайдалануға болады.

OpenAPI анықтамалық нұсқаулығы

Сценарийлер мысалы

OpenAPI анықтамалық нұсқаулығында төмендегі кестеде көрсетілген Python сценарийлерінің мысалдары бар. Мысалдар OpenAPI әдістерін қалай шақыруға болатынын және желіні қорғаудың әртүрлі тапсырмаларын автоматты түрде орындауға болатынын көрсетеді, мысалы, "негізгі/қосалқы" иерархияны құру, Kaspersky Security Center Linux бағдарламасында тапсырмаларды іске қосу немесе тарату нүктелерін тағайындау. Сіз мысалдарды сол күйінде басқара аласыз немесе олардың негізінде жеке сценарийлер жасай аласыз.

OpenAPI әдістерін шақыру және скриптілерді іске қосу үшін:

Басқару сервері орнатылған құрылғыда KlAkOAPI.tar.gz мұрағатынан KlAkOAPI пакетін орнатыңыз.

KlAkOAPI пакеті әдеттегі операцияларды орындайтын үлгілер жиынын қамтиды. OpenAPI әдістерін шақыруға, үлгілерді және скриптілеріңізді тек басқару сервері мен KlAkOAPI пакеті орнатылған құрылғыларда іске қосуға болады. Осы пакетті қамтитын KlAkOAPI.tar.gz мұрағаты Kaspersky Security Center Linux орнату қалтасында орналасқан.

Kaspersky Security Center OpenAPI пайдаланушы сценарийлері мен әдістері мысалдарын салыстыру

Мысалы	Мысалдың мақсаты	Сценарий
KlAkParams оқиғалар журналы	`klAkParams` деректер құрылымын пайдалану арқылы деректерді шығарып, өңдей аласыз. Мысалда осы деректер құрылымымен қалай жұмыс істеу керектігі көрсетілген. Шығару мысалын әртүрлі тәсілдермен көрсетуге болады. HTTP әдісін жіберу үшін деректерді алуға немесе оларды кодта пайдалануға болады.	Бақылау және есеп беру
"Негізгі/қосалқы" иерархияны құру және жою	Сіз қосалқы Басқару серверін қосып, осылайша "Басты сервер - қосалқы сервер" иерархиялық қатынасын орната аласыз. Немесе қосалқы Басқару серверін иерархиядан шығаруға болады.	Басқару серверлерінің иерархиясын жасау: қосалқы Басқару серверін қосу және Басқару серверлерінің иерархиясын жою
Желі тізімінің файлдарын көрсетілген құрылғыға қосылым шлюзі арқылы жүктеңіз	Сіз өзіңіздің құрылғыңыздағы Желілік агентке қосылым шлюзі арқылы қосыла аласыз, содан кейін желілер тізімі бар файлды компьютерге жүктей аласыз.	Тарату нүктелері мен қосылым шлюздерін конфигурациялау

Мысалы	Мысалдың мақсаты	Сценарий
Негізгі Басқару сервері қоймасында сақталған лицензиялық кілтті қосалқы Басқару серверлеріне орнатыңыз	Сіз негізгі Басқару серверіне қосыла аласыз, одан қажетті лицензиялық кілтті жүктей аласыз және сол кілтті иерархияға кіретін барлық қосалқы Басқару серверлеріне жібере аласыз.	Басқарылатын бағдарламаларды лицензиялау
Пайдаланушының тиімді құқықтары туралы есепті жасаңыз	Сіз әртүрлі есептерді жасай аласыз. Мысалы, сіз осы мысалды қолдана отырып, тиімді пайдаланушы құқықтары туралы есеп жасай аласыз. Бұл есепте пайдаланушының тобы мен рөліне байланысты құқықтары туралы ақпарат берілген. Есепті HTML, PDF немесе Excel пішімінде жүктеуге болады.	Есепті жасау және қарау
Құрылғыда тапсырманы іске қосыңыз	Сіз өзіңіздің құрылғыңыздағы Желілік агентке қосылым шлюзі арқылы қосыла аласыз, содан кейін қажетті тапсырманы іске қоса аласыз.	Тапсырманы қолмен іске қосу
Топтағы құрылғылар үшін тарату нүктелерін тіркеу	Сіз басқарылатын құрылғыларды тарату нүктелеріне тағайындай аласыз (бұрын "жаңарту агенттері" деп аталған).	Kaspersky дерекқорлары мен бағдарламаларын жаңарту
Барлық топтарды атап көрсету	Басқару топтарымен әртүрлі әрекеттерді орындауға болады. Мысалда келесілерді қалай орындау керектігі көрсетілген: • "Басқарылатын құрылғылар" түбірлік тобы идентификаторын алу. • Топ иерархиясы бойынша жылжытуға болады. • Топтардың толық иерархиясын олардың атаулары мен ұяшықтарымен бірге алыңыз.	Басқару серверін конфигурациялау
Тапсырмаларды тізімдеу, тапсырмалар статистикасын сұрау және тапсырмаларды іске қосу	Сіз келесі ақпаратты оқып таныса аласыз: • Тапсырманы орындау тарихы. • Тапсырманың ағымдағы күйі. • Әртүрлі күйлердегі тапсырмалар саны. Сондай-ақ, сіз тапсырманы іске қоса аласыз. Әдепкі бойынша, мысал статистиканы шығарғаннан кейін тапсырманы іске қосады.	Тапсырмаларды басқару
Тапсырманы жасау және іске қосу	Сіз тапсырманы жасай аласыз. Мысалда келесі тапсырма параметрлерін көрсетіңіз: • Түрі • Іске қосу тәсілі • Атауы • Тапсырма қолданылатын құрылғы тобы Әдепкі бойынша, мысалда "Хабарды көрсету" түріндегі тапсырма жасалады. Бұл тапсырманы барлық басқарылатын Басқару сервері құрылғылары үшін іске қосуға болады. Қажет болса, сіз өзіңіздің тапсырма параметрлерін көрсете аласыз.	Тапсырманы жасау
Лицензиялық кілттерді атап көрсету	Басқару серверінің басқарылатын құрылғыларында орнатылған Kaspersky бағдарламаларына арналған барлық белсенді лицензиялық кілттердің тізімін алуға болады. Тізімде әрбір лицензиялық кілт туралы егжей-тегжейлі мәлімет, мысалы атауы, түрі немесе жарамдылық мерзімі келтірілген.	Қолданылатын лицензиялық кілттер туралы ақпаратты қарап шығу
Ішкі пайдаланушыны жасау және іздеу	Есепті жазбаны одан әрі жұмыс істеу үшін жасай аласыз.	Ішкі пайдаланушының есептік жазбасын қосу
Пайдаланушы санатын жасау	Сіз қажетті параметрлері бар бағдарламалар санатын жасай аласыз.	Қолмен толықтырылатын бағдарламалар санатын жасау
Пайдаланушыларды SrvView арқылы атап көрсету	Сіз Басқару серверінен егжей-тегжейлі ақпаратты сұрау үшін SrvView класын қолдана аласыз. Мысалы, осы мысалды қолдана отырып, пайдаланушылар тізімін ала аласыз.	Пайдаланушылар мен пайдаланушы рөлдерді басқару
Ішкі пайдаланушыларды жасаңыз, Android орнату пакетін жасаңыз және электрондық поштамен жіберіңіз	SecurityPolicy класы арқылы ішкі пайдаланушыларды, Android орнату пакетін жасап, оны пайдаланушыларға электрондық пошта арқылы жібере аласыз.	Ішкі пайдаланушының есептік жазбасын қосу

OpenAPI арқылы Kaspersky Security Center Linux бағдарламасымен өзара әрекеттесетін бағдарламалар

Кейбір бағдарламалар OpenAPI арқылы Kaspersky Security Center Linux бағдарламасымен өзара әрекеттеседі. Мұндай қолданбаларға, мысалы, Kaspersky мақсатты шабуылдардан қорғау платформасы немесе Kaspersky Security for Virtualization кіреді. Бұл сонымен қатар OpenAPI негізінде сіз әзірлейтін арнаулы клиенттік қолданба болуы мүмкін.

OpenAPI арқылы Kaspersky Security Center Linux бағдарламасымен өзара әрекеттесетін бағдарламалар Басқару серверіне қосылады. Басқару серверіне қосылу үшін рұқсат етілген IP мекенжайларының тізімін конфигурациялаған болсаңыз, Kaspersky Security Center Linux OpenAPI пайдаланатын бағдарламалар орнатылған құрылғылардың IP мекенжайларын қосыңыз. Сіз қолданатын бағдарлама OpenAPI-мен жұмыс істейтінін білу үшін осы бағдарламаның анықтамасын қараңыз.

Провайдерлер үшін үздік тәжірибелер

Бұл бөлімде Kaspersky Security Center Linux жүйесін конфигурациялау және пайдалану жолы туралы ақпарат берілген.

Құжатта бағдарламаны орналастыру, конфигурациялау және пайдалану бойынша ұсыныстар, сондай-ақ бағдарлама жұмыс істеген кезде туындайтын типтік мәселелерді шешу тәсілдері бар.

Kaspersky Security Center Linux орналастыруды жоспарлау

Kaspersky Security Center Linux құрамдастарын ұйым желісінде орналастыруды жоспарлағанда, жобаның өлшемі мен ауқымын, әсіресе, келесі факторларды есепке алуыңыз керек:

- Құрылғылардың жалпы санын
- MSP клиенттерінің саны

Бір басқару сервері көп дегенде 50 000 құрылғыға қолдау көрсетеді. Ұйым желісіндегі құрылғылардың жалпы саны 50 000-нан асса, сервер провайдерінің жағында бірнеше басқару серверін орнату және орталықтан ыңғайлы түрде басқару үшін иерархияға біріктіру керек.

Бір басқару серверінде 500-ге дейін виртуалды сервер жасауға болады, сондықтан әрбір 500 MSP клиентіне бөлек басқару сервері қажет.

Орналастыруды жоспарлау кезеңінде Басқару серверіне X.509 арнайы сертификатын белгілеу қажеттілігін ескеру қажет. Басқару серверіне X.509 арнайы сертификатын белгілеу келесі жағдайларда орынды болуы мүмкін (толық емес тізім):

- SSL termination proxy арқылы SSL трафигін инспекциялау үшін;
- сертификат өрістерінің қажетті мәндерін белгілеу үшін;
- сертификаттың қажетті криптографиялық беріктігін қамтамасыз ету үшін.

Басқару серверіне интернеттен қатынасуды ұсыну

Клиенттің желісінде орналастырылған құрылғылар Басқару серверіне интернет арқылы жүгіне алуы үшін, Басқару серверінің келесі порттарын қолжетімді ету керек:

- 13000 TCP – Басқару серверінің TLS порты, осы портқа клиент желісінде орналастырылған Желілік агенттер қосылады
- 8061 TCP – автономды пакеттерді Kaspersky Security Center Web Console құралдары көмегімен жариялауға арналған HTTPS порты

- 8060 TCP – автономды пакеттерді Kaspersky Security Center Web Console құралдары көмегімен жариялауға арналған HTTP порты
- 13292 TCP – бұл TLS порты тек ұялы құрылғыларды басқару қажет болғанда ғана керек
- 8080 TCP – Kaspersky Security Center Web Console-ге арналған HTTPS порты

Kaspersky Security Center Linux стандартты конфигурациясы

MSP серверлерінде бір немесе бірнеше Басқару сервері орналасқан. Серверлер саны қолжетімді аппараттық жасақтаманың болуына байланысты, сондай-ақ қызмет көрсетілетін MSP клиенттерінің санына немесе басқарылатын құрылғылардың жалпы санына байланысты таңдалуы мүмкін.

Бір басқару сервері көп дегенде 50 000 құрылғыға қолдау көрсетеді. Таяу болашақта басқарылатын құрылғылардың санын көбейту мүмкіндігін ескеру қажет: бір Басқару серверіне біршама аз құрылғыларды қосу қажет болуы мүмкін.

Бір басқару серверінде 500-ге дейін виртуалды сервер жасауға болады, сондықтан әрбір 500 MSP клиентіне бөлек басқару сервері қажет.

Егер бірнеше Сервер болса, оларды иерархияға біріктіру ұсынылады. Басқару серверлерінің иерархиясының болуы саясат пен тапсырмалардың қайталануын болдырмауға, барлық басқарылатын құрылғылардың көпшілігімен олардың барлығы бір Басқару серверімен басқарылатындай жұмыс істеуге: құрылғыларды іздеуге, құрылғы таңдауларын жасауға, есептер жасауға мүмкіндік береді.

MSP клиентіне сәйкес келетін әрбір виртуалды серверде бір немесе бірнеше тарату нүктесін тағайындау керек. MSP клиенттері мен Басқару сервері арасындағы байланыс интернет арқылы жүзеге асырылатындықтан, тарату нүктелері үшін *Жаңартуларды тарату орындарының қоймаларына жүктеп алу* тапсырмасын, тарату нүктелері жаңартуларды Басқару серверінен емес, тікелей Kaspersky серверлерінен жүктеп алатындай етіп жасаған жөн.

Егер MSP клиентінің желісінде құрылғылардың бір бөлігі интернетке тікелей қатынаса алмаса, онда тарату нүктелерін қосылым шлюзі режиміне ауыстыру керек. Бұл жағдайда, MSP клиентінің желісіндегі құрылғылардағы Желілік агенттер Басқару серверіне тікелей емес, шлюз арқылы қосылады (синхрондау мақсатында).

Басқару серверінің MSP клиентінің желісінде сауалнама өткізе алмайтыны әбден мүмкін болғандықтан, бұл функцияны орындау міндетін тарату нүктелерінің біріне жүктеген жөн.

Басқару сервері MSP клиентінің желісінде NAT артында орналасқан басқарылатын құрылғыларға 15000 UDP портына хабарландыру жібере алмайды. Бұл мәселені шешу үшін тарату нүктелері рөлін атқаратын және қосылым шлюзі режимінде іске қосылған құрылғылардың сипаттарында басқару серверінің үздіксіз қосылымы режимін қосқан пайдалы болуы мүмкін (**Басқару серверінен ажыратпау** опциясы). Егер тарату нүктелерінің жалпы саны 300-ден аспаса, тұрақты қосылу режимі қолжетімді болады.

MSP клиенті қызметкерлердің Android және iOS құрылғыларын басқарғысы келуі мүмкін. Басқару сервері мобильдік құрылғыларды TLS, TCP 13292 порты арқылы басқарады.

Тарату нүктелері туралы

Желілік агенті орнатылған құрылғыны тарату нүктесі ретінде пайдалануға болады. Бұл режимде, Желілік агент келесі функцияларды орындай алады:

- Файлдарды клиент құрылғыларына тасымалдау, соның ішінде:
  - Kaspersky дерекқорлары мен бағдарламалық жасақтама модульдері

    Жаңартуларды басқару серверінен немесе Kaspersky серверлерінен шығарып алуға болады. Соңғы жағдайда, тарату нүктесі болып табылатын құрылғы үшін *Жаңартуларды тарату орындарының қоймаларына жүктеп алу* тапсырмасы жасалуы тиіс.
  - Үшінші тарап бағдарламалық жасақтамасының жаңартулары
  - Орнату пакеттері
- Бағдарламалық жасақтаманы басқа құрылғыларға орнату, соның ішінде құрылғыларда Желілік агенттерді бастапқы орналастыруды орындау.
- Жаңа құрылғыларды анықтау және бұрыннан белгілі құрылғылар туралы ақпаратты жаңарту мақсатымен желіні сұрастыру. Тарату нүктесі Басқару серверімен бірдей құрылғыларды табу әдістерін қолдануы мүмкін.

Тарату нүктелерін ұйымның желісіне орналастыру келесі мақсаттарды көздейді:

- Егер жаңарту көзі Басқару сервері болса, Басқару серверіне түсетін жүктемені азайтыңыз.
- Интернет-трафикті оңтайландыру, өйткені бұл жағдайда MSP клиентінің желісіндегі әрбір құрылғыға жаңартулар алу үшін Kaspersky серверлеріне немесе Басқару серверіне жүгінудің қажеті жоқ.
- MSP клиенті желісінің NAT артындағы (Басқару серверіне қатысты) құрылғыларға Басқару серверіне қатынасу мүмкіндігін ұсыну Басқару серверіне келесі әрекеттерді орындауға мүмкіндік береді:
  - IPv4 немесе IPv6 желілеріндегі UDP арқылы құрылғыларға хабарландырулар жіберу
  - IPv4 немесе IPv6 желісінде сауалнама өткізу
  - Бастапқы орналастыруды орындау
  - Push-сервер ретінде әрекет ету

Тарату нүктесі басқару тобына тағайындалады. Бұл жағдайда, тарату нүктесінің әрекет ету ауқымы осы басқару тобындағы және оның барлық ішкі топтарындағы құрылғылар болады. Бұл арада, тарату нүктесі ретінде әрекет ететін құрылғы, өзі тағайындалған басқару тобына тиесілі болмауы керек.

Сіз тарату нүктесін қосылым шлюзі етіп жасай аласыз. Бұл жағдайда, тарату нүктесінің әрекет ету ауқымындағы құрылғылар Басқару серверіне тікелей емес, шлюз арқылы қосылады. Бұл режим Желілік агенті мен Басқару сервері бар құрылғылар арасында тікелей байланыс орнату мүмкін болмайтын сценарийлерде пайдалы.

Тарату нүктелері рөлін атқаратын құрылғылар рұқсатсыз қол жеткізудің кез келген түрінен, соның ішінде физикалық тұрғыдан қорғалуы тиіс.

Басқару серверлерінің иерархиясы

Кейбір клиенттік компаниялар, мысалы, MSP клиенттері бірнеше Басқару серверлерін пайдалана алады. Бірнеше шашыраңқы Серверлерді басқару ыңғайсыз, сондықтан оларды иерархияға біріктірген жөн. Linux операциялық жүйесі бар Басқару сервері Сервер иерархиясында Басты сервер ретінде де, Қосалқы сервер ретінде де жұмыс істей алады. Linux операциялық жүйесі бар Басты сервер Linux және Windows операциялық жүйелері бар Қосалқы серверлерді басқара алады. Windows операциялық жүйесінде жұмыс істейтін негізгі сервер Linux операциялық жүйесінде жұмыс істейтін қосалқы серверді басқара алады.

Екі Басқару сервері арасындағы "негізгі – қосалқы" өзара іс-қимылы келесі мүмкіндіктер ұсынады:

- Қосалқы Басқару сервер саясаттарды, тапсырмаларды, пайдаланушы рөлдерін және орнату пакеттерін негізгі Басқару серверден алады, параметрлердің қайталануы жойылады.
- Басқару сервердегі құрылғыны таңдауларға қосалқы Басқару серверлердегі құрылғылар қосылуы мүмкін.
- Басты Басқару сервердегі есептерге қосалқы Басқару серверлердегі деректер (соның ішінде егжей-тегжейлі) қосылуы мүмкін.
- Негізгі Басқару серверін Қосалқы Басқару сервері үшін жаңарту көзі ретінде пайдалануға болады.

Негізгі Басқару сервері жоғарыда берілген параметрлер аясында деректерді виртуалды емес, тәуелді басқару серверлерінен ғана алады. Бұл шектеулер негізгі басқару серверімен бір дерекқорды пайдаланатын виртуалды басқару серверлеріне қолданылмайды.

Басқару серверлерінің иерархиясы көптиістілік режиміне қолдау көрсетеді. Бұл режим негізгі әкімшіге бірнеше клиентті орталықтан дербес басқаруға мүмкіндік береді. Әрбір клиент ұйымы немесе кеңсе басқалардан оқшауланған және клиент деп аталады. Бірнеше басқарылатын құрылғыны байланыстырылған деректермен, параметрлермен, саясаттармен және тапсырмалармен бірге тенантқа бөлуге және пайдаланушы құқықтарын тенант арқылы конфигурациялауға болады.

Негізгі ұйымның инфрақұрылымына орнатылған негізгі басқару сервері негізгі тенант ретінде әрекет етеді. Негізгі басқару сервері қосалқы немесе виртуалдық басқару серверлеріне, оның оқшауланған тенанттарына өз оқиғаларын дербес қабылдауға және өңдеуге, сондай-ақ өз ресурстарымен, қызметтерімен және конфигурацияларымен жұмыс істеуге мүмкіндік береді.

Бірнеше клиент ұйымы бар қызмет провайдері әрбір клиент ұйымына дабылдарды біріктіру және жауап беру әрекеттерін қамтитын Kaspersky Security Center Linux функцияларын дербес қамтамасыз ете алады. Бұған қол жеткізу үшін қызмет провайдері әрбір клиент ұйымы үшін тенанттар ретінде қосалқы немесе виртуалдық басқару серверлерін қосады. Қызмет провайдері өз қызметкерлері мен ресурстары көмегімен қызметтерді жеткізеді.

Виртуалды Басқару серверлері

Физикалық Басқару серверінің шеңберінде бірнеше виртуалды Басқару серверлерін құруға болады, олардың көпшілігі қосалқы Серверлерге ұқсас. Қатынасуды бақылау тізіміне (ACL) негізделген қатынасуды бөлу моделімен салыстырғанда, виртуалды Серверлер моделі анағұрлым функционалды болып келеді және оқшаулаудың үлкен дәрежесін ұсынады. Саясат пен тапсырма құрылғыларына тағайындауға арналған басқару топтарының құрылымынан басқа, әрбір виртуалды Басқару серверінің өзіндік тағайындалмаған құрылғылар тобы, өзіндік есептер жиынтығы, құрылғыларды таңдау және оқиғалар, орнату пакеттері, жылжыту ережелері және т.б. бар. MSP клиенттерін максималды түрде өзара оқшаулау мақсатында, белгілі бір тапсырмалар үшін қолданылатын виртуалды Басқару серверлерін таңдау ұсынылады. Сонымен қатар, әрбір MSP клиенті үшін виртуалды Серверді құру клиенттерге Kaspersky Security Center Web Console арқылы өз желісін басқару бойынша негізгі мүмкіндіктерді ұсынуға мүмкіндік береді.

Виртуалды Серверлер көбінесе қосалқы Басқару серверлеріне ұқсас болып келеді, алайда олардың келесі айырмашылықтары бар:

- виртуалды Серверде көптеген жаһандық параметрлер мен өзіндік TCP порттары жоқ;
- виртуалды Серверде қосалқы Серверлер болуы мүмкін емес;
- виртуалды Серверде өзінің виртуалды Серверлері болуы мүмкін емес;
- физикалық Басқару серверінде, оның барлық виртуалды Серверлерінің басқарылатын құрылғыларынан (карантин элементтері, бағдарламалар тізімдемесі және т.б.) құрылғылар, топтар, оқиғалар мен нысандар көрінеді;
- виртуалды Сервер желіні тек оған қосылған тарату нүктелері арқылы сканерлей алады.

Орналастыру және бастапқы конфигурациялау

Kaspersky Security Center Linux қолданбасы таратылған бағдарлама болып саналады. Kaspersky Security Center Linux құрамына келесі қолданбалар кіреді:

- Басқару сервері – ұйымның құрылғыларын басқару және деректерді ДҚБЖ-де сақтау үшін жауапты орталық құрамдас.
- Kaspersky Security Center Web Console – қарапайым операцияларды орындауға арналған Басқару серверінің веб-интерфейсі. Бұл құрамдасты аппараттық және бағдарламалық жасақтамаға қойылатын талаптарға сай келетін кез келген құрылғыға орнатуға болады.
- Желілік агент – құрылғыда орнатылған қауіпсіздік бағдарламасын басқару, сондай-ақ құрылғы туралы ақпаратты алу үшін қолданылады. Желілік агенттер ұйымның құрылғыларына орнатылады.

Kaspersky Security Center Linux бағдарламасын ұйымның желісінде орналастыру келесі тәсілдермен жүзеге асырылады:

- Басқару серверін орнату;
- Kaspersky Security Center Web Console орнату;
- Желілік агент пен қауіпсіздік бағдарламаларын ұйымның құрылғыларына орнату.

Басқару серверін орнату бойынша ұсыныстар

Осы бөлімде Басқару серверін орнатуға қатысты ұсынымдар бар. Бөлімде клиент құрылғыларында Желілік агентті орналастыруға арналған Басқару серверін қамтитын құрылғыда ортақ қатынасы бар қалталарды қолдану сценарийлері де бар.

Істен шығуға төзімді кластерде Басқару серверінің қызметтеріне арналған есептік жазбалар жасау

Kaspersky Security Center Linux жүйесін ақауларға төзімді кластерге орналастыруды бастамай тұрып, Kaspersky Security Center Linux қызметтеріне арналған есептік жазбалар жасауыңыз керек.

Ол үшін белсенді түйінде, белсенді емес түйінде және файл серверінде келесі қадамдарды орындаңыз:

1. "kladmins" деп аталатын топ жасаңыз және барлық үш топқа бірдей GID тағайындаңыз.
2. "ksc" деп аталатын есептік жазбаны жасаңыз және барлық үш пайдаланушы есептік жазбасына бірдей UID тағайындаңыз. Жасалған есептік жазбалар үшін негізгі топ ретінде kladmins көрсетіңіз.
3. "rightless" деп аталатын есептік жазбаны жасаңыз және барлық үш пайдаланушы есептік жазбасына бірдей UID тағайындаңыз. Жасалған есептік жазбалар үшін негізгі топ ретінде kladmins көрсетіңіз.

ДҚБЖ таңдау

Төмендегі кестеде ДҚБЖ рұқсат етілген нұсқалары және оларды ұсынымдары мен қолдану шектеулері аталған.

ДҚБЖ ұсынымдар және шектеулер

ДҚБЖ	Ұсынымдар және шектеулер
MySQL (қолдау көрсетілетін нұсқаларды қараңыз)	20 000-нан аз құрылғылар үшін бір Басқару серверін пайдалануды жоспарласаңыз, осы ДҚБЖ пайдаланыңыз.
MariaDB (қолдау көрсетілетін нұсқаларды қараңыз)	20 000-нан аз құрылғылар үшін бір Басқару серверін пайдалануды жоспарласаңыз, осы ДҚБЖ пайдаланыңыз.
PostgreSQL, Postgres Pro (қолдау көрсетілетін нұсқаларды қараңыз)	50 000-нан аз құрылғылар үшін бір Басқару серверін пайдалануды жоспарласаңыз, осы ДҚБЖ пайдаланыңыз.
Tantor (қолдау көрсетілетін нұсқаларды қараңыз)	50 000-нан аз құрылғылар үшін бір Басқару серверін пайдалануды жоспарласаңыз, осы ДҚБЖ пайдаланыңыз. Tantor-ға ДҚБЖ тек Astra Linux Special Edition RUSB.10015-01 арнайы шығарылымында (1.8 операциялық жаңарту) қолдау көрсетіледі.

Таңдалған ДҚБЖ жүйесін қалай орнату керектігі туралы мәліметтер оның құжаттамасында келтірілген.

Қолданбалық жасақтаманы түгендеу тапсырмасын өшіру және Басқару сервердің қолданбаларды іске қосу туралы хабарландыруларын өшіру (Kaspersky Endpoint Security саясатының параметрлерінде) ұсынылады.

Егер сіз PostgreSQL немесе Postgres Pro ДҚБЖ орнатуды шешсеңіз, суперпайдаланушының құпиясөзін енгізгеніңізге көз жеткізіңіз. Егер құпиясөз көрсетілмесе, Басқару сервері дерекқорға қосылмауы мүмкін.

MySQL, MariaDB, PostgreSQL немесе Postgres Pro орнатсаңыз, ДҚБЖ дұрыс жұмыс істеуін қамтамасыз ету үшін ұсынылатын параметрлерді қолданыңыз.

PostgreSQL, MariaDB немесе MySQL ДҚБЖ пайдалансаңыз, **Оқиғалар** қойындысы таңдалған клиент құрылғысы үшін оқиғалардың толық тізімін көрсетпеуі мүмкін. Бұл, ДҚБЖ оқиғалардың өте көп санын сақтаған кезде орын алады. Келесі әрекеттердің бірін орындау арқылы көрсетілетін оқиғалар санын көбейтуге болады:

- Керек емес оқиғаларды жою.
- Керек емес оқиғаларды сақтау мерзімін қысқарту.

Құрылғы үшін Басқару серверінде тіркелген оқиғалардың толық тізімін көру үшін Есептерді пайдаланыңыз.

Басқару серверінің мекенжайын көрсету

Басқару серверін орнатқан кезде, басқару серверінің DNS атауын немесе статикалық IP мекенжайын көрсетуіңіз керек. Бұл мекенжай, әдепкі бойынша Желілік агенттің орнату пакеттерін жасау кезінде қолданылады. Содан кейін Kaspersky Security Center Web Console құралдары көмегімен басқару сервері хостының мекенжайын өзгертуге болады; әлдеқашан жасалған желілік агенттің орнату пакеттерінде мекенжай автоматты түрде өзгермейді.

Әрекетсіз қосылымдарды жүргізу

Қосылым тұрақтылығын жақсарту үшін қосылым шлюзі құрылғыларында келесі keepalive параметрлерін конфигурациялауды ұсынамыз:

- `net.ipv4.tcp_keepalive_intvl` біріншіден кейін keepalive хабарларын жіберу жиілігін көрсетеді. Бұл параметрді `1` деп орнатыңыз.
- `net.ipv4.tcp_keepalive_probes` қосылым аяқталды деп есептелгенге дейін қанша жауапсыз keepalive хабарларын жіберуге болатынын білдіреді. Бұл параметрді `10` деп орнатыңыз.
- `net.ipv4.tcp_keepalive_time` бірінші keepalive хабарын жібермей тұрып, соңғы деректер пакетінен кейін қанша уақыт күту қажеттігін көрсетеді. Бұл параметрді `900` деп орнатыңыз.

Keepalive параметрлерін конфигурациялау үшін:

1. etc/sysctl.conf файлын ашыңыз.
2. Келесі параметр мәндерін қосыңыз:

```
net.ipv4.tcp_keepalive_intvl = 1
net.ipv4.tcp_keepalive_probes = 10
net.ipv4.tcp_keepalive_time = 900
```

3. keepalive параметрлерін жаңарту үшін келесі пәрменді орындаңыз:

```
sudo sysctl -p /etc/sysctl.conf
```

4. Параметр мәндері қолданылғанына көз жеткізу үшін келесі пәрмендерді орындаңыз:

```
sudo sysctl net.ipv4.tcp_keepalive_intvl
sudo sysctl net.ipv4.tcp_keepalive_probes
sudo sysctl net.ipv4.tcp_keepalive_time
```

Желілік агент пен қауіпсіздік қолданбаларын орналастыру

Ұйымдағы құрылғыларды басқару және оларды қауіптерден қорғау үшін олардың әрқайсысына желілік агент пен Kaspersky қауіпсіздік қолданбасын орнатуыңыз керек.

Қорғанысты орналастыру туралы ақпарат алу үшін Желілік агент пен қауіпсіздік қолданбасын орнату бөлімін қараңыз.

Мобильдік құрылғыны қорғау туралы ақпарат алу үшін Мобильдік құрылғыны басқару бөлімін қараңыз.

Microsoft Windows XP-де желілік агент келесі операцияларды дұрыс орындамауы мүмкін: жаңартуларды тікелей Kaspersky серверлерінен жүктеп алу (тарату нүктесі ретінде); KSN прокси-сервері ретінде жұмыс істеу (тарату нүктесі ретінде); және үшінші тараптар осалдықтарын анықтау (осалдықтар мен патчтарды басқаруды қолданған кезде).

Ұйым-клиент желісінде қорғанысты конфигурациялау

Басқару сервері орнатылғаннан кейін, Kaspersky Security Center Web Console ашылады және тиісті шебер арқылы бастапқы реттеу әрекетін орындауды сұрайды. Бағдарламаны жылдам іске қосу шеберінің жұмысы уақытында түпкі басқару тобында келесі саясаттар мен тапсырмалар жасалады:

- Kaspersky Endpoint Security саясаты
- Kaspersky Endpoint Security жаңарту топтық тапсырмасы
- Kaspersky Endpoint Security құрылғысын тексерудің топтық тапсырмасы
- Желілік агент саясаты
- Осалдықтарды іздеу тапсырмасы (Желілік агенттің тапсырмасы)
- Жаңартуларды орнату және осалдықты түзету тапсырмасы (Желілік агенттің тапсырмасы)

Саясаттар мен тапсырмалар осы ұйым үшін оңтайлы емес немесе тіпті жарамсыз болуы мүмкін әдепкі бойынша параметрлермен жасалады. Сондықтан жасалған нысандардың сипаттарын қарастырып, қажет болса, өзгерістерді қолмен енгізу керек.

Осы бөлім Басқару серверінің саясаттарын, тапсырмаларын және басқа параметрлерін қолмен конфигурациялау туралы ақпаратты, сондай-ақ тарату нүктелері, басқару тобының құрылымын құру, тапсырмалардың иерархиясы мен басқа конфигурациялар туралы ақпаратты қамтиды.

Kaspersky Endpoint Security саясатын қолмен конфигурациялау

Бұл бөлімде жылдам іске қосу шебері арқылы жасалған Kaspersky Endpoint Security саясатын конфигурациялау жолы туралы ұсыныстар берілген. Саясат сипаттары терезесінде конфигурациялауды орындауға болады.

Параметрді өңдеген кезде, жұмыс станциясында параметр мәнін өңдеуге тыйым салу не рұқсат беру үшін параметрді құлыптауға не құлпын ашуға болатынын ескеріңіз.

Кеңейтілген қорғаныс бөлімінде саясатты конфигурациялау

Бұл бөлімнің параметрлерінің толық сипаттамасы Kaspersky Endpoint Security for Windows құжаттамасында берілген.

Кеңейтілген қорғаныс бөлімінде Kaspersky Endpoint Security for Windows үшін Kaspersky Security Network қолданысын конфигурациялауға болады. Сондай-ақ, Әрекеттерді талдау, Эксплойттан қорғаныс, Хост-компьютерге басып кіруді болдырмау және Зиянды әрекеттерді шегіндіру сияқты Kaspersky Endpoint Security for Windows модульдерін конфигурациялауға болады.

Kaspersky Security Network ішкі бөлімінде **Kaspersky Security Network** опциясын қосуға кеңес беріледі. Бұл параметрді пайдалану желі трафигін қайта таратуға және оңтайландыруға көмектеседі. **Kaspersky Security Network** опциясы өшірілсе, KSN серверлерін тікелей пайдалануды қосуға болады.

Негізгі қорғаныс бөліміндегі саясатты конфигурациялау

Бұл бөлімнің параметрлерінің толық сипаттамасы Kaspersky Endpoint Security for Windows құжаттамасында берілген.

Саясат сипаттары терезесінің **Essential Threat Protection** бөлімінде **Firewall** және **File Threat Protection** ішкі бөлімдерінде қосымша параметрлерді көрсету ұсынылады.

Firewall ішкі бөлімі клиент құрылғыларында қолданбалардың желілік әрекетін бақылауға көмектесетін параметрлерді қамтиды. Клиент құрылғысы келесі күйлердің бірі берілген желіні пайдаланады: жалпыға қолжетімді, жергілікті немесе сенімді. Желі күйіне байланысты Kaspersky Endpoint Security құрылғыдағы желілік белсенділікке рұқсат етуі немесе тыйым салуы мүмкін. Ұйымыңызға жаңа желіні қосқан кезде, оған сәйкес желілік күйді беруіңіз керек. Мысалы, егер ноутбук клиент құрылғысы болса, бұл құрылғы жалпыға қолжетімді немесе сенімді желіні пайдалануы ұсынылады, өйткені ноутбук әрқашан жергілікті желіге қосылған болмайды. **Firewall** ішкі бөлімінде ұйымда қолданылатын желілерге күйлерді дұрыс тағайындағаныңызды тексеруге болады.

Желілер тізімін тексеру үшін:

1. Саясат сипаттарында **Essential Threat Protection** → **Firewall** бөліміне өтіңіз.
2. **Available networks** бөлімінде **Settings** түймесін басыңыз.
3. Ашылған **Firewall** терезесінде желілер тізімін көру үшін **Желі** қойындысына өтіңіз.

File Threat Protection ішкі бөлімінде желі дискілерін сканерлеуді өшіруге болады. Желілік дисктерді тексеру желілік дисктерге айтарлықтай жүктемені тудыра алады. Тікелей файл серверлерінде тексеруді жүзеге асырған жөн.

Желілік дискіні тексеруді өшіру үшін:

1. Саясат сипаттарында **Essential Threat Protection** → **File Threat Protection** бөліміне өтіңіз.
2. **Security level** бөлімінде **Settings** түймесін басыңыз.
3. Ашылған **File Threat Protection** терезесіндегі **General** қойындысында **All network drives** құсбелгі ұяшығын тазалаңыз.

Қосымша параметрлер бөліміндегі саясатты конфигурациялау

Бұл бөлім параметрлерінің толық сипаттамасы Kaspersky Endpoint Security құжаттамасында берілген.

Төменде **Жалпы параметрлер** бөліміндегі Kaspersky Endpoint Security саясат сипаттары терезесінде орындау ұсынылатын қосымша конфигурация қадамдары сипатталған.

Қосымша параметрлер бөлімі, есептер және қоймалар ішкі бөлімі

Деректерді басқару серверіне жіберу бөлімінде **Іске қосылатын қолданбалар туралы ақпарат** жалаушасына назар аударыңыз. Бұл жалауша қойылған кезде, басқару сервері дерекқоры ұйымның желісіндегі құрылғылардағы барлық қолданба модульдерінің барлық нұсқалары туралы ақпаратты сақтайды. Көрсетілген ақпарат Kaspersky Security Center Linux дерекқорында (ондаған гигабайт) айтарлықтай көлемді алуы мүмкін. Сондықтан жоғары деңгейлі саясатта әлі де **Іске қосылатын қолданбалар туралы ақпарат** жалаушасы қойылса, оны алу керек.

Қосымша параметрлер бөлімі, интерфейс ішкі бөлімі

Kaspersky Security Center Web Console арқылы ұйымыңыздың желісіндегі қорғанысты орталықтан басқару қажет болса, жұмыс станцияларында Kaspersky Endpoint Security пайдаланушы интерфейсін көрсетуді өшіру керек (**Пайдаланушымен өзара әрекеттесу** бөліміндегі **Қолданба интерфейсін көрсету** жалаушасын алып тастау арқылы) және құпиясөзбен қорғауды (**Құпиясөзбен қорғау** бөліміндегі **Құпиясөзбен қорғауды қосу** жалаушасын қою арқылы) керек.

Оқиғаларды конфигурациялау бөліміндегі саясатты конфигурациялау

Оқиғаларды конфигурациялау бөлімінде төменде аталған оқиғалардан басқа барлық оқиғаны басқару серверінде сақтауды өшіру керек:

- **Маңызды** қойындысында:
  - *Application autorun is disabled*
  - *Access denied*
  - *Application startup prohibited*
  - *Disinfection impossible*
  - *End User License Agreement violated*
  - *Could not load encryption module*
  - *Cannot start two tasks at the same time*
  - *Active threat detected. Advanced Disinfection should be started*
  - *Network attack detected*
  - *Not all components were updated*
  - *Activation error*
  - *Error enabling portable mode*
  - *Error in interaction with Kaspersky Security Center*
  - *Error disabling portable mode*
  - *Error changing application components*
  - *Error applying file encryption / decryption rules*
  - *Policy cannot be applied*
  - *Process terminated*
  - *Network activity blocked*
- **Функционалдық ақау** қойындысында: *Invalid task settings. Settings not applied*

- **Ескерту** қойындысында:
  - *Self-Defense is disabled*
  - *Incorrect reserve key*
  - *User has opted out of the encryption policy*
- **Ақпараттық** қойындысында: *Бағдарламаны сынақ режимде іске қосуға тыйым салынған*

Kaspersky Endpoint Security жаңарту топтық тапсырмасын қолмен конфигурациялау

Басқару сервері жаңарту көзі рөлін атқарса, Kaspersky Endpoint Security үшін ұсынылған оңтайлы жоспарлау опциясы — **Тапсырманы бастау үшін автоматты түрде араластырылған кідірісті пайдалану** құсбелгі ұяшығы таңдалған **Қоймаға жаңа жаңартулар жүктеп алынған уақыт**.

Егер әрбір тарату нүктесі үшін Kaspersky серверлерінен жаңартуларды қоймаға жүктеудің жергілікті тапсырмасы жасалса, онда Kaspersky Endpoint Security жаңартудың топтық тапсырмасы үшін кесте бойынша мезгіл-мезгіл іске қосу оңтайлы және ұсынылатын болып саналады. Бұл жағдайда, автономизация кезеңінің мәні 1 сағат болып орнатылуы керек.

Kaspersky Endpoint Security құрылғысын тексеру топтық тапсырмасын қолмен конфигурациялау

Бағдарламаны жылдам іске қосу шебері құрылғыны тексерудің топтық тапсырмасын жасайды. Топтық тексеру тапсырмасының автоматты түрде орнатылған кестесі ұйымыңызға сәйкес келмесе, ұйымда қабылданған жұмыс процесі ережелеріне негізделген бұл тапсырма үшін ең қолайлы кестені қолмен орнату қажет.

Мысалы, тапсырма үшін автоматты рандомизациясы бар **Жұма күні 19:00-де іске қосу** кестесі таңдалған және **Өткізіп алынған тапсырмаларды іске қосу** жалаушасы алынған. Демек, егер ұйымның құрылғылары жұма күндері сағат 18:30-да сөндірілсе, онда құрылғыны сканерлеу тапсырмасы ешқашан іске қосылмайды. Бұл жағдайда топтық тексеру тапсырмасын қолмен орнату қажет.

Осалдықтарды және қажетті жаңартуларды іздеу тапсырмасы кестесін конфигурациялау

Бағдарламаны жылдам іске қосу шебері Желілік агент үшін *Осалдықтарды және қажетті жаңартуларды іздеу* топтық тапсырмасын жасайды. Әдепкі бойынша тапсырма үшін автоматты рандомизациясы бар **Сейсенбі күндері 19:00-де іске қосу** кестесі таңдалды және **Өткізіп алған тапсырмаларды іске қосу** жалаушасы орнатылды.

Егер ұйым жұмысының регламенті осы уақытта құрылғыларды сөндіруді қарастырса, онда *Осалдықтарды және қажетті жаңартуларды іздеу* тапсырмасы құрылғыны қосқаннан кейін (сәрсенбі күні таңертең) іске қосылады. Мұнда жүріс-тұрыс жағымсыз болуы мүмкін, өйткені осалдықтарды іздеу құрылғының процессоры мен диск ішкі жүйесіне жоғары жүктеме түсіруі мүмкін. Ұйымда қабылданған жұмыс регламентіне сүйене отырып, тапсырманың оңтайлы кестесін конфигурациялау керек.

Жаңартуларды орнату және осалдықты түзету топтық тапсырмасын қолмен конфигурациялау

Бағдарламаны жылдам іске қосу шебері Желілік агент үшін жаңартуларды орнату және осалдықтарды іздеу топтық тапсырмасын жасайды. Әдепкі бойынша автоматты түрде рандомизациясы бар күн сайын 1:00-де тапсырманы іске қосу конфигурацияланған, **Өткізіп алынған тапсырмаларды іске қосу** параметрі сөндірілген.

Егер ұйымның жұмыс регламенті құрылғыны түнде сөндіруді қарастырса, онда жаңартуларды орнату тапсырмасы ешқашан іске қосылмайды. Ұйымда қабылданған жұмыс регламентіне сүйеніп, осалдықтарды іздеу тапсырмасының оңтайлы кестесін белгілеу керек. Сонымен қатар, жаңартуларды орнату нәтижесінде құрылғыны қайта іске қосу қажет болуы мүмкін екендігін ескерген жөн.

Басқару топтары құрылымын құру және тарату нүктелерін тағайындау

Kaspersky Security Center Linux-тегі басқару топтарының құрылымы келесі функцияларды орындайды:

- Саясаттардың әрекет ету ауқымын белгілеу.

  Саясат профильдерінің көмегімен құрылғыларда қатысты параметрлерді қолданудың балама жолы бар. Бұл жағдайда саясаттардың ауқымы мысалы, құрылғы тегтерімен немесе пайдаланушы рөлдерімен орнатылады.

- Топтық тапсырмалардың әрекет ету ауқымын белгілеу.

  Басқару топтарының иерархиясына негізделмеген топтық тапсырмалардың әрекет ету ауқымын белгілеу тәсілдемесі бар: құрылғыларды таңдау және арнайы құрылғылар үшін тапсырмаларды қолдану.

- Құрылғыларға, виртуалды және қосалқы Басқару серверлеріне қатынасу құқықтарын белгілеу.

- Тарату нүктелерін тағайындау.

Басқару топтарының құрылымын құру кезінде тарату нүктелерін оңтайлы түрде тағайындау үшін ұйым желісінің топологиясын ескеру қажет. Тарату нүктелерінің оңтайлы таралуы арқасында ұйым желісіндегі желілік трафикті азайтуға мүмкіндік беріледі.

MSP клиентінің ұйымдық құрылымына және желілер топологиясына байланысты, басқару топтары құрылымының келесі типтік конфигурацияларын ажыратуға болады:

- Бір кеңсе

- Көптеген шағын оқшауланған кеңселер

MSP клиентінің типтік конфигурациясы: бір кеңсе

"Бір кеңсе" типтік конфигурациясында барлық құрылғылар ұйымның желісінде орналаса отырып, бір-бірін "көреді". Ұйымның желісі тар арналармен байланысқан бірнеше бөлектенген бөліктен (желіден немесе желі сегменттерінен) құралуы мүмкін.

Басқару топтарының құрылымын құрудың келесі тәсілдері болуы мүмкін:

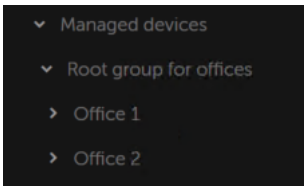
- Желі топологиясын ескере отырып, басқару тобының құрылымын құру. Басқару топтарының құрылымы желінің топологиясын нақты түрде көрсетуге міндетті емес. Желінің бөлектенген бөліктеріне қандай да бір басқару топтарының сай келуі жеткілікті. Тарату нүктелерін автоматты түрде тағайындауды қолдануға немесе тарату нүктелерін қолмен тағайындауға болады.

- Желінің топологиясын білдірмейтін басқару топтарының құрылымын құру. Бұл жағдайда, тарату нүктелерін автоматты түрде тағайындауды өшіру және желінің әрбір бөлектенген бөлігінде түбірлік басқару тобына, мысалы, **Басқарылатын құрылғылар** тобына бір немесе бірнеше құрылғыны тарату нүктелері ретінде тағайындау керек. Барлық тарату нүктелері бір деңгейде болады және бірдей "ұйым желісінің барлық құрылғылары" әрекет ету ауқымына ие болады. Желілік агенттердің әрқайсысы, бағыты ең қысқа болып саналатын тарату нүктесіне қосылатын болады. Тарату нүктесіне апаратын бағытты tracert немесе traceroute утилитасының көмегімен трассалауға болады.

MSP клиентінің типтік конфигурациясы: көптеген шағын оқшауланған кеңселер

Бұл типтік конфигурация, бәлкім, басты кеңсемен интернет арқылы байланысқан көптеген шағын қашықтағы кеңселерге сәйкес келеді. Қашықтағы кеңселердің әрқайсысы NAT артында орналасқан, яғни бір қашықтағы кеңседен екіншісіне қосылу мүмкін емес – кеңселер бір-бірінен оқшауланған.

Конфигурация басқару топтарының құрылымында міндетті түрде көрсетілуі керек: қашықтағы кеңселердің әрқайсысы үшін жеке басқару тобын құру керек (төмендегі суреттегі **1-кеңсе**, **2-кеңсе** топтары).



Қашықтағы кеңселер басқару топтарының құрылымында көрсетілген

Кеңсеге сай келетін әрбір басқару тобына бір немесе бірнеше тарату нүктесін тағайындау керек. Дискіде жеткілікті орны бар қашықтағы кеңсе құрылғыларын тарату нүктелері ретінде тағайындау керек. Мысалы, **1-кеңсе** тобында орналастырылған құрылғылар **1-кеңсе** басқару тобына тағайындалған тарату нүктелеріне жүгінетін болады.

Егер кейбір пайдаланушылар ноутбуктері бар кеңселер арасында физикалық түрде жылжытылатын болса, әр қашықтағы кеңседе жоғарыда аталған тарату нүктелеріне тағы екі және немесе одан да көп құрылғыны таңдап, оларды жоғарғы деңгейдегі басқару тобына тарату нүктелері ретінде тағайындау керек (жоғарыдағы суреттегі **Кеңселерге арналған түбірлік топ** тобы).

1-кеңсе басқару тобында болған, бірақ физикалық түрде **2-кеңсе** тобына сәйкес келетін кеңсеге көшірілген ноутбук. Жылжытқаннан кейін, ноутбуктағы Желілік агент **1-кеңсе** тобына тағайындалған тарату нүктелеріне жүгінуге тырысатын болады, бірақ бұл тарату нүктелері қолжетімді болмайды. Сонда Желілік агент **Кеңселерге арналған түбірлік топ** тобына тағайындалған тарату нүктелеріне жүгіне бастайды. Қашықтағы кеңселер бір-бірінен алшақ орналасқандықтан, **Кеңселерге арналған түбірлік топ** басқару тобына тағайындалған барлық тарату нүктелерінен **2-кеңсе** тобына тағайындалған тарату нүктелеріне жүгіну ғана сәтті болады. Яғни, ноутбук өзінің бастапқы кеңсесіне сәйкес келетін басқару тобында бола отырып, қазіргі уақытта физикалық түрде орналасқан кеңсенің тарату нүктесін қолдана беретін болады.

Саясаттар иерархиясы, саясат профильдерін қолдану

Осы бөлім саясаттарды басқару топтарындағы құрылғыларға қолдану ерекшеліктері туралы ақпаратты қамтиды. Осы бөлім саясаттардың профильдері туралы ақпаратты да қамтиды.

Саясаттар иерархиясы

Kaspersky Security Center Linux жүйесінде параметрлердің дара жиынтығын бірнеше құрылғыға қолдану үшін саясаттарды қолданыңыз. Мысалы, G тобы үшін анықталған P бағдарламасы саясатының әрекет ету ауқымы сипаттарында **Тектік топтан иелену** жалаушасы алынған ішкі топтарды қоспағанда, G басқару тобында және барлық оның ішкі топтарында орналасқан P бағдарламасы орнатылған басқарылатын құрылғылар болып табылады.

Саясат оның ішіндегі параметрлердің жанында "құлыптардың" (🔒) болуымен жергілікті параметрлерден ерекшеленеді. Саясат сипаттарында орнатылған құлып оған сәйкес параметр (немесе параметрлер тобы) біріншіден, тиімді параметрлерді қалыптастырған кезде пайдаланылуы керектігін, екіншіден, төмендегі саясатқа жазылуы керектігін білдіреді.

Құрылғыда әрекет ететін параметрлерді қалыптастыруды келесі түрде көрсетуге болады: саясаттан құлпы орнатылмаған параметрлердің мәндері алынады, кейін олардың үстіне жергілікті параметрлердің мәндері жазылады, кейін алған мәндердің үстіне саясаттан алынған құлпы орнатылған параметрлердің мәндері жазылады.

Бірдей бағдарламаның саясаттары бір-біріне басқару топтарының иерархиясы бойынша әрекет етеді: жоғарыдағы саясаттың орнатылған құлпы бар параметрлері төмендегі саясаттың аттас параметрлерін қайта жазады.

Ерекше саясат түрі бар - автономды пайдаланушыларға арналған саясат. Бұл саясат құрылғы автономды режимге ауысқан кезде құрылғыда күшіне енеді. Автономды пайдаланушыларға арналған саясаттар басқа саясаттарға басқару топтарының иерархиясы бойынша әрекет етпейді.

Саясат профильдері

Тек қана басқару топтарының иерархиясына сүйене отырып құрылғыларға саясаттарды қолдану көптеген жағдайларда ыңғайсыз. Әртүрлі басқару топтары үшін саясаттың бірнеше көшірмелерін жасау және одан әрі осы саясаттардың мазмұнын қолмен синхрондау қажеттілігі туындауы мүмкін.

Мұндай мәселелерге жол бермеу үшін Kaspersky Security Center Linux *саясат профильдеріне* қолдау көрсетеді. Саясат профилі, саясат параметрлерінің аталған ішкі жиынтығы болып табылады. Параметрлердің осы ішкі жиынтығы құрылғыларға саясатпен бірге таралады және келесі шартты – *профильді белсендіру шартын* орындаған кезде саясатты толықтырады. Профильдер клиент құрылғысында (компьютерде, ұялы құрылғыда) әрекет ететін "негізгі" саясаттан ерекшеленетін параметрлерді ғана қамтиды. Профильді белсендірген кезде, профиль белсендірілгенге дейін құрылғыда әрекет еткен саясат параметрлері өзгереді. Бұл параметрлер профильде көрсетілген мәндерді қабылдайды.

Саясаттардың профильдері қазір келесі шектеулерге ие:

- саясатта ең көбі 100 профиль болуы мүмкін;
- саясаттың профилі басқа профильдерді қамти алмайды;
- саясаттың профилі хабарландыру параметрлерін қамти алмайды.

Профильдің мазмұны

Саясаттың профилі келесі құрамдас бөліктерді қамтиды:

- Атауы. Атаулары бірдей профильдер бір-біріне ортақ ережелері бар басқару топтарының иерархиясы арқылы әсер етеді.
- Саясат параметрлерінің қосалқы жиынтығы. Барлық параметрлері бар саясатқа қарағанда, профильде шынымен керек (құлып орнатылған) параметрлер ғана бар.
- Белсендіру шарты – құрылғы сипаттарының логикалық өрнегі. Профиль профильді белсендіру шарты шынайы болған кезде ғана белсенді (саясатты толықтырады). Қалған жағдайларда профиль белсенді емес және ескерілмейді. Логикалық өрнекте құрылғының келесі сипаттары қатыса алады:
  - автономды режим күйі;
  - желілік орта сипаттары – Желілік агентті қосудың белсенді ережесінің атауы;
  - құрылғыда көрсетілген тегтердің болуы немесе болмауы;
  - Active Directory бөлімшесінде құрылғының орналасқан жері: айқын (құрылғы тікелей көрсетілген бөлімшеде орналасқан) немесе айқын емес (құрылғы кез келген тіркеме деңгейінде көрсетілген бөлімшенің ішінде орналасқан бөлімшеде орналасқан);
  - құрылғының Active Directory қауіпсіздік тобындағы мүшелігі (айқын немесе айқын емес);
  - құрылғы иесінің Active Directory қауіпсіздік тобындағы мүшелігі (айқын немесе айқын емес).
- Профильді сөндіру жалаушасы. Сөндірілген профильдер әрқашан ескерілмейді, оларды белсендіру шарттары шынайылыққа тексерілмейді.
- Профильдің басымдығы. Профильдерді белсендіру шарттары тәуелсіз, сондықтан бір уақытта бірден бірнеше профильдер белсендірілуі мүмкін. Егер белсенді профильдер параметрлердің талассыз жинақтарын қамтыса, онда ешқандай мәселелер туындамайды. Дегенмен екі белсенді профильде бірдей параметрдің әртүрлі мәндері болса, түсініксіздік орын алады. Бұл түсініксіздікке профиль басымдықтары арқылы жол бермеу керек: түсініксіздік айнымалысының мәні басымдығы жоғарырақ профильден (профильдер тізімінде жоғары бағаланған) алынады.

Саясаттар иерархия бойынша бір-біріне әрекет еткен кезде профильдердің жағдайы

Аттас профильдер саясаттарды біріктіру ережелеріне сәйкес біріктіріледі. Жоғарғы саясаттың профильдері төменгі саясаттың профильдерінен басымдырақ. Егер "жоғарғы" саясатта параметрлерді өзгертуге тыйым салынса (құлып батырмасы басылған), "төменгі" саясатта "жоғарғы" саясаттағы профильді белсендіру шарттары пайдаланылады. Егер "жоғарғы" саясатта параметрлерді өзгертуге рұқсат етілсе, онда "төменгі" саясаттағы профильді белсендіру шарттары пайдаланылады.

Саясат профилі белсендіру шартында **Құрылғы офлайн режимде** қамти алғандықтан, профиль одан әрі қолдау көрсетілмейтін автономды пайдаланушылар үшін саясаттардың функционалдығын толығымен ауыстырады.

Автономды пайдаланушыларға арналған саясат профильдерді қамтуы мүмкін, бірақ оның профильдерін белсендіру құрылғы автономды режимге ауыспайынша туындамайды.

Тапсырмалар

Kaspersky Security Center Linux *тапсырмаларды* құру және іске қосу арқылы құрылғыларда орнатылған Kaspersky қауіпсіздік бағдарламаларының жұмысын басқарады. Тапсырмалардың көмегімен бағдарламаларды орнату, іске қосу және тоқтату, файлдарды сканерлеу, бағдарламалардың дерекқорлары мен модульдерін жаңарту, бағдарламалармен басқа әрекеттер орындалады.

Бағдарлама үшін басқару плагині орнатылған жағдайда ғана тапсырма жасай аласыз.

Тапсырмалар Басқару серверінде және құрылғыларда орындалуы мүмкін.

Басқару серверінде орындалатын тапсырмалар:

- Есептерді автоматты түрде жеткізу
- Жаңартуларды Басқару серверінің қоймасына жүктеп алу
- Басқару сервері деректерінің сақтық көшірмесін жасау
- Дерекқорларға қызмет көрсету

Құрылғыларда тапсырмалардың келесі түрлері орындалады:

- *Жергілікті тапсырмалар* – нақты құрылғыда орындалатын тапсырмалар.

  Жергілікті тапсырмаларды тек әкімші Kaspersky Security Center Web Console-інің құралдары арқылы ғана емес, қашықтағы құрылғының пайдаланушысы да өзгерте алады (мысалы, қауіпсіздік бағдарламасының интерфейсінде). Егер жергілікті тапсырманы басқарылатын құрылғыда әкімші де, пайдаланушы да бір уақытта өзгерткен болса, онда әкімші енгізген өзгерістер басым болып күшіне енеді.

- *Топтық тапсырмалар* – бұл аталған топтың барлық құрылғыларында орындалатын тапсырмалар.

  Егер тапсырманың сипаттарында басқаша көрсетілмесе, топтық тапсырма аталған топтың ішкі топтарына да таралады. Топтық тапсырмалар (міндетті емес) осы топқа және ішкі топтарға орналастырылған қосалқы және виртуалды Басқару серверлеріне қосылған құрылғыларда да жұмыс істейді.

- *Глобалдық тапсырмалар* – бұл басқару топтарына кіретіндігіне қарамастан, таңдалған құрылғыларда орындалатын тапсырмалар.

Әр бағдарлама үшін сіз топтық тапсырмалардың, глобалдық тапсырмалардың және жергілікті тапсырмалардың кез келген санын жасай аласыз.

Тапсырма параметрлеріне өзгертулер енгізуге, тапсырмалардың орындалуын бақылауға, тапсырмаларды көшіруге, экспорттауға және импорттауға, сондай-ақ жоюға болады.

Құрылғыдағы тапсырмаларды іске қосу тек осы тапсырмалар жасалған бағдарлама іске қосылған жағдайда ғана орындалады.

Тапсырмаларды орындау нәтижелері оқиғалардың жүйелік журналында және Kaspersky Security Center Linux оқиғалар журналында орталықтандырылған түрінде Басқару серверінде де, әр құрылғыда жергілікті түрінде де сақталады.

Тапсырмалар параметрлерінде құпия деректерді пайдаланбаңыз. Мысалы, домен әкімшісінің құпиясөзін көрсетпеуге тырысыңыз.

Құрылғыны жылжыту ережелері

Құрылғыларды жылжыту ережелері көмегімен басқару топтарында құрылғыларды орналастыру процесін автоматтандыру ұсынылады. Жылжыту ережесі үш негізгі бөліктен тұрады: атауы, орындау шарттары (құрылғы атрибуттарының логикалық өрнегі) және мақсатты басқару тобы. Құрылғының атрибуттары ережені орындау шартына сай келсе, онда ереже құрылғыны мақсатты басқару тобына көшіреді.

Құрылғыны жылжыту ережелерінің басымдықтары бар. Басқару сервері құрылғының атрибуттарын әрбір ережені орындау шартына сай келу тұрғысынан, ережелер басымдығының азаюы тәртібінде тексереді. Құрылғының атрибуттары ережені орындау шартына сай келсе, онда құрылғы мақсатты топқа көшіріледі және бұл құрылғы үшін ережелерді өңдеу осымен тоқтайды. Егер құрылғының атрибуттары бірден бірнеше ережеге сай келсе, онда құрылғы үлкен басымдыққа ие ереженің мақсатты тобына көшіріледі (ережелер тізімінде жоғары тұр).

Құрылғыны жылжыту ережелері айқын емес түрде жасалуы мүмкін. Мысалы, қашықтан орнату тапсырмасының немесе пакетінің сипаттарында, Желілік агентті орнатқаннан кейін құрылғы кіруі тиісті басқару тобы көрсетілуі мүмкін. Сондай-ақ, жылжыту ережелерін Kaspersky Security Center Linux әкімшісі айқын түрде **Активтерді басқару → Жылжыту ережелері** бөлімінде жасай алады.

Жылжыту ережесі, әдепкі бойынша құрылғыларды басқару топтарында бір рет бастапқы орналастыруға арналған. Ереже бөлінбеген құрылғыларды бір рет қана жылжытады. Егер құрылғы бір рет осы ережемен көшірілген болса, тіпті құрылғыны тағайындалмаған құрылғылар тобына қолмен қайтарған жағдайда да, ереже оны қайтадан көшірмейді. Бұл, жылжыту ережелерін қолданудың ұсынылатын тәсілі.

Басқару топтарында әлдеқашан орналастырылған құрылғыларды жылжытуға болады. Бұл үшін ереже сипаттарында **Тек басқару тобында орналастырылмаған құрылғыларды жылжыту** жалаушасын алып тастаңыз.

Басқару топтарында әлдеқашан орналастырылған құрылғыларға қолданылатын жылжыту ережелерінің болуы, Басқару серверіне түсетін жүктемені едәуір арттырады.

Тек басқару тобында орналастырылмаған құрылғыларды жылжыту жалаушасы автоматты түрде жасалған жылжыту ережелерінің сипаттарында бұғатталған. Мұндай ережелер *Бағдарламаларды қашықтан орнату* тапсырмасын қосқанда немесе автономды орнату пакетін жасағанда құрылады.

Бір құрылғыда көп рет әрекет ете алатын жылжыту ережесін жасауға болады.

Бір құрылғы топтан топқа көп рет жылжыту, мысалы, құрылғыға арнайы саясатты қолдану, арнайы топтық тапсырманы іске қосу, белгілі бір тарату нүктесінен жаңарту мақсатында басқарылатын құрылғылармен жұмыс істеу тәсілдемесінен аулақ болу қатаң ұсынылады.

Мұндай сценарийлерге қолдау көрсетілмейді, өйткені олар Басқару серверіне және желілік трафикке жүктеу бойынша онша тиімсіз. Сондай-ақ, бұл сценарийлер Kaspersky Security Center Linux жұмыс моделіне қарама-қайшы келеді (әсіресе, қатынасу құқықтары, оқиғалар мен есептер саласында). Басқа шешім іздеу, мысалы, саясат профильдерін, құрылғыларды таңдауға арналған тапсырмаларды қолдану, әдістемеге сәйкес желілік агенттерді тағайындау керек.

Бағдарламалық жасақтаманы санаттау

Қолданбаларды іске қосуды бақылаудың негізгі құралы *Kaspersky* санаттары болып табылады (бұдан әрі *KL санаттар*). KL санаттары Kaspersky Security Center Linux әкімшілеріне бағдарламалық жасақтаманы санатқа жатқызуға қолдау көрсетуді жеңілдетуге және басқарылатын құрылғыларға өтетін трафикті азайтуға көмектеседі.

Реттелмелі санаттарды бірде-бір KL санатқа түспейтін бағдарламалар үшін ғана жасау керек (мысалы, тапсырысқа әзірленген бағдарламалар үшін). Реттелмелі санаттар бағдарламаның дистрибутиві (MSI) негізінде немесе дистрибутивтері бар қалтаның негізінде жасалады.

Егер KL санаттармен категорияланбаған бағдарламалық жасақтаманың үлкен толықтырылатын топтамасы болса, автоматты түрде жаңартылатын санатты жасаған жөн. Мұндай санат автоматты түрде дистрибутивтері бар қалтаны өзгерту кезінде орындалатын файлдардың бақылау сомаларымен толықтырылады.

Басқару сервері параметрлерін сақтық көшірмелеу және қалпына келтіру

Басқару серверінің параметрлерін және ол қолданатын дерекқорды сақтық көшірмелеу үшін сақтық көшірмелеу тапсырмасы және klbackup утилитасы қарастырылған. Сақтық көшірме Басқару серверінің барлық негізгі параметрлері мен нысандарын қамтиды: Басқару серверінің сертификаттары, басқарылатын құрылғылардың дисктерін шифрлау кілттері-шебері, лицензияларға арналған кілттер, барлық мазмұны, тапсырмалары, саясаттары және тағы басқасы бар басқару топтарының құрылымы. Сақтық көшірмеге ие болып, Басқару серверінің жұмысын аз уақытта - ондаған минуттан екі сағатқа дейін қалпына келтіруге болады.

Сақтық көшірме болмаса, ақау сертификаттардың және Басқару серверінің барлық параметрлерінің қайтарымсыз жоғалуына әкелуі мүмкін. Ол үшін Kaspersky Security Center Linux жүйесін басынан бастап қайта конфигурациялау және желілік агентті ұйым желісіне қайтадан бастапқы орнату қажет болады. Сонымен қатар, басқарылатын құрылғылардың дисктерін шифрлау кілттері-шебері де жоғалады, бұл Kaspersky Endpoint Security-мен құрылғыларда шифрланған деректердің қайтарымсыз жоғалу қаупін тудырады. Сондықтан сақтық көшірудің штаттық тапсырмасы көмегімен Басқару серверінің сақтық көшірмелерін үнемі жасаудан бас тарту керек.

Жылдам іске қосу шебері басқару сервері параметрлерінің сақтық көшірме тапсырмасын жасайды және оны күнде 04:00-де іске қосылатындай орнатады. Сақтық көшірмелер әдепкісінше /var/opt/kaspersky/KSC_Backups* қалтасында сақталады.

Сақтық көшірме маңызды деректерді қамтиды, сондықтан сақтық көшірмелеу тапсырмасында және klbackup утилитасында сақтық көшірмелерді құпиясөзбен қорғау қарастырылған. Әдепкі бойынша сақтық көшірмелеу тапсырмасы бос құпиясөзбен жасалады. Сақтық көшірмелеу сипаттарында құпиясөзді міндетті түрде белгілеу керек. Бұл талапты сақтамау Басқару серверінің сертификаттарының кілттері, лицензияларға арналған кілттер және басқарылатын құрылғылардың дисктерін шифрлау кілттері-шебері шифрланбаған болатынына әкеледі.

Үнемі сақтық көшірмелеумен қатар, барлық маңызды өзгерістердің алдында, соның ішінде Басқару серверін жаңа нұсқаға дейін жаңартудың алдында және Басқару серверінің патчтарын орнатудың алдында сақтық көшірмені жасау керек.

> Сақтық көшірмеден қалпына келтіру klbackup утилитасы көмегімен сақтық көшірме жасалған нұсқадағы (немесе барынша жаңа) Басқару серверінің жаңа ғана орнатылған және жұмысқа қабілетті данасында орындалады.

Қалпына келтіру әрекеті орындалатын басқару серверінің данасында бірдей түрдегі DBMS және бірдей не кейінгі нұсқасы қолданылуы керек. Басқару серверінің нұсқасы сондай (ұқсас немесе барынша жаңа патчпен) немесе барынша жаңа болуы мүмкін.

Осы бөлімде параметрлерді және Басқару серверінің нысандарын қалпына келтірудің типтік сценарийлері сипатталған.

Басқару сервері бар құрылғы істен шықты

Егер ақау нәтижесінде Басқару сервері бар құрылғы істен шықса, келесі әрекеттерді орындау ұсынылады:

- Жаңа басқару серверіне бірдей DNS атауы тағайындалуы керек.

  Желілік агенттер орналастырылған кезде статикалық IP мекенжайы желілік агенттің орнату пакетінде орнатылған болса, жаңа басқару серверіне сол IP мекенжайын тағайындау керек. Сондай-ақ желілік агент қосылатын басқару серверін анықтайтын қосылым мекенжайын пайдалануға болады (бұл мекенжайды klnagchk утилитасын қолданып, басқарылатын құрылғыларда алуға болады).

- `var/opt/kaspersky/klnagent_srv/iam/iam_config.yaml` IAM конфигурация файлында `server_iam.ksc_address` параметрін бұрын пайдаланылған басқару сервері сертификатының тақырыптың балама атауында (SAN) көрсетілген дәл сол басқару серверінің мекенжайына орнатыңыз. Толығырақ ақпарат алу үшін келесі мақаланы қараңыз: Басқару сервері мекенжайын IAM сервер конфигурациясына қосу.

- Сол немесе барынша жаңа нұсқада, сондай түрдегі ДҚБЖ қолдана отырып Басқару серверін орнату. Сол немесе барынша жаңа патчы бар Сервердің нұсқасын немесе барынша жаңа нұсқаны орнатуға болады. Орнатқан соң шебердің көмегімен бастапқы конфигурациялауды орындамаған жөн.

- klbackup утилитасын іске қосыңыз және қалпына келтіру әрекетін орындаңыз. Сәтті қалпына келтіргеннен кейін Web Console веб-консолін қайта орнатыңыз.

Басқару серверінің параметрлері немесе дерекқор зақымдалған

Егер Басқару сервері параметрлердің немесе дерекқордың зақымдалуы нәтижесінде жұмысқа қабілетсіз болса (мысалы, қуат ақаулығы себебінен), қалпына келтірудің келесі сценарийін қолдану ұсынылады:

1. Зақымданған құрылғыда файлдық жүйені тексеруді орындау.

2. Басқару серверінің жұмысқа қабілетсіз нұсқасын деинсталляциялау.

3. Сол түрдегі, сол немесе барынша жаңа нұсқадағы ДҚБЖ қолдана отырып Басқару серверін қайтадан орнату. Сол немесе барынша жаңа патчы бар Сервердің нұсқасын немесе барынша жаңа нұсқаны орнатуға болады. Орнатқан соң шебердің көмегімен бастапқы конфигурациялауды орындамаған жөн.

4. klbackup утилитасын іске қосыңыз және қалпына келтіру әрекетін орындаңыз.

Басқару серверін klbackup штаттық утилитасынан басқа кез келген тәсілмен қалпына келтіруге болмайды.

Басқару серверін үшінші тараптың бағдарламалық жасақтамасымен қалпына келтіру әрекеті таратылған қолданбаның Kaspersky Security Center Linux жүйесіндегі түйіндерде деректердің бейсинхрондалуына, осылайша қолданбаның дұрыс жұмыс істемеуіне әкеледі.

Автономды пайдаланушыларға арналған қосылым профильдері туралы

Ноутбуктерді (бұдан әрі - "құрылғылар") пайдаланатын автономды пайдаланушылар жұмыс істеген кезде, құрылғының желідегі ағымдағы жайғасымына байланысты Басқару серверіне қосылу тәсілін өзгерту немесе Басқару серверлері арасында ауысу қажет болуы мүмкін.

Бір Басқару серверінің әртүрлі мекенжайларын пайдалану

Желілік агенті орнатылған құрылғылар әртүрлі уақыт аралығында ұйымның ішкі желісінен де, интернеттен де Басқару серверіне де қосыла алады. Бұл жағдайда, Желілік агент Басқару серверіне қосылу үшін әртүрлі мекенжайларды қолдануы қажет болуы мүмкін: интернеттен қосылған кезде Сервердің сыртқы мекенжайы және ішкі желіден қосылған кезде Сервердің ішкі мекенжайы.

Бұл үшін, Желілік агент саясатының сипаттарында интернеттен Басқару серверіне қосылу үшін профиль қосыңыз. Саясат сипаттары, **Байланыстардың профильдері** салынған бөлімінде профильді қосыңыз (**Қосылымдар** бөлімі). Профиль жасау терезесінде **Тек жаңартуларды алу үшін пайдалану** параметрін өшіріп, **Қосылым параметрлерін осы профильде көрсетілген Басқару серверінің параметрлерімен синхрондау** параметрін таңдау керек. Басқару серверіне кіру үшін қосылым шлюзі қолданылса (мысалы, "Интернет қосылымы: желілік агентті DMZ режимінде қосылым шлюзі ретінде пайдалану" бөлімінде сипатталғандай Kaspersky Security Center Linux конфигурациясында), қосылым профилінің тиісті өрісінде қосылым шлюзінің мекенжайын көрсетуіңіз керек.

Ағымдағы желіге байланысты Басқару серверлері арасында ауысу

Егер ұйымда әртүрлі Басқару серверлері бар бірнеше кеңселер болса және олардың арасында Желілік агенті орнатылған құрылғылардың бір бөлігі жылжытылса, онда Желілік агент құрылғы орналасқан кеңсенің жергілікті желісін Басқару серверіне қосылуы керек.

Бұл жағдайда, Желілік агент саясатының сипаттарында бастапқы үйдегі Басқару сервері орналасқан үйдегі кеңсені қоспағанда, әрбір кеңсе үшін Басқару серверіне қосылу профилін жасау керек. Байланыс профильдерінде тиісті Басқару серверлерінің мекенжайларын көрсетіп, **Тек жаңартуларды алу үшін пайдалану** параметрін таңдаңыз немесе өшіріңіз:

- Желілік агент үйдегі Басқару серверімен синхрондауды қажет етсе, ал жергілікті Сервер тек жаңартуларды жүктеу үшін пайдаланылса, параметрді таңдаңыз;
- Желілік агент жергілікті Басқару сервері тарапынан толығымен басқарылуы қажет болса, параметрді өшіріңіз.

Әрі қарай, сіз жасалған профильдерге ауысу шарттарын конфигурациялауыңыз керек: "үйдегі кеңсені" қоспағанда, кеңселердің әрқайсысы үшін кемінде бір шарт. Мұндай шарттардың әрқайсысының мәні кеңселердің біріне тән бөлшектерді желілік ортада табуға негізделеді. Егер шарт шындыққа айналса, тиісті профиль белсендіріледі. Егер шарттардың ешқайсысы дұрыс болмаса, Желілік агент үйдегі Басқару серверіне ауысады.

Желілік агентті басқа Басқару серверіне ауыстырып қосу туралы

Kaspersky Security Center Linux-те желінің келесі сипаттамалары өзгерген кезде клиент құрылғысының желілік агентін басқа басқару серверіне ауыстыру опциясы берілген:

- **DHCP сервері мекенжайына арналған шарт** – желідегі DHCP (Dynamic Host Configuration Protocol) серверінің IP мекенжайын өзгерту.

  DHCP сервері мекенжайына арналған шарт параметрі әзірше қолжетімді емес.

- **Әдепкі қосылым шлюзінің мекенжайына арналған шарт** – желінің негізгі шлюзін өзгерту.
- **DNS доменіне арналған шарт** – ішкі желінің DNS суффиксін өзгерту.
- **DNS сервері мекенжайына арналған шарт** – желідегі DNS серверінің IP мекенжайын өзгерту.
- **WINS сервері мекенжайына арналған шарт** – желідегі WINS серверінің IP мекенжайын өзгерту. Бұл параметр Windows операциялық жүйелері орнатылған құрылғылар үшін ғана қолжетімді.
- **Атау шешіміне арналған шарт** – клиент құрылғысында NetBIOS атауы немесе DNS атауы өзгерді.
- **Қосалқы желіге арналған шарт** – ішкі желі маскасы мен мекенжайын өзгерту.
- **Windows доменінің қолжетімділігіне арналған шарт** – клиент құрылғысы қосылып тұрған Windows доменінің күйін өзгерту. Бұл параметр Windows операциялық жүйелері орнатылған құрылғылар үшін ғана қолжетімді.
- **SSL қосылым мекенжайының қолжетімділігіне арналған шарт** – клиент құрылғысы көрсетілген сервермен (атауы:порты) SSL қосылымын орната алады немесе орната алмайды (сіз таңдаған параметрге байланысты). Қосылым үшін жоғары жүктемені және жиі желілік агент сұрауларын өңдей алатын бағдарламалық жасақтамасы бар арнайы серверді пайдалану керек. Басқару серверінің портын көрсетпеңіз. Әрбір Сервер үшін сіз SSL сертификатын қосымша түрде көрсете аласыз. Бұл жағдайда желілік агент SSL қосылымының мүмкіндігін тексерумен қатар, басқару серверінің сертификатын тексереді. Сертификаттар сай келмесе, қосылым орнатылмайды.

Желілік агентті Серверге қосудың бастапқы параметрлері Желілік агентті орнату кезінде белгіленеді. Алдағыда, Желілік агентті басқа Басқару серверлеріне ауыстырып қосу ережелері қалыптастырылған болса, Агент желі сипаттамаларының өзгертілуіне келесідей жауап қайтарады:

- Егер желінің сипаттамалары қалыптастырылған ережелердің ешбіріне сай келмесе, онда Желілік агент осы ережеде көрсетілген Басқару серверіне қосылады. Бұл ережемен белгіленген болса, клиент құрылғыларына орнатылған бағдарламалар автономды пайдаланушыларға арналған саясаттарға өтеді.

- Ережелердің ешбірі орындалмай жатса, онда Желілік агент орнату кезінде белгіленген Басқару серверіне қосылу бастапқы параметрлеріне қайта оралады. Клиент құрылғыларында орнатылған бағдарламалар белсенді саясаттарға қайта оралады.

- Басқару сервері қолжетімді болмаса, онда Желілік агент автономды пайдаланушыларға арналған саясаттарды қолданады.

> Желілік агент, **Басқару сервері қолжетімсіз болғанда автономды пайдаланушы режиміне ауысу** параметрі Желілік агент саясатының параметрлерінде қосылған болса ғана автономды пайдаланушыларға арналған саясатқа ауысып қосылады.

Желілік агентті Басқару серверіне қосу параметрлері қосылым профилінде сақталады. Қосылым профилінде сіз клиент құрылғыларын автономды пайдаланушыларға арналған саясаттарға көшіру ережелерін жасай аласыз, сондай-ақ профильді жаңартуларды жүктеп алу үшін қолданылатындай етіп конфигурациялай аласыз.

Автономды пайдаланушылар үшін қосылым профилін жасау

Желілік агентті автономды пайдаланушыларға арналған Басқару серверіне қосу профилін жасау үшін:

1. Егер сіз басқарылатын құрылғылар тобы үшін қосылым профилін жасағыңыз келсе, сол топтың Желілік агентінің саясатын ашыңыз. Бұл үшін келесі әрекеттерді орындаңыз:

   a. Бағдарламаның негізгі терезесінде **Активтерді басқару** → **Саясаттар** бөліміне өтіңіз.

   b. Қосылу профилін жасау қажет басқару тобын таңдаңыз:

      - Түбірлік топ үшін келесі қадамға өтуге болады.

      - Ішкі топ үшін беттің жоғарғы жағындағы **Иерархияны көрсету** түймесін басыңыз, содан кейін ашылатын терезеде ішкі топтың атауын басыңыз.

      Таңдалған топ жолы беттің жоғарғы жағында көрсетіледі. Қажет болса, топқа өту үшін басқару тобының атауы бар сілтемені басуға болады. Әдепкісінше жолдағы соңғы сілтеме белсенді емес. Сондай-ақ **Иерархияны жасыру** түймесін басу арқылы иерархия терезесін жабуға болады.

   c. Басқарылатын құрылғылар тобы үшін Желілік агент саясатын қосыңыз. Егер сіз оны әлдеқашан жасаған болсаңыз, саясат сипаттарын ашу үшін Желілік агент саясатының атауын басыңыз.

2. Егер сіз белгілі бір басқарылатын құрылғы үшін қосылым профилін жасағыңыз келсе, келесі әрекеттерді орындаңыз:

   a. Бағдарламаның негізгі терезесінде **Активтерді басқару** → **Активтер (құрылғылар)** бөліміне өтіңіз.

   b. Қажетті басқарылатын құрылғының атауын басыңыз.

c. Ашылған басқарылатын құрылғы сипаттары терезесінде **Бағдарламалар** қойыншасына өтіңіз.

d. Тек таңдалған басқарылатын құрылғы қолданылатын Желілік агент саясатының атауын басыңыз.

3. Ашылған сипаттар терезесінде **Бағдарлама параметрлері → Қосылым мүмкіндігі → Байланыс профильдері бөліміне өтіңіз.**

4. **Басқару серверіне байланыс профильдері** бөлімінде **Қосу** түймесін басыңыз.

   Әдепкі бойынша, қосылым профильдері тізімі <Офлайн-режим> және <Үйдегі Басқару сервері> профильдерін қамтиды. Профильдер өзгерту және жою үшін қолжетімді емес.

   <Офлайн-режим> профилінде қосылуға арналған Сервер көрсетілмейді. Осы профильге өту кезінде, Желілік агент қандай да бір Серверге қосылуға тырыспайды, ал клиент құрылғыларында орнатылған бағдарламалар болса автономды пайдаланушыларға арналған саясаттарды қолданады. <Офлайн-режим> профилі құрылғыны желіден ажырату шарттарында қолданылады.

   <Үйдегі Басқару сервері> профилінде, Желілік агентті орнату кезінде белгіленген қосылуға арналған Сервер көрсетілген. <Үйдегі Басқару сервері> профилі, басқа желіде жұмыс істеген құрылғы қайтадан үйдегі Басқару серверіне қосылатын шарттарда қолданылады.

5. Ашылған **Профильді конфигурациялау** терезесінде қосылым профилінің параметрлерін конфигурациялаңыз:

   - **Профиль атауы**

     Енгізу өрісінде қосылым профилінің атауын қарауға немесе өзгертуге болады.

   - **Басқару серверінің мекенжайы**

     Профильді белсендіру кезінде клиент құрылғысы қосылуы тиісті Басқару серверінің мекенжайы.

   - **Порт нөмірі**

     Қосылым орындалатын порт нөмірі.

   - **SSL порты**

     SSL протоколының көмегімен қосылым орындалатын порт нөмірі.

   - **SSL байланысын пайдалану**

     Бұл параметр қосулы болса, қосылым қорғалған порт арқылы орындалатын болады (SSL протоколының көмегімен).

     Әдепкі бойынша, параметр қосулы. Сіздің қосылымыңыз қауіпсіз болып қала беруі үшін, бұл параметрді өшірмеу ұсынылады.

   - Интернетке қосу үшін прокси-серверді қолдану керек болса, **Прокси-серверді пайдалану** параметрін таңдаңыз. Параметр таңдалған болса, параметрлерді енгізу өрістері қолжетімді болады. Прокси-серверге қосылудың келесі параметрлерін конфигурациялаңыз:

     - **Мекенжай**

       Kaspersky Security Center Linux-ті интернетке қосу үшін прокси-сервер мекенжайы.

     - **Порт нөмірі**

       Kaspersky Security Center Linux прокси-қосылымы орнатылатын порт нөмірі.

- **Прокси-сервердегі аутентификация**

  Жалауша қойылған болса, енгізу өрістерінде прокси-сервердегі түпнұсқалық растама үшін есептік деректерді көрсетуге болады.

- **Пайдаланушы аты**

  Прокси-серверге қосылатын пайдаланушы есептік жазбасы (**Прокси-сервердегі аутентификация** жалаушасы қойылған болса, өріс қолжетімді болады).

- **Құпиясөз**

  Прокси-серверге қосылуға мүмкіндік беретін пайдаланушы құпиясөзі (**Прокси-сервердегі аутентификация** жалаушасы қойылған болса, өріс қолжетімді болады).

  Енгізілген құпиясөзді қарау үшін, **Көрсету** түймесін басып, оны қажетті уақыт бойы ұстап тұрыңыз.

- **Қосылым шлюзінің мекенжайы**

  Клиент құрылғыларын Басқару серверіне қосатын шлюз мекенжайы.

- **Басқару сервері қолжетімсіз болғанда автономды пайдаланушы режиміне ауысу**

  Қосылу кезінде клиент құрылғысында орнатылған бағдарламалар автономды режимдегі құрылғыларға арналған саясаттардың профильдерін және Басқару сервері қолжетімді болмаса, автономды пайдаланушыларға арналған саясаттардың профильдерін қолдануы үшін осы жалаушаны қойыңыз. Бағдарлама үшін автономды пайдаланушыларға арналған саясат анықталмаған болса, бағдарлама белсенді саясатты қолданатын болады.

  Параметр өшірулі болса, бағдарламалар белсенді саясаттарды қолданатын болады.

  Әдепкі бойынша, жалауша алынып тасталған.

- **Тек жаңартуларды алу үшін пайдалану**

  Бұл параметр қосулы болса, профиль клиент құрылғысында орнатылған бағдарламалар жаңартуларды жүктеп алған кезде ғана қолданылатын болады. Қалған операциялар үшін Басқару серверіне қосылу Желілік агентті орнату кезінде белгіленген бастапқы қосылу параметрлерімен орындалатын болады.

  Әдепкі бойынша, параметр қосулы.

- **Қосылым параметрлерін осы профильде көрсетілген Басқару серверінің параметрлерімен синхрондау**

  Бұл параметр қосулы болса, Желілік агент профильдің сипаттарында көрсетілген параметрлерді қолдана отырып, Басқару серверіне қосылады.

  Бұл параметр өшірулі болса, Желілік агент орнату кезінде көрсетілген бастапқы параметрлерді қолдана отырып, Серверге қосылады.

  Тек жаңартуларды алу үшін пайдалану параметрі таңдалса, бұл параметр қолжетімді.

  Әдепкі бойынша, параметр өшірулі.

Нәтижесінде, Желілік агентті автономды пайдаланушыларға арналған Басқару серверіне қосу профилі жасалады. Желілік агентті осы профиль арқылы Серверге қосқан кезде, клиент құрылғысында орнатылған бағдарламалар автономды режимдегі құрылғыларға арналған саясаттарды немесе автономды пайдаланушыларға арналған саясаттарды қолданатын болады.

Басқарылатын құрылғыларға қашықтан қатынасу

Бұл бөлімде басқарылатын құрылғыларға қашықтан қатынасу туралы ақпарат бар.

Басқарылатын құрылғы мен Басқару сервері арасындағы тұрақты байланысты қамтамасыз ету үшін "Басқару серверімен байланысты үзбеу" параметрін қолдану

Push-серверлерді қолданбасаңыз, Kaspersky Security Center Linux басқарылатын құрылғылар мен басқару сервері арасында үздіксіз байланысты қамтамасыз етпейді. Басқарылатын құрылғылардағы Желілік агенттер мезгіл-мезгіл қосылым орнатып, Басқару серверімен синхрондалады. Мұндай синхрондау кезеңінің мерзімділігі Желілік агенттің саясатында белгіленеді. Ерте синхрондау қажет болса, онда Басқару сервері (немесе қажет болса, тарату нүктесі) қол қойылған желілік пакетті IPv4 желісі немесе IPv6 желісі арқылы Желілік агенттің UDP портына жібереді. Әдепкі бойынша порт нөмірі – 15000. Басқару серверінен басқарылатын құрылғыға UDP бойынша қосылу мүмкін болмаса, онда синхрондау әрекеті, синхрондау кезеңі ішінде Желілік агентті Серверге кезекті рет мезгіл-мезгіл қосу кезінде жүзеге асырылады.

Желілік агентті басқару серверіне алдын ала қоспайынша, жергілікті тапсырмаларды іске қосу және тоқтату немесе басқарылатын қолданбалар үшін статистиканы алу сияқты кейбір операцияларды орындау мүмкін емес. Бұл мәселені шешу үшін, егер сіз push-серверлерді қолданбасаңыз, сіз басқарылатын құрылғы мен Басқару сервері арасында тұрақты қосылымды қамтамасыз ететін **Басқару серверімен байланысты үзбеу** параметрін қолдана аласыз.

Басқарылатын құрылғы мен Басқару сервері арасындағы тұрақты қосылымды қамтамасыз ету үшін:

1. Бағдарламаның негізгі терезесінде **Активтерді басқару** → **Активтер (құрылғылар)** бөліміне өтіңіз.

   Басқарылатын құрылғылардың тізімі көрсетіледі.

2. Басқарылатын құрылғылар тізімінде қажетті құрылғының атауы бар сілтемеден өтіңіз.

3. Құрылғы сипаттары терезесінің **Жалпы** бөлімінде **Басқару серверімен байланысты үзбеу** опциясын қосыңыз.

Басқарылатын құрылғы мен Басқару сервері арасында тұрақты қосылым орнатылған.

Басқару серверімен байланысты үзбеу параметрі таңдалған құрылғылардың жалпы саны 300-ден аспауы тиіс.

Құрылғыны Басқару серверіне қосу уақытын тексеру туралы

Құрылғы өшірілген кезде Желілік агент Басқару серверін өшіру туралы хабарлайды. Kaspersky Security Center Web Console-де бұл құрылғы өшірілген деп көрсетіледі. Алайда, Агент барлық жағдайда Басқару серверіне хабарлай алмайды. Сол себепті басқару сервері әрбір құрылғыға арналған **Басқару серверіне қосылған** атрибутын (бұл атрибут мәні Kaspersky Security Center Web Console-дегі **Жалпы** бөлімінің құрылғы сипаттарында көрсетілген) және оны желілік агенттің ағымдағы параметрлеріндегі синхрондау аралығына қатысты салыстырады. Құрылғы үш синхрондау кезеңінен артық уақыт бойы байланысқа шықпаса, онда мұндай құрылғы өшірулі болып белгіленеді.

Мәжбүрлеп синхрондау туралы

Kaspersky Security Center Linux басқарылатын құрылғыларға арналған күйді, параметрлерді, тапсырмалар мен саясаттарды автоматты түрде синхрондағанына қарамастан, кейбір жағдайларда әкімші белгілі бір құрылғы үшін нақты уақытта синхрондау орындалып қойғанын нақты білуі қажет.

Басқарылатын құрылғының сипаттар терезесінде **Мәжбүрлеп синхрондау** түймесі бар. Kaspersky Security Center Linux синхрондау пәрменін жүргізген кезде, басқару сервері құрылғыға қосылуға әрекет жасайды. Егер бұл әрекет сәтті болса, мәжбүрлеп синхрондау орындалады. Әйтпесе, мәжбүрлеп синхрондау Желілік агент Сервермен байланыс орнатқаннан кейін ғана орындалады.

Өлшеу нұсқаулығы

Бұл нұсқаулықта Kaspersky Security Center Linux бағдарламасын масштабтау туралы ақпарат ұсынылған.

Осы нұсқаулық туралы

Kaspersky Security Center Linux өлшеу нұсқаулығы (сондай-ақ, бұдан әрі Kaspersky Security Center), Kaspersky Security Center орнатуды және басқаруды жүзеге асыратын мамандарға және Kaspersky Security Center пайдаланатын ұйымдарға техникалық қолдау көрсететін мамандарға арналған.

Барлық ұсыныстар мен есептеулер, Kaspersky Security Center Kaspersky бағдарламалық жасақтамасы орнатылған құрылғылардың қорғанысын басқаратын желілер үшін келтірілген.

Әртүрлі жұмыс шарттарында оңтайлы өнімділікке қол жеткізу және оны сақтау үшін, желідегі құрылғылардың санын, желі топологиясын және өзіңізге қажетті Kaspersky Security Center функциялар жиынтығын ескеруіңіз қажет.

Нұсқаулықта келесі ақпарат келтірілген:

- Kaspersky Security Center шектеулері
- Kaspersky Security Center өзекті түйіндері – Басқару серверлері мен тарату нүктелері үшін есептеу туралы:
  - Басқару серверлері мен тарату нүктелеріне қойылатын аппараттық талаптар туралы
  - Басқару серверлерінің саны мен иерархиясын есептеу туралы
  - Тарату нүктелерінің саны мен конфигурациясын есептеу туралы
- Желідегі құрылғылар санына байланысты, дерекқордағы оқиғаларды сақтау параметрлерін конфигурациялау туралы
- Өнімділікті оңтайландыруға қатысты жалпы қабылданған озық тәжірибелер
- Kaspersky Security Center оңтайлы өнімділігін қамтамасыз ету үшін кейбір тапсырмалардың параметрлерін конфигурациялау туралы
- Kaspersky Security Center Басқару сервері мен әрбір қорғалатын құрылғы арасындағы трафикті (желіге түсетін жүктемені) тұтыну туралы

Бұл нұсқаулыққа келесі жағдайларда жүгіну ұсынылады:

- Kaspersky Security Center орнату алдында ресурстарды жоспарлау кезінде
- Kaspersky Security Center орналастырылған желі өлшемінің елеулі өзгерістерін жоспарлау кезінде
- Желінің шектеулі сегментінде (сынақ ортасы) Kaspersky Security Center-ді пайдаланудан корпоративтік желіде Kaspersky Security Center-ді толық ауқымды түрде орналастыруға көшкен кезде
- Kaspersky Security Center қолданылатын функциялары жиынтығына өзгерістер енгізілген кезде

Басқару серверлері үшін есептеулер

Бұл бөлімде Басқару серверлері ретінде пайдаланылатын құрылғыларға арналған аппараттық және бағдарламалық талаптар келтірілген. Сондай-ақ, ұйым желісінің конфигурациясына байланысты Басқару серверлерінің санын және олардың иерархиясын есептеу бойынша ұсыныстар берілген.

Құрылғыларға Басқару сервері мен ДҚБЖ-ны орнатқаннан кейін, осы құрылғыларға Kaspersky Endpoint Security for Linux орнатуды ұсынамыз. Kaspersky Endpoint Security аппараттық құралдарына қойылатын талаптарды Kaspersky Endpoint Security for Linux анықтамасынан қараңыз.

Kaspersky Endpoint Security for Linux бағдарламасы Kaspersky Managed Detection and Response және Kaspersky Endpoint Detection and Response Expert (on-premise) шешімдерімен біріктірілген кезде тудыратын жүктеме Kaspersky Security Center Linux және Kaspersky Security Center Linux бағдарламаларын бірлесіп орнату есептеулерінде ескерілмейді.

Басқару сервері үшін аппараттық ресурстарды есептеу

Бұл бөлімде Басқару серверіне арналған аппараттық ресурстарды жоспарлау кезінде басшылыққа алуға болатын есептеулер келтірілген.

ДҚБЖ және Басқару серверіне арналған аппараттық талаптар

Төмендегі кестелерде тестілеу кезінде алынған ДҚБЖ мен Басқару серверінің ұсынылған минималды аппараттық талаптары келтірілген. Қолдау көрсетілетін операциялық жүйелер мен ДҚБЖ толық тізімі аппараттық және бағдарламалық талаптар тізбесінде келтірілген.

> Басқару сервері орнатылған құрылғыда swap файлын қосу керек. swap файлының ең аз өлшемі жедел жад көлемінен 1.5 есе үлкен болуы керек.

Құрылғыларға Басқару сервері мен ДҚБЖ-ны орнатқаннан кейін, осы құрылғыларға Kaspersky Endpoint Security for Linux орнатуды ұсынамыз.
Бірлесіп орнату үшін сізде кемінде 225 IOPS болуы керек және Басқару серверінің талаптарына 1,5 ГБ жедел жадыны (DBMS) қосу керек.
Kaspersky Endpoint Security аппараттық құралдарына қойылатын талаптарды Kaspersky Endpoint Security for Linux анықтамасынан қараңыз.

Желіде 50,000 құрылғы бар

Басқару сервері бар құрылғының конфигурациясы

Жабдық	Мән
Процессор	8 ядро (12 ядро ұсынылады), 2500 МГц

ЖЖҚ	16 ГБ
Диск кеңістігі	300 ГБ, 150 IOPS немесе одан жоғары

PostgreSQL ДҚБЖ орнатылған құрылғының конфигурациясы

Жабдық	Мән
Процессор	16 ядро, 2500 МГц
ЖЖҚ	32 ГБ
Диск кеңістігі	300 ГБ, 150 IOPS немесе одан жоғары

Ақауларға төзімді кластерге арналған түйіндер конфигурациясы

Жабдық	Мән
Процессор	16 ядро, 2500 МГц
ЖЖҚ	32 ГБ
Диск кеңістігі	500 ГБ, 300 IOPS немесе одан жоғары
Желілік интерфейс контроллері	1 Гбит/с

Басқару сервері және PostgreSQL ДҚБЖ орнатылған құрылғы конфигурациясы

Жабдық	Мән
Процессор	24 ядро (28 ядро ұсынылады), 2500 МГц
ЖЖҚ	48 ГБ
Диск кеңістігі	600 ГБ, 300 IOPS немесе одан жоғары

Желіде 30,000 құрылғы бар

Басқару сервері бар құрылғының конфигурациясы

Жабдық	Мән
Процессор	6 ядро (8 ядро ұсынылады), 2500 МГц
ЖЖҚ	12 ГБ
Диск кеңістігі	200 ГБ, 150 IOPS немесе одан жоғары

PostgreSQL ДҚБЖ орнатылған құрылғының конфигурациясы

Жабдық	Мән
Процессор	12 ядро, 2500 МГц
ЖЖҚ	22 ГБ
Диск кеңістігі	250 ГБ, 150 IOPS немесе одан жоғары

Ақауларға төзімді кластерге арналған түйіндер конфигурациясы

Жабдық	Мән
Процессор	16 ядро, 2500 МГц
ЖЖҚ	32 ГБ
Диск кеңістігі	500 ГБ, 300 IOPS немесе одан жоғары
Желілік интерфейс контроллері	1 Гбит/с

Басқару сервері және PostgreSQL ДҚБЖ орнатылған құрылғы конфигурациясы

Жабдық	Мән
Процессор	16 ядро (20 ядро ұсынылады), 2500 МГц
ЖЖҚ	34 ГБ
Диск кеңістігі	450 ГБ, 300 IOPS немесе одан жоғары

Желіде 10,000 құрылғы бар

Басқару сервері бар құрылғының конфигурациясы

Жабдық	Мән
Процессор	4 ядро (6 ядро ұсынылады), 2500 МГц
ЖЖҚ	8 ГБ
Диск кеңістігі	100 ГБ, 150 IOPS немесе одан жоғары

PostgreSQL ДҚБЖ орнатылған құрылғының конфигурациясы

Жабдық	Мән
Процессор	6 ядро, 2500 МГц
ЖЖҚ	10 ГБ
Диск кеңістігі	200 ГБ, 150 IOPS немесе одан жоғары

Ақауларға төзімді кластерге арналған түйіндер конфигурациясы

Жабдық	Мән
Процессор	16 ядро, 2500 МГц
ЖЖҚ	32 ГБ
Диск кеңістігі	500 ГБ, 300 IOPS немесе одан жоғары
Желілік интерфейс контроллері	1 Гбит/с

Басқару сервері және PostgreSQL ДҚБЖ орнатылған құрылғы конфигурациясы

Жабдық	Мән
Процессор	8 ядро (14 ядро ұсынылады), 2500 МГц
ЖЖҚ	18 ГБ
Диск кеңістігі	300 ГБ, 300 IOPS немесе одан жоғары

Желіде 1000 құрылғы бар

Басқару сервері бар құрылғының конфигурациясы

Жабдық	Мән
Процессор	2 ядро, 2500 МГц
ЖЖҚ	6 ГБ
Диск кеңістігі	10 ГБ, 150 IOPS немесе одан жоғары

PostgreSQL ДҚБЖ орнатылған құрылғының конфигурациясы

Жабдық	Мән
Процессор	2 ядро, 2500 МГц
ЖЖҚ	4 ГБ
Диск кеңістігі	20 ГБ, 150 IOPS немесе одан жоғары

Ақауларға төзімді кластерге арналған түйіндер конфигурациясы

Жабдық	Мән
Процессор	16 ядро, 2500 МГц
ЖЖҚ	32 ГБ
Диск кеңістігі	500 ГБ, 300 IOPS немесе одан жоғары
Желілік интерфейс контроллері	1 Гбит/с

Басқару сервері және PostgreSQL ДҚБЖ орнатылған құрылғы конфигурациясы

Жабдық	Мән
Процессор	4 ядро, 2500 МГц
ЖЖҚ	10 ГБ
Диск кеңістігі	30 ГБ, 300 IOPS немесе одан жоғары

Тестілеу келесі конфигурациялармен жүргізілді:

- Басқару серверінде тарату нүктелерін автоматты түрде тағайындау қосылған немесе тарату нүктелері ұсынылған кестеге сәйкес қолмен тағайындалған;
- PostgreSQL ДҚБЖ жүйесі plpgsql-ден басқа кеңейтімдерді қамтымайды.

ДҚБЖ орнатылған құрылғыда дерекқор шамамен 100 ГБ дискілік орынды, ал транзакциялар журналы шамамен 200 ГБ дискілік орынды алады.

Дерекқорда орынды есептеу

Дерекқордағы орынды келесі формула бойынша шамамен бағалауға болады:

(600 * C + 2.3 * E + 2.5 * A + 1.2 * N * F), КБ,

мұндағы

- "C" – құрылғылар саны.

  Егер басқарылатын құрылғылар құрамында динамикалық виртуалды машиналар болса, онда "C" — бұл динамикалық емес басқарылатын құрылғылар саны мен **Басқару серверіне техникалық қызмет көрсету** тапсырмасының екі рет қатар іске қосылуы аралығында жасалған, Желілік агенті бар динамикалық виртуалды машиналар санының қосындысы.

- "E" – сақталатын оқиғалар саны.

- "A" – Active Directory нысандарының жиынтық саны:
  - Құрылғылардың есептік жазбалары
  - Пайдаланушы есептік жазбалары
  - Қауіпсіздік топтарының есептік жазбалары
  - Active Directory бөлімшелері

  Active Directory сканерлеу өшірулі болса, онда "A" нөлге тең болып саналуы керек.
- N – соңғы құрылғыдағы түгенделетін орындалатын файлдардың орташа саны.
- F – орындалатын файлдар түгенделген соңғы құрылғылардың саны.

Егер сіз Kaspersky Endpoint Security саясатының параметрлерінде Басқару серверін іске қосылатын бағдарламалар туралы хабардар етуді қосуды жоспарласаңыз, онда іске қосылатын бағдарламалар туралы ақпаратты дерекқорда сақтау үшін қосымша (0,03 * C) ГБ қажет болады.

Жұмыс барысында, дерекқорда *бос кеңістік* (unallocated space) деп аталатын орын пайда болады. Сондықтан, дерекқор файлының нақты өлшемі көбінесе дерекқордағы орын көлемінен шамамен екі есе көп.

Транзакциялар журналының өлшемін нақты шектеу ұсынылмайды. MAXSIZE параметрінің әдепкі мәнін қалдыру ұсынылады.

Дискідегі орынды есептеу

/var/opt/kaspersky/klnagent_srv/ қалтасы үшін қажетті басқару сервері дискісіндегі орынды келесі формула арқылы шамамен есептеуге болады:

(724 * C + 0.15 * E + 0.17 * A), КБ

мұндағы

- "C" – құрылғылар саны.

  Егер басқарылатын құрылғылар құрамында динамикалық виртуалды машиналар болса, онда "C" — бұл динамикалық емес басқарылатын құрылғылар саны мен **Басқару серверіне техникалық қызмет көрсету** тапсырмасының екі рет қатар іске қосылуы аралығында жасалған, Желілік агенті бар динамикалық виртуалды машиналар санының қосындысы.
- "E" – сақталатын оқиғалар саны.
- "A" – Active Directory нысандарының жиынтық саны:
  - Құрылғылардың есептік жазбалары
  - Пайдаланушы есептік жазбалары
  - Қауіпсіздік топтарының есептік жазбалары
  - Active Directory бөлімшелері

Active Directory сканерлеу өшірулі болса, онда "A" нөлге тең болып саналуы керек.

Басқару серверлерінің саны мен конфигурациясын есептеу

Негізгі Басқару серверіндегі жүктемені азайту үшін, әр басқару тобына жеке Басқару серверін тағайындауға болады. Негізгі Серверге бағынатын Басқару серверлерінің саны 500-ден аспауы керек.

Басқару серверлерінің конфигурациясын ұйымыңыздағы желінің қалай конфигурацияланғанына байланысты құру ұсынылады.

Динамикалық виртуалды машиналарды Kaspersky Security Center бағдарламасына қосу бойынша ұсыныстар

Динамикалық виртуалды машиналар статикалық виртуалды машиналарға қарағанда көбірек ресурстарды пайдаланады.

Динамикалық виртуалды машиналар туралы қосымша ақпаратты Динамикалық виртуалды машиналарды қолдау бөлімінен қараңыз.

Жаңа динамикалық виртуалды машинаны қосқанда, Kaspersky Security Center Linux жүйесі Kaspersky Security Center Web Console консолінде осы динамикалық виртуалды машинаның жазбасын жасайды және динамикалық виртуалды машинаны басқару топқа жылжытады. Содан соң, динамикалық виртуалды машина Басқару сервері дерекқорына қосылады. Басқару сервері осы динамикалық виртуалды машинада орнатылған Желілік агентпен толық синхрондалған.

Ұйымның желісінде Желілік агент әрбір динамикалық виртуалды машина үшін келесі желілік тізімдерді жасайды:

- Жабдық
- Орнатылған бағдарламалық жасақтама
- Анықталған осалдықтар
- Бағдарламаларды басқару құрамдасының оқиғалары мен орындалатын файл тізімдері

Желілік агент осы желілік тізімдерді Басқару серверіне жібереді. Желілік тізімдердің өлшемі динамикалық виртуалды машинада орнатылған құрамдастарға байланысты, сондай-ақ Kaspersky Security Center Linux және дерекқорларды басқару жүйесінің (ДҚБЖ) өнімділігіне әсер етуі мүмкін. Жүктеме сызықты емес түрде өсуі мүмкін екенін ескеріңіз.

Пайдаланушы динамикалық виртуалды машинамен жұмыс істеп, оны өшіргеннен кейін, бұл машина виртуалды инфрақұрылымнан жойылады, ол туралы жазбалар Басқару сервері дерекқорынан жойылады.

Бұл әрекеттердің барлығы Kaspersky Security Center Linux бағдарламасы мен Басқару сервері дерекқорының көп ресурсын пайдаланады әрі Kaspersky Security Center Linux және ДҚБЖ өнімділігін төмендетуі мүмкін. Kaspersky Security Center Linux бағдарламасына 20 000-ға дейін динамикалық виртуалды машинаны қосу ұсынылады.

Қосылған динамикалық виртуалды машиналар стандартты операцияларды орындаса (мысалы, дерекқорды жаңарту) және ең көбі жадтың 80%-н және қолжетімді ядролардың 75-80%-н тұтынса, Kaspersky Security Center Linux бағдарламасына 20 000-нан астам динамикалық виртуалды машинаны қосуға болады.

Динамикалық виртуалды машинада саясат, бағдарламалық жасақтама немесе операциялық жүйе параметрлерін өзгерту ресурстарды тұтынуды азайтуы немесе арттыруы мүмкін. Ресурстардың 80-95%-н тұтыну оңтайлы болып саналады.

Тарату нүктелері мен қосылым шлюздеріне арналған есептеулер

Бұл бөлімде тарату нүктелері ретінде пайдаланылатын құрылғыларға қойылатын аппараттық талаптар және ұйым желісінің конфигурациясына байланысты тарату нүктелері мен қосылым шлюздерінің санын есептеу бойынша ұсыныстар берілген.

Тарату нүктесі үшін талаптар

Windows және Linux жүйесімен жұмыс істейтін тарату нүктелеріне қойылатын аппараттық және бағдарламалық жасақтама талаптары осы мақалада сипатталған.

Басқару серверінде қашықтан орнату тапсырмалары болған жағдайда, тарату нүктесі бар құрылғыда орнатылатын орнату пакеттерінің жиынтық өлшеміне тең келетін диск кеңістігі қосымша түрде қажет болады.

Басқару серверінде жаңартуларды (патчтарды) орнату және тарату нүктесі бар құрылғыдағы осалдықтарды түзету тапсырмасының бір немесе бірнеше данасы болған кезде барлық орнатылатын патчтардың екі еселенген жиынтық өлшеміне тең диск кеңістігі қосымша түрде қажет болады.

Егер тарату нүктелері дерекқорлар мен бағдарлама модульдеріне жаңартуларды тікелей Kaspersky жаңарту серверлерінен алатын схеманы пайдалансаңыз, тарату нүктелері интернет желісіне қосылған болуы керек.

Басқару серверін тарату нүктесі ретінде тағайындамаған жөн, себебі басқару серверіне түсетін жүктеме артады.

Windows негізіндегі тарату нүктелеріне қойылатын аппараттық талаптар

Windows негізіндегі тарату нүктелеріне қойылатын минималды аппараттық талаптар

Клиенттік құрылғылар саны	Процессор	ЖЖҚ	Жедел жад көлемі, түзетулерді басқару қосылған	Диск кеңістігі
10 000	4 ядро, 2500 МГц	8 ГБ	8 ГБ	120 ГБ
5000	4 ядро, 2500 МГц	6 ГБ	8 ГБ	120 ГБ
1000	2 ядро, 2500 МГц	4 ГБ	8 ГБ	120 ГБ

Linux жұмыс істейтін тарату нүктелеріне қойылатын аппараттық талаптар

Linux жүйесінде жұмыс істейтін тарату нүктелеріне қойылатын минималды аппараттық талаптар

Клиенттік құрылғылар саны	Процессор	ЖЖҚ	Диск кеңістігі
10 000	4 ядро, 2500 МГц	10 ГБ	120 ГБ
5000	4 ядро, 2500 МГц	8 ГБ	120 ГБ
1000	2 ядро, 2500 МГц	6 ГБ	120 ГБ

Тарату нүктелерінің саны мен конфигурациясын есептеу

Желіде клиент құрылғылары неғұрлым көп болса, тарату нүктелері да соғұрлым көп қажет болады. Тарату нүктелерін автоматты түрде тағайындауды өшірмеу ұсынылады. Тарату нүктелерін автоматты түрде тағайындау қосылған кезде, егер клиент құрылғыларының саны айтарлықтай көп болса, Басқару сервері тарату нүктелерін тағайындайды және олардың конфигурациясын анықтайды.

Арнайы бөлінген тарату нүктелерін пайдалану

Егер сіз тарату нүктелері ретінде белгілі бір құрылғыларды (мысалы, бұл үшін бөлінген серверлер) пайдалануды жоспарласаңыз, онда тарату нүктелерін автоматты түрде тағайындауды пайдаланбауға болады. Бұл жағдайда, тарату нүктелері ретінде тағайындағыңыз келетін құрылғыларда дискіде жеткілікті бос орын бар екеніне, олар үнемі өшірілмейтініне және "ұйқы режимі" өшірілгеніне көз жеткізіңіз.

Желілік құрылғылардың санына байланысты бір сегменті бар желідегі бірегей тағайындалған тарату нүктелерінің саны

Желі сегменттерінің әрқайсысындағы клиент құрылғыларының саны	Тарату нүктелерінің саны
300-нан кем	0 (тарату нүктелері керек емес)
300-нан артық	Қолайлы: (N/10 000 + 1), ұсынылады: (N/5000 + 2), мұндағы N желідегі құрылғылар саны

Желілік құрылғылардың санына байланысты бірнеше сегменті бар желідегі бірегей тағайындалған тарату нүктелерінің саны

Желі сегментіндегі клиент құрылғыларының саны	Тарату нүктелерінің саны
10-нан кем	0 (тарату нүктелері керек емес)
10–100	1
100-нан артық	Қолайлы: (N/10 000 + 1), ұсынылады: (N/5000 + 2), мұндағы N желідегі құрылғылар саны

Клиент құрылғыларын (жұмыс станцияларын) тарату нүктелері ретінде пайдалану

Егер сіз әдеттегі клиент құрылғысын (жұмыс станциясын) тарату нүктесі ретінде пайдалануды жоспарласаңыз, байланыс арналары мен Басқару серверіне шамадан тыс жүктемені болдырмау үшін төмендегі кестеде көрсетілгендей тарату нүктесін тағайындау ұсынылады:

Желілік құрылғылардың санына байланысты желінің бір сегментін қамтитын желідегі тарату нүктелерінің рөлін атқаратын жұмыс станцияларының саны

Желі сегменттерінің әрқайсысындағы клиент құрылғыларының саны	Тарату нүктелерінің саны
300-нан кем	0 (тарату нүктелері керек емес)
300-нан артық	(N/300 +1), мұндағы N – желідегі құрылғылардың саны; кемінде 3 тарату нүктесі

Желілік құрылғылардың санына байланысты желінің бірнеше сегментін қамтитын желідегі тарату нүктелерінің рөлін атқаратын жұмыс станцияларының саны

Желі сегментіндегі клиент құрылғыларының саны	Тарату нүктелерінің саны
10-нан кем	0 (тарату нүктелері керек емес)
10–30	1
31–300	2
300-нан артық	(N/300 +1), мұндағы N – желідегі құрылғылардың саны; кемінде 3 тарату нүктесі

Егер тарату нүктесі өшірілген болса немесе басқа себептерге байланысты қолжетімді болмаса, онда басқарылатын құрылғылар жаңартулар алу үшін осы тарату нүктесінің әрекет ету ауқымынан Басқару серверіне жүгіне алады.

Қосылым шлюздерінің санын есептеу

Егер сіз қосылым шлюзін пайдалануды жоспарласаңыз, бұл функция үшін бөліп берілген құрылғыны пайдалану ұсынылады.

Бір қосылым шлюзі 10000-нан аспайтын басқарылатын құрылғыға қызмет көрсетеді.

Тапсырмалар мен саясаттар үшін оқиғалар туралы ақпаратты сақтау

Бұл бөлімде Басқару сервері дерекқорында оқиғаларды сақтаумен байланысты есептеулер келтірілген және оқиғалар санын азайту және осылайша Басқару серверіне түсетін жүктемені азайту бойынша ұсыныстар берілген.

Әдепкі бойынша, әр тапсырманың және әр саясаттың сипаттарында тапсырманы орындауға және саясатты қолдануға байланысты барлық оқиғалардың журналында сақталуы көрсетілген.

Алайда, егер тапсырма жеткілікті жиі (мысалы, аптасына бір реттен көп) және құрылғылардың жеткілікті көп санында (мысалы, 10 000-нан астам) іске қосылса, оқиғалар саны тым көп болуы және оқиғалар дерекқорды толтыруы мүмкін. Бұл жағдайда, тапсырманың сипаттарында қалған екі нұсқаның бірін көрсету ұсынылады:

- **Тапсырманы орындау барысына қатысты оқиғаларды сақтау**. Бұл жағдайда, тапсырма орындалған әрбір құрылғыдан дерекқорға тек тапсырманың іске қосылуы, оның барысы және оның орындалуы туралы ақпарат келеді (сәтті, ескертумен немесе қатемен).

- **Тек тапсырманы орындау нәтижелерін сақтау**. Бұл жағдайда, тапсырма орындалған әрбір құрылғыдан дерекқорға тек тапсырманың орындалуы туралы ақпарат (сәтті, ескертумен немесе қатемен) келеді.

Егер саясат құрылғылардың жеткілікті көп саны үшін анықталса (мысалы, 10 000-нан астам), оқиғалар саны да тым көп болуы және оқиғалар дерекқорды толтыруы мүмкін. Бұл жағдайда, саясат сипаттарында тек маңызды оқиғаларды таңдап, оларды сақтауды қосу ұсынылады. Барлық басқа оқиғаларды сақтауды өшіру ұсынылады.

Осылайша, сіз дерекқордағы оқиғалардың санын азайтасыз, дерекқордағы оқиғалар кестесін талдаумен байланысты сценарийлердің жұмыс жылдамдығын арттырасыз және критикалық оқиғаларды оқиғалардың көп санымен ығыстыру қаупін азайтасыз.

Сондай-ақ, тапсырмаға немесе саясатқа қатысты оқиғаларды сақтау мерзімін қысқартуға болады. Әдепкі бойынша, бұл мерзім тапсырмамен байланысты оқиғалар үшін жеті күнді және саясатқа қатысты оқиғалар үшін 30 күнді құрайды. Сақтау мерзімі өзгерген кезде ұйымыңызда қабылданған жұмыс тәртібін және жүйе әкімшісінің әрбір оқиғаны талдауға қанша уақыт бөле алатынын ескеріңіз.

Оқиғаларды сақтау параметрлеріне келесі жағдайлардың кез келгенінде өзгерістер енгізген жөн:

- топтық тапсырмалардың аралық күйлерінің өзгеруі туралы және саясаттарды қолдану туралы оқиғалар Kaspersky Security Center Linux дерекқорындағы барлық оқиғалардың едәуір пайызын алады;
- Операциялық жүйенің оқиғалар журналында дерекқорда сақталатын оқиғалардың жалпы санына белгіленген шектен асқан кезде оқиғаларды автоматты түрде жою туралы жазбалар пайда болады.

Күніне бір құрылғыдан келетін оқиғалардың оңтайлы саны 20-дан аспауы керек деген негізде оқиғаларды тіркеу параметрлерін таңдаңыз. Қажет болса, желіңіздегі құрылғылар саны салыстырмалы түрде аз болған жағдайда ғана (10 000-нан аз), оқиғалардың ең көп санын аздап көбейтуге болады.

Көптеген құрылғыны басқаратын басқару серверіне арналған ең озық тәжірибелер

ДҚБЖ пайдаланудың озық тәжірибелері

Басқару серверіне техникалық қызмет көрсету тапсырмасын жүйелі түрде орындау мүмкіндігін реттеңіз (әсіресе PostgreSQL ДҚБЖ пайдалансаңыз).

ДҚБЖ қалтасын IOC тексерісінен шығарыңыз.

Саясаттар мен саясат профильдеріне арналған озық тәжірибелер

Құрамдасқа (мысалы, Windows үшін Kaspersky Endpoint Security) арналған белсенді саясаттардың санын азайтыңыз. Саясаттарды саясат профильдерімен ауыстыруға болады.

Көптеген құрылғыны басқаратын басқару серверіне арналған ең озық тәжірибелер

Бір уақытта орындалып жатқан тапсырмалардың, әсіресе қашықтан орнату немесе пачтарды басқару тапсырмаларының санын азайтыңыз.

Тапсырмалар санын азайтыңыз және құрылғы таңдауларымен жұмыс істейтін тапсырмаларға арналған кестені оңтайландырыңыз.

Оқиғаларды конфигурациялау саясатының параметрлері бөлімінде сақталатын оқиға түрлерінің санын азайтыңыз.

Оқиғаларды сақтаудың ең озық тәжірибелері

Қолданбаларды басқару компонентінен ұқсас оқиғалардың жиілігін азайтыңыз. Мәліметтер алу үшін келесі мақаланы қараңыз: Жиі болатын оқиғаларды бұғаттау туралы.

Құрамдастар (мысалы, Windows үшін Kaspersky Endpoint Security) оқиғаларын және осалдықтарды жабудың ақпараттық оқиғаларын сақтау мерзімін азайтыңыз.

Жаңарту тапсырмалары сияқты жалпы тапсырмаларға арналған тапсырма сипаттарында **Тапсырманы орындау барысына қатысты оқиғаларды сақтау** параметрін қосыңыз. Мәліметтер алу үшін келесі мақаланы қараңыз: Тапсырмалар мен саясаттар үшін оқиғалар туралы ақпаратты сақтау.

Түгендеу тапсырмасының параметрлерін оңтайландырыңыз. Мәліметтер алу үшін келесі мақаланы қараңыз: Түгендеу тапсырмасы.

Кейбір тапсырмалардың ерекшеліктері мен оңтайлы параметрлері

Кейбір тапсырмалар желідегі құрылғылар санымен байланысты ерекшеліктерге ие. Бұл бөлімде осындай тапсырмалар үшін параметрлерді оңтайлы конфигурациялау бойынша ұсыныстар берілген.

Құрылғыларды анықтау, деректерді сақтық көшірмелеу тапсырмасы, дерекқорға қызмет көрсету тапсырмасы және Kaspersky Endpoint Security жаңарту топтық тапсырмалары Kaspersky Security Center Linux базалық функционалдығына кіреді.

Түгендеу тапсырмасы Осалдықтар мен патчтарды басқару мүмкіндігіне кіреді және бұл мүмкіндік белсендірілмесе, қолжетімді емес.

Құрылғыны табу жиілігі

Әдепкі бойынша белгіленген құрылғыларды іздеу жиілігін арттыру ұсынылмайды, себебі бұл доменнің контроллерлеріне шамадан тыс жүктеме түсіруі мүмкін. Керісінше, сіздің ұйымыңыздың қажеттіліктері мүмкіндік беретін ең төменгі жиілікпен сауалнама өткізу кестесін белгілеу ұсынылады. Төмендегі кестеде оңтайлы кестені есептеу бойынша ұсыныстар берілген.

Құрылғыларды анықтау кестесі

Желідегі құрылғылардың саны	Құрылғыларды табу үшін ұсынылатын жиілік
10,000-нан кем	Әдепкі бойынша белгіленген немесе сирек
10 000 және одан да көп	Тәулігіне бір рет немесе сирек

Басқару сервері деректерінің резервтік қоймасы және дерекқорға қызмет көрсету тапсырмалары

Басқару сервері келесі тапсырмаларды орындау кезінде жұмысын тоқтатады:

- Басқару сервері деректерінің сақтық көшірмесін жасау
- Басқару серверіне техникалық қызмет көрсету

Бұл тапсырмалар орындалып жатқанда, деректер дерекқорға келіп түсе алмайды.

Осы тапсырмалардың кестесін, олардың орындалуы уақыт бойынша Басқару серверінің басқа тапсырмаларын орындаумен қиылыспайтындай етіп өзгерту керек болуы мүмкін.

Kaspersky Endpoint Security жаңарту топтық тапсырмалары

Жаңартулар көзі Басқару сервері болса, онда Kaspersky Endpoint Security 10 және одан да жоғары нұсқасын жаңартудың топтық тапсырмалары үшін, **Тапсырманы іске қосуды тарату үшін аралықты автоматты түрде анықтау** жалаушасы қойылған **Қоймаға жаңартуларды жүктеу кезінде** кестесі ұсынылады.

Kaspersky серверлерінен жаңартуларды қоймаға жүктеу жергілікті тапсырмасын әрбір тарату нүктесінде жасаған болсаңыз, онда Kaspersky Endpoint Security жаңартудың топтық тапсырмасы үшін мерзімді кестені белгілеу ұсынылады. Бұл жағдайда, автономизация кезеңінің мәні бір сағатты құрауы тиіс.

Түгендеу тапсырмасы

Орнатылған файлдар туралы ақпаратты алу арқылы дерекқорға түсетін жүктемені азайтуға болады. Ол үшін, Kaspersky Endpoint Security бағдарламасына арналған түгендеу тапсырмасын стандартты бағдарламалар жинағы орнатылған бірнеше эталондық құрылғыларда орындау ұсынылады.

Басқару сервері бір құрылғыдан алынатын орындалатын файлдар саны 150 000-нан аса алмайды. Осы шектеуге жеткеннен кейін, Kaspersky Security Center Linux жаңа файлдарды алмайды.

Әдеттегі клиент құрылғысындағы файлдар саны, әдетте, 60 000-нан аспайды. Файл серверіндегі орындалатын файлдардың саны үлкенірек болуы және тіпті 150 000 шегінен асып кетуі мүмкін.

Басқару сервері мен қорғалатын құрылғылар арасында желіге түсетін жүктеме туралы ақпарат

Бұл бөлімде өлшеулер жүргізілген шарттарды көрсете отырып, желідегі трафикті сынап өлшеу нәтижелері келтіріледі. Сіз осы ақпаратты ұйымның ішіндегі (немесе қорғалатын құрылғылары орналасқан ұйым мен Басқару сервері арасында) арналардың желілік инфрақұрылымы мен өткізу қабілетін жоспарлау кезінде анықтамалық ақпарат ретінде пайдалана аласыз. Сондай-ақ, желінің өткізу қабілетін біле отырып, сіз деректерді берумен байланысты белгілі бір операцияны орындауға қанша уақыт кететінін долбарлап бағалай аласыз.

Әртүрлі сценарийлерді орындау кезіндегі трафик шығыны

Төмендегі кестеде әртүрлі сценарийлерді орындау кезінде Басқару сервері мен басқарылатын құрылғы арасындағы трафикті сынап өлшеу нәтижелері келтірілген.

Құрылғыны Басқару серверімен синхрондау әдепкі бойынша 15 минут сайын немесе одан сирек болады. Алайда, егер сіз Басқару серверінде саясат немесе тапсырма параметрлерін өзгертсеңіз, онда осы саясат (немесе тапсырма) қолданылатын құрылғыларды мерзімінен бұрын синхрондау жүзеге асырылады және жаңа параметрлер құрылғыларға беріледі.

Басқару сервері мен басқарылатын құрылғы арасындағы трафик

Сценарий	Серверден әрбір басқарылатын құрылғыға дейінгі трафик	Әрбір басқарылатын құрылғыдан Серверге дейінгі трафик
Дерекқорлары жаңартылған Kaspersky Endpoint Security for Linux бағдарламасын орнату	390 МБ	3.3 МБ
Желілік агентті орнату	75 МБ	397 КБ
Желілік агент пен Kaspersky Endpoint Security for Linux бағдарламасын бірлесіп орнату	459 МБ	3.6 МБ
Пакеттегі дерекқорларды жаңартпай, антивирустық дерекқорларды бастапқы жаңарту (Kaspersky Security Network-ке қатысу өшірілсе)	113 МБ	1,8 МБ
Антивирустық дерекқорларды тәулік сайын жаңарту (Kaspersky Security Network-ке қатысу өшірілсе)	22 МБ	373 МБ
Құрылғыдағы дерекқорларды жаңартқанға дейін бастапқы синхрондау (саясат пен тапсырмаларды беру)	382 КБ	446 КБ
Құрылғыдағы дерекқорларды жаңартқаннан кейін бастапқы синхрондау	20 КБ	157 КБ
Басқару серверінде өзгертулер болмаған кезде синхрондау (кесте бойынша)	18 КБ	23 КБ
Топ саясатында бір параметр өзгерген кезде синхрондау (мерзімінен бұрын, өзгерту енгізілгеннен кейін бірден)	19 КБ	20 КБ
Топтық тапсырмада бір параметр өзгертілгеннен кейін синхрондау (мерзімінен бұрын, өзгерту енгізілгеннен кейін бірден)	14 КБ	11 КБ
Мәжбүрлеп синхрондау	110 КБ	109 КБ
Вирус анықталды оқиғасы (1 вирус)	44 КБ	50 КБ
Вирус анықталды оқиғасы (10 вирус)	58 КБ	77 КБ

Сценарий	Серверден әрбір басқарылатын құрылғыға дейінгі трафик	Әрбір басқарылатын құрылғыдан Серверге дейінгі трафик
Бағдарламалар тізімдемесі кестесін қосқаннан кейінгі бір реттік трафик	10 КБ-қа дейін	12 КБ-қа дейін
Бағдарламалар тізімдемесі тізімі қосылған кездегі күн сайынғы трафик	840 КБ-қа дейін	1 МБ-қа дейін

Трафиктің тәулік ішіндегі орташа шығыны

Басқару сервері мен басқарылатын құрылғы арасындағы тәулігіне орташа трафик шығыны:

- Серверден басқарылатын құрылғыға дейінгі трафик – 840 КБ.
- Басқарылатын құрылғыдан Серверге дейінгі трафик – 1 МБ.

Трафик келесі жағдайларда өлшенді:

- Басқарылатын құрылғыға Желілік агент және Kaspersky Endpoint Security for Linux орнатылды.
- Құрылғы тарату нүктесі болып тағайындалмаған.
- Осалдықтар мен патчтарды басқару қосылмаған.
- Басқару серверімен синхрондау кезеңі 15 минутты құрады.

Шектеулер тізімі

Kaspersky Security Center Linux қолданбаның жұмыс істеуі үшін критикалық емес келесі шектеулерге ие:

- 10373324: Егер түйіндердің ешқайсысында Желілік агент орнатылмаған болса, индикатор күйін есептеу кезінде тек ағымдағы белсенді түйін ескеріледі. Егер Желілік агент түйіндердің біріне орнатылған болса, бұл түйін тек белсенді болған кезде ғана ескеріледі. Сондықтан, индикатор күйін есептеу кезінде барлық түйіндерді ескеру үшін әр түйінге Желілік агент орнату керек және әрбір түйін кем дегенде бір рет белсенді болуы керек.

- 8994760: Егер сізде виртуалды Басқару серверлерінде қол жеткізу құқықтарыңыз болса, бірақ негізгі Басқару серверінде қол жеткізу құқықтарыңыз болмаса және сіз Kaspersky Security Center Linux жүйесіне кіруге тырыссаңыз, қате пайда болады және **Сұрауыңызды қазір өңдеу мүмкін емес. Біраз уақыт өткен соң қайта өңдеп көріңіз** деген қате туралы хабарлама дұрыс емес. Қате мәтіні келесідей болуы керек: **Қол жеткізу рұқсаттарыңызды тексеріңіз. Негізгі серверде немесе виртуалды сервер нұсқаларының біреуінде ғана қол жеткізу құқықтарыңыз болуы тиіс. Бас әкімшіге хабарласып, әрекетті қайталап көріңіз**

- 10085767: Kaspersky Security Center Linux жүйесіне көшкен кезде есеп ауқымы дұрыс көрсетілмеуі мүмкін.

- 10292104: Kaspersky Security Center Web Console 15.1 немесе 15.2 нұсқасында Kaspersky Endpoint Detection and Response Optimum плагинін 16.3 нұсқасына жаңартсаңыз, **Дабылдар** бөлімінде дабылдар көрсетілмеуі мүмкін.

- 10308380: Қолданба санатын жасағаннан кейін, егер сіз оның қасиеттерін растау диалогтық терезесінен **ОК** түймесін басу арқылы ашуға тырыссаңыз, қасиеттер терезесі ашылмайды.

- 10253149: Қолданба саясаттары үшін **Оқиғаларды конфигурациялау** қойындысында жаппай оқиға таңдалса, мұндай оқиғалардың Басқару серверге немесе ДҚБЖ өнімділігіне әсері туралы ескертуі бар **Көбірек көрсету** ашылмалы блогы көрсетілмейді.

- 10127434: Егер негізгі Басқару серверінде Kaspersky Security Center Web Console жүйесіне кіріп тұрған кезде **Тапсырмалар** бөлімін, содан кейін иерархия терезесін ашсаңыз, виртуалды сервер негізгі сервер ретінде көрсетіледі.

- 9302142: **Желілік агентті DMZ режимінде қосылым шлюзі ретінде пайдалану** опциясы Microsoft Windows жүйесінде Arm жүйесінде қолдау көрсетілмейді.

- 9065814: Samba 4 доменіндегі Windows негізіндегі құрылғыдан домен аутентификациясын жасау кезінде қате орын алуы мүмкін.

- 9335676: Жоғары қолжетімділіктегі ДҚБЖ кластеріндегі негізгі түйінді ауыстырғаннан кейін, Kaspersky Security Center Web Console веб-консоліне кіру мүмкін болмауы немесе айтарлықтай кешіктірілуі ықтимал. Егер Kaspersky Security Center Web Console веб-консолі 10 минуттан астам уақыт бойы қол жетімсіз болып қалса, келесі пәрменді пайдаланып IAM қызметін қайта іске қосыңыз:

  ```
  systemctl restart kliam_srv.service
  ```

- 9157005, 9157085: Windows басқарылатын құрылғыда *Қажетті жаңартуларды орнату және осалдықтарды түзету* опциясы қосылған кезде **Орнатуды құрылғыны қайта жүктеу немесе өшіру сәтінде бастау** тапсырмасын іске қосқан кезде, тапсырма қатемен сәтсіз аяқталуы мүмкін. Бұл мәселе көптеген жаңартулар орнатуға жоспарланған кезде пайда болуы мүмкін. Мәселені шешу үшін тапсырманы **Орнатуды құрылғыны қайта жүктеу немесе өшіру сәтінде бастау** опциясын қоспай іске қосыңыз.

- 9272534: Егер пайдаланушылар кестесінде 50 000-нан астам пайдаланушы болса, тек алғашқы 50 000 пайдаланушы көрсетіледі, ал қалған пайдаланушылар көрсетілмейді.

- 9291235: Басқару серверінің 16.1 нұсқасындағы сақтық көшірмені қалпына келтіргеннен кейін, Kaspersky Security Center Web Console кіру бетін көрсетеді. Сәтті аутентификациядан кейін, екі факторлы аутентификация үшін бір реттік қауіпсіздік коды сұралады. Жарамды бір реттік қауіпсіздік коды енгізілгенде, бір реттік қауіпсіздік кодының дұрыс емес екенін көрсететін қате туралы хабарлама көрсетіледі. Бұл жағдайда бірнеше минут күтіп, Kaspersky Security Center Web Console веб-консоліне қайта кіру үшін бетті қолмен жаңартыңыз. Сақтық көшірмені қалпына келтіру процесі толығымен аяқталғаннан кейін, аутентификация келесі әрекетте сәтті болады.

- 7939561: Қорғалған пайдаланушы есептік жазбасын өзгерту әрекеті кезінде **Есептік жазба қорғанысы** тіркелгі деректерін енгізу терезесіндегі **Бас тарту** түймесін басу қатеге әкеледі.

- 8562938: Басқару серверінің саясат сипаттарында мобильдік құрылғыларға арналған портты ашу мобильдік құрылғыларды басқару мүмкіндігін қоспайды және мобильдік сертификатты құруды іске қоспайды. Мобильдік құрылғыларды басқару мүмкіндігін қосу үшін мобильдік құрылғылар порты басқару серверінің сипаттарында ашылуы керек.

- 8732282: Active Directory ішіндегі есептік жазба сипаттарында **Пайдаланушы құпиясөзді өзгерте алмайды** опциясы қосылған пайдаланушы үшін Active Directory қызметіндегі **Құпиясөзді ысыру** жауап әрекеті орындалмайды. Домен контроллерінің әкімшісі бұл пайдаланушы үшін **Пайдаланушы құпиясөзді өзгерте алмайды** опциясын өшіруі немесе құпиясөзді қолмен қайта орнатуы керек. Бұл мәселе сізде Kaspersky Security: Бизнеске арналған Кәсіби лицензиясы болса, Active Directory интеграциясы қосылған болса және пайдаланушы Active Directory қауіпсіздік тобына қосылған болса орын алады.

- 8688182: Пайдаланушыда Active Directory қызметіндегі есептік жазба сипаттарында **Құпиясөздің мерзімі ешқашан аяқталмайды** опциясы қосылған болса, **Құпиясөзді ысыру** жауап әрекетін орындағаннан кейін, **Құпиясөздің мерзімі ешқашан аяқталмайды** опциясы өшіріледі және келесі кіру кезінде пайдаланушыдан домен құпиясөзін өзгерту сұралады. Бұл мәселе сізде Kaspersky Security: Бизнеске арналған Кәсіби лицензиясы болса, Active Directory интеграциясы қосылған болса және пайдаланушы Active Directory қауіпсіздік тобына қосылған болса орын алады.

- 8703857: Kaspersky Security Center Web Console және басқару веб-плагинідері үшін прокси-сервер қосылымы прокси-сервер негізгі аутентификацияны қолдайтын жағдайда ғана орнатылады.

- 7911778: Arm архитектурасы бар операциялық жүйе қосылған және уақыты басқару серверінің уақытымен синхрондалмаған құрылғыдан желілік агентті жою үшін **Бағдарламаны қашықтан жою** тапсырмасын іске қоссаңыз, желілік агент құрылғыдан сәтті жойылғаннан кейін де, тапсырма күйі **Орындалуда** опциясынан **Аяқталды** опциясына өзгермейді. Бұл мәселені шешу үшін **Бағдарламаны қашықтан жою** тапсырмасын іске қоспай тұрып, желілік агент орнатылған құрылғыдағы уақытты басқару сервері бар құрылғыдағы уақытпен синхрондаңыз.

- 6896585: Атында кирилл таңбалары бар құрылғыда Kaspersky Security Center Linux орнатылған болса, басқарылатын құрылғы KSN-ге KSN прокси-сервер қызметі арқылы қосыла алмайды.

- 7523299: CentOS 6.6 басқаруыме жұмыс істейтін басқарылатын құрылғыда өз процесінің жұмысы аяқталғаннан кейін, Желілік агент қайта іске қосылмайды.

- 7835858: Kaspersky Security Center Web Console 15.2 немесе одан кейінгі нұсқа ішіндегі **N күн сайын** және **Апта күндері бойынша** жоспарлау параметрлерімен тапсырма жасасаңыз, содан кейін тапсырманы Kaspersky Security Center Web Console немесе Administration Console алдыңғы нұсқаларымен ашсаңыз (мысалы, тапсырма Linux және Windows негізіндегі болуы мүмкін қосымша басқару серверлерінде де қолданылса), жоспарлау параметрлері дұрыс көрсетілмеуі немесе қате пайда болуы мүмкін.

- 7208621: *Тарату нүктелерінің қоймасыға жаңартуларды жүктеп алу* немесе *Жаңартуларды тексеру* тапсырмасын импортталған кезде, **Тапсырма тағайындалатын құрылғыларды таңдау** параметрі қосулы болады. Бұл тапсырмаларды құрылғы таңдауларына немесе бекітілген құрылғыларға тағайындау мүмкін емес. *Тарату нүктелерінің қоймасыға жаңартуларды жүктеп алу* немесе *Жаңартуларды тексеру* тапсырмасын белгілі бір құрылғыларға тағайындасаңыз, тапсырма дұрыс импортталмайды.

- 6511063: **Бағдарламалар тізімдемесі** бөлімдегі бағдарлама Linux операциялық жүйесі бар құрылғыда табылса, бағдарлама сипаттарында онымен байланысты орындалатын файлдар туралы ақпарат жоқ.

- 5915107: Әріптік пішімімен есептерде бет үзілімі мәтін жолын көлденеңінен кесіп алуы мүмкін.

- 5556109: Бірнеше желілік адаптері бар басқарылатын құрылғы Басқару серверіне қосылу үшін пайдаланылатын желілік адаптерден ерекшеленетін желілік адаптердің MAC мекенжайы туралы ақпаратты Басқару серверіне жібереді.

- 9093038: Орнатудан кейін Kaspersky Security Center Linux басқару сервері іске қосылмаса және операциялық жүйе журналында kladminserver_srv.service туралы 213/SECUREBITS қатесі болса, супер пайдаланушы ретінде келесі пәрмендерді орындаңыз:

  ```
  mkdir -p /etc/systemd/system/kladminserver_srv.service.d
  echo "[Service]" > /etc/systemd/system/kladminserver_srv.service.d/override.conf
  echo "AmbientCapabilities=CAP_IPC_LOCK" >> /etc/systemd/system/kladminserver_srv.service.d/override.conf
  mkdir -p /etc/systemd/system/klwebsrv_srv.service.d
  echo "[Service]" > /etc/systemd/system/klwebsrv_srv.service.d/override.conf
  echo "AmbientCapabilities=CAP_IPC_LOCK" >> /etc/systemd/system/klwebsrv_srv.service.d/override.conf
  ```

  Орнатудан кейін Kaspersky Security Center Web Console іске қосылмаса және операциялық жүйе журналында KSCWebConsole.service туралы 213/SECUREBITS қатесі болса, супер пайдаланушы ретінде келесі пәрмендерді орындаңыз:

  ```
  mkdir -p /etc/systemd/system/KSCSvcWebConsole.service.d
  echo "[Service]" > /etc/systemd/system/KSCSvcWebConsole.service.d/override.conf
  echo "AmbientCapabilities=CAP_IPC_LOCK" >> /etc/systemd/system/KSCSvcWebConsole.service.d/override.conf
  mkdir -p /etc/systemd/system/KSCWebConsoleManagement.service.d
  echo "[Service]" > /etc/systemd/system/KSCWebConsoleManagement.service.d/override.conf
  echo "AmbientCapabilities=CAP_IPC_LOCK" >> /etc/systemd/system/KSCWebConsoleManagement.service.d/override.conf
  mkdir -p /etc/systemd/system/KSCWebConsoleNATS.service.d
  echo "[Service]" > /etc/systemd/system/KSCWebConsoleNATS.service.d/override.conf
  echo "AmbientCapabilities=CAP_IPC_LOCK" >> /etc/systemd/system/KSCWebConsoleNATS.service.d/override.conf
  mkdir -p /etc/systemd/system/KSCWebConsolePlugin.service.d
  echo "[Service]" > /etc/systemd/system/KSCWebConsolePlugin.service.d/override.conf
  echo "AmbientCapabilities=CAP_IPC_LOCK" >> /etc/systemd/system/KSCWebConsolePlugin.service.d/override.conf
  mkdir -p /etc/systemd/system/KSCWebConsole.service.d
  echo "[Service]" > /etc/systemd/system/KSCWebConsole.service.d/override.conf
  echo "AmbientCapabilities=CAP_IPC_LOCK" >> /etc/systemd/system/KSCWebConsole.service.d/override.conf
  ```

  Орнатқаннан кейін kliam_srv қызметі іске қосылмаса және операциялық жүйе журналында қызметке қатысты 213/SECUREBITS қатесі болса, супер пайдаланушы ретінде келесі пәрмендерді орындаңыз:

  ```
  mkdir -p /etc/systemd/system/kliam_srv.service.d
  echo "[Service]" > /etc/systemd/system/kliam_srv.service.d/override.conf
  echo "AmbientCapabilities=CAP_IPC_LOCK" >> /etc/systemd/system/kliam_srv.service.d/override.conf
  ```

- 9165434: NTLM аутентификациясы Қорғалған пайдаланушылар тобындағы пайдаланушы есептік жазбалары үшін жұмыс істемейді.

Техникалық қолдау қызметіне жүгіну

Бұл бөлімде техникалық қолдауды алу тәсілдері мен шарттары туралы ақпарат бар.

Техникалық қолдау алу жолдары

Егер сіз Kaspersky Security Center Linux құжаттамасында немесе бағдарлама туралы басқа ақпарат көздерінде өз сұрағыңыздың шешімін таппаған болсаңыз, Kaspersky Техникалық қолдау қызметіне хабарласыңыз. Техникалық қолдау қызметінің қызметкерлері Kaspersky Security Center Linux орнату және пайдалану туралы сұрақтарыңызға жауап береді.

Kaspersky ұйымы Kaspersky Security Center Linux бағдарламасы оның өмірлік циклі бойы қолдау көрсетеді (бағдарламалардың өмірлік циклі бетін қараңыз). Техникалық қолдау қызметіне хабарласпас бұрын техникалық қолдау көрсету ережелерімен танысыңыз.

Сіз Техникалық қолдау қызметінің мамандарымен келесі тәсілдердің бірімен байланыса аласыз:

- Техникалық қолдау қызметінің веб-сайтына кіру
- Kaspersky CompanyAccount порталынан техникалық қолдау қызметіне сұрау жіберу арқылы

Kaspersky CompanyAccount арқылы техникалық қолдау

Kaspersky CompanyAccount – бұл Kaspersky бағдарламаларын қолданатын ұйымдарға арналған портал. Kaspersky CompanyAccount порталы пайдаланушылардың Kaspersky мамандарымен электрондық сұрау салу арқылы өзара іс-қимыл жасауына арналған. Kaspersky CompanyAccount порталында электрондық сұрауларды Kaspersky мамандары тарапынан өңдеу күйін қадағалап, электрондық сұраулардың тарихын сақтауға болады.

Сіз өзіңіздің ұйымыңыздың барлық қызметкерлерін бір Kaspersky CompanyAccount есептік жазбасының шеңберінде тіркей аласыз. Бір есептік жазба, сізге тіркелген қызметкерлерден Kaspersky ұйымына жіберілген электронды сұрауларды орталықтан басқаруға, сондай-ақ Kaspersky CompanyAccount порталында осы қызметкерлердің құқықтарын басқаруға мүмкіндік береді.

Kaspersky CompanyAccount порталы келесі тілдерде қолжетімді:

- Ағылшын тілі
- Испан тілі
- Итальян тілі
- Неміс тілі
- Поляк тілі
- Португал тілі

- Орыс тілі
- Француз тілі
- Жапон тілі

Kaspersky CompanyAccount туралы толығырақ Техникалық қолдау қызметі веб-сайтынан біле аласыз.

Басқару серверінің қоқыс файлдарын алу

Басқару серверінің қоқыс файлдары белгілі бір уақытта Басқару сервері процестері туралы барлық ақпаратты қамтиды. Басқару серверінің қоқыс файлдары /var/lib/systemd/coredump каталогында сақталады. Қоқыс файлдары Kaspersky Security Center Linux пайдаланылған кезде сақталады және қолданба жойылған кезде біржола жойылады. Қоқыс файлдары Kaspersky автоматты түрде жіберілмейді.

Басқару сервері бұзылса, Kaspersky техникалық қолдау қызметіне хабарласуға болады. Техникалық қолдау қызметінің маманы Kaspersky-де әрі қарай талдау үшін сізден басқару серверінің дамп файлдарын жіберуді сұрауы мүмкін.

Қоқыс файлдарында жеке деректер болуы мүмкін. Оны Kaspersky жібермес бұрын ақпаратты рұқсатсыз кіруден қорғау ұсынылады.

Бағдарлама мәліметтері көздері

Kaspersky веб-сайтындағы Kaspersky Security Center Linux беті

Kaspersky Security Center Linux бетінде бағдарлама, оның мүмкіндіктері мен жұмыс ерекшеліктері туралы мәлімет ала аласыз.

Білім базасындағы Kaspersky Security Center Linux беті

Білім базасы – Kaspersky Техникалық қолдау қызметі веб-сайтындағы бөлім.

Білім базасындағы Kaspersky Security Center Linux бетінде бағдарламаны сатып алу, орнату және қолдану туралы пайдалы ақпаратты, ұсыныстарды және жиі қойылатын сұрақтарға жауаптарды қамтитын мақалаларды таба аласыз.

Білім базасындағы мақалалар Kaspersky Security Center Linux және Kaspersky басқа да бағдарламаларымен байланысты сұрақтарға жауап бере алады. Сонымен қатар, Білім базасының мақалаларында Техникалық қолдау қызметі жаңалықтары болуы мүмкін.

Kaspersky бағдарламаларын пайдаланушылар қауымдастығында талқылау

Сіздің сұрағыңызға тез арада жауап беру қажет болмаса, сіз оны Kaspersky мамандарымен және біздің форумдағы басқа да пайдаланушылармен талқылай аласыз.

Пайдаланушылар форумында, сіз жарияланған тақырыптарды қарай аласыз, өз пікірлеріңізді қалдыра аласыз, талқылау үшін жаңа тақырыптарды жасай аласыз.

> Онлайн-анықтаманы көрсету үшін интернет қосылымы керек.

Мәселеңіздің шешімін таба алмасаңыз, Техникалық қолдау қызметіне хабарласыңыз.

Глоссарий

Cloud Discovery

Cloud Discovery пайдаланушылардың бұлттық сервистерге қол жеткізуін басқарады. Бұлттық сервистерге, мысалы, Microsoft Teams, Salesforce, Microsoft Office 365 кіреді. Бұлттық сервистер санаттарға топтастырылған, мысалы, *Файлдармен алмасу*, *Мессенджерлер*, *Электрондық пошта*.

FileTransferBridge

Kaspersky қолданбаларының жаңартуларын жергілікті жеткізуді қамтамасыз ететін Kaspersky Security Center Linux ішкі компоненті. FileTransferBridge Желілік агентке (klnagent) біріктірілген және әрбір басқарылатын құрылғыда жергілікті түрде жұмыс істейді.

Kaspersky қолданбалары жаңартуларды Kaspersky Security Center Linux жүйесінен алған кезде, Желілік агент жаңарту файлдарын Басқару серверінен немесе тарату нүктесінен жүктеп алады. Содан кейін FileTransferBridge файлдарды жергілікті түрде орнатылған Kaspersky қолданбаларына тасымалдап, дерекқор жаңартулары мен бағдарламалық жасақтама патчтарының сенімді жеткізілуін қамтамасыз етеді.

FileTransferBridge 30522 және 30523 TCP порттарын пайдаланады. Порттар тек localhost (127.0.0.1) интерфейсінде жұмыс істейді және сыртқы желілерден кіріс қосылымдарды қабылдамайды.

HTTPS

Шифрлауды қолдана отырып шолғыш пен веб-сервер арасында деректерді жіберудің қауіпсіз протоколы. HTTPS корпоративтік немесе қаржылық деректер сияқты жабық ақпаратқа қатынасу үшін пайдаланылады.

iOS MDM құрылғы

iOS MDM протоколы бойынша iOS MDM серверіне қосылатын ұялы құрылғы. iOS MDM протоколы бойынша iOS операциялық жүйесі бар құрылғылар қосылуы және басқарылуы мүмкін.

iOS MDM сервері

Клиент құрылғысына орнатылатын және iOS ұялы құрылғыларын Басқару серверіне қосуға және оларды Apple Push Notifications (APNs) сервисі көмегімен басқаруға мүмкіндік беретін Kaspersky Security Center құрамдасы.

JavaScript

Веб-беттердің мүмкіндіктерін кеңейтетін бағдарламалау тілі. JavaScript қолдана отырып жасалған веб-беттер веб-сервердегі деректермен веб-бетті жаңартусыз қосымша әрекеттерді орындауға (мысалы, интерфейс элементтерінің түрін өзгерту немесе қосымша терезелерді ашу) қабілетті. JavaScript, қолдана отырып жасалған веб-беттерді қарау үшін шолғыш параметрлерінде JavaScript қолдауды қосу керек.

Kaspersky Private Security Network (KPSN)

Kaspersky Private Security Network – бұл Kaspersky бағдарламалары орнатылған құрылғыларды пайдаланушыларға өз құрылғыларынан Kaspersky Security Network бағдарламасына деректерді жібермей, Kaspersky Security Network дерекқорларына және басқа да статистикалық деректерге қатынасуды қамтамасыз ететін шешім. Kaspersky Private Security Network келесі себептердің бірі бойынша Kaspersky Security Network бағдарламасына қатыса алмайтын ұйымдарға арналған:

- Құрылғылар интернетке қосылмаған.
- Кез келген деректерді елден немесе корпоративтік желіден (LAN) тыс жерге жіберуге заңмен немесе корпоративті қауіпсіздік саясаттарымен тыйым салынады.

Kaspersky Security Center Linux Web Server

Басқару серверінің құрамына орнатылатын Kaspersky Security Center Linux құрамдасы. Веб-сервер жеке орнату пакеттерін, iOS MDM профильдерін, сондай-ақ ортақ қатынасы бар қалтадағы файлдарды желі арқылы беруге арналған.

Kaspersky Security Center Linux әкімшісі

Kaspersky Security Center Linux қашықтан орталықтандырылған басқару жүйесі арқылы бағдарламаның жұмысын басқаратын адам.

Kaspersky Security Center System Health Validator (SHV)

Microsoft NAP-пен Kaspersky Security Center Linux бағдарламасының бірлескен жұмысы кезінде операциялық жүйенің жұмысқа қабілетін тексеруге арналған Kaspersky Security Center Linux бағдарламасының құрамдасы.

Kaspersky Security Center операторы

Kaspersky Security Center көмегімен басқарылатын қорғаныс жүйесінің күйі мен жұмысын бақылайтын пайдаланушы.

Kaspersky жаңарту серверлері

Kaspersky бағдарламаларына дерекқорлар мен модульдердің жаңартуларын жіберетін Kaspersky HTTP серверлері мен HTTPS серверлері.

Network Location Awareness (NLA)

Операциялық жүйеге ағымдағы желіні анықтауға көмектесетін Windows қызметі. NLA желідегі өзгерістерді анықтайды және құрылғының қауіпсіздік конфигурациясын реттейді.

Provisioning профилі

iOS ұялы құрылғысында қолданбалардың жұмысына арналған параметрлер жиынтығы. Provisioning профилі лицензия туралы ақпаратты қамтиды және белгілі бір қолданбаға байланысты.

SSL

Жергілікті желілерде және интернетте деректерді шифрлау протоколы. SSL клиент пен сервер арасында қорғалған қосылыстарды жасау үшін веб-қолданбаларда қолданылады.

Антивирустық дерекқорлар

Антивирустық дерекқорларды шығарған сәтте Kaspersky белгілі компьютерлік қауіпсіздік қауіптері туралы ақпаратты қамтитын дерекқорлар. Антивирустық деректорлардағы енгізілімдер сканерленген нысандардан зиянды кодты анықтауға мүмкіндік береді. Антивирустық дерекқорларды Kaspersky мамандары жасайды және олар сағат сайын жаңарып отырады.

Антивирустық қорғаныс провайдері

Kaspersky шешімдері негізінде ұйым-клиенттің желілерінің антивирустық қорғаныс қызметтерін ұсынатын ұйым.

Арнайы құрылғыға арналған тапсырма

Ерікті басқару топтарынан арнайы клиент құрылғылары үшін анықталған және оларда орындалатын тапсырма.

Әкімшілік құқықтар

Exchange ұйымының ішінде Exchange нысандарын басқаруға арналған пайдаланушы құқықтары мен өкілеттіліктерінің деңгейі.

Әкімшінің жұмыс станциясы

Kaspersky Security Center Web Console-ін ашатын құрылғы. Бұл құрамдас Kaspersky Security Center Linux басқару интерфейсі болып табылады.

Әкімші жұмыс станциясынан Kaspersky Security Center Linux серверлік бөлігін басқарады. Әкімшінің жұмыс станциясын қолданып, әкімші Kaspersky бағдарламаларының дерекқорында қалыптастырылған ұйымның желісін орталықтандырылған қорғанысының жүйесін құрады.

Бағдарлама параметрлері

Оның тапсырмаларының барлық түрлері үшін ортақ және жалпы бағдарламаның жұмысы үшін жауапты бағдарлама жұмысының параметрлері: мысалы, бағдарлама өнімділігінің параметрлері, есептерді жүргізу параметрлері, сақтық қойманың параметрлері.

Бағдарламаларды орталықтандырылған басқару

Kaspersky Security Center ұсынатын басқару қызметтері көмегімен бағдарламаны қашықтан басқару.

Бағдарламаны тікелей басқару

Жергілікті интерфейс арқылы бағдарламаны басқару

Басқару консолі

Windows негізінде Kaspersky Security Center құрамдасы (бұдан әрі MMC негізіндегі Басқару консолі). Бұл құрамдас Басқару серверінің және Желілік агенттің басқару қызметтеріне қатысты реттелмелі интерфейс болып табылады. Басқару консолі Kaspersky Security Center Web Console баламасы болып табылады.

Басқару сервері

Ұйым желісіне орнатылған Kaspersky бағдарламалары туралы ақпаратты орталықтандырылған сақтау функцияларын жүзеге асыратын Kaspersky Security Center Linux бағдарламасының құрамдасы. Басқару сервері осы бағдарламаларды да басқара алады.

Басқару сервері деректерін сақтық көшірмелеу

Сақтық көшірмелеу утилитасы көмегімен жүргізілетін сақтық сақтауға және кейін қалпына келтіруге арналған Басқару серверінің деректерін көшірмелеу. Утилита мыналарды сақтауға көмектеседі:

- Басқару серверінің дерекқоры (оқиғаның Басқару серверінде сақталған саясаттар, тапсырмалар, бағдарлама параметрлері)
- Басқару топтарының құрылымы және клиент құрылғылары туралы конфигурациялық ақпарат
- Қашықтан орнатуға арналған бағдарламалар дистрибутивтерінің қоймасы (Packages, Uninstall, Updates қалталарының мазмұны)
- Басқару сервері сертификаты

Басқару сервері сертификаты

Басқару сервері келесі мақсаттарда қолданатын сертификат:

- Kaspersky Security Center Web Console-іне қосылу кезінде Басқару серверінің аутентификациясы;
- басқарылатын құрылғыларда Басқару серверінің Желілік агентпен қауіпсіз өзара әрекеттесуі;
- негізгі басқару сервері қосалқы басқару серверіне қосылған кезде басқару серверлерінің түпнұсқалық растамасы.

Сертификат автоматты түрде Басқару серверін орнатқан кезде жасалады, содан соң Басқару серверінде сақталады.

Басқару серверінің деректерін қалпына келтіру

Сақтық қоймаға сақталған ақпараттың негізінде сақтық көшірмелеу утилитасы көмегімен Басқару серверінің деректерін қалпына келтіру. Утилита мыналарды қалпына келтіруге көмектеседі:

- Басқару серверінің дерекқоры (оқиғаның Басқару серверінде сақталған саясаттар, тапсырмалар, бағдарлама параметрлері)
- Басқару топтарының құрылымы және клиент құрылғылары туралы конфигурациялық ақпарат
- Қашықтан орнатуға арналған бағдарламалар дистрибутивтерінің қоймасы (Packages, Uninstall, Updates қалталарының мазмұны)
- Басқару сервері сертификаты

Басқару серверінің клиенті (Клиент құрылғысы)

Желілік агент және Kaspersky басқарылатын бағдарламалары орнатылған құрылғы, сервер немесе жұмыс станциясы.

Басқару тобы

Орындалатын функцияларға және оларға орнатылатын Kaspersky бағдарламалар жиынтығына сәйкес біріктірілген арнайы құрылғылар. Құрылғылар оларды біртұтас құрылғы ретінде басқару ыңғайлылығы үшін топтастырылады. Топтың құрамына басқа топтар кіруі мүмкін. Топқа орнатылған әрбір бағдарлама үшін топтық саясаттар жасалуы және топтық тапсырмалар қалыптастырылуы мүмкін.

Басқарылатын құрылғылар

Басқару топтарының біріне қосылатын ұйым желісінің құрылғылары.

Белсенді кілт

Бағдарламаның жұмысы үшін ағымдағы сәтте қолданылатын кілт.

Виртуалды Басқару сервері

Ұйым-клиенттің желісін қорғау жүйесін басқаруға арналған Kaspersky Security Center Linux бағдарламасының құрамдасы.

Виртуалды Басқару сервері қосалқы Басқару серверінің жеке жағдайы болып табылады және физикалық Басқару серверімен салыстырғанда келесі негізгі шектеулерге ие:

- Виртуалды Басқару сервері тек негізгі Басқару серверінің құрамында ғана жұмыс істей алады.
- Виртуалды басқару сервері жұмыс істеген кезде негізгі Басқару серверінің негізгі дерекқорын пайдаланады. Деректерді сақтық көшірмелеу және қалпына келтіру тапсырмаларына, сондай-ақ жаңартуларды тексеру және жүктеу тапсырмаларына виртуалды Басқару серверінде қолдау көрсетілмейді.
- Виртуалды сервер үшін қосалқы Басқару серверлерін (соның ішінде виртуалды) құруға қолдау көрсетілмейді.

Вирустық шабуыл

Құрылғыға вирус кіргізудің бірқатар мақсатты амалдары

Демилитаризацияланған аймақ (DMZ)

Демилитаризацияланған аймақ - бұл жаһандық желідегі сұрауларға жауап беретін серверлер орналасқан жергілікті желінің сегменті. Ұйымның жергілікті желісінің қауіпсіздігін қамтамасыз ету мақсатында демилитаризацияланған аймаққа қатынас шектелген және желілік экранмен қорғалған.

Есептік деректер және қатынасу диспетчері (IAM)

Домен аутентификациясын (бірыңғай кіру) пайдалануға мүмкіндік беретін басқару серверінің компоненті. Бірыңғай кіру функциясы пайдаланушыға корпоративтік желіде құпиясөзді қайта енгізбей-ақ Kaspersky Security Center Web Console веб-консолінде қауіпсіз аутентификацияны қосуға мүмкіндік береді.

Жалпы сертификат

Пайдаланушының ұялы құрылғысын сәйкестендіруге арналған сертификат.

Жаңарту

Kaspersky жаңартулар серверінен алынатын жаңа файлдарды ауыстыру немесе қосу рәсімі (дерекқор немесе бағдарламалық модульдер).

Желілік агент

Нақты желілік түйінге орнатылған (жұмыс станциясы немесе сервер) Басқару сервері және Kaspersky бағдарламалары арасында өзара әрекеттесуді жүргізетін Kaspersky Security Center Linux бағдарламасының құрамдасы. Бұл құрамдас Microsoft Windows жүйелері үшін әзірленген барлық бағдарламалар үшін бірыңғай болып табылады. UNIX операциялық жүйелері мен оларға ұқсас және macOS арналған Kaspersky бағдарламалары үшін Желілік агенттің бөлек нұсқалары бар.

Желінің антивирустық қорғанысы

Ұйым желісінің құрылғыларына вирустар мен спам жіберудің ықтималдығын азайтатын, желілік шабуылдар, фишинг пен басқа қауіптерді болдырмайтын техникалық және ұйымдық шаралар кешені. Антивирустық желі қорғанысы қауіпсіздік бағдарламалары мен сервистерін қолданған кезде, сондай-ақ ұйымда ақпараттық қауіпсіздік саясаты болған кезде және сақталған кезде артады.

Желінің қорғаныс күйі

Ұйым желісі құрылғыларының қорғалу дәрежесін сипаттайтын ағымдағы қорғаныс күйі. Желіні қорғау күйі желі құрылғыларында орнатылған қауіпсіздік бағдарламаларының болуы, лицензиялық кілттерді пайдалану, анықталған қауіптердің саны мен түрлері сияқты факторларды қамтиды.

Жеңіл N агенті (LWNGT)

Мобильдік құрылғыларда Kaspersky Endpoint Security-мен өзара әрекет протоколы. LWNGT (мобильдік протокол деп те аталады) мобильдік құрылғыларға желілік агентті орнатпай-ақ желілік агент ретінде жұмыс істейді.

Жергілікті тапсырма

Бөлек клиент компьютерінде анықталған және орындалатын тапсырма.

Жергілікті түрде орнату

Қауіпсіздік бағдарламасының дистрибутивінен орнатуды қолмен іске қосуды немесе құрылғыға алдын ала жүктелген жарияланған орнату пакетін қолмен іске қосуды көздейтін ұйым желісінің құрылғысына қауіпсіздік бағдарламасын орнату.

Ішкі пайдаланушылар

Ішкі пайдаланушы есептік жазбалары виртуалды Басқару серверлерімен жұмыс істеу үшін пайдаланылады. Kaspersky Security Center Linux бағдарламасында ішкі пайдаланушылар шынайы пайдаланушы құқықтарына ие.

Ішкі пайдаланушы есептік жазбалары тек Kaspersky Security Center Linux ішінде жасалады және пайдаланылады. Ішкі пайдаланушылар туралы мәліметтер операциялық жүйеге берілмейді. Ішкі пайдаланушылардың аутентификациясын Kaspersky Security Center Linux жүзеге асырады.

Кеңінен таратын домен

Барлық түйіндері OSI (Open Systems Interconnection Basic Reference Model) желілік моделі деңгейінде кеңінен таратын арнаның көмегімен деректерді бір-біріне жібере алатын компьютерлік желінің логикалық учаскесі.

Кілт файлы

Сынақ немесе коммерциялық лицензия бойынша Kaspersky бағдарламасын қолдануға көмектесетін xxxxxxxx.key көру файлы.

Клиент әкімшісі

Ұйым-клиенттің антивирустық қорғанысын қамтамасыз етуге жауапты ұйым-клиенттің қызметкері.

Конфигурациялық профиль

iOS MDM ұялы құрылғылары үшін параметрлер мен шектеулер жиынтығын қамтитын саясат.

Қалпына келтіру

Нысан карантинге қоюға, емдеуге немесе жоюға дейін сақталған бастапқы орналасқан жерінің қалтасына немесе пайдаланушы көрсеткен басқа қалтаға түпнұсқа нысанды карантиннен немесе сақты қоймадан жылжыту.

Қашықтан орнату

Kaspersky Security Center Linux бағдарламасы ұсынатын құралдар көмегімен Kaspersky бағдарламаларын орнату.

Қолданбалар дүкені

Kaspersky Security Center Linux бағдарламасының құрамдасы. Қолданбалар дүкені пайдаланушылардың Android құрылғысына қолданбаларды орнату үшін пайдаланылады. Қолданбалар дүкенінде қолданбалардың apk-файлдарын және Google Play-де қолданбаларға сілтемелерді жариялауға болады.

Қолжетімді жаңарту

Құрамына белгілі кезеңде жиналған жедел жаңартулар жиынтығы және бағдарлама архитектурасындағы өзгерістер қосылған Kaspersky бағдарламалар модульдерінің жаңарту бумасы.

Қолмен орнату

Қауіпсіздік бағдарламасының дистрибутивінен ұйым желісінің құрылғысына қауіпсіздік бағдарламасын орнату. Қолмен орнату үшін әкімшінің немесе басқа IT-маманның тікелей қатысуы қажет. Кәдімгі орнату егер қашықтан орнату қатемен аяқталған пайдаланылады.

Қорғаныс күйі

Компьютердің қорғалу деңгейін сипаттайтын ағымдағы қорғаныс күйі.

Қосылым шлюзі

Қосылым шлюзі – ерекше режимде жұмыс істейтін Желілік агент. Қосылым шлюзі басқа Желілік агенттерінен қосылымдарды қабылдайды және оларды Сервермен орнатылған өзінің қосылымы арқылы Басқару серверіне туннельдейді. Әдеттегі Желілік агенттен айырмашылығы, қосылым шлюзі Басқару серверімен байланыс орнатпайды, тек Басқару серверінен қосылымдарды күтеді.

Қосымша (немесе резервтегі) лицензиялық кілт

Бағдарламаны қолдану құқығын растайтын, бірақ ағымдағы сәтте қолданылмайтын кілт.

Құрылғының иесі

Құрылғының иесі – бұл әкімші құрылғымен қандай да бір жұмыстарды орындау қажет болса байланысатын құрылғының пайдаланушысы.

Лицензия мерзімі

Сіз бағдарлама функцияларын және қосымша қызметтерді пайдалана алатын кезең. Қолжетімді функциялар мен қосымша қызметтер көлемі лицензияның түріне байланысты.

Оқиғалар қоймасы

Kaspersky Security Center Linux-те туындайтын оқиғалар туралы ақпаратты сақтауға арналған Басқару серверінің дерекқорының бөлігі.

Оқиғаның маңыздылық деңгейі

Kaspersky бағдарламасының жұмысында бекітілген оқиғаның сипаттамасы. Келесі маңыздылық деңгейлері бар:

- Критикалық оқиға
- Функционалдық ақау
- Ескерту
- Ақпараттық хабар

Бірдей түрдегі оқиғалар оқиға орын алған жағдайға байланысты әртүрлі маңыздылық деңгейлеріне ие болуы мүмкін.

Орнату пакеті

Kaspersky Security Center қашықтан басқару жүйесімен Kaspersky бағдарламасын қашықтан орнату үшін қалыптастырылатын файлдар жиынтығы. Орнату пакеті бағдарламаны орнатуға және бірден орнатқаннан кейін оның жұмысқа қабілетін қамтамасыз етуге қажетті параметрлер жиынтығын қамтиды. Параметрлердің мәндері әдепкі бойынша бағдарлама параметрлерінің мәндеріне сәйкес келеді. Орнату пакеті бағдарлама дистрибутивінің құрамына кіретін kpd және kud кеңейтімдері бар файлдардың негізінде жасалады.

Осалдық

Зиянды бағдарламалық жасақтама өндірушілері операциялық жүйеге немесе бағдарламаға ену және оның тұтастығын бұзу үшін қолдана алатын операциялық жүйенің немесе бағдарламаның кемшілігі. Операциялық жүйедегі көптеген осалдықтар, оның жұмысын сенімсіз етеді, өйткені операциялық жүйеге енгізілген вирустар операциялық жүйенің өзінде де, орнатылған бағдарламаларда да ақаулық тудыруы мүмкін.

Патчтың маңыздылық деңгейі

Патчтың сипаттамасы. Үшінші тараптың немесе Microsoft патчтары үшін бес маңыздылық деңгейі бар:

- Критикалық
- Жоғары
- Орташа
- Төмен
- Белгісіз

Үшінші тараптың немесе Microsoft патчының маңыздылық деңгейі патч жабатын осалдықтың анағұрлым қолайсыз критикалық деңгейімен анықталады.

Провайдер әкімшісі

Антивирустық қорғаныс қызметтерінің провайдерінің қызметкері. Kaspersky шешімдері негізінде жасалған антивирустық қорғаныс жүйелерін орнату, пайдалану жұмыстарын орындайды, сондай-ақ клиенттерді техникалық қолдайды.

Профиль

Microsoft Exchange серверіне қосылған кезде Exchange ұялы құрылғылардың жағдайы параметрлерінің жиынтығы.

Рөлдік топ

Бірдей әкімшілік құқықтары бар Exchange ActiveSync ұялы құрылғылар пайдаланушыларының тобы.

Сақтық көшірме қоймасы

Сақтық көшірмелеу утилитасы көмегімен жасалатын Басқару серверінің деректерінің көшірмелерін сақтауға арналған арнайы қалта.

Саясат

Саясат бағдарлама жұмысының параметрлерін және басқару тобының құрылғыларында орнатылған бағдарламаны конфигурациялауға қатынасты анықтайды. Әр бағдарлама үшін өз саясатын жасау қажет. Сіз әр басқару тобындағы құрылғыларға орнатылған бағдарламалар үшін көптеген саясаттар жасай аласыз, бірақ басқару тобының шегінде тек бір саясат бір уақытта әр бағдарламаға пайдаланылуы мүмкін.

Тапсырма

Kaspersky бағдарламасы орындайтын функциялар тапсырмалар түрінде іске асырылған, мысалы: Файлдарды нақты уақыт режимінде қорғау, Құрылғыны толықтай тексеру, дерекқорды жаңарту.

Тапсырма параметрлері

Әр тапсырма түрі үшін ерекше бағдарлама жұмысының параметрлері.

Тарату нүктесі

Жаңартуларды тарату, бағдарламаларды қашықтан орнату, басқару тобы және/немесе кеңінен таратылатын доменнің құрамында құрылғылар туралы ақпаратты алу үшін пайдаланылатын Желілік агент орнатылған құрылғы. Тарату нүктелері жаңартуларды тарату кезінде және желідегі трафикті оңтайландыру үшін Басқару серверіне жүктемені азайтуға арналған. Тарату нүктелері автоматты түрде Басқару серверімен немесе қолмен әкімшімен тағайындалуы мүмкін. Тарату нүктесі бұрын жаңарту агенті деп аталды.

Топтық тапсырма

Басқару тобы үшін анықталған және осы басқару тобының құрамына кіретін барлық клиент құрылғыларында орындалатын тапсырма.

Түпнұсқалық растама агенті

Қатты жүктеу дискін шифрлаудан кейін шифрланған қатты дисктерге қатынасу үшін және операциялық жүйені жүктеу үшін түпнұсқалық растама рәсімінен өтуге көмектесетін интерфейс.

Үйдегі Басқару сервері

Үйдегі Басқару сервері – бұл Желілік агентті орнатқан кезде белгіленген Басқару сервері. Үйдегі Басқару сервері Желілік агентті қосу профильдерінің параметрлерінде пайдаланыла алады.

Үйлесімсіз бағдарлама

Үшінші тараптың антивирустық бағдарламасы немесе Kaspersky Security Center Linux арқылы басқаруға қолдау көрсетпейтін Kaspersky бағдарламасы.

Үшінші тарап коды туралы ақпарат

Үшінші тарап коды туралы ақпарат бағдарламаны орнату қалтасында орналасқан legal_notices.txt файлында бар.

Тауар белгілері туралы хабарландырулар

Тіркелген сауда белгілері мен қызмет белгілері - тиісті иелерінің жеке меншігі.

Adobe, Acrobat, Flash, PostScript және Shockwave – Adobe компаниясының АҚШ-тағы және/немесе басқа елдердегі тіркелген сауда белгілері немесе сауда белгілері.

AMD, AMD64 – Advanced Micro Devices, Inc сауда белгілері немесе тіркелген сауда белгілері.

Amazon, Amazon Web Services, AWS, Amazon EC2, AWS Marketplace – Amazon.com, Inc. немесе компанияның үлестес тұлғаларының сауда белгілері.

Apache – тіркелген тауар белгісі немесе Apache Software Foundation компаниясының АҚШ-тағы және (немесе) басқа елдердегі тауар белгісі.

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, Touch ID – Apple Inc. тауар белгілері.

Arm – АҚШ және/немесе басқа елдердегі Arm Limited (немесе оның еншілес компанияларының) тіркелген сауда белгісі.

Bluetooth ауызша тауар белгісі мен логосы Bluetooth SIG, Inc. компаниясына тиесілі.

Ubuntu, LTS – Canonical Ltd. компаниясының тіркелген тауар белгісі.

Cisco, Cisco Jabber, Cisco Systems, IOS – Cisco Systems, Inc. және/немесе оның үлестес компанияларының тауар белгілері немесе АҚШ-та және басқа елдерде тіркелген тауар белгілері.

Citrix, XenServer – Cloud Software Group, Inc. компаниясының және/немесе АҚШ-дағы және/немесе басқа елдердегі еншілес компаниялардың тіркелген сауда белгілері немесе сауда белгілері.

Corel – тауар белгісі немесе Канадада, Америка Құрама Штаттарында және басқа елдерде тіркелген Corel корпорациясының және/немесе оның еншілес компанияларының тауар белгісі.

Cloudflare, Cloudflare логотипі және Cloudflare Workers – Cloudflare, Inc. компаниясының сауда белгілері және/немесе АҚШ-та және басқа юрисдикцияларда тіркелген сауда белгілері.

Dropbox – Dropbox, Inc. тауар белгісі.

Radmin – Famatech компаниясының тіркелген тауар белгісі.

Firebird белгісі – Firebird қорының тіркелген тауар белгісі.

Foxit – Foxit корпорациясының тіркелген тауар белгісі.

FreeBSD белгісі – FreeBSD қорының тіркелген тауар белгісі.

Google, Android, Chrome, Chromium, Dalvik, Firebase, Google Chrome, Google Earth, Google Play, Google Maps, Google Public DNS, Hangouts, YouTube – Google LLC тауар белгілері.

EulerOS, FusionCompute, FusionSphere – Huawei Technologies Co., Ltd. тауар белгілері.

Intel, Core, Xeon – Intel корпорациясының немесе оның еншілес компанияларының сауда белгілері.

IBM, QRadar – дүние жүзі бойынша көптеген юрисдикцияларда тіркелген International Business Machines Corporation тауар белгілері.

Node.js – Joyent, Inc. тауар белгісі.

Linux – АҚШ-та және басқа елдерде тіркелген Linus Torvalds тауар белгісі.

Logitech – тіркелген тауар белгісі немесе Logitech компаниясының АҚШ-тағы және (немесе) басқа елдердегі тауар белгісі.

Microsoft, Active Directory, ActiveSync, BitLocker, Excel, Forefront, Internet Explorer, InfoPath, Hyper-V, Microsoft Edge, MultiPoint, MS-DOS, PowerShell, PowerPoint, SharePoint, SQL Server, Office 365, OneNote, Outlook, Skype, Tahoma, Visio, Win32, Windows, Windows PowerShell, Windows Media, Windows Server, Windows Phone, Windows Vista, Windows Azure – Microsoft компаниялар тобының тауар белгілері болып табылады.

Mozilla, Firefox, Thunderbird – АҚШ-та және басқа елдерде тіркелген Mozilla Foundation тауар белгілері.

Novell – Америка Құрама Штаттарында және басқа елдерде тіркелген Novell Enterprises Inc. тауар белгісі.

OpenSSL – OpenSSL Software Foundation құқық иесінің тауар белгісі болып табылады.

OpenVPN – OpenVPN, Inc. компаниясының тіркелген сауда белгісі.

Oracle, Java, JavaScript, TouchDown – Oracle Corporation және/немесе оның үлестес компанияларының тіркелген тауар белгілері.

Parallels, Parallels логотипі және Coherence – Parallels International GmbH компаниясының тауар белгілері немесе тіркелген тауар белгілері.

Chef – тауар белгісі немесе АҚШ-та және/немесе басқа елдерде тіркелген Progress Software Corporation және/немесе еншілес не үлестес компаниялардың бірінің тауар белгісі.

Puppet – тауар белгісі немесе Puppet, Inc. компаниясының тіркелген тауар белгісі.

Python – тауар белгісі немесе Python Software Foundation тіркелген тауар белгісі.

Red Hat, Fedora, Red Hat Enterprise Linux – Америка Құрама Штаттарында және басқа елдерде тіркелген Red Hat Inc. тауар белгілері.

Ansible – Red Hat, Inc. компаниясының АҚШ-та және басқа елдерде тіркелген тауар белгісі.

CentOS – Америка Құрама Штаттарында және басқа елдерде тіркелген Red Hat Inc. тауар белгісі.

BlackBerry тауар белгісі Research In Motion Limited компаниясына тиесілі, АҚШ-та тіркелген және басқа елдерде тіркеуге берілуі немесе тіркелуі мүмкін.

Rocky Linux – The Rocky Enterprise Software Foundation компаниясының сауда белгісі.

Samsung – SAMSUNG компаниясының АҚШ-тағы немесе басқа елдердегі тауар белгісі.

Debian – Software in the Public Interest, Inc. тіркелген тауар белгісі.

Splunk, SPL – тауар белгілері және АҚШ-та және басқа елдерде тіркелген Splunk, Inc. сауда белгілері.

SUSE – АҚШ-та және басқа елдерде тіркелген SUSE LLC тауар белгісі.

Symbian тауар белгісінің иесі Symbian Foundation Ltd.

OpenAPI – Linux Foundation тауар белгісі.

UNIX – АҚШ-та және басқа елдерде тіркелген тауар белгісі, қолданылуы X/Open Company Limited тарапынан лицензияланған.

Zabbix – Zabbix SIA тіркелген тауар белгісі.