kaspersky

Kaspersky Security Center 15.1 Linux

Мазмұны

Kaspersky Security Center Linux бағдарламасына анықтама

Жаңа функциялар

- Не жаңалық

Аппараттық және бағдарламалық талаптар

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

Жұмысқа кірісу

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

Лицензиялау және белсендіру

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

Орналастыру және конфигурациялау

- Желідегі құрылғыларды табу
- Тарату нүктелері және/немесе қосылым шлюздеріне арналған есептеулер
- Үшінші тарап қауіпсіздік қолданбаларын алмастыру
- "Лаборатория Касперского" қолданбалары. Орталықтандырылған орналастыру
- Желі қорғанысын конфигурациялау

- "Лаборатория Касперского" қолданбалары. Дерекқорлар мен қолданба модульдерін жаңарту

Мониторинг

- Бақылау және есеп беру
- Cloud Discovery

Осалдықтар мен патчтарды басқару

- Үшінші тарап бағдарламаларындағы осалдықтарды анықтау және түзету

Кеңейтілген мүмкіндіктер

- Оқиғаларды SIEM жүйелеріне экспорттау
- Өлшеу нұсқаулығы (тек анықтама)

Не жаңалық

Kaspersky Security Center 15.1 Linux

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

- 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 "Касперский Зертханасы" 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.

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

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

- Windows жүйесіне арналған Kaspersky Endpoint Security жүйесінен Windows Server жүйесіне арналған Kaspersky Security нұсқасына жаңарту бұдан былай мақсатты құрылғыны қайта жүктеуді қажет етпейді.

- 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.
- Пайдаланушының қолданудан алған әсері жақсартылды, соның ішінде:
  - Бекітілген**Бекітілген****Kaspersky Security Center Web Console бөлімдерін бекіту** 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 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 *Сценарийлерді қашықтан іске қосу* 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** бөлікшесінде 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 қолданбасында 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 "Касперский Зертханасы" 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 "Касперский Зертханасы" 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 **Ескертуді көру** сілтемесін басу арқылы қауіптердің даму тізбегін ашуға болады.
- Kaspersky Security Center Linux енді кластерлік технологияны қолдайды. Басқару топта серверлердің кластерлері немесе массивтері болса, **Басқарылатын 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 қолданбасында 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 қолданба 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 "Касперский Зертханасы" қолданбаларының дистрибутивтерін және басқару веб-плагиндерін жүктеп алуға және жаңартуға мүмкіндік береді.

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

- "Лаборатория Касперского" серверлеріне қатынасу енді автоматты түрде тексеріледі. Жүйелік DNS арқылы серверлерге қатынасу мүмкін болмаса, қолданба 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 орындарының қоймаларына жүктеп алу*

Kaspersky Security Center 14 Linux

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

- *Жаңартуларды Басқару серверінің қоймасына жүктеп алу* тапсырмасынан бөлек, "Лаборатория Касперского" қауіпсіздік қолданбаларына арналған антивирустық дерекқорларды енді *Жаңартуларды тарату орындарының қоймаларына жүктеп алу* тапсырмасы арқылы жүктеп алуға болады.

- Басқарылатын құрылғылардағы антивирустық дерекқорлар мен қолданба 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 "Лаборатория Касперского" жаңартулар серверлерінен тек "Лаборатория Касперского" қауіпсіздік қолданбалары сұраған жаңартуларды жүктейді. Бұл жүктелген деректердің өлшемін азайтады.

- Енді сіз антивирустық дерекқорлар мен қолданба модульдерін жүктеп алу үшін айырмашылық файлдардың жүктеу функциясын пайдалана аласыз. Айырмашылықтар файлы дерекқор немесе қолданба модульдері файлдарының екі нұсқасы арасындағы айырмашылықтарды сипаттайды. Айырмашылық файлдарын пайдалану трафикті ұйымыңыздың желісінде сақтайды, өйткені айырмашылық файлдары бүкіл дерекқор және қолданба модульдері 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 қолданба ретінде қолдайды.

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 "Лаборатория Касперского" қауіпсіздік қолданбаларын орнатуға, тексеру және жаңарту тапсырмаларын қашықтан іске қосуға, сондай-ақ басқарылатын қолданбалардың 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 қолданбасы 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.

- "Лаборатория Касперского" қолданбалары негізінде құрылған антивирустық қауіпсіздік жүйесін басқару.

- "Лаборатория Касперского" қолданбаларын және басқа үшінші тарап қолданбаларын қашықтан орнатуды орындау.

- "Лаборатория Касперского" қолданбаларының лицензиялық кілттерін клиент құрылғыларына орталықтан тарату, кілттердің қолданылуын бақылау және лицензиялардың жарамдылық мерзімін ұзарту.

- Қолданбалар мен құрылғылардың жұмысы туралы статистика мен есептер алу.

- "Лаборатория Касперского" қолданбаларының 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 қолданбалары карантинге немесе сақтық көшірмелеуге орналастырылған файлдармен, сондай-ақ қауіпсіздік қолданбалары өңдеуді кейінге қалдырған файлдармен орталықтандырылған түрде жұмыс істеу.

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

Kaspersky Security Center Linux қолданбасын "Лаборатория Касперского" арқылы сатып алсаңыз, қолданбаны біздің сайттан жүктеп алуға болады. Қолданбаны іске қосу үшін қажетті ақпарат төлем жасалғаннан кейін сізге электрондық пошта арқылы жіберіледі.

Аппараттық және бағдарламалық талаптар

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

Басқару серверіне қойылатын талаптар

Ең төменгі аппараттық талаптар:

- Жиілігі 1,4 ГГц немесе одан жоғары процессор.
- Жедел жад: 4 ГБ.
- Дискідегі бос орын көлемі: 10 ГБ (/var/opt/kaspersky/klnagent_srv).

Келесі операциялық жүйелерге қолдау көрсетіледі:

- Debian GNU/Linux 11.x (Bullseye) 64 разрядты.
- Debian GNU/Linux 12 (Bookworm) 64 разрядты.
- Ubuntu Server 20.04 LTS (Focal Fossa) 64 разрядты.
- Ubuntu Server 22.04 LTS (Jammy Jellyfish) 64 разрядты.
- CentOS Stream 9 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.
- 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 (жаңарту 1.6) 64 разрядты.
- Astra Linux Special Edition RUSB.10015-01 (жаңарту 1.7) 64 разрядты.
- Astra Linux Special Edition RUSB.10015-01 (жаңарту 1.8) 64 разрядты.
- Astra Linux Special Edition RUSB.10015-16 (1-шығарылым, жаңарту 1.6) 64 разрядты.

- Astra Linux Special Edition RUSB.10015-17 (жаңарту 1.7.3) 64 разрядты.
- Astra Linux Special Edition RUSB.10015-37 (жаңарту 7.7) 64 разрядты.
- Astra Linux Common Edition (жаңарту 2.12) 64 разрядты.
- Альт СП Сервер 10 64 разрядты.
- Альт Сервер 10 64 разрядты.
- Альт 8 СП Сервер (ЛКНВ.11100-01) 64 разрядты.
- Альт 8 СП Сервер (ЛКНВ.11100-02) 64 разрядты.
- Альт 8 СП Сервер (ЛКНВ.11100-03) 64 разрядты.
- Oracle Linux 7 64 разрядты.
- Oracle Linux 8 64 разрядты.
- Oracle Linux 9 64 разрядты.
- РЕД ОС 7.3 Сервер 64 разрядты.
- РЕД ОС 7.3 Сертификатталған редакция 64 разрядты.
- РЕД ОС 8 Сертификатталған редакция 64 разрядты.
- РОСА "КОБАЛЬТ" 7.9 64 разрядты.

Әдепкі параметрлері бар EXT4 файлдық жүйесін пайдалану ұсынылады.

Келесі виртуалдандыру платформаларына қолдау көрсетіледі:

- VMware vSphere 6.7.
- VMware vSphere 7.0.
- VMware vSphere 8.0.
- VMware Workstation 16 Pro.
- VMware Workstation 17 Pro.
- Microsoft Hyper-V Server 2012 64 разрядты.
- Microsoft Hyper-V Server 2012 R2 64 разрядты.
- Microsoft Hyper-V Server 2016 64 разрядты.
- Microsoft Hyper-V Server 2019 64 разрядты.
- Microsoft Hyper-V Server 2022 64 разрядты.

- Citrix XenServer 7.1 LTSR.
- Citrix XenServer 8.x.
- Parallels Desktop 17.
- Oracle VM VirtualBox 6.x.
- Oracle VM VirtualBox 7.x.
- Kernel-based Virtual Machine (Басқару сервері қолдайтын барлық Linux операциялық жүйелері).

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

- MySQL 5.7 Community 32 разрядты/64 разрядты.
- MySQL 8.0 32 разрядты/64 разрядты.
- MariaDB 10.1 (жинағы 10.1.30 және одан да жоғары) 32 разрядты/64 разрядты.
- 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 10.5.17 және одан да жоғары) 32 разрядты/64 разрядты.
- MariaDB 10.6 (жинағы 10.6.9 және одан да жоғары) 32 разрядты/64 разрядты.
- MariaDB 10.11 (жинағы 10.11.3 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.
- Postgres Pro 13.x (барлық редакция) 64 разрядты.
- Postgres Pro 14.x (барлық редакция) 64 разрядты.
- Postgres Pro 15.x (барлық редакция) 64 разрядты.
- Platform V Pangolin 5.4.0 64 разрядты.
- Jatoba 4 64 разрядты.

Web Console консоліне қойылатын талаптар

Kaspersky Security Center Web Console Server сервері

Ең төменгі аппараттық талаптар:

- Процессор: 4 ядро, жиілігі 2,5 ГГц-тен бастап.
- Жедел жад: 8 ГБ.
- Дискідегі бос орын көлемі: 40 ГБ (/var/opt/kaspersky).

Келесі операциялық жүйелердің бірі (тек 64 разрядты нұсқалар):

- Debian GNU/Linux 11.x (Bullseye).
- Debian GNU/Linux 12 (Bookworm).
- Ubuntu Server 20.04 LTS (Focal Fossa).
- Ubuntu Server 22.04 LTS (Jammy Jellyfish).
- CentOS Stream 9.
- Red Hat Enterprise Linux Server 7.x.
- Red Hat Enterprise Linux Server 8.x.
- Red Hat Enterprise Linux Server 9.x.
- SUSE Linux Enterprise Server 12 (барлық жаңартулар пакеттері).
- SUSE Linux Enterprise Server 15 (барлық жаңартулар пакеттері).
- Astra Linux Special Edition RUSB.10015-01 (жаңарту 1.6).
- Astra Linux Special Edition RUSB.10015-16 (1-шығарылым, жаңарту 1.6).
- Astra Linux Special Edition RUSB.10015-01 (жаңарту 1.7).
- Astra Linux Special Edition RUSB.10015-17 (жаңарту 1.7.3).
- Astra Linux Special Edition RUSB.10015-01 (жаңарту 1.8).
- Astra Linux Special Edition RUSB.10015-37 (жаңарту 7.7).
- Astra Linux Common Edition (жаңарту 2.12).
- Альт СП Сервер 10.
- Альт Сервер 10.
- Альт 8 СП Сервер (ЛКНВ.11100-01).
- Альт 8 СП Сервер (ЛКНВ.11100-02).
- Альт 8 СП Сервер (ЛКНВ.11100-03).
- Oracle Linux 7.

- Oracle Linux 8.
- Oracle Linux 9.
- РЕД ОС 7.3 Сервер.
- РЕД ОС 7.3 Сертификатталған редакция.
- РЕД ОС 8 Сертификатталған редакция.
- РОСА "КОБАЛЬТ" 7.9.
- Kernel-based Virtual Machine (Kaspersky Security Center Web Console сервері қолдайтын барлық Linux операциялық жүйелері).

Клиент құрылғылары

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

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

Браузерлер:

- Google Chrome 125.0.6422.76 және одан жоғары (ресми құрастыру).
- Microsoft Edge 111.0.1661.41 және одан жоғары.
- Safari 17.1 for macOS.
- Яндекс Браузері 23.5.0.2271 және одан жоғары.
- Mozilla Firefox Extended Support Release 115.9.1 немесе одан жоғары.

Басқару 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 бағдарламалық жасақтама талаптары: Perl тілі интерпретаторының 5.10 немесе одан жоғары нұсқасы орнатылуы керек.

Желілік агент Қолдау көрсетілетін платформалар

Операциялық жүйелер. Microsoft Windows жұмыс	Microsoft Windows Embedded POSReady 2009, соңғы Service Pack-пен, 32 разрядты.

станциялары	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, 64 разрядты. Microsoft Windows 10 TH2 (November 2015) Home/Pro/Pro for Workstations/Enterprise/Education, 64 разрядты. Microsoft Windows 10 RS1 (August 2016) Home/Pro/Pro for Workstations/Enterprise/Education, 64 разрядты. Microsoft Windows 10 RS2 (April 2017) Home/Pro/Pro for Workstations/Enterprise/Education, 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. Microsoft Windows 11 Home/Pro/Pro for Workstations/Enterprise/Education, 64 разрядты. Microsoft Windows 11 22H2 Home/Pro/Pro for Workstations/Enterprise/Education, 64 разрядты. Microsoft Windows 11 23H2 Home/Pro/Pro for Workstations/Enterprise/Education, 64 разрядты. Microsoft Windows 11 24H2 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). 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 Small Business Server 2011 Standard/Essentials 64 разрядты. Microsoft Windows MultiPoint Server 2011 Standard/Premium 64 разрядты. 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/Core Mode/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 2022 21H2 Standard/Datacenter 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. 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.

CentOS 6.7 and later 32 разрядты.

CentOS 6.x (6.6 дейін), 32 разрядты/64 разрядты.

CentOS 7.x 64 разрядты.

CentOS Stream 8 64 разрядты.

CentOS Stream 9 64 разрядты.

CentOS Stream 9 ARM 64 разрядты.

Red Hat Enterprise Linux Server 6.x 32 разрядты/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.

SUSE Linux Enterprise Server 12 (барлық жаңарту пакеттері) 64 разрядты.

SUSE Linux Enterprise Server 15 (барлық жаңарту пакеттері) 64 разрядты.

SUSE Linux Enterprise Server 15 (барлық жаңарту пакеттері) ARM, 64 разрядты.

openSUSE 15 64 разрядты.

EulerOS 2.0 SP10, 64 разрядты.

EulerOS 2.0 SP10 ARM 64 разрядты.

Astra Linux Special Edition RUSB.10015-01 (жаңарту 1.5) 64 разрядты.

Astra Linux Special Edition RUSB.10015-01 (жаңарту 1.6) 64 разрядты.

Astra Linux Special Edition RUSB.10015-16 (1-шығарылым, жаңарту 1.6) 64 разрядты.

Astra Linux Special Edition RUSB.10015-17 (жаңарту 1.7.3) 64 разрядты.

Astra Linux Special Edition RUSB.10015-01 (жаңарту 1.7) 64 разрядты.

Astra Linux Special Edition RUSB.10015-01 (жаңарту 1.8) 64 разрядты.

Astra Linux Special Edition RUSB.10015-37 (жаңарту 7.7) 64 разрядты.

Astra Linux Special Edition RUSB.10152-02 (жаңарту 4.7) ARM 64 разрядты.

Astra Linux Common Edition (жаңарту 2.12) 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 Сервер 10 64 разрядты.

Альт Сервер 10 ARM 64 разрядты.

Альт Жұмыс станциясы 10 32 разрядты/64 разрядты.

	Альт 8 СП Жұмыс станциялары (8.4) ARM, 64 разрядты. Альт 8 СП Сервер (8.4) 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 (LKNV.11100-01) 32 разрядты/64 разрядты. Альт 8 СП Жұмыс станциясы (LKNV.11100-02) 32 разрядты/64 разрядты. Альт 8 СП Жұмыс станциясы (LKNV.11100-03) 32 разрядты/64 разрядты. Mageia 4 32 разрядты. Oracle Linux 7 64 разрядты. Oracle Linux 8 64 разрядты. Oracle Linux 9 64 разрядты. Linux Mint 20.x 64 разрядты. Linux Mint 21.1 және одан жоғары 64 разрядты. AlterOS 7.5 немесе одан жоғары 64 разрядты. GosLinux IC6/7.17, 64 разрядты. GosLinux IC6/7.2, 64 разрядты. SberOS 3.2.0, 64 разрядты. Platform V SberLinux OS Server (SLO) 8.8. РЕД ОС 7.3 ARM 64 разрядты. РЕД ОС 7.3 Сервер 64 разрядты. РЕД ОС 7.3 Сертификатталған редакция 64 разрядты. РЕД ОС 8 Сертификатталған редакция 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. Atlant, Alcyone build, 2022.02 нұсқасы, 64 разрядты. MSVSPHERE 9.2 SERVER 64 разрядты. MSVSPHERE 9.2 ARM 64 разрядты. SynthesisM Server 8.6 64 разрядты. SynthesisM Client 8.6 64 разрядты. OSnova 2.10. Kylin 10 64 разрядты. EMIAS 1.0 64 разрядты. Amazon Linux 2 64 разрядты. MosOS 15.4 Arbat, 64 разрядты. M OS (Moscow Electronic School), 64 разрядты.

Операциялық жүйелер. macOS	macOS Monterey (12.x). macOS Ventura (13.x). macOS Sonoma (14.x). Желілік агент үшін Intel сияқты Apple Silicon (M1) архитектурасына қолдау көрсетіледі.
Виртуализация платформалары	VMware vSphere 8.0. Microsoft Hyper-V Server 2016 64 разрядты. Microsoft Hyper-V Server 2019 64 разрядты. Microsoft Hyper-V Server 2022 64 разрядты. Citrix XenServer 7.1 LTSR. Citrix XenServer 8.x. Parallels Desktop 17. Oracle VM VirtualBox 6.x. Oracle VM VirtualBox 7.x. Kernel-based Virtual Machine (Желілік агент қолдайтын барлық Linux операциялық жүйелері).

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 "Лаборатория Касперского" қауіпсіздік қолданбасымен бірге жеткізіледі.

"Лаборатория Касперского" үйлесімді қолданбалары мен шешімдері

Kaspersky Security Center Linux "Лаборатория Касперского" келесі қолданбаларын қашықтан орнатуды және басқаруды қолдайды:

- Kaspersky Endpoint Security for Windows 12.0 және одан жоғары (файл серверлерін қолдайды).
- Kaspersky Endpoint Security for Linux 11.2 және одан жоғары (файл серверлерін қолдайды).
- Kaspersky Endpoint Security for Linux Elbrus Edition 10 және одан жоғары.
- Kaspersky Endpoint Security for Linux ARM Edition 11.2 және одан жоғары.
- Kaspersky Endpoint Security for Mac 11.3 және одан жоғары.
- Kaspersky Industrial CyberSecurity for Linux Nodes 1.3 және одан жоғары.
- Kaspersky Industrial CyberSecurity for Nodes 3.2 және одан жоғары.
- Kaspersky Industrial CyberSecurity for Networks 3.2 және одан жоғары.
- Kaspersky Endpoint Agent 3.15 және одан жоғары.
- Kaspersky Embedded Systems Security for Windows 3.2 және одан жоғары.
- Kaspersky Embedded Systems Security for Linux 3.3 және одан жоғары.
- Kaspersky Security for Virtualization 5.2 Light Agent және одан да жоғары.

Kaspersky Security Center Linux келесі шешімдерге кіреді:

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

Қолданбалар мен шешімдердің нұсқалары туралы толық ақпарат алу үшін "Қолданбалардың өмірлік циклі" бетін қараңыз.

Шектеулер тізімі

Kaspersky Security Center Linux келесі шектеулермен Windows жүйесіне арналған Kaspersky Endpoint Security басқаруына қолдау көрсетеді: Kaspersky Sandbox құрамдасына қолдау көрсетілмейді.

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

Жеткізу жиынтығы

Қолданбаны "Лаборатория Касперского" интернет-дүкендері (мысалы, https://www.kaspersky.ru сайтында) немесе серіктес компаниялар арқылы сатып алуға болады.

Интернет-дүкен арқылы Kaspersky Security Center Linux сатып ала отырып, сіз қолданбаны интернет-дүкеннің сайтынан көшіресіз. Қолданбаны іске қосу үшін қажетті ақпарат төлем жасалғаннан кейін сізге электрондық пошта арқылы жіберіледі.

Басқару сервері мен Kaspersky Security Center Web Console веб-консолінің үйлесімділігі туралы

Kaspersky Security Center Linux басқару сервері мен Kaspersky Security Center Web Console соңғы нұсқасын пайдалану ұсынылады. Әйтпесе Kaspersky Security Center Linux функцияларына шектеу қойылуы мүмкін.

Сіз Kaspersky Security Center Linux 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:

- Kaspersky Security Center Linux 15.1 қолданбасына қосылған Web Console консолі келесі нұсқадағы Kaspersky Security Center Linux басқару серверіне қолдау көрсетеді: 15 және 14.2.
- Kaspersky Security Center Linux 15.1 қолданбасына қосылған басқару сервері Kaspersky Security Center Web Console веб-консолінің келесі нұсқаларына қолдау көрсетеді: 15 және 14.2.

Kaspersky Security Center нұсқаларын салыстыру: Windows негізінде және Linux негізінде

"Лаборатория Касперского" Kaspersky Security Center қолданбасын Windows және Linux платформаларына арналған жергілікті шешім ретінде ұсынады. Windows операциялық жүйесіне арналған шешімде сіз Басқару серверін Windows операциялық жүйесі орнатылған құрылғыға орнатасыз. Linux негізіндегі шешімде Linux операциялық жүйесі орнатылған құрылғыға орнатуға арналған Басқару сервері нұсқасы бар. Бұл анықтама Kaspersky Security Center Linux туралы ақпаратты қамтиды. Linux негізіндегі шешім туралы толық ақпарат алу үшін Kaspersky Security Center for Linux 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 қолданбасының мүмкіндіктерін салыстыру

Функция немесе сипат	Kaspersky Security Center 14.2 Windows	Kaspersky Security Center 15.1 Linux
Басқару серверінің орналасуы	Жергілікті	Жергілікті
Дерекқорды басқару жүйесінің (ДҚБЖ) орналасуы	Жергілікті	Жергілікті
Басқару серверін орнатуға арналған операциялық жүйе	Windows	Linux
Басқару консолінің түрі	Жергілікті және веб-интерфейс	Веб-интерфейс
Веб-интерфейсі бар Басқару консолін орнатуға арналған операциялық жүйе	Windows немесе Linux	Linux

Басқару серверлерінің иерархиясы	✓	✓
Басқару топтары иерархиясы	✓	✓
Желіде сауалнама өткізу	✓	✓
Басқарылатын құрылғылардың ең көп саны	100 000	50 000 (PostgreSQL және Postgres Pro көмегімен)
Windows, macOS және Linux басқаратын құрылғыларды қорғау	✓	✓
Ұялы құрылғыларды қорғау	✓	–
Виртуалды машиналарды қорғау	✓	✓
Жария бұлтты инфрақұрылымды қорғау	✓	–
Құрылғылардың қауіпсіздігін басқару	✓	✓
Пайдаланушыға бағытталған қауіпсіздікті басқару	✓	✓
Қолданба саясаттары	✓	✓
"Лаборатория Касперского" қолданбаларына арналған тапсырмалар	✓	✓
Kaspersky Security Network	✓	✓
KSN прокси-сервері	✓	✓
Kaspersky Private Security Network	✓	✓
"Лаборатория Касперского" қолданбаларының лицензиялық кілттерін орталықтан тарату	✓	✓
Антивирустық дерекқорларды автоматты түрде жаңарту	✓	✓
Виртуалды Басқару серверлерін қолдау	✓	✓
Үшінші тарап қолданбаларының жаңартуларын орнату және үшінші тарап қолданбаларындағы осалдықтарды іздеу	✓	✓
Басқарылатын құрылғыларда болған оқиғалар туралы хабарландырулар	✓	✓
Пайдаланушы есептік жазбаларын жасау, есептік жазбаларды бақылау	✓	✓
Домендік түпнұсқалық растамасын пайдаланып консольге кіру	✓	✓ (бірыңғай кіруге (SSO) уақытша қолдау көрсетілмейді)
SIEM жүйелерімен біріктіру	✓	✓ (тек Syslog пайдалану арқылы)
Саясаттар мен тапсырмалардың күйін мониторингтеу	✓	✓
Ақауларға төзімді Kaspersky Security Center кластерін орналастыру	✓	✓
Басқару серверін ақауларға төзімді Windows Server кластеріне орнату	✓	–

Басқару серверінің статистикасын үшінші тарап қолданбаларына жіберу үшін SNMP пайдалану	✓	–
Клиент құрылғыларын қашықтан диагностикалау	✓	✓
Клиент құрылғысының жұмыс үстеліне қашықтан қосылу	✓	–
Нысанды тексерумен жұмыс	✓	✓
"Лаборатория Касперского" қолданбаларын автоматты түрде жаңарту	✓	✓
Клиент құрылғыларында операциялық жүйелерді орналастыру	✓	–
Орнату пакеттерін және басқа файлдарды жариялауға арналған веб-сервер	✓	✓
Endpoint Detection and Response арқылы тіркелген алерттерді көру және олармен жұмыс істеу	✓	✓
Басқару серверін WSUS сервері ретінде пайдалану	✓	–
Kaspersky Managed Detection and Response-пен біріктіру	✓	✓
Аномалияларды бейімделумен басқаруды қолдау көрсету	✓	✓
Басқару топтарындағы кластерлер мен сервер массивтеріне қолдау көрсету	✓	✓
Үшінші тарап лицензиясын басқару	✓	–

Kaspersky Security Center Cloud Console туралы

Kaspersky Security Center қолданбасын жергілікті түрде жұмыс істейтін қолданба ретінде қолдансаңыз, демек, сіз Kaspersky Security Center қолданбасын, соның ішінде Басқару серверін жергілікті құрылғыға орнатып, Microsoft Management Console (MMC) Басқару консолі негізінде Басқару консолі арқылы немесе Kaspersky Security Center Web Console көмегімен желі қауіпсіздігі жүйесін басқарасыз.

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

Kaspersky Security Center Cloud Console 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.

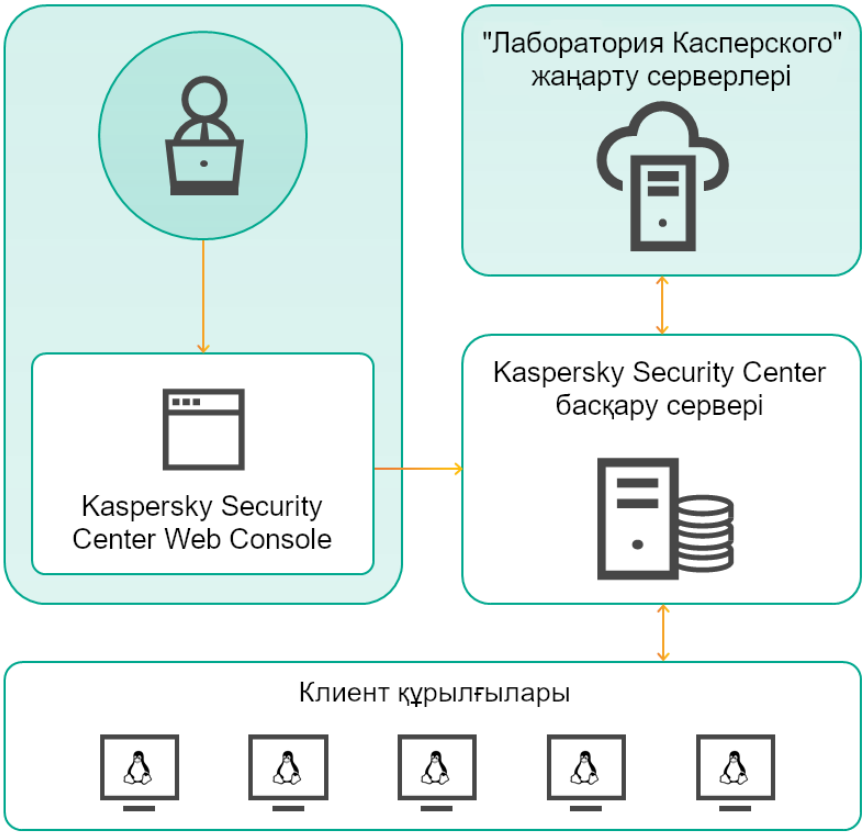
Kaspersky Security Center Cloud Console және функционалдылығы туралы көбірек ақпарат Kaspersky Security Center Cloud Console құжаттамасында және Kaspersky Endpoint Security for Business құжаттамасында қолжетімді.

Архитектура және негізгі ұғымдар

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

Қолданба архитектурасы

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



Kaspersky Security Center Linux қолданбасы архитектурасы

Kaspersky Security Center Linux қолданбасы келесі негізгі құрамдастарды қамтиды:

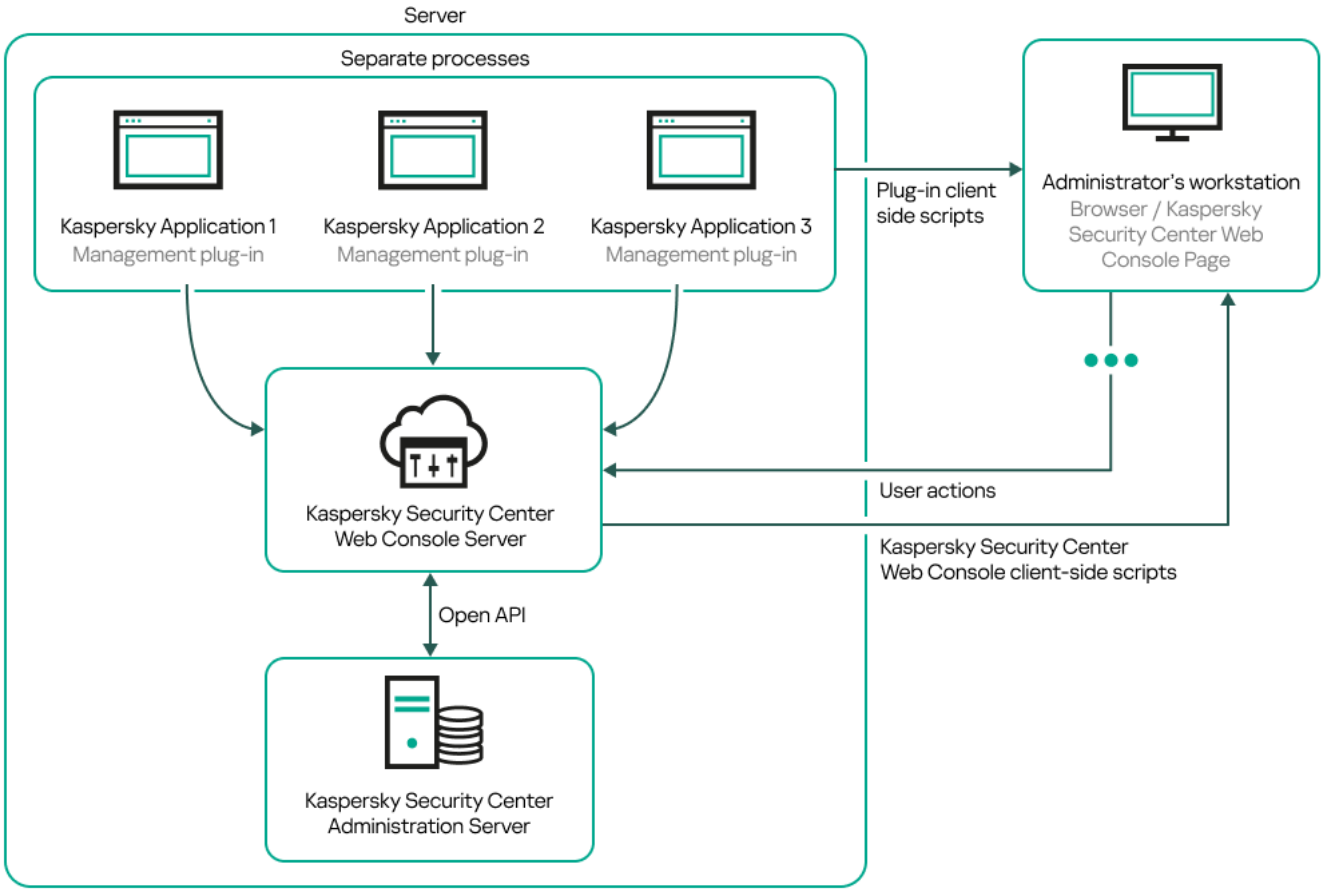
- **Kaspersky Security Center Web Console**. Бұл Kaspersky Security Center басқаратын ұйым-клиент желісін қорғау жүйесін құруға және басқаруға арналған веб-интерфейс.
- **Kaspersky Security Center Басқару сервері** (бұдан әрі *Сервер* деп те аталады). Ұйымның желісінде орнатылған қолданбалар және оларды басқару туралы ақпаратты орталықтандырылған сақтау функцияларын жүзеге асырады.
- **"Лаборатория Касперского" жаңарту серверлері**. "Лаборатория Касперского" қолданбаларына дерекқорлар мен модульдердің жаңартуларын жіберетін "Лаборатория Касперского" HTTP серверлері мен HTTPS серверлері.

- **KSN серверлері**. Серверлерде файлдардың, веб-ресурстардың және бағдарламалық жасақтаманың беделі туралы "Лаборатория Касперского" жедел білім базасы бар. Kaspersky Security Network "Лаборатория Касперского" қолданбаларының 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 "Лаборатория Касперского" қауіпсіздік қолданбаларының 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 "Лаборатория Касперского" қолданбаларын басқару плагиндерін (әр қолданба 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 серверінде және клиент құрылғыларында ашылуы тиісті порттар атап 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. Әдепкі бойынша порт мәндерін Басқару сервері сипаттары терезесі **Веб-сервер** бөлімінде өзгерте аласыз.
8061	klcsweb	TCP (TLS)	Клиент құрылғыларына жарияланған орнату пакеттерін беру	Орнату пакеттерін жариялау. Әдепкі бойынша порт мәндерін Басқару сервері сипаттары терезесі **Веб-сервер** бөлімінде өзгерте аласыз.
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 қосылым порттарын конфигурациялау кезінде Желілік агенттерден қосылымдарды қабылдау үшін әдепкі порт нөмірін өзгертуге болады. Басқару серверлерінің иерархиясын жасау кезінде Қосалқы Басқару серверлерінен қосылымдарды қабылдау үшін әдепкі порт нөмірін өзгертуге болады.
13000	klserver	UDP	Желілік агенттерден құрылғыларды өшіру туралы ақпарат қабылдау	Клиент құрылғыларын басқару. Әдепкі бойынша порт мәндерін Басқару сервері саясатының сипаттары терезесінде өзгерте аласыз.
13299	klserver	TCP (TLS)	Kaspersky Security Center Web Console веб-консолінен Басқару серверіне қосылымдар алу; Басқару серверінен OpenAPI арқылы қосылымдар алу	Kaspersky Security Center Web Console, OpenAPI.

				Әдепкі бойынша порт нөмірін Басқару сервері сипаттары терезесінде (**Жалпы** бөлімнің **Қосылу порттары** бөлікшесінде) немесе Басқару серверлерінің иерархиясын жасаған кезде өзгерте аласыз.
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.
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.
17000	klactprx	TCP (TLS)	Басқарылатын құрылғылардан қолданбаларды 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.
19170	klserver	HTTPS (TLS)	klsctunnel утилитасы көмегімен басқарылатын құрылғылармен байланысты туннельдеу	Басқарылатын құрылғыларға Kaspersky Security Center Web Console веб-консолі арқылы қашықтан қосылу. Әдепкі порт нөмірін klscflag утилитасын пайдаланып өзгерте аласыз.

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

Төмендегі кестеде, Kaspersky Security Center Web Console Server серверінде ашылуы тиісті 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 ашық болуы тиісті порт 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 бойынша порт мәндерін Басқару сервері саясатының сипаттары 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.

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 ашылуы тиісті порттар көрсетілген. Атап көрсетілген порттар, Желілік агенттер қолданатын порттарға қосымша ретінде, тарату нүктелерінің рөлін атқаратын құрылғыларда ашылуы тиіс (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 алу	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.

Kaspersky Security Center Web Console қолданбасы 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.

Kaspersky Security Center Web Console қолданбасы қолданатын порттар

Порт нөмірі	Қызмет атауы	Протокол	Портты тағайындау	Ай
2001	KSCWebConsolePlugin	HTTPS	KSCWebConsoleManagementService қызметінен сұраулар алу үшін басқару плагинінің процестері пайдаланатын API порты.	Басқару плагинд node процес іске қос
1329, 2003	KSCWebConsoleManagementService	HTTPS	Бір құрылғыда жұмыс істейтін KSCWebConsoleManagementService	Kaspers Security Web Co

			қызметінен сұраулар алу үшін пайдаланылатын API порттары.	құрамда жаңарту
2005	KSCWebConsole	HTTPS	Дәл сол құрылғыда жұмыс істейтін KSCWebConsoleManagementService қызметінен сұраулар алу үшін пайдаланылатын API порты.	Kaspers Security Web Co қолданб node процес іске қос
8200	–	HTTP	HashiCorp Vault арқылы сертификаттар жасау үшін қолданылатын API порты (толық ақпарат HashiCorp Vault сайтында).	Kaspers Security Web Co веб-кон орнату Kaspers Security Web Co құрамда жаңарту
4150, 4151, 4152	KSCWebConsoleMessageQueue	HTTPS	Kaspersky Security Center Web Console және басқару плагиндері арасындағы байланыс үшін пайдаланылатын Message Broker API порттары.	Kaspers Security Web Co және ба плагинд арасынд өзара іс

Негізгі ұғымдар

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

Басқару сервері

Kaspersky Security Center құрамдастары клиент құрылғыларында орнатылған "Лаборатория Касперского" қолданбаларын 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 Kaspersky Security Center Linux орнату бөлімін қараңыз.

Басқару сервері келесі функцияларды орындайды:

- басқару топтары құрылымын сақтау;
- клиент құрылғыларының конфигурациясы туралы ақпаратты сақтау;
- қолданбалардың дистрибутивтерінің қоймаларын ұйымдастыру;
- клиент құрылғыларына қолданбаларды қашықтан орнату және қолданбаларды жою;
- "Лаборатория Касперского" дерекқорлары мен қолданба модульдерін жаңарту;
- клиент құрылғыларындағы саясат пен тапсырмаларды басқару;
- клиент құрылғыларында болған оқиғалар туралы ақпаратты сақтау;
- "Лаборатория Касперского" қолданбаларының жұмысы туралы есептерді қалыптастыру;
- клиент құрылғыларына лицензиялық кілттерді тарату, кілт туралы ақпаратты сақтау;
- тапсырмалардың орындалу барысы туралы хабарландырулар жіберу (мысалы, клиент құрылғысында вирустарды анықтау).

Қолданба 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 қолданбасын қолданып жатсаңыз, онда қолданба 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 бағдарламасын қызмет өндірушілерімен пайдалану. Провайдерге Kaspersky Security Center 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 қолданбасының 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 "Лаборатория Касперского" қолданбаларын 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://<Веб-сервер атауы>:<HTTPS порты>/public/<нысан>`

мұндағы

- `<Веб-сервер атауы>` – Kaspersky Security Center Веб-серверінің атауы.
- `<HTTPS порты>` – әкімші белгілеген Веб-сервер HTTPS порты. HTTPS портын Басқару сервері сипаттары терезесінің **Веб-сервер** бөлімінде белгілеуге болады. Әдепкі бойынша 8061-порт орнатылған.
- `<нысан>` – 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.

Желілік агент

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

Желілік агент құрылғыларға келесі атрибуттар жиынтығы бар қызмет ретінде орнатылады:

- "Kaspersky Security Center Желілік агенті" атауымен;
- операциялық жүйені іске қосу кезінде автоматты түрде іске қосу түрімен;
- LocalSystem есептік жазбасы көмегімен.

Желілік агент орнатылған құрылғы *басқарылатын құрылғы* немесе *құрылғы* деп аталады. Желілік агентті келесі әдістермен орнатуға болады:

- Басқару сервері қоймасындағы орнату пакеті (Басқару сервері орнатылуы керек).
- Орнату пакеті "Лаборатория Касперского" веб-серверлерінде орналасқан.

Басқару серверін орнату кезінде Желілік агенттің серверлік нұсқасы Басқару серверімен бірге автоматты түрде орнатылады. Басқару сервері бар құрылғыны басқару үшін Linux үшін Желілік агентті осы құрылғыға орнату ұсынылады. Бұл жағдайда Linux үшін Желілік агент орнатылады және Басқару серверімен бірге орнатылған Желілік агенттің сервер нұсқасына қарамастан тәуелсіз жұмыс істейді.

Желілік агентті іске қосатын процестердің атаулары:

- klnagent64.service (64 разрядты операциялық жүйе үшін);
- klnagent.service (32 разрядты операциялық жүйе үшін).

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:

- Қолданбалардың жұмысының бірыңғай параметрлері – топтық саясаттар көмегімен.
- Барлық қолданбалардың бірыңғай жұмыс режимі – белгілі бір параметрлер жиынтығы бар топтық тапсырмаларды құру арқылы. Топтық тапсырмалар мысалдарына: жалпы орнату пакетін жасау және орнату, қолданба дерекқорлары мен модульдерін жаңарту, құрылғыны талап бойынша тексеру және тұрақты қорғанысты 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, егер кәсіпорын қызметкері бухгалтер лауазымынан әзірлеуші лауазымына ауысса, сіз сол қызметкердің компьютерін "Бухгалтерлер" басқару тобынан "Әзірлеушілер" басқару тобына ауыстыра аласыз. Осылайша, әзірлеуші үшін қажетті қолданба параметрлері құрылғыға автоматты түрде жіберіледі.

Басқарылатын құрылғы

Басқарылатын құрылғы — бұл Желілік агент орнатылған, Linux операциялық жүйесі бар құрылғы. Сіз мұндай құрылғыларды, құрылғыларда орнатылған қолданбаларға 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 20 000-ға дейінгі құрылғыларға қызмет көрсете алады.

Тағайындалмаған құрылғы

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

Желіде жаңа құрылғы анықталған кезде, ол Тағайындалмаған құрылғының 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 "Лаборатория Касперского" қолданбаларын 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 "Лаборатория Касперского" қолданбалары тарапынан қашықтан басқару үшін қолданылатын арнайы құрамдас. Басқару веб-плагині *басқару плагині* деп те аталады. Басқару плагині Kaspersky Security Center Web Console қолданбасы мен "Лаборатория Касперского" белгілі бір бағдарламасы арасындағы интерфейс болып табылады. Басқару плагині көмегімен қолданба үшін тапсырмалар мен саясаттарды конфигурациялауға болады.

Сіз басқару веб-плагиндерін "Лаборатория Касперского" Техникалық қолдау қызметі веб-сайтынан жүктеп ала аласыз.

Басқару плагині келесі мүмкіндіктерді ұсынады:

- Қолданбаның тапсырмалары мен параметрлерін жасауға және өзгертуге арналған интерфейс.
- "Лаборатория Касперского" қолданбалары мен құрылғыларды қашықтан орталықтандырылған түрде конфигурациялау үшін саясаттар мен саясаттар профильдерін жасауға арналған өзгертуге арналған интерфейс.
- Қолданбалар қалыптастырған оқиғаларды беру.
- Қолданбаның 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 "Лаборатория Касперского" қолданбасының параметрлері жиынтығы. "Лаборатория Касперского" қолданбаларының бірнешеуін басқару тобының құрылғыларына орната аласыз. Kaspersky Security Center бағдарламасы басқару тобындағы "Лаборатория Касперского" қолданбасының әрқайсысы үшін бір саясаттан ұсынады. Саясат келесі мәртебелердің біріне ие:

Саясат күйі

Күй	Сипаттамасы
Белсенді	Бұл, құрылғыға қатысты қолданылатын ағымдағы саясат. "Лаборатория Касперского" қолданбасы үшін әрбір басқару тобында тек бір саясат белсенді болуы мүмкін. "Лаборатория Касперского" қолданбасының 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 қолданба үшін түрлі мәндері бар бірнеше саясатты конфигурациялауға болады.
- Бір қолданба 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 қолданба 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 "Лаборатория Касперского" қауіпсіздік қолданбаларының жұмысын басқарады. Тапсырмалардың көмегімен қолданбаларды орнату, іске қосу және тоқтату, файлдарды сканерлеу, қолданбалардың дерекқорлары мен модульдерін жаңарту, қолданбалармен басқа әрекеттер орындалады.

Қолданба 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 деректерін сақтық көшірмелеу;
- дерекқорларға қызмет көрсету;
- эталондық құрылғының операциялық жүйесінің кескінінің орнату пакетін жасау.

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 қолданбасының 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 қолданба 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 қолданба 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 – бұл тапсырма орындалатын құрылғылардың ішкі жиынтығы. 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.

- 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 қолданбаның жергілікті параметрлерінің өзара байланысы

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

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

Клиент құрылғысындағы қолданба 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 қолданба саясатта көрсетілгеннен гөрі жергілікті параметр мәнін пайдаланады. Бұл жағдайда, параметрдің мәні қолданбаның жергілікті параметрлері арқылы өзгеруі мүмкін.

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

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

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

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

Тарату нүктесі

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

- "Лаборатория Касперского" қолданбаларын және басқа жеткізушілердің қолданбалық 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 тағайындау мүмкін емес.

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. Қолданбаның 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.

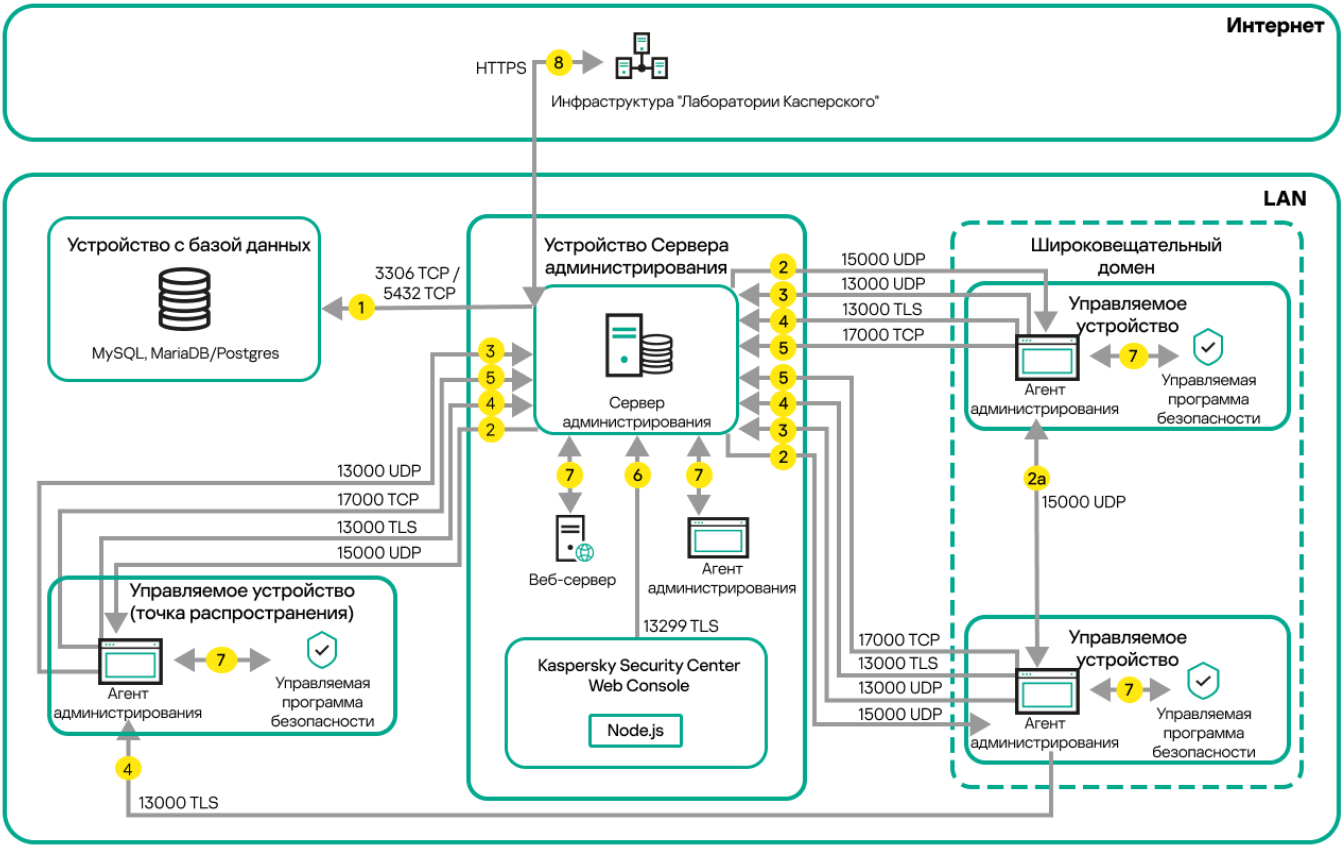
- Сондай-ақ, желідегі қосылым шлюздерін пайдалануға болады. Мысалы, автоматты түрде тағайындалатын тарату нүктелері өзінің әрекет ету ауқымында дәл солай қосылым шлюздеріне айналады. Алайда, ішкі желіде қосылым шлюздері айтарлықтай артықшылықтар бермейді. Олар Басқару сервері қабылдаған желілік қосылымдардың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

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.

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 серверінің осы құрылғылармен байланысу 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 SSL порты арқылы қабылдайды.

   Егер сіз Kaspersky Security Center бағдарламасының алдыңғы нұсқаларының бірін қолдансаңыз, онда сіздің желіңізде Басқару сервері 14000 қорғалмаған порты арқылы Желілік агенттерден қосылымдарды қабылдай алады. Kaspersky Security Center нұсқасы да 14000-порт бойынша Желілік агенттерді қосуды қолдайды, бірақ 13000 қорғалған 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 "Лаборатория Касперского" серверлеріне тікелей интернет арқылы жібереді.

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

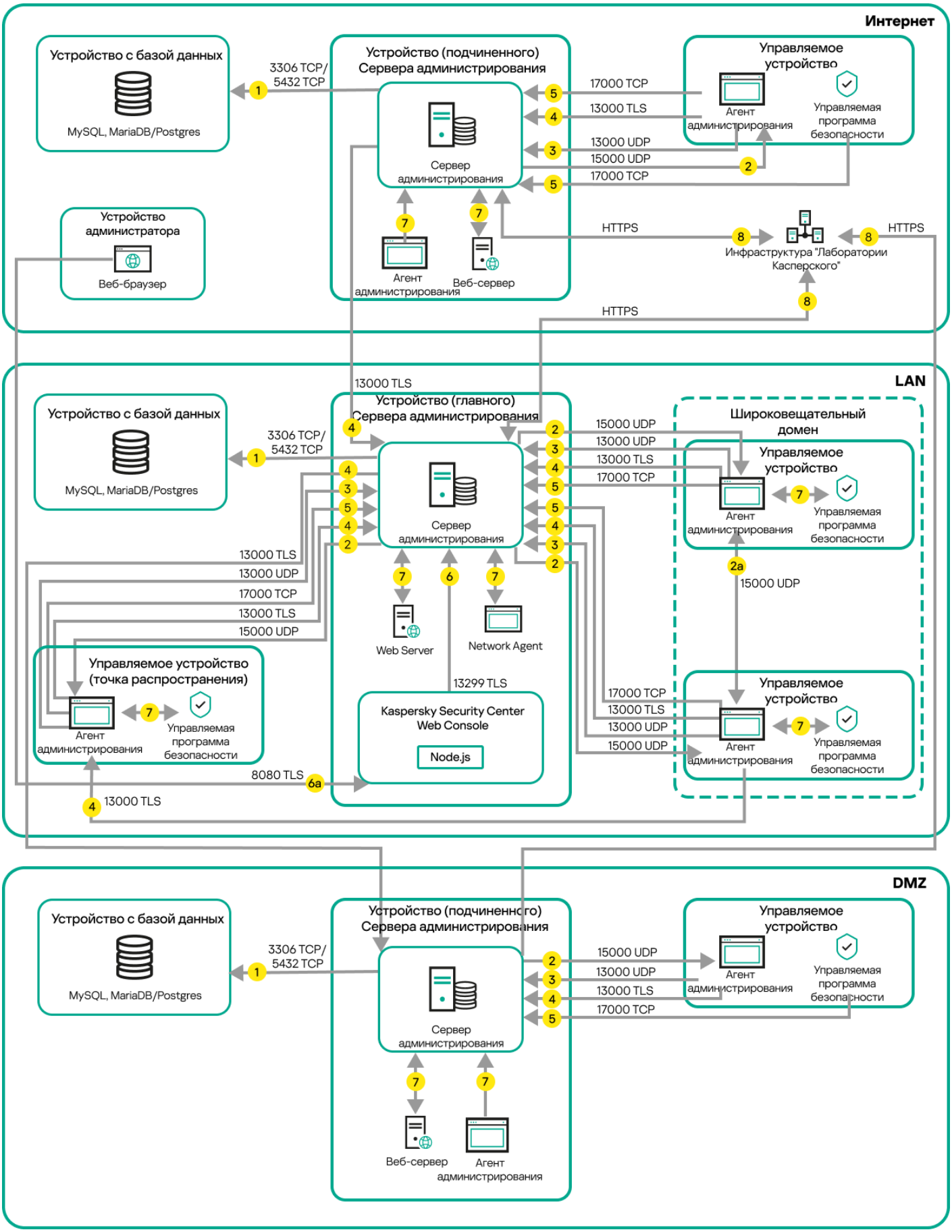
7. Бір құрылғыдағы қолданбалар жергілікті трафикпен алмасады (не Басқару серверінде, не басқарылатын құрылғыда). Сыртқы порттарды ашу қажет емес.

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

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

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 серверінің осы құрылғылармен байланысу 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 SSL порты арқылы қабылдайды.

   Егер сіз Kaspersky Security Center бағдарламасының алдыңғы нұсқаларының бірін қолдансаңыз, онда сіздің желіңізде Басқару сервері 14000 қорғалмаған порты арқылы Желілік агенттерден қосылымдарды қабылдай алады. Kaspersky Security Center Linux нұсқасы да 14000-порт бойынша Желілік агенттерді қосуды қолдайды, бірақ 13000 қорғалған 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 "Лаборатория Касперского" серверлеріне тікелей интернет арқылы жібереді.

6. Kaspersky Security Center Web Console Server 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.

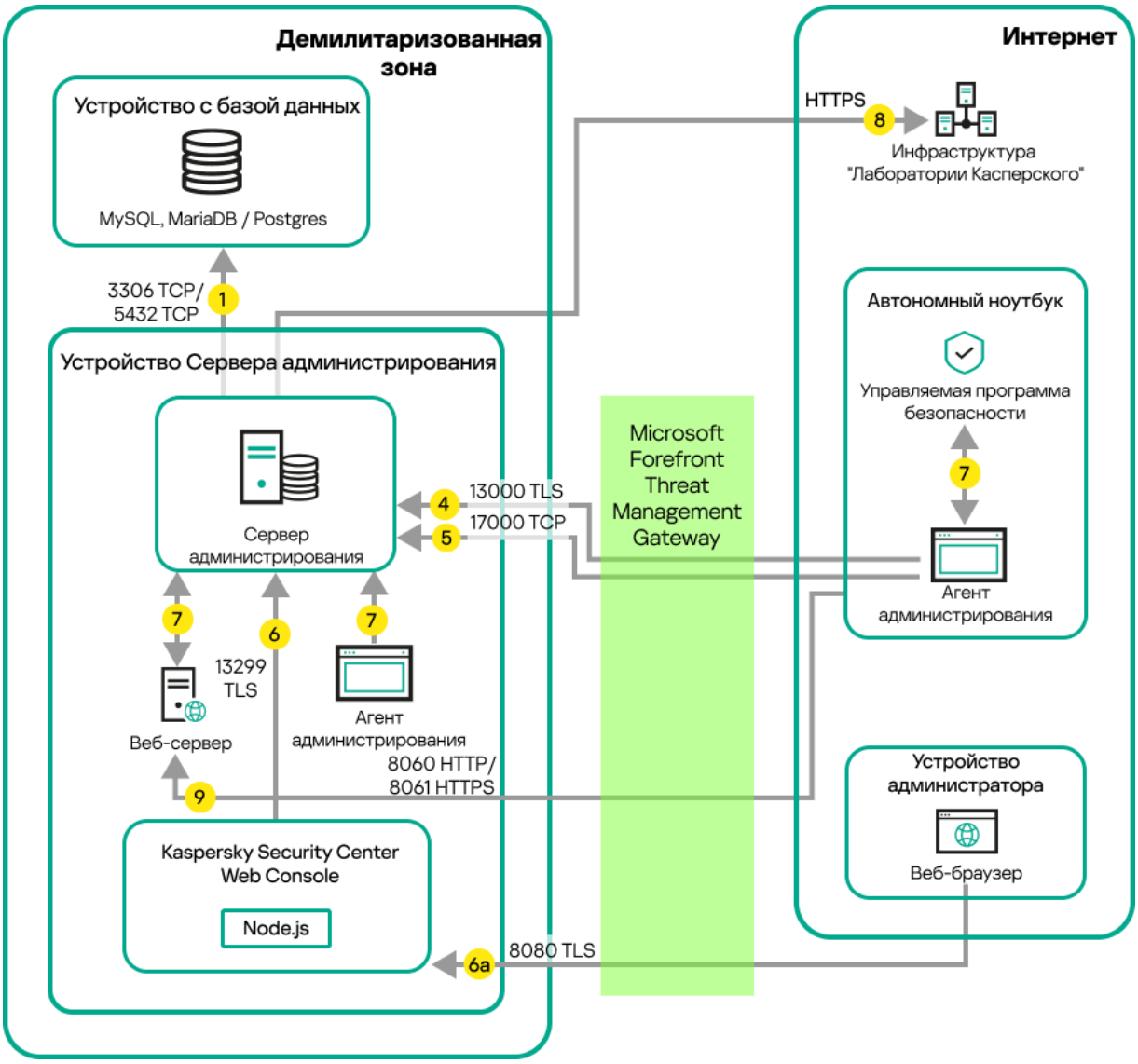
7. Бір құрылғыдағы қолданбалар жергілікті трафикпен алмасады (не Басқару серверінде, не басқарылатын құрылғыда). Сыртқы порттарды ашу қажет емес.

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

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

Жергілікті желі (LAN) ішіндегі басқару сервері, интернеттегі басқарылатын құрылғылар; желілік экранды пайдалану

Төмендегі суретте, Басқару сервері жергілікті желі (LAN) ішінде, ал басқарылатын құрылғылар интернетте болатын деректер трафигі көрсетілген. Бұл суретте сіз таңдаған корпоративтік желілік экран қолданылады. Қосымша ақпарат алу үшін осы қолданбаның құжаттамасын қараңыз.



Жергілікті желідегі басқару сервері; басқарылатын құрылғылар басқару серверіне корпоративтік желілік экран арқылы қосылады

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

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 серверінің осы құрылғылармен байланысу 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 SSL порты арқылы қабылдайды.

   Егер сіз Kaspersky Security Center бағдарламасының алдыңғы нұсқаларының бірін қолдансаңыз, онда сіздің желіңізде Басқару сервері 14000 қорғалмаған порты арқылы Желілік агенттерден қосылымдарды қабылдай алады. Kaspersky Security Center Linux нұсқасы да 14000-порт бойынша Желілік агенттерді қосуды қолдайды, бірақ 13000 қорғалған 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 "Лаборатория Касперского" серверлеріне тікелей интернет арқылы жібереді.

6. Kaspersky Security Center Web Console Server 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 қолданбалар жергілікті трафикпен алмасады (не Басқару серверінде, не басқарылатын құрылғыда). Сыртқы порттарды ашу қажет емес.

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

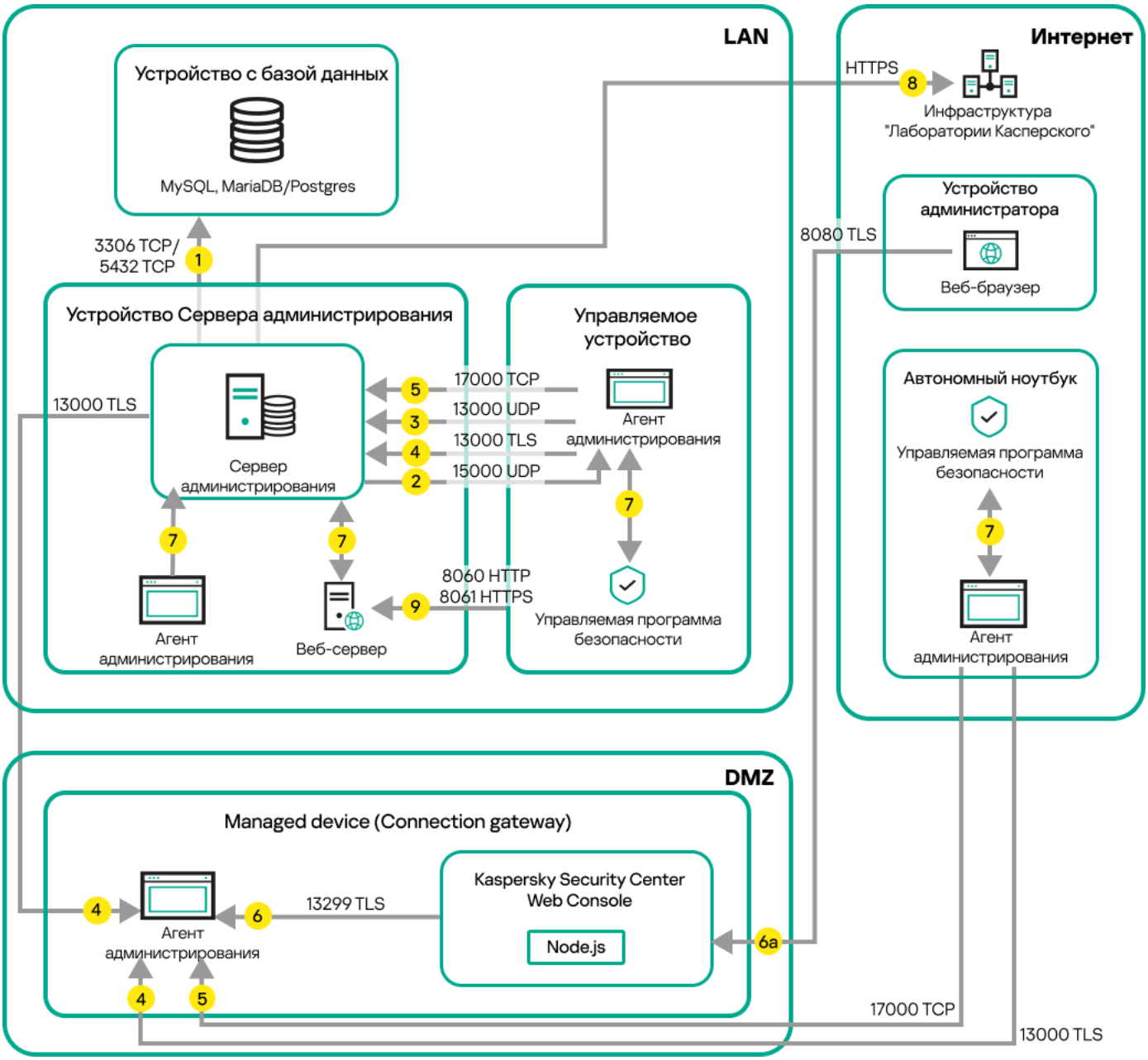
   Басқару серверіңізде интернетке қатысыңыздың болуын қаламасаңыз, осы деректерді қолмен басқаруыңыз қажет.

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

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 Microsoft Forefront Threat Management Gateway (TMG) немесе корпоративтік брандмауэрді қолданғыңыз келмесе, ұсынылады.



Басқару серверіне қосылым шлюзі арқылы қосылған басқарылатын ұялы құрылғылар

Бұл суретте басқарылатын құрылғылар демилитаризацияланған аймақта (DMZ) орналасқан қосылым шлюзі арқылы Басқару серверіне қосылған. TMG немесе корпоративтік брандмауэр қолданылмайды.

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 серверінің осы құрылғылармен байланысу 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 SSL порты арқылы қабылдайды.

   Егер сіз Kaspersky Security Center бағдарламасының алдыңғы нұсқаларының бірін қолдансаңыз, онда сіздің желіңізде Басқару сервері 14000 қорғалмаған порты арқылы Желілік агенттерден қосылымдарды қабылдай алады. Kaspersky Security Center Linux нұсқасы да 14000-порт бойынша Желілік агенттерді қосуды қолдайды, бірақ 13000 қорғалған 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 "Лаборатория Касперского" серверлеріне тікелей интернет арқылы жібереді.

6. Kaspersky Security Center Web Console Server 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 қолданбалар жергілікті трафикпен алмасады (не Басқару серверінде, не басқарылатын құрылғыда). Сыртқы порттарды ашу қажет емес.

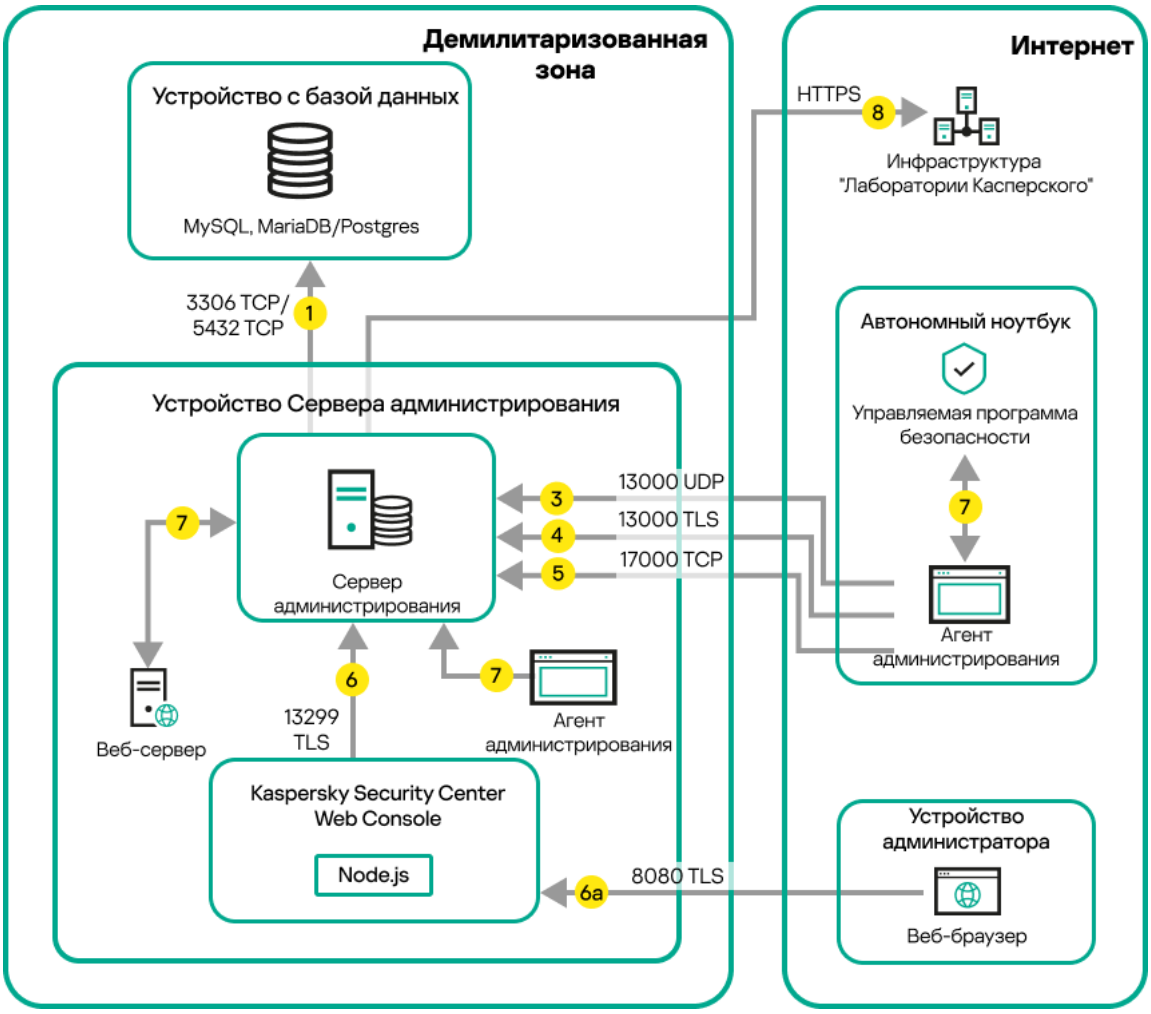
8. Басқару серверінен "Лаборатория Касперского" серверлеріне жіберілетін деректер (мысалы, KSN деректері, лицензиялар туралы ақпарат) және "Лаборатория Касперского" серверлерінен Басқару серверіне жіберілетін деректер (мысалы, қолданбаларды жаңарту және антивирустық дерекқорларды жаңарту) HTTPS протоколы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

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

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

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 серверінің осы құрылғылармен байланысу 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 SSL порты арқылы қабылдайды.

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

4a. Демилитаризацияланған аймақтағы қосылым шлюзі 13000 SSL 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 SSL 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 "Лаборатория Касперского" серверлеріне тікелей интернет арқылы жібереді.

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

6a. 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 қолданбалар жергілікті трафикпен алмасады (не Басқару серверінде, не басқарылатын құрылғыда). Сыртқы порттарды ашу қажет емес.

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

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

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

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.

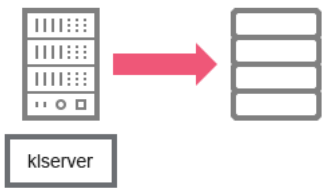
Шартты белгілер

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)
	UDP трафигі (меңзер бағыты трафик бағытын білдіреді)
	ДҚБЖ тасымалдау
	Демилитаризацияланған аймақ шекаралары

Басқару сервері және ДҚБЖ

Басқару сервер деректері дерекқорға түседі.

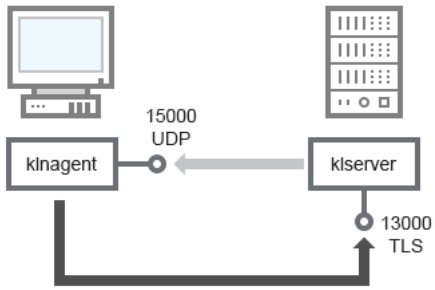


Басқару сервері және ДҚБЖ

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

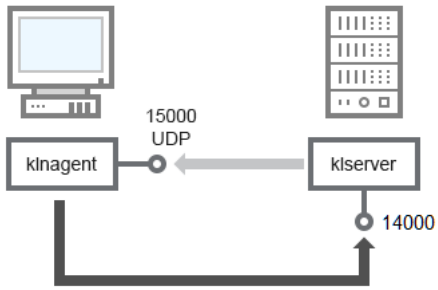
Басқару сервері және клиент құрылғысы: Қауіпсіздік қолданбасын басқару

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



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

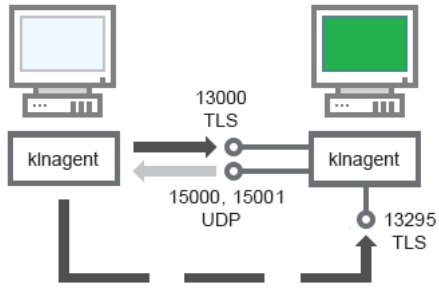
Схемаларға түсініктемелер алу үшін төмендегі кестені қараңыз.

Басқару сервері және клиент құрылғысы: Қауіпсіздік қолданбасын 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.

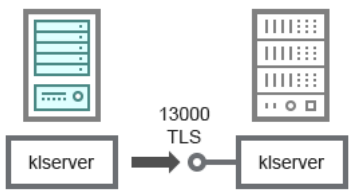
Тарату нүктесі арқылы бағдарламалық жасақтаманы жаңарту (трафик)

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 алу

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.

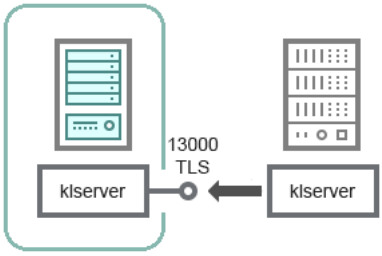


Схемаға түсініктемелер алу үшін төмендегі кестені қараңыз.

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

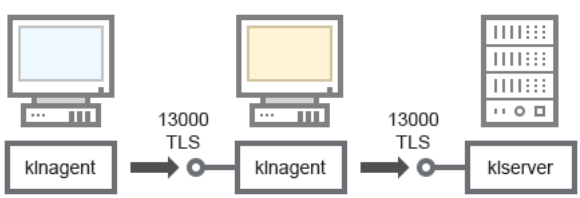
Схемада Басқару серверлерінің иерархиясы көрсетілген, онда демилитаризацияланған аймақтағы қосалқы Сервер басты Серверден қосылымды қабылдайды (схемаға түсініктемелер алу үшін төмендегі кестені қараңыз). Серверлерді иерархияға біріктіру кезінде екі Сервердің 13299-порты қолжетімді болуы керек. Kaspersky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



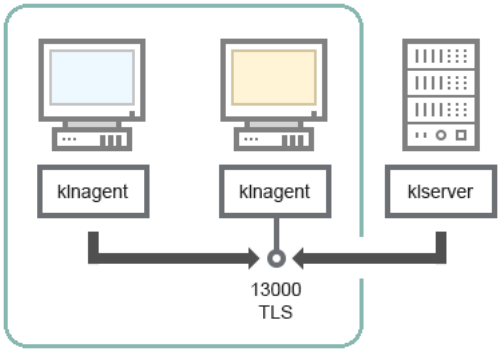
Басқару сервері, желі сегментіндегі қосылымдар шлюзі және клиент құрылғысы

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



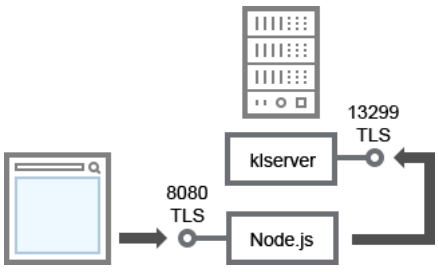
Демилитаризацияланған аймақтағы Басқару сервері, қосылымдар шлюзі және клиент құрылғысы

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	Протокол	Портты тағайындау

		процесс атауы		
Басқару сервері	13299	klserver	TCP (TLS)	Kaspersky Security Center Web Console веб-консолінен OpenAPI арқылы Басқару серверіне қосылымдар алу
Kaspersky Security Center Web Console сервері немесе Басқару сервері	8080	Node.js: серверлік JavaScript	TCP (TLS)	Kaspersky Security Center Web Console серверінен қосылымдар алу

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 "Лаборатория Касперского" қолданбаларын орнатыңыз.

Алдын ала талаптар

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

Егер сіз Kaspersky Security Center-ді қолданып көргіңіз келсе, "Лаборатория Касперского" веб-сайтынан отыз 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 негіздегі 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. Деректер басқа дерекқорға ішінара және қолмен тасымалдана алады.

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 қолданбасы орнатылған құрылғыға орнатыңыз.

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

   Әдепкі бойынша, қолданба 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 "Лаборатория Касперского" және басқа өндірушілердің қолданбаларын 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 қолданбаларын орнату**

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

    Қолданбаны қашықтан орнатуды орындау үшін қорғанысты орналастыру шеберін іске қосыңыз.

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

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

13. **Лицензиялық кілттерді клиент құрылғыларына тарату**

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

14. **"Лаборатория Касперского" қолданбаларының саясаттарын конфигурациялау**

    Әртүрлі құрылғыларда қолданбалардың 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, "Лаборатория Касперского" қолданбалары туралы есептер жасай аласыз, басқарылатын құрылғылардағы қолданбалардан алынған оқиғаларды таңдауды конфигурациялап, көре аласыз және хабарландырулар тізімін көре аласыз.

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

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=<value>
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
```

`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.

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.

Kaspersky Security Center Linux бағдарламасымен жұмыс істеу үшін PostgreSQL немесе Postgres Pro серверін конфигурациялау

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`

PostgreSQL және Postgres Pro үшін ұсынылатын параметрлер:

- `shared_buffers` = ДҚБЖ орнатылған құрылғының жедел жады көлемінің 25%-ы

  Егер жедел жад 1 ГБ-тан аз болса, онда әдепкі бойынша мәнді қалдырыңыз.

- `max_stack_depth` = стектің максималды өлшемі (осы КБ мәнін алу үшін '`ulimit -s`' пәрменін орындаңыз) минус 1 МБ

- `temp_buffers = 24MB`

- `work_mem = 16MB`

- `max_connections = 151`

- `max_parallel_workers_per_gather = 0`

- `maintenance_work_mem = 128 MB`

Өзгерістер күшіне енуі үшін postgresql.conf файлын жаңартқаннан кейін серверді қайта іске қосыңыз немесе қайта жүктеңіз. Қосымша ақпарат алу үшін PostgreSQL құжаттамасын қараңыз.

PostgreSQL және Postgres Pro үшін есептік жазбаларды жасау және конфигурациялау туралы қосымша ақпаратты келесі бөлімінен қараңыз: PostgreSQL және Postgres Pro бағдарламаларымен жұмыс істеу үшін есептік жазбаларды конфигурациялау.

PostgreSQL және Postgres Pro серверінің параметрлері, сондай-ақ осы параметрлерді қалай көрсету керектігі туралы толық ақпаратты ДҚБЖ бойынша тиісті құжаттамадан қараңыз.

Kaspersky Security Center Linux орнату

Бұл бөлімде Kaspersky Security Center Linux орнату тәсілі сипатталған.

Орнату алдында:

- ДҚБЖ орнатыңыз.
- Kaspersky Security Center Linux орнатқыңыз келетін құрылғыда қолдау көрсетілетін Linux дистрибутивтерінің бірі жұмыс істейтініне көз жеткізіңіз.

Құрылғыңызда орнатылған Linux дистрибутивіне сәйкес келетін ksc64_[нұсқа_нөмірі]_amd64.deb немесе ksc64-[нұсқа_нөмірі].x86_64.rpm орнату файлын пайдаланыңыз. Орнату файлын "Лаборатория Касперского" сайтынан жүктеу арқылы аласыз.

Kaspersky Security Center Linux жүйесін орнату үшін төмендегі нұсқауларда көрсетілген пәрмендерді root артықшылықтары бар есептік жазба астында іске қосыңыз.

Kaspersky Security Center Linux орнату үшін:

1. Құрылғыңызда Astra Linux 1.8 немесе одан жоғары нұсқасы болса, осы қадамдағы іс-әрекеттерді орындаңыз. Құрылғыңыз басқа операциялық жүйемен жұмыс істесе, келесі қадамға өтіңіз.

   a. /etc/systemd/system/kladminserver_srv.service.d директориясын және келесі мазмұны бар override.conf деп аталатын файлды жасаңыз:
   ```
   [Service]
   User=
   User=ksc
   CapabilitiesParsec=PARSEC_CAP_PRIV_SOCK
   ExecStart=
   ExecStart=/opt/kaspersky/ksc64/sbin/klserver -d from_wd
   ```

   b. /etc/systemd/system/klwebsrv_srv.service.d директориясын және келесі мазмұны бар override.conf деп аталатын файлды жасаңыз:
   ```
   [Service]
   User=
   User=ksc
   CapabilitiesParsec=PARSEC_CAP_PRIV_SOCK
   ExecStart=
   ExecStart=/opt/kaspersky/ksc64/sbin/klcsweb -d from_wd
   ```

2. kladmins тобын және артықшылықсыз ksc есептік жазбасын жасаңыз. Есептік жазба kladmins тобының мүшесі болуы керек. Ол үшін келесі пәрмендерді ретімен орындаңыз:
   ```
   # adduser ksc
   # groupadd kladmins
   # gpasswd -a ksc kladmins
   # usermod -g kladmins ksc
   ```

3. Kaspersky Security Center Linux орнатуды іске қосыңыз. Linux дистрибутивіңізге байланысты келесі пәрмендердің бірін орындаңыз:

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

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 қабылдауыңыз қажет.

   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 қажет.

6. Сұрау көрсетілген кезде келесі параметрлерді енгізіңіз:

a. Басқару серверінің DNS атын немесе статикалық IP мекенжайын енгізіңіз. Жергілікті орнату үшін – `127.0.0.1`.

b. Басқару сервері SSL портының нөмірін енгізіңіз. Әдепкі бойынша порт нөмірі – 13000.

c. Басқаруды жоспарлап отырған құрылғылардың шамамен санын есептеңіз:

- Егер сізде 1-ден 100-ге дейін желілік құрылғы болса, 1 енгізіңіз.
- Егер сізде 101-ден 1000-ға дейін желілік құрылғы болса, 2 енгізіңіз.
- Егер сізде 1000-нан астам желілік құрылғы болса, 3 енгізіңіз.

d. Қызметтер үшін қауіпсіздік тобының атын енгізіңіз. Әдепкі бойынша `kladmins` тобы пайдаланылады.

e. Басқару сервері қызметін іске қосу үшін есептік жазбаның атауын енгізіңіз. Есептік жазба көрсетілген қауіпсіздік тобының мүшесі болуы керек. Әдепкі бойынша `ksc` есептік жазба пайдаланылады.

f. Басқа қызметтерді іске қосу үшін есептік жазбаның атауын енгізіңіз. Есептік жазба көрсетілген қауіпсіздік тобының мүшесі болуы керек. Әдепкі бойынша `ksc` есептік жазба пайдаланылады.

g. 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.

h. Дерекқор орнатылған құрылғының DNS атауын немесе IP мекенжайын енгізіңіз. Жергілікті орнату үшін – `127.0.0.1`.

i. 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.

j. Дерекқор атауын енгізіңіз.

k. Дерекқорға қатынасу үшін пайдаланылатын дерекқордың root есептік жазбасының атауын енгізіңіз.

l. Дерекқорға қатынасу үшін пайдаланылатын дерекқордың root есептік жазбасының құпия сөзін енгізіңіз.

Қызметтердің қосылуын және автоматты түрде іске қосылуын күтіңіз:

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

m. Басқару серверінің әкімшісінің рөлін орындайтын есептік жазбаны жасаңыз. Пайдаланушының аты мен құпиясөзін енгізіңіз. Пайдаланушыны жасау үшін келесі пәрменді пайдалануға болады:
`/opt/kaspersky/ksc64/sbin/kladduser -n ksc -p <құпиясөз>`

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) (a-z);
  - сандар (0-9);
  - арнайы таңбалар (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;).

Пайдаланушы қосылды және Kaspersky Security Center Linux орнатылды.

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`

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:

- Дерекқорды басқару жүйесін (ДҚБЖ) орнатыңыз.
- Kaspersky Security Center Linux орнатқыңыз келетін құрылғыда қолдау көрсетілетін Linux дистрибутивтерінің бірі жұмыс істейтініне көз жеткізіңіз.

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. Құрылғыңызда Astra Linux 1.8 немесе одан жоғары нұсқасы болса, осы қадамдағы іс-әрекеттерді орындаңыз. Құрылғыңыз басқа операциялық жүйемен жұмыс істесе, келесі қадамға өтіңіз.

a. /etc/systemd/system/kladminserver_srv.service.d директориясын және келесі мазмұны бар override.conf деп аталатын файлды жасаңыз:

```
[Service]
User=
User=ksc
CapabilitiesParsec=PARSEC_CAP_PRIV_SOCK
ExecStart=
ExecStart=/opt/kaspersky/ksc64/sbin/klserver -d from_wd
```

b. /etc/systemd/system/klwebsrv_srv.service.d директориясын және келесі мазмұны бар override.conf деп аталатын файлды жасаңыз:

```
[Service]
User=
User=ksc
CapabilitiesParsec=PARSEC_CAP_PRIV_SOCK
ExecStart=
ExecStart=/opt/kaspersky/ksc64/sbin/klcsweb -d from_wd
```

3. "kladmins" тобын және "kladmins" тобының мүшесі болуы тиіс артықшылықсыз "ksc" есептік жазбасын 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
```

4. Жауап файлын (TXT пішімінде) жасаңыз және жауап файлына `VARIABLE_NAME=variable_value` пішіміндегі айнымалылар тізімін қосыңыз. Әрбір айнымалы бөлек жолға қосылады. Жауап файлы төмендегі кестеде көрсетілген айнымалыларды қамтуы керек.

5. Түбірлік ортадағы `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:

- `# apt install /<path>/ksc64_[ нұсқа_нөмірі ]_amd64.deb`
- `# yum install /<path>/ksc64-[ нұсқа_нөмірі ].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 ksc -p < құпиясөз >`, мұнда құпиясөз кемінде 8 таңбадан тұруы керек.

Интерактивті емес режимде Kaspersky Security Center Linux орнату параметрлері ретінде пайдаланылатын жауап файлының айнымалылары

Айнымалының атауы	Міндетті	Сипаттамасы	Ы
`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	Құры немe

		мекенжайы.	
KLSRV_UNATT_PORT_SRV	Жоқ	Басқару серверінің порт нөмірі. Параметр міндетті емес. Әдепкі бойынша, 14000 мәні көрсетілген.	Порт
KLSRV_UNATT_PORT_SRV_SSL	Жоқ	Басқару сервері SSL портының нөмірі. Параметр міндетті емес. Әдепкі бойынша, 13000 мәні көрсетілген.	Порт
KLSRV_UNATT_PORT_KLOAPI	Жоқ	Басқару сервері KLOAPI портының нөмірі. Параметр міндетті емес. Әдепкі бойынша, 13299 мәні көрсетілген.	Порт
KLSRV_UNATT_PORT_GUI	Жоқ	Басқару сервері GUI портының нөмірі. Параметр міндетті емес. Әдепкі бойынша, 13291 мәні көрсетілген.	Порт
KLSRV_UNATT_NETRANGETYPE	Жоқ	Басқаруды жоспарлап отырған құрылғылардың шамамен саны. Параметр міндетті емес. Әдепкі бойынша, 1 мәні көрсетілген.	1 1-д желіл 2 101 желіл 3 100 желіл
KLSRV_UNATT_DBMS_TYPE	Иә	Дерекқорды басқару жүйесінің түрі: MySQL (MariaDB) немесе Postgres.	mysq неме post
KLSRV_UNATT_DBMS_INSTANCE	Иә	Дерекқор серверінің IP мекенжайы.	IP ме
KLSRV_UNATT_DBMS_PORT	Иә	Дерекқор серверінің порты. MySQL (MariaDB) үшін әдепкі мән – 3306; Postgres үшін – 5432.	3306 неме 5432
KLSRV_UNATT_DB_NAME	Иә	Дерекқор атауы.	kav
KLSRV_UNATT_DBMS_LOGIN	Иә	Дерекқорға рұқсаты бар пайдаланушының атауы.	
KLSRV_UNATT_DBMS_PASSWORD	Иә	Дерекқорға рұқсаты бар пайдаланушының құпиясөзі.	
KLSRV_UNATT_KLADMINSGROUP	Иә	Қызметтер үшін қауіпсіздік тобының атауы.	klad
KLSRV_UNATT_KLSRVUSER	Иә	Басқару сервері қызметін іске қосу үшін есептік жазбаның атауы. Учетная запись должна быть членом группы безопасности, указанной в переменной KLSRV_UNATT_KLADMINSGROUP.	ksc
KLSRV_UNATT_KLSVCUSER	Иә	Басқа қызметтерді іске қосу үшін есептік жазбаның атауы. Учетная запись должна быть	ksc

		членом группы безопасности, указанной в переменной KLSRV_UNATT_KLADMINSGROUP.	
Басқару сервері Kaspersky Security Center Linux ақауларға төзімді кластері ретінде орналастырылатын бо келесі қосымша айнымалыларды қамтуы керек:			
KLFOC_UNATT_NODE	Иә	Түйін нөмірі (1 немесе 2).	1 неме 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.	Virt Неме Exte
Егер KLFOC_UNATT_CONN_MODE айнымалысы VirtualAdapter мәніне орнатылса, жауап файлы келесі қос айнымалыларды қамтуы керек:			
KLFOC_UNATT_CONN_MODE_VA_NAME	Осы айнымалылардың бірі қажет	Виртуалды желілік адаптердің атауы.	
KLFOC_UNATT_CONN_MODE_VA_IPV4		Виртуалды желілік адаптердің IP мекенжайы.	IP ме
KLFOC_UNATT_CONN_MODE_VA_IPV6		Виртуалды желілік адаптердің IPv6 мекенжайы.	IPv6

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 Security Center Linux орнатқыңыз келетін құрылғыда қолдау көрсетілетін Linux дистрибутивтерінің бірі жұмыс істейтініне көз жеткізіңіз.
- kaspersky_astra_pub_key.gpg қолданбасының кілтін жүктеп алыңыз.

ksc64_[нұсқа_нөмірі]_amd64.deb орнату файлын пайдаланыңыз. Орнату файлын "Лаборатория Касперского" сайтынан жүктеу арқылы аласыз.

Осы нұсқаулықтары пәрмендерді root есептік жазбасы астында іске қосыңыз.

Kaspersky Security Center Linux жүйесін Astra Linux Special Edition (Жаңарту 1.7.2) және Astra Linux Special Edition (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. Қолданба кілті үшін директория жасаңыз:

   ```
   mkdir -p /etc/digsig/keys/legacy/kaspersky/
   ```

4. Алдыңғы қадамда жасалған директорияға қолданба кілтін салыңыз:

   ```
   cp kaspersky_astra_pub_key.gpg /etc/digsig/keys/legacy/kaspersky/
   ```

5. Дискілердің жедел жадын жаңартыңыз:

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

   Жүйені қайта жүктеңіз.

6. Құрылғыңызда Astra Linux 1.8 немесе одан жоғары нұсқасы болса, осы қадамдағы іс-әрекеттерді орындаңыз. Құрылғыңыз басқа операциялық жүйемен жұмыс істесе, келесі қадамға өтіңіз.

   a. /etc/systemd/system/kladminserver_srv.service.d директориясын және келесі мазмұны бар override.conf деп аталатын файлды жасаңыз:

   ```
   [Service]
   User=
   User=ksc
   CapabilitiesParsec=PARSEC_CAP_PRIV_SOCK
   ExecStart=
   ExecStart=/opt/kaspersky/ksc64/sbin/klserver -d from_wd
   ```

   b. /etc/systemd/system/klwebsrv_srv.service.d директориясын және келесі мазмұны бар override.conf деп аталатын файлды жасаңыз:

   ```
   [Service]
   User=
   User=ksc
   CapabilitiesParsec=PARSEC_CAP_PRIV_SOCK
   ExecStart=
   ExecStart=/opt/kaspersky/ksc64/sbin/klcsweb -d from_wd
   ```

7. kladmins тобын және артықшылықсыз ksc есептік жазбасын жасаңыз. Есептік жазба kladmins тобының мүшесі болуы керек. Ол үшін келесі пәрмендерді ретімен орындаңыз:

   ```
   # adduser ksc
   # groupadd kladmins
   # gpasswd -a ksc kladmins
   # usermod -g kladmins ksc
   ```

8. Kaspersky Security Center Linux орнатуды іске қосыңыз:

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

9. Kaspersky Security Center Linux конфигурациясын іске қосыңыз:

   ```
   # /opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl
   ```

10. 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 қабылдауыңыз қажет.

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 қажет.

11. 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:

- Егер сізде 1-ден 100-ге дейін желілік құрылғы болса, 1 енгізіңіз.
- Егер сізде 101-ден 1000-ға дейін желілік құрылғы болса, 2 енгізіңіз.
- Егер сізде 1000-нан астам желілік құрылғы болса, 3 енгізіңіз.

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. Дерекқор орнатылған құрылғының IP мекенжайын енгізіңіз.

i. Дерекқор портының нөмірін енгізіңіз. Бұл порт Басқару серверімен байланысу үшін пайдаланылады. Әдепкі бойынша порт нөмірі – 3306.

j. Дерекқор атауын енгізіңіз.

k. Дерекқорға қатынасу үшін пайдаланылатын дерекқордың root есептік жазбасының атауын енгізіңіз.

l. Дерекқорға қатынасу үшін пайдаланылатын дерекқордың root есептік жазбасының құпия сөзін енгізіңіз.

Қызметтердің қосылуын және автоматты түрде іске қосылуын күтіңіз:

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

m. 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) (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`

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-[жинақ_нөмірі].x86_64.deb.
- RPM негізіндегі операциялық жүйелер үшін: ksc-web-console-[жинақ_нөмірі].x86_64.rpm.
- Альт 8 СП үшін: ksc-web-console-[жинақ_нөмірі]-alt8p.x86_64.rpm.

Орнату файлын "Лаборатория Касперского" 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 "Лаборатория Касперского" сайтынан жүктеп алуға болады. Егер сіз Лицензиялық келісімнің шарттарымен келіспесеңіз, қолданбаны орнатпаңыз.

3. Kaspersky Security Center Web Console веб-консолін Басқару сервері қосу параметрлері бар жауаптар файлын жасаңыз. Файл атауы ksc-web-console-setup.json. Файл келесі директорияда орналасқан: /etc/ksc-web-console-setup.json.

   Минималды параметрлер жиынтығы, мекенжайы және әдепкі бойынша порты бар жауаптар файлының мысалы:

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

   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 қолданбасын бірдей .rpm 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.

   - .deb файлынан Kaspersky Security Center Web Console алдыңғы нұсқасын орнату немесе жаңарту үшін келесі пәрменді іске қосыңыз:
     ```
     $ sudo dpkg -i ksc-web-console-[нұсқа_нөмірі].x86_64.deb
     ```
   - Kaspersky Security Center Web Console-ін .RPM файлынан орнату үшін келесі пәрмендердің біреуін орындаңыз:
     ```
     $ sudo rpm -ivh --nodeps ksc-web-console-[жинақ_нөмірі].x86_64.rpm
     ```
     Немесе
     ```
     $ sudo alien -i ksc-web-console-[жинақ_нөмірі].x86_64.rpm
     ```
   - Kaspersky Security Center Web Console алдыңғы нұсқасын жаңарту үшін келесі пәрмендердің бірін орындаңыз:
     - RPM операциялық жүйелері бар құрылғылар үшін:
       ```
       $ sudo rpm -Uvh --nodeps --force ksc-web-console-[жинақ_нөмірі].x86_64.rpm
       ```
     - Debian операциялық жүйелері бар құрылғылар үшін:
       ```
       $ sudo dpkg -i ksc-web-console-[жинақ_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.

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.

Минималды параметрлер жиынтығы, мекенжайы және әдепкі бойынша порты бар жауаптар файлының мысалы:

```
{
 "address": "127.0.0.1",
 "port": 8080,
 "defaultLangId": 1049,
 "enableLog": false,
 "trusted": "127.0.0.1|13299|/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer|KSC Server",
  "acceptEula": true,
 "certPath": "/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer",
 "webConsoleAccount": "Топ1:Пайдаланушы1",
 "managementServiceAccount": "Топ1:Пайдаланушы2",
 "serviceWebConsoleAccount": "Топ1:Пайдаланушы3",
 "pluginAccount": "Топ1:Пайдаланушы4",
 "messageQueueAccount": "Топ1:Пайдаланушы5"
}
```

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 мән
address	Kaspersky Security Center Web Console Server серверінің мекенжайы (міндетті параметр).	Жол мәні.
port	Kaspersky Security Center Web Console Server сервері Басқару серверіне қосылу үшін пайдаланатын порт нөмірі (міндетті параметр).	Сандық мән.

`defaultLangId`	Пайдаланушы интерфейсі тілі (әдепкі бойынша `1033`).	Тілдің сандық коды: • Неміс тілі: `1031` • Ағылшын тілі: `1033` • Испан тілі: `3082` • Испан тілі (Мексика): `2058` • Француз тілі: `1036` • Жапон тілі: `1041` • Қазақ тілі: `1087` • Поляк тілі: `1045` • Португал тілі (Бразилия): `1046` • Орыс тілі: `1049` • Түрік тілі: `1055` • Жеңілдетілген қытай тілі: `4` • Дәстүрлі қытай тілі: `31748` Егер мән көрсетілмесе, ағылшын тілі қол
`enableLog`	Kaspersky Security Center Web Console белсенділік журналын қосу немесе өшіру.	Логикалық мән: • `true` – белсенділік журналын қосу (ə • `false` – белсенділік журналын өшіру

`trusted`	Kaspersky Security Center Web Console бағдарламасына қосылуға рұқсат етілген сенімді Басқару серверлері тізімі. Әрбір Басқару сервері үшін келесі параметрлер белгіленуі керек:
	• Басқару сервері мекенжайы;
	• Басқару серверіне қосылу үшін Kaspersky Security Center Web Console қолданбасы пайдаланатын OpenAPI порты (әдепкі бойынша 13299);
	• Басқару серверінің сертификатына апаратын жол;
		Келесі пішімдегі жол мәні:
		`" сервер мекенжайы | порт | сертифи`
		Мысалы:
		`"X.X.X.X|13299|/cert/server-1.ce`
		`1 ||Y.Y.Y.Y|13299|/cert/server-2.`

	• кіру терезесінде көрсетілетін Басқару серверінің атауы. Параметрлер тік сызық таңбаларымен бөлінген. Егер бірнеше Басқару сервері көрсетілсе, оларды тік сызықтың екі таңбасымен бөліңіз.	
`acceptEula`	Лицензиялық келісімнің шарттарын қабылдайсыз ба. Лицензиялық келісімнің шарттары бар файл орнату файлымен бірге жүктеледі.	Логикалық мән: • `true` – Мен Лицензиялық келісімді то және оның шарттарын қабылдайтын • `false` – Мен Лицензиялық келісімнің қабылдамаймын (әдепкі бойынша тан Егер мәні көрсетілмесе, Kaspersky Secu орнату қолданбасы Лицензиялық келісім Лицензиялық келісімнің шарттарын қабы сұрайды.
`certDomain`	Егер сіз сертификат жасағыңыз келсе, сертификат жасалуы керек доменнің атауын көрсету үшін осы параметрді пайдаланыңыз.	Жол мәні.
`certPath`	Егер сіз бар сертификатты пайдаланғыңыз келсе, сертификат файлының жолын көрсету үшін осы параметрді пайдаланыңыз.	Жол мәні. Қолданыстағы сертификатты қолдану үш `"/var/opt/kaspersky/klnagent_srv/` жолын көрсетіңіз. Пайдаланушы сертиф сақталатын каталогқа жолды көрсетіңіз.
`keyPath`	Егер сіз бар сертификатты пайдаланғыңыз келсе, кілт файлының жолын көрсету үшін осы параметрді пайдаланыңыз.	Жол мәні.
`webConsoleAccount`	KSCWebConsole қызметі жұмыс істейтін есептік жазба.	Келесі пішімдегі жол мәні: `" group name` Мысалы: `" Group1 : User1 "`. Егер мән көрсетілмесе, Kaspersky Secu орнатушысы әдепкі бойынша `user_man` жазбасын жасайды.
`managementServiceAccount`	KSCWebConsoleManagement қызметі жұмыс істейтін есептік жазба.	Келесі пішімдегі жол мәні: `" group name` Мысалы: `" Group1 : User1 "`. Егер мән көрсетілмесе, Kaspersky Secu орнатушысы әдепкі бойынша `user_nod` жазбасын жасайды.
`serviceWebConsoleAccount`	KSCSvcWebConsole қызметі жұмыс істейтін есептік жазба.	Келесі пішімдегі жол мәні: `" group name` Мысалы: `" Group1 : User1 "`. Егер мән көрсетілмесе, Kaspersky Secu орнатушысы әдепкі бойынша `user_svc` жазбасын жасайды.
	KSCWebConsolePlugin қызметі	

`pluginAccount`	жұмыс істейтін есептік жазба.	Келесі пішімдегі жол мәні: `"group name` Мысалы: `"Group1:User1"`. Егер мән көрсетілмесе, Kaspersky Secu орнатушысы әдепкі бойынша `user_web` жазбасын жасайды.
`messageQueueAccount`	KSCWebConsoleMessageQueue қызметі жұмыс істейтін есептік жазба.	Келесі пішімдегі жол мәні: `"group name` Мысалы: `"Group1:User1"`. Егер мән көрсетілмесе, Kaspersky Secu орнатушысы әдепкі бойынша `user_mes` жазбасын жасайды.

`webConsoleAccount`, `managementServiceAccount`, `serviceWebConsoleAccount`, `pluginAccount` немесе `messageQueueAccount` параметрлерін көрсетіп жатсаңыз, онда конфигурацияланатын пайдаланушы есептік жазбалары бір қауіпсіздік тобына жататынына көз жеткізіп алыңыз. Егер бұл параметрлер көрсетілмесе, Kaspersky Security Center Web Console орнатушысы әдепкі бойынша қауіпсіздік тобын жасайды, содан кейін осы топта әдепкі бойынша атаулары бар пайдаланушы есептік жазбаларын 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 "Лаборатория Касперского" сайтынан жүктеп алуға болады. Егер сіз Лицензиялық келісімнің шарттарымен келіспесеңіз, қолданбаны орнатпаңыз.

3. Kaspersky Security Center Web Console веб-консолін Басқару сервері қосу параметрлері бар жауаптар файлын жасаңыз. Файл атауы ksc-web-console-setup.json. Файл келесі директорияда орналасқан: /etc/ksc-web-console-setup.json.

   Минималды параметрлер жиынтығы, мекенжайы және әдепкі бойынша порты бар жауаптар файлының мысалы:

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

4. `/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. Қолданба кілті үшін директория жасаңыз:

   ```
   mkdir -p /etc/digsig/keys/legacy/kaspersky/
   ```

7. Қолданба кілтін алдыңғы қадамда жасалған `/opt/kaspersky/ksc64/share/kaspersky_astra_pub_key.gpg` каталогына 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 "Лаборатория Касперского" сайтынан жүктеу арқылы аласыз.

   - Kaspersky Security Center Web Console алдыңғы нұсқасын орнату немесе жаңарту үшін келесі пәрменді іске қосыңыз:

     ```
     $ sudo dpkg -i ksc-web-console-[нұсқа_нөмірі].x86_64.deb
     ```

   - Kaspersky Security Center Web Console алдыңғы нұсқасын жаңарту үшін келесі пәрмендердің бірін орындаңыз:

     ```
     $ sudo dpkg -i ksc-web-console-[жинақ_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.

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.

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 ақауларға төзімді Kaspersky Security Center Linux кластеріне Kaspersky Security Center Web Console-іне қосылуға мүмкіндік беретін `сенімді` орнату параметрін көрсетіңіз. Бұл параметрдің жол мәні келесі пішімге ие:
   ```
   "trusted": "server address|port|certificate path|server name"
   ```
   `trusted` орнату параметрінің құрамдастарын көрсетіңіз:

   - **Басқару сервері мекенжайы**. Кластер түйіндерін дайындау кезінде қосымша желілік адаптерді жасасаңыз, адаптердің IP мекенжайын ақауларға төзімді Kaspersky Security Center Linux кластерінің мекенжайы ретінде пайдаланыңыз. Не болмаса, өзіңіз пайдаланып жатқан үшінші тарап теңгергішінің IP мекенжайын көрсетіңіз.

   - **Басқару серверінің порты**. Kaspersky Security Center Web Console веб-консолі Басқару серверіне қосылу үшін пайдаланатын OpenAPI порты (әдепкі бойынша 13299).

   - **Басқару сервері сертификаты**. Басқару серверінің сертификаты ақауларға төзімді Kaspersky Security Center Linux кластерінің ортақ деректер қоймасында орналасқан. Сертификат файлына әдепкі бойынша жол: <shared data folder>\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.

   - **Басқару серверінің атауы**. Kaspersky Security Center Web Console-іне кіру терезесінде көрсетілетін ақауларға төзімді Kaspersky Security Center Linux кластерінің атауы.

3. Kaspersky Security Center Web Console стандартты орнатуды жалғастырыңыз.

Сәтті аяқталғаннан кейін, жұмыс үстелінде таңбаша пайда болады және сіз Kaspersky Security Center Web Console бағдарламасына кіре аласыз.

Кластер түйіндері мен файл сервері туралы ақпаратты көру үшін **Табу және орналастыру** → **Тағайындалмаған құрылғылар** бөліміне өтуге болады.

Ақауларға төзімді Kaspersky Security Center Linux кластерін орналастыру

Бұл бөлімде ақауларға төзімді Kaspersky Security Center Linux кластері туралы жалпы ақпарат, сондай-ақ ақауларға төзімді Kaspersky Security Center Linux кластерін дайындау және желіде орналастыру нұсқаулары берілген.

Сценарий: Kaspersky Security Center Linux ақауларға төзімді 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.

Алдын ала талаптар

Сізде ақауларға төзімді кластер талаптарына сәйкес келетін жабдық бар.

"Лаборатория Касперского" қолданбаларын орналастыру келесі кезеңдерден тұрады:

1. **Kaspersky Security Center Linux қызметтері үшін есептік жазбаларды жасау**

   Белсенді түйінде, пассивті түйінде және файл серверінде келесі қадамдарды орындаңыз:

   1. "kladmins" деп аталатын домен тобын 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.

2. **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.

3. **Белсенді және пассивті түйіндерді дайындау**

   Белсенді және пассивті түйіндер ретінде жұмыс істеу үшін бірдей аппараттық және бағдарламалық жасақтамасы бар екі компьютерді дайындаңыз.

   Нұсқаулар: ақауларға төзімді Kaspersky Security Center Linux кластері үшін түйіндерді дайындау.

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

   Сіздің екі нұсқаңыз бар:

   - MariaDB Galera Cluster пайдаланғыңыз келсе, сізге арнайы ДҚБЖ компьютері қажет емес. Әрбір түйінге MariaDB Galera кластерін орнатыңыз.
   - Кез келген басқа қолдау көрсетілетін ДҚБЖ пайдаланғыңыз келсе, таңдалған ДҚБЖ-ны берілген компьютерге орнатыңыз.

5. **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 түйінге, содан кейін пассивті түйінге орнату керек.

   Сондай-ақ, Kaspersky Security Center Web Console веб-консолін кластер түйіні болып табылмайтын бөлек құрылғыға орната аласыз.

6. **Істен шығуға төзімді кластерді тестілеу**

   Істен шығуға төзімді кластерді дұрыс конфигурациялағаныңызға және оның дұрыс жұмыс істеп тұрғанына көз жеткізіңіз. Мысалы, сіз Kaspersky Security Center Linux қызметтерінің бірін белсенді түйінде тоқтата аласыз: kladminserver, klnagent, ksnproxy, klactprx немесе klwebsrv. Қызмет тоқтағаннан кейін, қорғауды басқару автоматты түрде пассивті түйінге ауысуы керек.

Нәтижелер

Ақауларға төзімді Kaspersky Security Center Linux кластері орналастырылды. Белсенді және пассивті түйіндер арасында ауысуға әкелетін оқиғалармен танысып шығыңыз.

Ақауларға төзімді Kaspersky Security Center Linux кластері туралы ақпарат

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.

Ақауларға төзімді Kaspersky Security Center Linux кластерінде барлық Kaspersky Security Center Linux қызметтері автоматты түрде басқарылады. Қызметтерді қолмен қайта іске қосуға тырыспаңыз.

Аппараттық және бағдарламалық талаптар

Ақауларға төзімді Kaspersky Security Center Linux кластерін орналастыру үшін сізде келесі жабдық болуы керек:

- Бірдей аппараттық және бағдарламалық жасақтамасы бар екі компьютер. Бұл компьютерлер белсенді және пассивті түйіндер ретінде әрекет етеді.
- EXT4 файлдық жүйесі бар Linux басқаратын файлдық сервері. Сіз файл сервері ретінде әрекет ететін бөлектенген компьютерді ұсынуыңыз қажет.

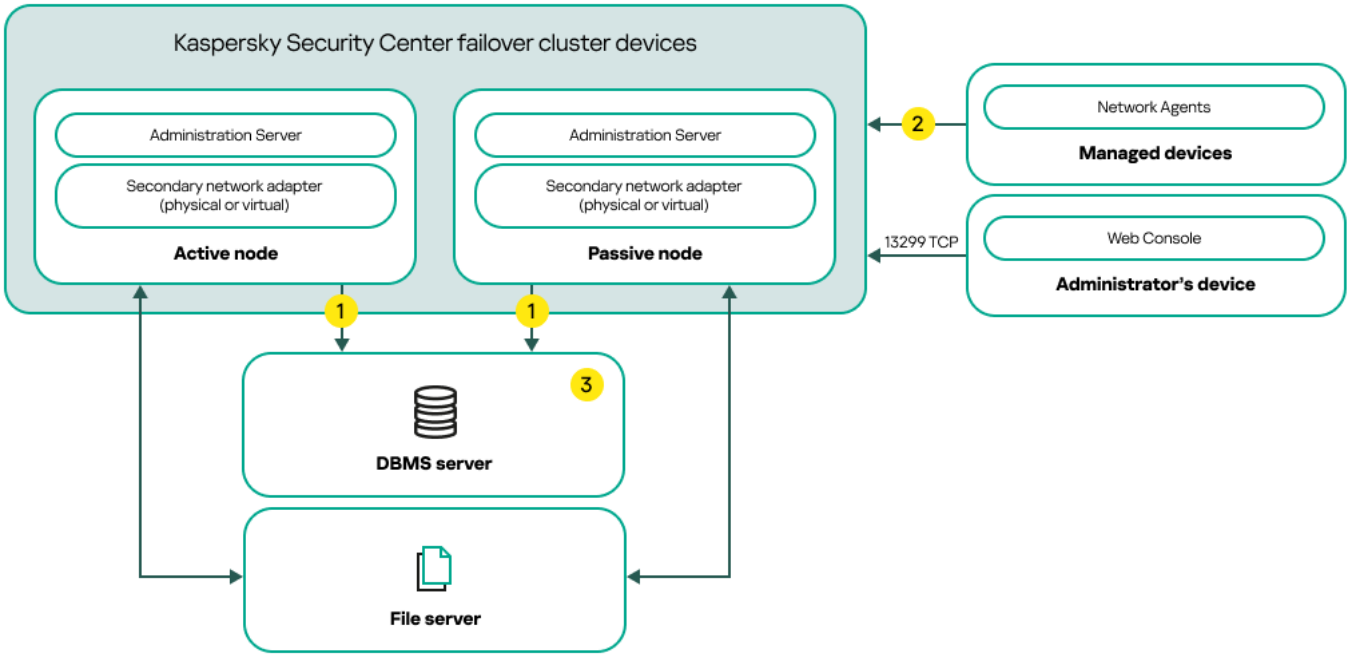
  Файл сервері, белсенді және пассивті түйіндер арасында желінің жоғары өткізу қабілеттілігін қамтамасыз еткеніңізге көз жеткізіңіз.

- Дерекқорды басқару жүйесі (ДҚБЖ) бар компьютер. MariaDB Galera Cluster-ін ДҚБЖ ретінде пайдалансаңыз, бұл мақсат үшін арнайы компьютер қажет емес.

Орналастыру схемалары

Kaspersky Security Center Linux ақауларға төзімді кластерін орналастыру үшін келесі схемалардың бірін таңдауға болады:

- Қосымша желілік адаптерді пайдаланатын схема.
- Үшінші тараптың жүктемені теңестіруін пайдаланатын схема.



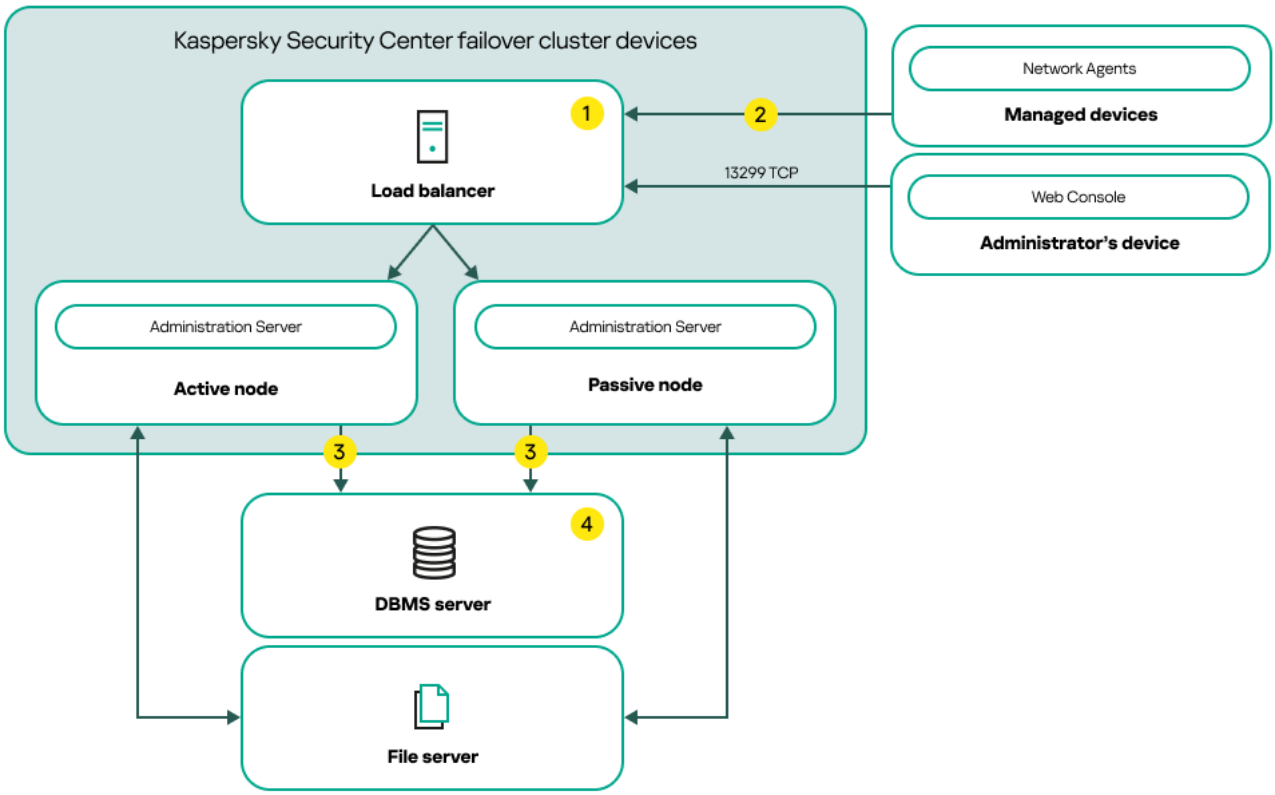
Қосымша желілік адаптерді пайдаланатын схема

Схеманың шартты белгілері:

1 Басқару сервері деректерді дерекқорға жібереді. MySQL сервері үшін 3306 порты немесе Microsoft SQL Server үшін 1433 порты сияқты дерекқор орналасқан құрылғыда қажетті порттарды ашыңыз. Толығырақ ақпарат ДҚБЖ құжаттамасында көрсетілген.

2 Басқарылатын құрылғыларда келесі порттарды ашыңыз: TCP 13000, UDP 13000 және TCP 17000.

3 Дерекқорды басқару жүйесі (ДҚБЖ) бар компьютер. MariaDB Galera Cluster-ін ДҚБЖ ретінде пайдалансаңыз, бұл мақсат үшін арнайы компьютер қажет емес. Әрбір түйінге MariaDB Galera кластерін орнатыңыз.



Үшінші тараптың жүктемені теңестіруін пайдаланатын схема

Схеманың шартты белгілері:

1 Жүктемені теңдестіру құрылғысының серверінде барлық Басқару сервері порттарын ашыңыз: TCP 13000, UDP 13000, TCP 13291, TCP 13299 және TCP 17000.

2 Басқарылатын құрылғыларда келесі порттарды ашыңыз: TCP 13000, UDP 13000 және TCP 17000.

3 Басқару сервері деректерді дерекқорға жібереді. MySQL сервері үшін 3306 порты немесе Microsoft SQL Server үшін 1433 порты сияқты дерекқор орналасқан құрылғыда қажетті порттарды ашыңыз. Толығырақ ақпарат ДҚБЖ құжаттамасында көрсетілген.

4 Дерекқорды басқару жүйесі (ДҚБЖ) бар компьютер. MariaDB Galera Cluster-ін ДҚБЖ ретінде пайдалансаңыз, бұл мақсат үшін арнайы компьютер қажет емес. Әрбір түйінге MariaDB Galera кластерін орнатыңыз.

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 қатемен аяқталды немесе пайдаланушы оны әдейі тоқтатты. Kaspersky Security Center Linux қызметтеріне мыналар жатады: kladminserver, klnagent, klactprx және klwebsrv.
- Белсенді түйін мен файл серверіндегі қойма арасындағы желілік қосылым доғарылды немесе үзілді.

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.

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 пәрмендерді орындаңыз:

   ```
   sudo yum install nfs-utils
   sudo mkdir -p /mnt/KlFocStateShare
   sudo mkdir -p /mnt/KlFocDataShare_klfoc
   sudo chown ksc:kladmins /mnt/KlFocStateShare
   sudo chown ksc:kladmins /mnt/KlFocDataShare_klfoc
   sudo chmod -R 777 /mnt/KlFocStateShare /mnt/KlFocDataShare_klfoc
   sudo sh -c "echo /mnt/KlFocStateShare *\(rw,sync,no_subtree_check,no_root_squash\) >>
   /etc/exports"
   sudo sh -c "echo /mnt/KlFocDataShare_klfoc *\
   (rw,exec,sync,no_subtree_check,no_root_squash\) >> /etc/exports"
   sudo cat /etc/exports
   sudo exportfs -a
   sudo systemctl start rpcbind
   sudo service nfs start
   ```

   Келесі пәрменді орындау арқылы автоматты іске қосуды қосыңыз:

   ```
   sudo systemctl enable rpcbind
   ```

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

Екі компьютерді ақауларға төзімді Kaspersky Security Center Linux кластері үшін белсенді және пассивті түйін ретінде жұмыс істеуге дайындаңыз.

Ақауларға төзімді Kaspersky Security Center Linux кластеріне түйіндерді дайындау үшін:

1. Аппараттық және бағдарламалық талаптарға сәйкес келетін екі компьютеріңіз бар екеніне көз жеткізіңіз. Бұл компьютерлер істен шығуға төзімді кластердің белсенді және пассивті түйіндері ретінде әрекет етеді.

2. Түйіндердің NFS клиенттері ретінде жұмыс істеуі үшін әрбір түйінге nfs-utils пакетін орнатыңыз.

   Келесі пәрменді орындаңыз:

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

3. Келесі пәрмендерді орындау арқылы қосылым нүктелерін жасаңыз:

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

4. Ортақ қалталарды сәтті орнатуға болатынын тексеріңіз. (Міндетті емес қадам)

   Келесі пәрмендерді орындаңыз:

   ```
   sudo mount -t nfs -o vers=4,nolock,local_lock=none,auto,user,rw {сервер}:
   {KlFocStateShare қалтасына жол} /mnt/KlFocStateShare
   ```

```
sudo mount -t nfs -o vers=4,nolock,local_lock=none,noauto,user,rw,exec {сервер}:
{KlFocDataShare_klfoc қалтасының жолы} /mnt/KlFocDataShare_klfoc
```

Мұнда {сервер}:{KlFocStateShare қалтасына жол} және {сервер }:{KlFocDataShare_klfoc қалтасына жол} – файл серверіндегі ортақ қалталарға желілік жолдар болып табылады.

Ортақ қалталарды сәтті қосқаннан кейін келесі пәрмендерді орындау арқылы оларды өшіріңіз:

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

5. Қосылым нүктелері мен ортақ қалталарды салыстырыңыз:

```
sudo vi /etc/fstab
{сервер}:{KlFocStateShare қалтасына жол} /mnt/KlFocStateShare nfs
vers=4,nolock,local_lock=none,auto,user,rw 0 0
{сервер}:{KlFocDataShare_klfoc қалтасының жолы} /mnt/KlFocDataShare_klfoc nfs
vers=4,nolock,local_lock=none,noauto,user,rw,exec 0 0
```

Мұнда {сервер}:{KlFocStateShare қалтасына жол} және {сервер }:{KlFocDataShare_klfoc қалтасына жол} – файл серверіндегі ортақ қалталарға желілік жолдар болып табылады.

6. Екі түйінді де қайта іске қосыңыз.

7. Келесі пәрмендерді орындау арқылы ортақ қалталарды іске қосыңыз:

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

8. Ортақ қалта рұқсаттары ksc:kladmins иелігінде екеніне көз жеткізіңіз.

Келесі пәрменді орындаңыз:

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

9. Түйіндердің әрқайсысында қосымша желілік адаптерді конфигурациялаңыз.

Қосымша желілік адаптер физикалық немесе виртуалды болуы мүмкін. Физикалық желілік адаптерді пайдаланғыңыз келсе, оны стандартты операциялық жүйе құралдары көмегімен қосыңыз және конфигурациялаңыз. Виртуалды желілік адаптерді пайдаланғыңыз келсе, оны үшінші тарап қолданбалары арқылы жасаңыз

Келесі әрекеттердің бірін орындаңыз:

- Виртуалды желілік адаптерді пайдаланыңыз.

  a. NetworkManager физикалық адаптерді басқару үшін пайдаланылып жатқанын тексеру үшін келесі пәрменді енгізіңіз:

  ```
  nmcli device status
  ```

  Егер шығыс деректерінде физикалық адаптер басқарылмайтын ретінде көрсетілсе, физикалық адаптерді басқару үшін NetworkManager бағдарламасын конфигурациялаңыз. Нақты конфигурациялау қадамдары дистрибутивіңізге байланысты.

  b. Интерфейстерді идентификациялау үшін келесі пәрменді пайдаланыңыз:

  ```
  ip a
  ```

  c. Конфигурациялық профиль жасаңыз:

  ```
  nmcli connection add type macvlan dev <физикалық интерфейс> mode bridge
  ifname <виртуалды интерфейс> ipv4.addresses <мекенжай маскасы> ipv4.method
  manual autoconnect no
  ```

- Физикалық желілік адаптерді немесе гипервизорды пайдаланыңыз. Бұл жағдайда NetworkManager бағдарламалық жасақтамасын өшіріңіз.

a. Мақсатты интерфейс үшін NetworkManager қосылымдарын жойыңыз:

```
nmcli con del <қосылым атауы>
```

Мақсатты интерфейске қосылымдар бар-жоғын тексеру үшін келесі пәрменді пайдаланыңыз:

```
nmcli con show
```

b. NetworkManager.conf файлын өзгертіңіз. Кілт файлы бөлімін тауып, мақсатты интерфейсті unmanaged-devices параметріне тағайындаңыз.

```
[keyfile]
unmanaged-devices=interface-name:<интерфейс атауы>
```

c. NetworkManager бағдарламасын қайта іске қосыңыз:

```
systemctl reload NetworkManager
```

Мақсатты интерфейс бұдан былай басқарылмайтынын тексеру үшін келесі пәрменді пайдаланыңыз:

```
nmcli dev status
```

- Үшінші тарап жүктеме теңестіргішін пайдаланыңыз. Мысалы, nginx серверін пайдалануға болады. Бұл жағдайда келесі әрекеттерді орындаңыз:

  a. nginx орнатылған Linux операциялық жүйесі бар бөлектенген компьютерді ұсыныңыз.

  b. Жүктемені теңестіруді конфигурациялаңыз. Негізгі сервер ретінде белсенді түйінді және резервтік сервер ретінде пассивті түйінді орнатыңыз.

  c. nginx серверінде барлық Басқару сервері порттарын ашыңыз: TCP 13000, UDP 13000, TCP 13291, TCP 13299 және TCP 17000.

Түйіндер дайындалды. Ақауларға төзімді Kaspersky Security Center Linux кластерін орналастыру үшін сценарий нұсқауларын орындаңыз.

Kaspersky Security Center Linux бағдарламасын ақауларға төзімді Kaspersky Security Center Linux кластерінің түйіндеріне орнату

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 қолданбаны белсенді түйінге, содан кейін пассивті түйінге орнатасыз. Орнату кезінде сіз қай түйіннің белсенді және қайсысы пассивті болатынын таңдайсыз.

Құрылғыңызда орнатылған Linux дистрибутивіне сәйкес келетін ksc64_[нұсқа_нөмірі]_amd64.deb немесе ksc64-[нұсқа_нөмірі].x86_64.rpm орнату файлын пайдаланыңыз. Орнату файлын "Лаборатория Касперского" сайтынан жүктеу арқылы аласыз.

KLAdmins домендік тобының пайдаланушысы ғана әр түйінге Kaspersky Security Center Linux бағдарламасын орната алады.

Негізгі (белсенді) түйінге орнату

Негізгі түйінге Kaspersky Security Center Linux орнату үшін:

1. Kaspersky Security Center Linux орнатқыңыз келетін құрылғыда қолдау көрсетілетін Linux дистрибутивтерінің бірі жұмыс істейтініне көз жеткізіңіз.

2. Пәрмен жолында осы нұсқаулықта көрсетілген пәрмендерді root есептік жазбасымен орындаңыз.

3. Kaspersky Security Center Linux орнатуды іске қосыңыз. Linux дистрибутивіңізге байланысты келесі пәрмендердің бірін орындаңыз:

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

4. Kaspersky Security Center Linux конфигурациясын іске қосыңыз:

   ```
   sudo /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 қабылдауыңыз қажет.

   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 қажет.

6. Басқару серверінің орнату режимі ретінде **кластердің Негізгі түйінін** таңдаңыз.

7. Сұрау көрсетілген кезде келесі параметрлерді енгізіңіз:

   a. Күйдің ортақ қалтасының қосылым нүктесіне жергілікті жолды енгізіңіз.

   b. Деректердің ортақ қалтасының қосылым нүктесіне жергілікті жолды енгізіңіз.

   c. Ақауларға төзімді кластердің қосылым режимін таңдаңыз: қосымша желілік адаптер немесе сыртқы жүктеме теңгергіші арқылы.

   d. Қосымша желілік адаптерді пайдалансаңыз, оның атауын енгізіңіз.

   e. Басқару серверінің DNS атауын немесе статикалық IP мекенжайын енгізу сұрауы туындаса, қосымша желілік адаптердің IP мекенжайын немесе сыртқы жүктеме теңгергішінің IP мекенжайын енгізіңіз.

   f. Басқару сервері SSL портының нөмірін енгізіңіз. Әдепкі бойынша порт нөмірі – 13000.

   g. Басқаруды жоспарлап отырған құрылғылардың шамамен санын есептеңіз:

      - Егер сізде 1-ден 100-ге дейін желілік құрылғы болса, 1 енгізіңіз.
      - Егер сізде 101-ден 1000-ға дейін желілік құрылғы болса, 2 енгізіңіз.
      - Егер сізде 1000-нан астам желілік құрылғы болса, 3 енгізіңіз.

   h. Қызметтер үшін қауіпсіздік тобының атын енгізіңіз. Әдепкі бойынша kladmins тобы пайдаланылады.

i. Басқару сервері қызметін іске қосу үшін есептік жазбаның атауын енгізіңіз. Есептік жазба көрсетілген қауіпсіздік тобының мүшесі болуы керек. Әдепкі бойынша ksc есептік жазба пайдаланылады.

j. Басқа қызметтерді іске қосу үшін есептік жазбаның атауын енгізіңіз. Есептік жазба көрсетілген қауіпсіздік тобының мүшесі болуы керек. Әдепкі бойынша ksc есептік жазба 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 root есептік жазбасының атауын енгізіңіз.

p. Дерекқорға қатынасу үшін пайдаланылатын дерекқордың root есептік жазбасының құпия сөзін енгізіңіз.

Қызметтердің қосылуын және автоматты түрде іске қосылуын күтіңіз:

- klnagent_srv
- kladminserver_srv
- klactprx_srv
- klwebsrv_srv

q. Басқару серверінің әкімшісінің рөлін орындайтын есептік жазбаны жасаңыз. Пайдаланушының аты мен құпиясөзін енгізіңіз. Пайдаланушының құпиясөзі 8 таңбадан кем немесе 256 таңбадан аспауы керек.

Пайдаланушы қосылып, 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. Пәрмен жолында осы нұсқаулықта көрсетілген пәрмендерді root есептік жазбасымен орындаңыз.
3. Kaspersky Security Center Linux орнатуды іске қосыңыз. Linux дистрибутивіңізге байланысты келесі пәрмендердің бірін орындаңыз:

- `sudo apt install /<path>/ksc64_[ нұсқа_нөмірі ]_amd64.deb`

- `sudo yum install /<path>/ksc64-[нұсқа_нөмірі].x86_64.rpm -y`

4. Kaspersky Security Center Linux конфигурациясын іске қосыңыз:

   `sudo /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 қабылдауыңыз қажет.

   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 қажет.

6. Басқару серверінің орнату режимі ретінде **Екіншілік кластер түйінін** таңдаңыз.

7. Сұралғанда, күйдің ортақ қалтасын қосу нүктесіне жергілікті жолды енгізіңіз.

Kaspersky Security Center Linux қолданбасы екіншілік түйінге орнатылған.

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`

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:

1. Белсенді түйінде /opt/kaspersky/ksc64/sbin мекенжайына өтіңіз.

2. Пәрмен жолын ашып, келесі пәрмендердің бірін орындаңыз:

   - Кластерді тоқтату үшін `klfoc -stopcluster --stp klfoc` пәрменін орындаңыз
   - Кластерді іске қосу үшін `klfoc -startcluster --stp klfoc` пәрменін орындаңыз

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.

Түйінге қызмет көрсетіліп, ол істен шығуға төзімді кластерге қосылады.

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 қол жеткізуге мүмкіндік береді. Осындай есептік жазба белгілі бір 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 қолданбасы 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.

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 толығырақ MySQL және MariaDB-мен жұмыс істеу үшін есептік жазбаларды конфигурациялау бөлімінен 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 теңшеу туралы толығырақ PostgreSQL немесе Postgres Pro жүйесімен жұмыс істеу үшін ДҚБЖ есептік жазбасын теңшеу 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.

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 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 қолданбасы (бұдан әрі - орнату қолданбасы) ДҚБЖ-не қатынасу үшін осы ДҚБЖ ішкі есептік жазбасын пайдаланады.

   Құпиясөзбен ДҚБЖ есептік жазбасын жасау үшін келесі пәрменді орындаңыз:

   ```
   /* KSCAdmin атты пайдаланушыны жасаңыз және KSCAdmin үшін құпиясөз беріңіз */
   CREATE USER 'KSCAdmin' 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 'KSCAdmin'@'%' IDENTIFIED WITH mysql_native_password BY '< құпиясөз >';
     ```

   - Қолданыстағы ДҚБЖ есептік жазбасының аутентификациясын өзгерту үшін келесі пәрменді орындаңыз:

     ```
     ALTER USER 'KSCAdmin'@'%' IDENTIFIED WITH mysql_native_password 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:

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

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 'KSCAdmin'`.

4. ДҚБЖ есептік жазбасына берілген артықшылықтар тізімін көру үшін келесі пәрменді орындаңыз:

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

5. Басқару сервері дерекқорын қолмен жасау үшін, келесі скриптті іске қосыңыз (бұл скриптте Басқару сервері дерекқорының атауы – *kav*):

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

   Сондай-ақ, ДҚБЖ есептік жазбасын жасайтын сценарийде көрсеткен дерекқордың атауын пайдаланыңыз.

6. 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.

Басқару серверін орнату үшін ДҚБЖ есептік жазбаларды конфигурациялау (Басқару серверінің дерекқорларын автоматты түрде жасау)

Басқару серверін орнату үшін ДҚБЖ есептік жазбасын конфигурациялау үшін:

1. PostgreSQL және Postgres Pro-мен жұмыс істеу үшін ортаны іске қосыңыз.
2. ДҚБЖ жүйесіне кіру үшін Postgres рөлін таңдаңыз. Сіз келесі рөлдердің бірін пайдалана аласыз:
   - *Postgres* пайдаланушысы (әдепкі бойынша Postgres рөлі).

     Егер сіз *Postgres* пайдаланушысын қолдансаңыз, оған қосымша құқықтар берудің қажеті жоқ.

     Әдепкі бойынша, *postgres* пайдаланушысында құпия сөз жоқ. Бірақ Kaspersky Security Center Linux жүйесін орнату құпия сөз қажет. *postgres* пайдаланушысы үшін құпия сөзді орнату үшін келесі сценарийді іске қосыңыз:

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

   - Postgres жаңа рөлі.

     Егер сіз жаңа Postgres рөлін пайдаланғыңыз келсе, сол рөлді жасаңыз және оған CREATEDB құқығын беріңіз. Ол үшін келесі скриптті іске қосыңыз (бұл скриптте *KCSAdmin* мәні рөлге ие):

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

     Жасалған рөл Басқару сервері дерекқорының иесі ретінде пайдаланылады (бұдан әрі - Сервер дерекқоры).
3. Басқару серверін орнатыңыз.

Орнату аяқталғаннан кейін, Сервер дерекқоры автоматты түрде жасалады және Басқару сервері жұмыс істеуге дайын.

Басқару серверін орнату үшін ДҚБЖ есептік жазбасын конфигурациялау (Басқару серверінің дерекқорларын қолмен жасау)

Басқару серверін орнату үшін ДҚБЖ есептік жазбасын конфигурациялау үшін:

1. Postgres-пен жұмыс істеу үшін ортаны іске қосыңыз.
2. Postgres рөлін және Басқару сервері дерекқорын жасаңыз. Содан кейін, рөлге Басқару сервері дерекқорындағы барлық құқықтарды беріңіз. Бұл үшін, *Postgres* дерекқорына *Postgres* пайдаланушысы ретінде кіріңіз және келесі скриптті іске қосыңыз (бұл скриптте *KCSAdmin* мәні рөлге ие, ал Басқару сервері дерекқорының атауы – *KAV*):

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

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

3. Жасалған Postgres рөліне келесі құқықтарды беріңіз:

   - Жалпыға ортақ схемадағы барлық кестелерге қатынасу құқықтары: ALL.
   - Жалпыға ортақ схемадағы барлық бірізділіктерге қатынасу құқықтары: ALL.

   Бұл үшін, Сервер дерекқорына *Postgres* пайдаланушысы ретінде кіріңіз және келесі скриптті іске қосыңыз (бұл скриптте *KCSAdmin* мәні рөлге ие):

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

4. Басқару серверін орнатыңыз.

Орнату аяқталғаннан кейін, Басқару сервері Басқару серверінің деректерін сақтау үшін құрылған дерекқорды пайдаланады. Басқару сервері жұмыс істеуге дайын.

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, қолданбаның құрамдастары арасында қауіпсіз өзара әрекеттесуді қамтамасыз ету үшін келесі сертификат түрлерін пайдаланады:

- Басқару сервері сертификаты;
- Веб-сервер сертификаты;
- Kaspersky Security Center Web Console сертификаты.

Әдепкі бойынша, Kaspersky Security Center өздігінен қол қойылған сертификаттарды пайдаланады (яғни, Kaspersky Security Center өзі берген). Қажет болса, ұйымыңыздың қауіпсіздік стандарттарына сәйкес өздігінен қол қойылған сертификаттарды пайдаланушы сертификаттарымен ауыстыра аласыз. 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.

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-іне қосылу кезінде Басқару серверінің аутентификациясы.
- Басқарылатын құрылғыларда Басқару серверінің және Желілік агенттің қауіпсіз өзара әрекеттесуі.
- Негізгі Басқару серверлерін қосалқы Басқару серверлеріне қосылған кезде түпнұсқалық растама.

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 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.

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.

Веб-сервер сертификаты

Сертификаттың арнайы түрін Kaspersky Security Center Басқару серверіне кіретін Веб-сервері пайдаланады. Бұл сертификат кейіннен басқарылатын құрылғыларға жүктеп салатын Желілік агенттің орнату пакеттерін жариялау үшін қажет. Ол үшін Веб-сервер әртүрлі сертификаттарды қолдана алады.

Веб-сервер басымдылық ретімен келесі сертификаттардың бірін пайдаланады:

1. Kaspersky Security Center Web Console көмегімен қолмен көрсетілген Веб-сервердің пайдаланушы сертификаты.

2. 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.

Kaspersky Security Center Linux-те қолданылатын пайдаланушы сертификаттарына қойылатын талаптар

Төмендегі кестеде, Kaspersky Security Center Linux түрлі құрамдастарына қатысты пайдаланушы сертификаттарына қойылатын талаптар көрсетілген.

Сертификат түрі	Талаптар	Түсіндірмелер
Жалпы сертификат, жалпы резервтік сертификат ("C", "CR")	Кілттің минималды ұзындығы: 2048. Негізгі шектеулер: • CA: Иә. • Жол ұзындығын шектеу: Жоқ. Қолданылатын кілттер: • 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.	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 барлық тізбегін қамтиды. Сертификат тақырыбының баламалы атауы (SAN) бар; яғни `subjectAltName` өрісінің мәні жарамды болып саналады. Сертификат серверлер сертификаттарына қойылатын браузерлердің қолданыстағы талаптарына, сондай-ақ CA/Browser Forum ағымдағы базалық талаптарына сай келеді.	–
Kaspersky Security Center Web Console сертификаты	Сертификаты көрсетілетін PEM контейнері жалпыға ортақ кілттердің барлық тізбегін қамтиды. Сертификат тақырыбының баламалы атауы (SAN) бар; яғни `subjectAltName` өрісінің мәні жарамды болып саналады. 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.

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 қолданбаға 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 үшін қажетті жаңа жауап файлын жасаңыз.

2. Жауап файлында `certPath` параметрі мен `keyPath` параметрі арқылы пайдаланушы сертификатының файлына және кілт файлына жолды көрсетіңіз.

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 <filename.pfx> -clcerts -nokeys | sed -ne '/-BEGIN CERTIFICATE-/,/-END CERTIFICATE-/p' > server.crt
   ```

   ```
   openssl pkcs12 -in <filename.pfx> -nocerts -nodes | sed -ne '/-BEGIN PRIVATE KEY-/,/-END PRIVATE KEY-/p' > key.pem
   ```

2. 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

Жаңа сертификат PKCS#12 пішімінде жасалуы керек (мысалы, ұйымның PKI арқылы) және оны сенімді сертификаттау орталығы (CA) шығаруы керек. Сондай-ақ, жаңа сертификат бүкіл сенім тізбегін және pfx немесе p12 кеңейтімі бар файлда сақталуы тиісті жеке кілтті қамтуы керек. Жаңа сертификат үшін төменде көрсетілген талаптар орындалуы керек.

Сертификат түрі: Жалпы сертификат, жалпы резервтік сертификат ("C", "CR")

Талаптар:

- Кілттің минималды ұзындығы: 2048.
- Негізгі шектеулер:
  - CA: Иә.

- Жол ұзындығын шектеу: Жоқ.

  Жолдың ұзындығын шектеу мәндері "None" мәнінен ерекшеленетін бүтін сан болуы мүмкін, бірақ 1-ден кем болмауы тиіс.

- 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.

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.

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

Басқару сервері сертификатын ауыстыру үшін:

Пәрмен жолында келесі пәрменді орындаңыз:

```
klsetsrvcert [-t <type> {-i <inputfile> [-p <password>] [-o <chkopt>] | -g <dnsname>}]
[-f <time>][-r <calistfile>][-l <logfile>]
```

klsetsrvcert утилитасын жүктеудің қажеті жоқ. Утилита Kaspersky Security Center Linux жеткізу жиынтығының құрамына кіреді. Ол Kaspersky Security Center Linux алдыңғы нұсқаларымен үйлеспейді.

klsetsrvcert утилитасының параметрлерінің сипаттамасы төмендегі кестеде келтірілген.

klsetsrvcert утилитасының параметрлерінің мәндері

Параметр	Мән
`-t <type>`	Ауыстырылатын сертификат түрі. `<type>` параметрінің ықтимал мәндері: • `C` – 13000 және 13291 порттары үшін жалпы сертификатты ауыстыру. • `CR` – 13000 және 13291 порттары үшін жалпы резервтік сертификатты ауыстыру.
`-f <time>`	Сертификатты ауыстыру кестесі "КК-АА-ЖЖЖЖ СС:ММ" пішімін қолданады (13000 және 13291 порттары үшін). Егер сіз жалпы немесе жалпы резервтік сертификатты жарамдылық мерзімі аяқталғанға дейін ауыстырғыңыз келсе, осы параметрді қолданыңыз. Басқарылатын құрылғылардың жаңа сертификатты пайдаланып Басқару серверімен синхрондау уақытын көрсетіңіз.
`-i <inputfile>`	Сертификаты бар контейнер және PKCS#12 пішіміндегі жеке кілт (p12 немесе pfx кеңейтімі бар файл).
`-p <password>`	p12 контейнерін қорғайтын құпиясөз. Сертификат пен жеке кілт контейнерде сақталады, сондықтан контейнер файлын шифрсыздау үшін құпиясөз қажет.
`-o <chkopt>`	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:<key length>` деп көрсетіңіз, мұндағы `<key length>` параметрі – қажетті кілт ұзындығы болып табылады. Әйтпесе, ағымдағы сертификат кілтінің ұзындығы пайдаланылады.
`-g <dnsname>`	Сертификат көрсетілген DNS атауымен жасалады.
`-r <calistfile>`	Сенімді сертификаттау орталығы қол қойған PEM пішіміндегі сенімді түбірлік сертификаттардың тізімі.
`-l <logfile>`	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 <inputfile> -p <password> -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 <inputfile> -p <password> -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.

Желілік агенттерді klmover утилитасын пайдаланып Басқару серверіне қосу

Басқару сервері сертификатын klsetsrvcert пәрмен жолының утилитасымен ауыстырғаннан кейін, байланыс үзілгендіктен Желілік агенттер мен Басқару сервері арасында SSL қосылымын орнату керек.

Жаңа Басқару сервер сертификатын көрсету және қосылымды қалпына келтіру үшін:

Пәрмен жолында келесі пәрменді орындаңыз:

```
klmover [-address <сервер мекенжайы>] [-pn <порт нөмірі>] [-ps <SSL портының нөмірі>]
[-nossl] [-cert <сертификат файлына апаратын жол>]
```

Бұл утилита Желілік агентті клиент құрылғысына орнатқан кезде Желілік агенттің орнату қалтасына автоматты түрде көшіріледі.

Зиянкестер құрылғыларды Басқару серверіңіздің басқаруынан шығаруына жол бермеу үшін klmover утилитасын іске қосқан кезде құпия сөзбен қорғауды міндетті түрде қосу ұсынылады. Құпия сөзбен қорғауды қосу үшін желі әкімшісі саясаты параметрлерінде**Жою құпиясөзін пайдалану** параметрін таңдаңыз.

klmover утилитасына жергілікті әкімші құқықтары қажет. klmover утилитасын іске қосу үшін құпия сөзді қорғауды жергілікті әкімші құқықтарынсыз жұмыс істейтін құрылғылар үшін орнатпауға болады.

Жою құпиясөзін пайдалану параметрі қосылса, Kaspersky Security Center Web Console жою құралының (cleaner.exe) құпия сөзбен қорғау мүмкіндігі де қосылады.

klmover утилитасының параметрлерінің сипаттамасы төмендегі кестеде келтірілген.

klmover утилитасының параметрлерінің мәндері

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.

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 Security for Mobile орнату пакеттерін жариялау үшін қажет. Қолданбаның ағымдағы конфигурациясына байланысты Веб-сервер сертификаты ретінде әртүрлі сертификаттарды қолдануға болады (толығырақ Kaspersky Security Center Linux сертификаттары туралы).

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 пайдаланушы сертификатыңыз Kaspersky Security Center Linux талаптарына және Apple сенімді сертификаттарына қойылатын талаптарға сай келеді ме екенін тексеріңіз. Қажет болса, сертификатты өзгертіңіз.

   Сертификатты жасау үшін kliossrvcertgen.exe утилитасын қолдануға болады.

2. Басты мәзірде қажетті Басқару сервері атауының жанындағы параметрлер (⚙) белгішесін басыңыз.

   Басқару серверінің сипаттары терезесі ашылады.

3. **Жалпы** қойыншасында **Веб-сервер** бөлімін таңдаңыз.

4. **HTTP протоколы бойынша** ішкі бөлімінде **Басқа сертификатты белгілеу** нұсқасын таңдап, **Сертификат өзгертілуде** түймесін басыңыз.

5. Ашылған терезеде, **Сертификат түрі** 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 (болса)** 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 (болса)** 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. Басты мәзірде қажетті Басқару сервері атауының жанындағы параметрлер (⚙) белгішесін 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 пайдаланушы сертификатыңыз Kaspersky Security Center Linux талаптарына және Apple сенімді сертификаттарына қойылатын талаптарға сай келеді ме екенін тексеріңіз. Қажет болса, сертификатты өзгертіңіз.

b. **Басқа сертификат** нұсқасын таңдап, **Сертификатты басқару** түймесін басыңыз және ашылған терезеде **Шолу** түймесін басыңыз.

c. Ашылған терезеде, **Сертификат түрі** 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 (болса)** 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 (болса)** өрісінде құпиясөзді енгізіңіз.

d. **Сақтау** түймесін, содан кейін **OK** түймесін басыңыз.

Ұялы құрылғы сертификаты Веб-сервер сертификаты ретінде пайдалану үшін қайта шығарылды.

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 қолданбасына 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 қажет (әдепкі бойынша 8080-порт қолданылады). Сіздің браузеріңізде JavaScript қосулы болуы тиіс.

Kaspersky Security Center Web Console веб-консоліне кіру үшін:

1. Браузерде <Басқару серверінің веб-мекенжайын>:<порт нөмірін> көрсетіңіз.

   Қолданбаға кіру беті көрсетіледі.

2. Бірнеше сенімді Басқару серверін қосқан болсаңыз, тізімнен қосылғыңыз келетін Басқару серверін таңдаңыз.

   Тек бір Басқару серверін қосқан болсаңыз, Басқару серверлерінің тізімі бұғатталған.

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:

     - `Username@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.

Жүйеге кіргеннен кейін, ақпараттық тақта сіз соңғы рет қолданған тіл және тақырыппен 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,

Бас мәзірде өз есептік жазбаңыздың параметрлеріне өтіп, **Шығу** тармағын таңдаңыз.

Kaspersky Security Center Web Console қолданбасы жабық, қолданбаға 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 оң жағындағы жұмыс аймағы.

Негізгі мәзір

Негізгі мәзір келесі бөлімдерден тұрады:

- **Басқару сервері**. Қазіргі уақытта қосылған Басқару серверінің атауын көрсетеді. Басқару сервері сипаттарын ашу үшін параметрлер белгішесін ( ) басыңыз.
- **Бақылау және есеп беру**. Желіңіздің инфрақұрылымы, қорғаныс күйі, сондай-ақ статистика туралы мәлімет береді.
- **Активтер (Құрылғылар)**. Құрамында активтерге арналған құралдар, сонымен қатар "Лаборатория Касперского" қолданбаларына арналған тапсырмалар мен саясаттар бар.
- **Пайдаланушылар және рөлдер**. Пайдаланушылар мен рөлдерді басқаруға, пайдаланушы құқықтарын конфигурациялауға, пайдаланушыларға рөлдерді тағайындауға және саясат профильдерін рөлдермен байланыстыруға мүмкіндік береді.
- **Операциялар**. Қолданбаны лицензиялау, шифрланған дискілерді және шифрлау оқиғаларын көру және басқару және үшінші тарап қолданбаларын басқару сияқты әртүрлі параметрлерді қамтиды. Бөлім, сонымен қатар, қолданбалар қоймаларына қол жеткізуге мүмкіндік береді.
- **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**. "Лаборатория Касперского" бизнес-шешімдері туралы ақпаратты қамтиды, сізге қажет шешімдерді таңдауға және "Лаборатория Касперского" сайтында осы шешімдерді сатып алуды жалғастыруға мүмкіндік береді.

- **Параметрлер**. Сізге сақталған күйді қалпына келтіру үшін веб-плагиннің ағымдағы күйінің деректерін сақтық көшірмелеуге мүмкіндік береді. Интерфейс тілі немесе тақырыбы сияқты интерфейстің сыртқы түріне қатысты жеке параметрлерді қамтиды.

- **Есептік жазбаңыздың мәзірі**. Kaspersky Security Center Linux анықтамасына сілтемені қамтиды. Сондай-ақ, Kaspersky Security Center Linux жүйесінен шығып, 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 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. Қажетті интерфейс тілін таңдаңыз.

Негізгі мәзір бөлімдерін бекіту және бекітуді болдырмау

Kaspersky Security Center Web Console веб-консолі бөлімдерін таңдаулыларыңызға қосу және оларға негізгі мәзірдегі **Бекітілген** бөлімнен жылдам қол жеткізу үшін бекітуге болады.

> Бекітілген элементтер болмаса, негізгі мәзірде **Бекітілген** бөлімі пайда болмайды.

Тек беттерді көрсететін бөлімдерді бекітуге болады. Мысалы, **Активтер (құрылғылар)** → **Басқарылатын құрылғылар** тармағына өтсеңіз, құрылғылар кестесі бар бет ашылады, яғни **Басқарылатын құрылғылар** бөлімін бекітуге болады. Егер негізгі мәзірде бөлімді таңдағаннан кейін терезе көрсетілсе немесе элемент көрсетілмесе, онда мұндай бөлімді бекіту мүмкін емес.

Бөлімді бекіту үшін:

1. Негізгі мәзірден тінтуірді бекіткіңіз келетін бөлімнің үстіне апарыңыз.

   Түйреуіш белгішесі (📌) көрсетіледі.

2. Түйреуіш белгішесін (📌) басыңыз.

Бөлім бекітілген және **Бекітілген** бөлімде көрсетіледі.

Бекітуге болатын элементтердің ең көп саны беске тең.

Сондай-ақ, таңдаулылардан элементтерді бекітуді болдырмау арқылы жоюға болады.

Бөлімді бекітуді болдырмау үшін:

1. Қолданбаның негізгі терезесінде **Бекітілген** бөліміне өтіңіз.
2. Тінтуірді бекітуді болдырмау керек бөлімнің үстіне апарып, бекітуді болдырмау белгішесін (📌) басыңыз.

Бөлім таңдаулылардан жойылды.

Бағдарламаны жылдам іске қосу шебері

Kaspersky Security Center Linux қолданбасы, 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 қолданбаға 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.

Қолданбаны жылдам іске қосу шебері **Басқарылатын құрылғылар** қалтасында саясаттары әлі жасалмаған қолданбалар 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, қолданба автоматты түрде қолданбаны 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. Басты мәзірде Басқару сервері атауының жанындағы параметрлер (⚙) белгішесін басыңыз.

   Басқару серверінің сипаттары терезесі ашылады.

2. **Жалпы** қойыншасында **Жалпы** бөлімін таңдаңыз.
3. **Бағдарламаны 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 "Лаборатория Касперского" басқарылатын қолданбалары 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:

- **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 түпнұсқалық растама**

  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 түпнұсқалық растама** жалаушасы қойылған болса, өріс қолжетімді болады).

- **Құпиясөз**

  Прокси-серверге қосылуға мүмкіндік беретін пайдаланушы құпиясөзі (**Прокси-сервердегі түпнұсқалық растама** 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 "Лаборатория Касперского" серверлерінен автоматты түрде жүктеледі.

3-қадам. Қорғау үшін активтерді таңдау

Желіңізде қолданылатын қорғаныс аумақтары мен операциялық жүйелерді таңдаңыз. Осы параметрлерді таңдағанда, желіңіздегі клиент құрылғыларына орнату үшін жүктеуге болатын "Лаборатория Касперского" серверлеріндегі қолданбаларды басқару плагиндері мен дистрибутивтеріне арналған сүзгілерді көрсетесіз. 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.

Қолданбаны жылдам іске қосу шеберін іске қоспай-ақ, қолжетімді орнату пакеттерінің тізімінен "Лаборатория Касперского" қолданбаларының 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.

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 қолданбалардың плагиндерін орнатуды конфигурациялау

Орнату үшін басқарылатын қолданбалардың плагиндерін таңдаңыз. "Лаборатория Касперского" 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. 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 "Лаборатория Касперского" 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.

- **Операциялық жүйе**

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.

"Лаборатория Касперского" қолданбалары үшін басқару плагиндерін қолданбаны 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 қолданбалардың 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 қолданба дистрибутиві болмаса, ағылшын тіліндегі дистрибутив таңдалады.

Кейбір дистрибутивтерді жүктеуді аяқтау үшін сіз Лицензиялық келісімді қабылдауыңыз қажет. **Қабылдау** түймесін басқан кезде Лицензиялық келісім мәтіні көрсетіледі. Шебердің келесі қадамына өту үшін сіз Лицензиялық келісімнің ережелері мен шарттарын, сондай-ақ "Лаборатория Касперского" Құпиялылық саясатының шарттарын қабылдауыңыз қажет. Егер сіз ережелер мен шарттарды қабылдамасаңыз, пакетті жүктелмейді.

Лицензиялық келісімнің ережелері мен шарттарын, сондай-ақ "Лаборатория Касперского" Құпиялылық саясатының шарттарын қабылдағаннан кейін, дистрибутивтерді жүктеу жалғасады. Болашақта орнату пакеттерін клиент құрылғыларында "Лаборатория Касперского" қолданбаларын 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. Келесі нұсқалардың бірін таңдаңыз:

- **Kaspersky Security Network бағдарламасын пайдалану шарттарын қабылдаймын**

  Kaspersky Security Center Linux және клиент құрылғыларында орнатылған басқарылатын қолданбалар, олардың жұмысы туралы ақпаратты Kaspersky Security Network қызметіне автоматты режимде жіберетін болады. Kaspersky Security Network-пен ынтымақтастық, вирустар мен қауіптер туралы деректерді барынша жылдам жаңартуды қамтамасыз ете отырып, туындаған қауіпсіздік қауіптеріне жауап беру жылдамдығын арттырады.

- **Kaspersky Security Network бағдарламасын пайдалану шарттарын қабылдамаймын**

  Kaspersky Security Center Linux және басқарылатын қолданбалар 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. Қолданбаны 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.

  Қолданбаны белсендіру кодының көмегімен белсендіру үшін, "Лаборатория Касперского" белсендіру серверлеріне қосылу мақсатында интернетке қатынасу талап етіледі.

  Қолданбаны 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 → «Лаборатория Касперского» лицензиялары** бөлімінде тарату болады.

- **Кілт файлын көрсетіңіз**

Кілт файлы – "Лаборатория Касперского" сізге ұсынатын key кеңейтімі бар файл. Кілт файлы қолданбаны белсендіретін кілтті қосуға арналған.

Кілт файлы сізге Kaspersky Security Center сатып алу кезінде көрсетілген электрондық пошта мекенжайына жіберіледі.

Қолданбаны кілт файлы арқылы белсендіру үшін "Лаборатория Касперского" белсендіру серверлеріне қосылудың қажет емес.

Қолданбаны 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 → «Лаборатория Касперского» лицензиялары** бөлімінде таратуға болады.

- Қолданбаны белсендіруді кейінге қалдырыңыз

Қолданбаны 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 өндірушілердің қолданбаларының 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 қолданбаларын жаңарту үшін келесі нұсқалардың бірін таңдаңыз:

- **Қажетті жаңартуларды іздеу**

  Осалдықтарды және қажетті жаңартуларды іздеу тапсырмасы, егер ол әлі 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, егер олар бұрын жасалмаса, 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.

Бағдарламаны жылдам іске қосу шеберін іске қоспай-ақ *Осалдықтарды және қажетті жаңартуларды іздеу* жасауға және *Қажетті жаңартуларды орнату және осалдықтарды түзету* 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.

11-қадам. Электрондық пошта арқылы хабарландыруларды жіберу әдісін конфигурациялау

Клиент құрылғыларында "Лаборатория Касперского" қолданбалары жұмыс істеген кезде тіркелетін оқиғалар туралы хабарландыру тарату параметрлерін конфигурациялаңыз. Бұл параметрлер қолданбалардың саясаттарында әдепкі бойынша мәндер ретінде пайдаланылады.

"Лаборатория Касперского" қолданбаларының туындайтын оқиғалары туралы хабарландырулар таратылымын конфигурациялау үшін келесі параметрлер қолжетімді:

- **Алушылар (электрондық пошта мекенжайлары)**

  Қолданба хабарландыру жіберетін пайдаланушылардың электрондық пошта мекенжайлары. Сіз бір немесе одан да көп мекенжайларды көрсете аласыз. Бірнеше мекенжайды көрсетсеңіз, оларды үтірлі нүктемен 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 конфигурация шебері жұмысын аяқтағаннан кейін желіңіздегі құрылғыларда қауіпсіздік қолданбаларын немесе Желілік агентті автоматты түрде орнату үшін қорғанысты орналастыру шеберін іске қосуға болады.

Қорғанысты орналастыру шебері

"Лаборатория Касперского" қолданбаларын орнату үшін қорғанысты орналастыру шеберін пайдалануға болады. Қорғанысты орналастыру шебері қолданбаларды арнайы жасалған орнату пакеттері арқылы және тікелей дистрибутивтерден қашықтан орнатуға мүмкіндік береді.

Қорғанысты орналастыру шебері келесі әрекеттерді орындайды:

- Қолданбаны орнату үшін орнату пакетін жүктейді (егер ол бұрын жасалмаған болса). Орнату пакеті осы жолда орналасқан: **Табу және орналастыру** → **Орналастыру және тағайындау** → **Орнату пакеттері**. Қолданбаны 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.

Қорғанысты орналастыру шеберін іске қосу

Қорғанысты орналастыру шеберін қолмен іске қосуға болады.

Қорғанысты орналастыру шеберін қолмен іске қосу үшін,

Қолданбаның 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.

1-қадам. Орнату пакетін таңдау

Орнатқыңыз келетін қолданбаның орнату пакетін таңдаңыз.

Қажетті қолданбаның орнату пакеті тізімде болмаса, **Қосу** түймесін басып, тізімнен қолданбаны таңдаңыз.

2-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.

3-қадам. Желілік агенттің нұсқасын таңдау

Желілік агенттен басқа қолданбаның орнату пакетін таңдаған болсаңыз, қолданбаны Kaspersky Security Center Басқару серверіне қосу үшін Желілік агентті де орнату қажет.

Желілік агенттің соңғы нұсқасын таңдаңыз.

4-қадам. Құрылғыларды таңдау

Қолданбаны орнатуды қажет ететін құрылғылардың тізімін көрсетіңіз:

- **Басқарылатын құрылғыларда орнату**

  Егер бұл нұсқа таңдалса, құрылғылар тобы үшін қолданбаны 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.

5-қадам. Қашықтан орнату тапсырмасының параметрлерін орнату

«Қашықтан орнату» тапсырмасы параметрлері тапсырмасы параметрлері терезесінде қолданбаны 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 қолданбаны (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 қолданбаны 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 қолданба клиент құрылғысында орнатылған болса, қайта орнатылмайды.

  Егер бұл параметр өшірулі болса, қолданба кез келген жағдайда орнатылады.

  Әдепкі бойынша, параметр қосулы.

- **Active Directory топтық саясаттарында бума 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.

6-қадам. Өшіріп қайта қосуды басқару

Қолданбаны 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 қолданба 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, қолданба 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, қолданба құрылғыны қайта жүктеуге мүмкіндік бермейді.

  Егер бұл параметр қосулы болса, құрылғыны қайта іске қоспас бұрын бұғатталған құрылғылардағы мұндай қолданбалар 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 қолданбаларды қолмен жауып, сол құрылғыларды қайта іске қосуы керек.

  Әдепкі бойынша, параметр өшірулі.

7-қадам. Орнатудың алдында үйлесімсіз қолданбаларды жою

Бұл қадам, сіз орналастыратын қолданба басқа қолданбалармен үйлесімді болмаса ғана болады.

Kaspersky Security Center Linux қолданбасы сіз орнатып жатқан қолданбамен үйлесімді емес қолданбаларды автоматты түрде жойғанын қаласаңыз, осы параметрді таңдаңыз.

Үйлесімсіз қолданбалар тізімі көрсетіледі.

Егер бұл параметр таңдалмаса, қолданба тек үйлесімсіз қолданбалары жоқ құрылғыларда орнатылады.

8-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.

9-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, қолданба 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, қолданбаны орнату үшін пайдаланушы есептік жазбасын көрсетуге болады.

  Орнату қолданбасы іске қосылатын пайдаланушы есептік жазбасын көрсету үшін **Қосу** түймесін басыңыз, **Жергілікті есептік жазба** таңдаңыз және пайдаланушы есептік жазбасының есептік 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.

10-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 15.1 нұсқасын орнатуға болады (13 нұсқасынан бастап). 15.1 нұсқасына дейін жаңарту кезінде Басқару серверінің алдыңғы нұсқасының барлық деректері мен параметрлері сақталады.

Kaspersky Security Center Linux жүйесін жаңартпастан бұрын, Басқару серверінің 15.1 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 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 қолданбамен ортақ пайдалануға жол берілмейді.

Желіңізде бірнеше Басқару серверлері болса, әрбір Серверді қолмен жаңарту қажет. Kaspersky Security Center Linux орталықтандырылған жаңартуды қолдамайды.

Сондай-ақ, Kaspersky Security Center Web Console веб-консолін жаңа нұсқаға дейін жаңарту қажет.

Басқару серверін 15.1 нұсқасына жаңартсаңыз, Желілік агент 15 немесе одан төмен нұсқасы үшін орнату пакеттерін жасай алмайтыныңызды ескеріңіз. Бұрын жасалған орнату пакеттері қолжетімді болады.

Kaspersky Security Center Linux қолданбасының алдыңғы нұсқасын жаңарту кезінде "Лаборатория Касперского" қолдау көрсетілетін қолданбаларының барлық орнатылған плагиндері сақталады. Басқару серверінің және Желілік агенттің плагиндері автоматты түрде жаңартылады. Жаңартуды бастамас бұрын, Басқару сервері деректерінің сақтық көшірмесін жасау ұсынылады.

Орнату файлы арқылы Kaspersky Security Center Linux жүйесінің алдыңғы нұсқасын жаңарту

Басқару серверін алдыңғы нұсқадан (13-нұсқадан бастап) 15.1 нұсқасына дейін жаңарту үшін Kaspersky Security Center Linux орнату файлын пайдаланып, жаңа нұсқаны алдыңғысының үстінен орнатуға болады.

Басқару серверін алдыңғы нұсқадан 15.1-нұсқаға дейін орнату файлын пайдаланып, жаңарту үшін:

1. "Лаборатория Касперского" сайтынан 15.1 нұсқасына арналған толық пакетімен Kaspersky Security Center Linux орнату файлын жүктеп алыңыз:
   - RPM негізіндегі операциялық жүйесі бар құрылғылар үшін: ksc64-<нұсқа нөмірі>.x86_64.rpm.
   - Debian негізіндегі операциялық жүйесі бар құрылғылар үшін: ksc64_<нұсқа нөмірі>_amd64.deb.

2. Басқару серверінде пайдаланатын пакеттер диспетчерін пайдаланып орнату пакетін жаңартыңыз. Мысалы, root артықшылықтары бар есептік жазба астындағы пәрмен жолы терминалында келесі пәрмендерді пайдалануға болады:

   - RPM негізіндегі операциялық жүйесі бар құрылғылар үшін:
     ```
     $ sudo rpm -Uvh --nodeps --force ksc64-<нұсқа нөмірі>.x86_64.rpm
     ```
   - Debian негізіндегі операциялық жүйесі бар құрылғылар үшін:
     ```
     $ sudo dpkg -i ksc64_<нұсқа нөмірі>_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.

4. Пәрмен жолы терминалында көрсетілетін Лицензиялық келісімді және Құпиялық саясатын оқыңыз. Лицензиялық келісімнің және Құпиялық саясатының барлық шарттарымен келіссеңіз:

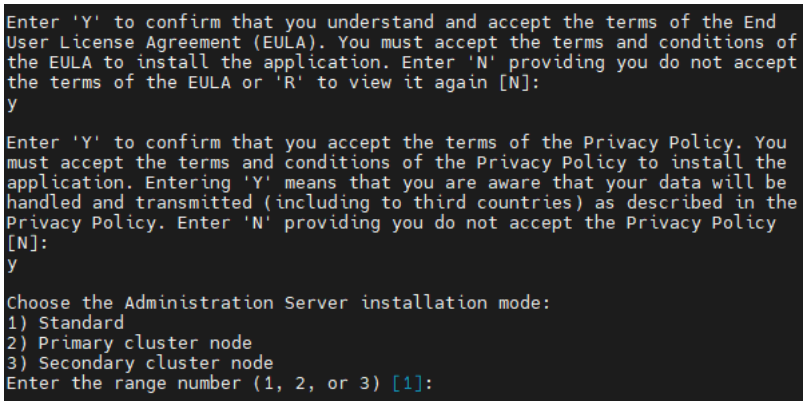
   a. Лицензиялық келісімнің талаптары мен шарттарын толығымен оқығаныңызды, түсінгеніңізді және қабылдағаныңызды растау үшін "Y" енгізіңіз.

   b. Деректерді өңдеуді сипаттайтын Құпиялық саясатын толық оқып, түсінгеніңізді және қабылдағаныңызды растау үшін "Y" тағы бір рет енгізіңіз.

   Қолданбаны 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. 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.

Сақтық көшірмені пайдаланып Kaspersky Security Center Linux жүйесінің алдыңғы нұсқасын жаңарту

Басқару серверін алдыңғы нұсқадан (13-нұсқадан бастап) 15.1 нұсқасына дейін жаңарту үшін, Kaspersky Security Center Linux жүйесінің жаңа нұсқасын орнатқаннан кейін Басқару сервер деректерінің сақтық көшірмесін жасауға және бұл деректерді қалпына келтіруге болады. Орнату кезінде қиындықтар туындаса, жаңарту алдында жасалған Сервер деректерінің сақтық көшірмесін пайдаланып Басқару серверінің алдыңғы нұсқасын қалпына келтіруге болады.

Деректердің сақтық көшірмесін жасау арқылы алдыңғы нұсқаның Басқару серверін 15.1 нұсқасына дейін жаңарту үшін:

1. Жаңарту алдында қолданбаның ескі нұсқасының Басқару серверіндегі деректердің сақтық көшірмесін жасаңыз.
2. Kaspersky Security Center Linux жүйесінің ескі нұсқасын жойыңыз.
3. Бұрынғы Басқару серверіне Kaspersky Security Center Linux 15.1 нұсқасын орнатыңыз.
4. Жаңарту алдында жасалған деректердің сақтық көшірмесінен Басқару сервері деректерін қалпына келтіріңіз.
5. 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.

Kaspersky Security Center Linux бағдарламасын ақауларға төзімді Kaspersky Security Center Linux кластерінің түйінінде жаңарту

Басқару серверінің 15.1-нұсқасын басқару серверінің анағұрлым ерте нұсқасы орнатылған (14-нұсқасынан бастап) ақауларға төзімді Kaspersky Security Center Linux кластерінің әрбір түйініне орната аласыз. 15.1 нұсқасына 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 ақауларға төзімді Kaspersky Security Center Linux кластерінің түйінінде жаңарту үшін:

1. "Лаборатория Касперского" сайтынан 15.1 нұсқасына арналған толық пакетімен Kaspersky Security Center Linux орнату файлын жүктеп алыңыз:

- RPM негізіндегі операциялық жүйесі бар құрылғылар үшін: ksc64-<нұсқа нөмірі>-<құрастыру нөмірі>.x86_64.rpm.

- Debian негізіндегі құрылғылар үшін: ksc64_<нұсқа нөмірі>-<құрастыру нөмірі>_amd64.deb.

2. Кластерді тоқтату.

3. Кластерге арналған ортақ қалталарды өшіріңіз және оларды Kaspersky Security Center Linux ақауларға төзімді кластері үшін файлдық серверді дайындау бөлімінде берілген параметрлер көмегімен қосыңыз.

4. Kaspersky Security Center Linux ақауларға төзімді кластері үшін файлдық серверді дайындау бөлімінде сипатталғандай, кластер түйіндеріндегі қосылу нүктелері мен ортақ қалталарды қайтадан салыстырыңыз.

5. Басқару серверінізде пайдаланатын пакеттер диспетчерін пайдаланып кластердің белсенді түйініндегі орнату пакетін жаңартыңыз.

   Мысалы, root артықшылықтары бар есептік жазба астындағы пәрмен жолы терминалында келесі пәрмендерді пайдалануға болады:

   - RPM негізіндегі операциялық жүйесі бар құрылғылар үшін:
     ```
     $ sudo rpm -Uvh --nodeps --force ksc64-<нұсқа нөмірі>-<құрастыру нөмірі>.x86_64.rpm
     ```

   - Debian негізіндегі операциялық жүйесі бар құрылғылар үшін:
     ```
     $ sudo dpkg -i 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.

7. Пәрмен жолы терминалында көрсетілетін Лицензиялық келісімді және Құпиялық саясатын оқыңыз. Лицензиялық келісімнің және Құпиялық саясатының барлық шарттарымен келіссеңіз:

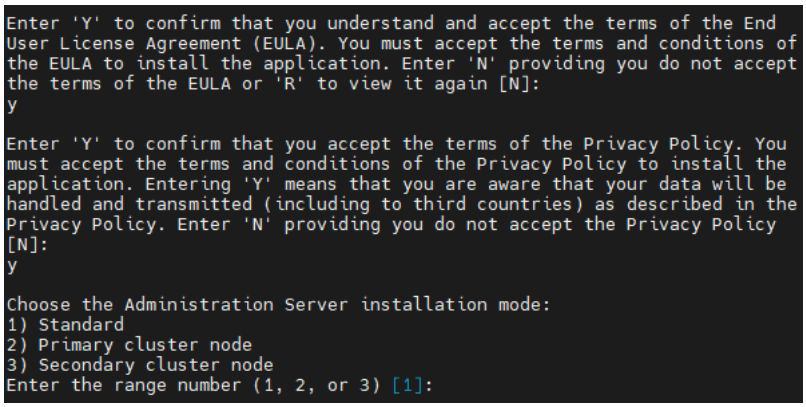
   a. Лицензиялық келісімнің талаптары мен шарттарын толығымен оқығаныңызды, түсінгеніңізді және қабылдағаныңызды растау үшін "Y" енгізіңіз.

   b. Деректерді өңдеуді сипаттайтын Құпиялық саясатын толық оқып, түсінгеніңізді және қабылдағаныңызды растау үшін "Y" тағы бір рет енгізіңіз.

   Қолданбаны орнату "Y" әрпін екі рет енгізгеннен кейін жалғасады.

8. Жаңартып жатқан түйінді "2" енгізу арқылы таңдаңыз.

   Төмендегі суретте соңғы екі қадам көрсетілген.



Әрі қарай, скрипт Басқару серверін жаңартуды конфигурациялайды және аяқтайды. Жаңарту кезінде жаңарту алдында өзгертілген Басқару серверінің параметрлерін өзгерте алмайсыз.

9. Пассивті түйінде 3-5 қадамдарды орындаңыз.

   6-қадамда түйінді таңдау үшін "3" енгізіңіз.

10. Кластерді іске қосу.

    Кез келген түйінде кластерді іске қосуға болатынын ескеріңіз. Кластерді пассивті түйінде іске қоссаңыз, ол белсенді түйінге айналады.

    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 үшін: ksc-web-console-[жинақ_нөмірі].x86_64.deb.
- RPM негізіндегі операциялық жүйелер үшін: ksc-web-console-[жинақ_нөмірі].x86_64.rpm.
- Альт 8 СП үшін: ksc-web-console-[жинақ_нөмірі]-alt8p.x86_64.rpm.

Орнату файлын "Лаборатория Касперского" 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 "Лаборатория Касперского" 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. Файл келесі директорияда орналасқан: /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.

Минималды параметрлер жиынтығы, мекенжайы және әдепкі бойынша порты бар жауаптар файлының мысалы:

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

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-консолін қосылуға рұқсат беру үшін жауап файлында `сенімді` орнату параметрін көрсетіңіз. Бұл параметрдің жол мәні келесі пішімге ие:

```
"trusted": "server address|port|certificate path|server name"
```

`trusted` орнату параметрінің құрамдастарын көрсетіңіз:

- **Басқару сервері мекенжайы**. Кластер түйіндерін дайындау кезінде қосымша желілік адаптерді жасасаңыз, адаптердің IP мекенжайын ақауларға төзімді Kaspersky Security Center Linux кластерінің мекенжайы ретінде пайдаланыңыз. Не болмаса, өзіңіз пайдаланып жатқан үшінші тарап теңгергішінің IP мекенжайын көрсетіңіз.

- **Басқару серверінің порты**. Kaspersky Security Center Web Console веб-консолі Басқару серверіне қосылу үшін пайдаланатын OpenAPI порты (әдепкі бойынша 13299).

- **Басқару сервері сертификаты**. Басқару серверінің сертификаты ақауларға төзімді Kaspersky Security Center Linux кластерінің ортақ деректер қоймасында орналасқан. Сертификат файлына әдепкі бойынша жол: <shared data folder>\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.

- **Басқару серверінің атауы**. Kaspersky Security Center Web Console-іне кіру терезесінде көрсетілетін ақауларға төзімді Kaspersky Security Center Linux кластерінің атауы.

> Kaspersky Security Center Web Console қолданбасын бірдей .rpm 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 rpm -Uvh --nodeps --force ksc-web-console-[жинақ_нөмірі].x86_64.rpm
     ```

   - Debian негізіндегі операциялық жүйесі бар құрылғылар үшін:
     ```
     $ sudo dpkg -i ksc-web-console-[жинақ_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 "Лаборатория Касперского" 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. Файл келесі директорияда орналасқан: /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.

   Минималды параметрлер жиынтығы, мекенжайы және әдепкі бойынша порты бар жауаптар файлының мысалы:

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

4. `/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. Қолданба кілтін алдыңғы қадамда жасалған /opt/kaspersky/ksc64/share/kaspersky_astra_pub_key.gpg каталогына 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 "Лаборатория Касперского" сайтынан жүктеу арқылы аласыз.

   Kaspersky Security Center Web Console алдыңғы нұсқасын жаңарту үшін келесі пәрмендердің бірін орындаңыз:

   ```
   $ sudo dpkg -i ksc-web-console-[жинақ_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 қолданбасына 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 тасымалдау тек Kaspersky Security Center 14.2 Windows жүйесінен Kaspersky Security Center Linux қолданбасына 15 нұсқасынан бастап мүмкін 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
- "Лаборатория Касперского" қолданбаларының 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 орналаспаған 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 жүйесінен деректерді экспорттау**

   Kaspersky Security Center Windows жүйесін ашып, деректерді тасымалдау шеберін іске қосыңыз.

3. **Деректерді Kaspersky Security Center Linux қолданбасына 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.

4. **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.
   - Қолданбаларды орнату пакеттерін жасау.
   - Виртуалды басқару серверлерін жасау.
   - Тарату нүктелерін тағайындау және конфигурациялау.
   - Құрылғыны жылжыту ережелерін жасау.
   - Құрылғыларға автоматты түрде тег қою ережелерін конфигурациялау.
   - Қолданбалар санаттарын жасау.

5. **Импортталған басқарылатын құрылғыларды Kaspersky Security Center Linux басқаруына жылжыту**

   Деректерді тасымалдауды аяқтаңыз, импортталған басқарылатын құрылғыларды Kaspersky Security Center Linux басқаруына жылжытыңыз. Kaspersky Security Center Linux жүйесінің ағымдағы нұсқасында мұны келесі жолдардың бірімен жасауға болады:

   - klmover утилитасын пайдалану арқылы.

     klmover утилитасын пайдаланыңыз және жаңа басқару сервері үшін қосылым параметрлерін көрсетіңіз.

   - Басқарылатын құрылғыларда желілік агентті орнату немесе қайта орнату арқылы.

     Желілік агентті орнату пакетін жасаңыз және орнату пакетінің сипаттарында жаңа басқару сервері үшін қосылым параметрлерін көрсетіңіз. Орнату пакетін пайдаланып, қашықтан орнату тапсырмасы арқылы импортталған басқарылатын құрылғыларға желілік агентті орнатыңыз. Толық ақпаратты Kaspersky Security Center Linux басқаруындағы басқарылатын құрылғыларды ауыстыру бөлімінен қараңыз.

     Сондай-ақ желілік агентті жергілікті түрде орнату үшін автономды орнату бумасын жасауға және пайдалануға болады.

6. **Желілік агентті соңғы нұсқаға жаңартыңыз.**

   Linux үшін желілік агентті Kaspersky Security Center нұсқасымен бірдей нұсқаға жаңарту ұсынылады.

7. **Басқарылатын құрылғылардың жаңа басқару серверінде көрінетініне көз жеткізіңіз.**

   Kaspersky Security Center Linux басқару серверінде басқарылатын құрылғылар тізімін ашыңыз (**Активтер (құрылғылар)** → **Басқарылатын 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 ең 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 қолданбалардың тапсырмалары мен саясаттары.
- Глобалдық тапсырмалар.
- Пайдаланушылық құрылғы таңдаулары.
- Басқару топтары құрылымы және оған кіретін құрылғылар.
- Деректері 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.

Тасымалдау шебері арқылы басқарылатын құрылғылар мен топтың байланыстырылған нысандарын экспорттау үшін:

1. Kaspersky Security Center Windows және Kaspersky Security Center Linux Басқару серверлері иерархияда орналасқанына 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 орналаспаса, Kaspersky Security Center Windows жүйесіне қосылған Kaspersky Security Center Web Console веб-консолін ашыңыз.
2. Қолданбаның 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 қолданбаларды таңдаңыз. Тек Kaspersky Security Center Linux қолдайтын қолданбаларды таңдаңыз. Қолдау көрсетілмейтін қолданбалардың нысандары әлі де экспортталады, бірақ жұмыс істемейді.

6. Глобалдық тапсырмаларды, таңдалған құрылғыларды және экспорттау есептерін таңдау үшін сол жақтағы сілтемелерді пайдаланыңыз. **Топ нысандары** сілтемесі пайдаланушылардың, ішкі пайдаланушылардың және қауіпсіздік топтарының рөлдерін, сондай-ақ қолданбалардың 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 тасымалдау үшін импорттау сәтті экспорттаудан кейін автоматты түрде басталады. Басқару сервері иерархиясын қолдаусыз деректерді тасымалдау үшін 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 SMP қолданбасына импорттау қажет.

Тасымалдау шебері арқылы басқарылатын құрылғылар мен топтың байланыстырылған нысандарын импорттау үшін:

1. Kaspersky Security Center Windows және Kaspersky Security Center Linux Басқару серверлері иерархияда орналасқанына 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 XDR Expert бағдарламасына қосылған Kaspersky Security Center Web Console ашыңыз.

     b. Қолданбаның 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 жию немесе кез келген әрекеттерді бірге орындау мүмкін емес. 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 **Активтер (құрылғылар)** 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 қосулыЖоқ** 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.

Kaspersky Security Center Linux бағдарламасының ағымдағы нұсқасында басқарылатын құрылғыларды Kaspersky Security Center Linux басқаруына не klmover утилитасы көмегімен немесе қашықтан орнату тапсырмасын пайдалану арқылы басқарылатын құрылғыларға Желілік агентті орнату арқылы жылжытуға болады.

Желілік агентті орнату арқылы Kaspersky Security Center Linux басқаруындағы басқарылатын құрылғыларды ауыстыру үшін:

1. Kaspersky Security Center Windows Басқару серверіне ауысыңыз.

2. **Табу және орналастыру** →**Орналастыру және тағайындау** →**Орнату пакеттері** бөліміне өтіңіз және бар Желілік агентті орнату пакетінің сипаттарын ашыңыз.

   Желілік агентті орнату бумасы бумалар тізімінде болмаса, жаңасын жүктеп алыңыз.

3. **Параметрлер** қойыншасында **Қосылым** бөлімін таңдаңыз. Kaspersky Security Center Linux Басқару сервері үшін қосылым параметрлерін көрсетіңіз.

4. 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.

5. Қолданбаны 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**Көзге көрінетін**Желілік агент орнатылған**Желілік агент орнатылған**Желілік агент іске қосулы**Желілік агент іске қосулыИә** мәні).

Басқару серверін конфигурациялау

Бұл бөлімде Kaspersky Security Center Басқару серверін конфигурациялау процесі мен сипаттары сипатталған.

Kaspersky Security Center Web Console веб-консолін Басқару серверіне қосу параметрлерін конфигурациялау

Басқару серверіне қосылу порттарын белгілеу үшін:

1. Басты мәзірде қажетті Басқару сервері атауының жанындағы параметрлер (⚙) белгішесін басыңыз.

   Басқару серверінің сипаттары терезесі ашылады.

2. **Жалпы** қойыншасында **Қосылу порттары** бөлімін таңдаңыз.

Таңдалған Басқару серверіне қосылудың негізгі параметрлері көрсетіледі.

Kaspersky Security Center Linux бағдарламасына кіру үшін рұқсат етілген IP мекенжайлары тізімін конфигурациялау

Әдепкі бойынша пайдаланушылар Kaspersky Security Center Linux жүйесіне Kaspersky Security Center Web Console-ін аша алатын кез келген құрылғыдан кіре алады. Басқару серверін, пайдаланушылар оған тек рұқсат етілген IP мекенжайлары бар құрылғылардан қосыла алатындай етіп конфигурациялауға болады. Бұл жағдайда, егер қаскүнем Kaspersky Security Center Linux есептік жазбасын ұрлап кетсе де, ол Kaspersky Security Center Linux бағдарламасы кіре алмайды, өйткені қаскүнемнің құрылғысының IP мекенжайы рұқсат етілген тізімде жоқ.

IP мекенжайы пайдаланушы Kaspersky Security Center Linux қолданбасына кіргенде немесе Kaspersky Security Center Linux OpenAPI арқылы Басқару серверімен өзара әрекеттесетін қолданбаны іске қосқанда тексеріледі. Осы кезде пайдаланушы құрылғысы 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 қолданбалардың 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 қолданбалар.

- Kaspersky Anti Targeted Attack Platform немесе Kaspersky Security for Virtualization сияқты OpenAPI арқылы Басқару серверімен өзара әрекеттесетін қолданбалар.

Сондықтан, жоғарыда аталған қолданбалар орнатылған құрылғылардың мекенжайларын көрсетіңіз.

Сіз IPv4 мекенжайлары мен IPv6 мекенжайларын орната аласыз. IP мекенжайлары ауқымдарын көрсету мүмкін емес.

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 "Лаборатория Касперского" басқарылатын қолданбалары үшін антивирустық дерекқорлар жаңартуларын жүктеу үшін интернетке қатынасуды конфигурациялау қажет.

Басқару серверінің интернетке қатынасу параметрлерін көрсету үшін:

1. Басты мәзірде Басқару сервері атауының жанындағы параметрлер (⚙) белгішесін басыңыз.

   Басқару серверінің сипаттары терезесі ашылады.

2. **Жалпы** қойындысында **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:

   - **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 түпнұсқалық растама**

     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 түпнұсқалық растама** жалаушасы қойылған болса, өріс қолжетімді болады).

- **Құпиясөз**

  Прокси-серверге қосылуға мүмкіндік беретін пайдаланушы құпиясөзі (**Прокси-сервердегі түпнұсқалық растама** 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 конфигурациялауға 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 сервер саясаттарды, тапсырмаларды, пайдаланушы рөлдерін және орнату пакеттерін Басты серверден алады, параметрлердің қайталануы жойылады.
- Басты Сервердегі құрылғыны таңдауларға қосалқы Серверлердегі құрылғылар қосылуы мүмкін.
- Басты сервердегі есептерге қосалқы 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, қосалқы Басқару серверлерінен ғана алады. Бұл шектеулер негізгі басқару серверімен бір дерекқорды пайдаланатын виртуалды басқару серверлеріне қолданылмайды.

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 басты Сервердің 13000-порты қосалқы Басқару серверлерінен қосылымдарды қабылдау үшін қолжетімді екеніне көз жеткізіңіз.
2. Болашақ негізгі Басқару серверінде параметрлер () белгішесін басыңыз.
3. Ашылатын сипаттар бетінде **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**

     Негізгі Басқару сервері SSL портының нөмірін көрсетіңіз. Әдепкі бойынша 13000-порт орнатылған.

   - **Басқару сервері API порты**

     OpenAPI арқылы қосылымдарды алу үшін негізгі Басқару сервері портының нөмірін көрсетіңіз. Әдепкі бойынша 13299-порт орнатылған.

   - **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.

Сіз көрсеткен есептік жазба үшін екі кезеңді тексеру өшірілгеніне көз жеткізіңіз. Егер бұл есептік жазба үшін екі кезеңді тексеру қосылса, онда сіз тек болашақ қосалқы Серверден ғана иерархия жасай аласыз (төмендегі нұсқауларды қараңыз). Бұл белгілі қате.

Егер қосылым параметрлері дұрыс болса, болашақ қосалқы Сервермен байланыс орнатылып, "негізгі/қосалқы" иерархиясы құрылады. Егер қосылым сәтсіз болса, қосылым параметрлерін тексеріңіз немесе болашақ қосалқы Сервердің сертификатын қолмен көрсетіңіз.

Болашақ қосалқы Сервер автоматты түрде Kaspersky Security Center Linux бағдарламасы жасаған өздігінен қол қойған сертификат арқылы түпнұсқалық растама жасайтындықтан, байланыс қатемен аяқталуы мүмкін. Нәтижесінде, браузер өзігінен қол қойған сертификатты жүктеуге тыйым салуы мүмкін. Бұл жағдайда келесі әрекеттердің бірін орындауға болады:

- 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.

Шебер жұмысын аяқтағаннан кейін "Басты сервер – Қосалқы сервер" 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.

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. Параметрлер белгішесін (⚙) басыңыз.

   b. Ашылатын сипаттар бетінде **Басқару серверлерінің иерархиясы** қойындысындағы **Жалпы** 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:

Басты мәзірде параметрлер (⚙) белгішесінің жанында орналасқан Басқару сервері атауын басыңыз.

Қосалқы (виртуалды) Басқару серверлерінің ашылмалы тізімі көрсетіледі.

Осы Басқару серверлерінің кез келгеніне оның атын басу арқылы өтуге болады.

Басқару топтары да көрсетіледі, бірақ олар белсенді емес және бұл мәзірде басқару үшін қолжетімді емес.

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.

     Қолданбаны 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. Қолданбаны 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 жасау және қосу үшін:

1. Басты мәзірде қажетті Басқару сервері атауының жанындағы параметрлер (⚙) белгішесін 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.

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.

     Қолданбаны 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. Қолданбаны 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. Басты мәзірде қажетті Басқару сервері атауының жанындағы параметрлер (⚙) белгішесін 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 функционалНысан ACL параметрлерін өзгерту →** Пайдаланушы рұқсаттары**Жалпы функционалНысан ACL параметрлерін өзгертуПайдаланушы рұқсаттары** құқығыңыз бар.

Қатынасу құқықтарын қолмен конфигурациялау

Виртуалды Басқару сервері әкімшісін тағайындау үшін:

1. Бас мәзірден қажетті виртуалды Басқару серверіне ауысыңыз:
   a. Басқару серверінің ағымдағы атауының оң жағындағы шеврон (›) белгішесін басыңыз.
   b. Қажетті Басқару серверін таңдаңыз.
2. Басты мәзірде Басқару сервері атауының жанындағы 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, **ОК** түймесін басыңыз.
   Қолданба таңдалған пайдаланушыны пайдаланушылар тізіміне, **Қатынасу құқықтары** қойындысына 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.

Қолданба өзгертілген пайдаланушы құқықтарын әкімші есептік жазбасында сақтайды.

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. Бас мәзірден қажетті виртуалды Басқару серверіне ауысыңыз:

a. Басқару серверінің ағымдағы атауының оң жағындағы шеврон (›) белгішесін басыңыз.

b. Қажетті Басқару серверін таңдаңыз.

3. Әкімші есептік жазбаның жаңа рөлін немесе бірнеше рөлдерін тағайындаңыз.

Қолданба 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

Клиент құрылғылары жұмыс істейтін Басқару серверін **Басқару серверін ауыстыру** тапсырмасы арқылы басқа Сервермен ауыстыруға болады. Тапсырма аяқталғаннан кейін, таңдалған клиент құрылғылары көрсетілген Басқару серверінің басқаруында болады. Құрылғыны басқаруды келесі Басқару серверлері арасында ауыстыруға болады:

- негізгі Басқару сервері және оның виртуалды Басқару серверлерінің бірі;
- бір негізгі Басқару серверінің екі виртуалды Басқару сервері.

Клиент құрылғылары жұмыс істейтін Басқару серверін басқа Сервермен ауыстыру үшін:

1. Негізгі қолданба терезесінде **Активтер (құрылғылар)** → **Тапсырмалар** бөліміне өтіңіз.
2. **Қосу** түймесін басыңыз.

   Жаңа тапсырма жасау шебері іске қосылады. Шебердің жұмысын жалғастыру үшін **Келесі** түймесін басыңыз.
3. Kaspersky Security Center қолданбасы үшін **Басқару серверін ауыстыру** 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. Таңдалған құрылғыларды басқару үшін пайдаланғыңыз келетін Басқару серверін таңдаңыз.
7. Есептік жазба параметрлерін белгілеңіз:

   - **Әдепкі есептік жазба**

     Тапсырма, сол тапсырманы орындайтын қолданба 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. **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.

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 көрсетіңіз.

12. **Сақтау** түймесін басыңыз.

    Тапсырма жасалды және конфигурацияланды.

13. Жасалған тапсырманы іске қосыңыз.

Тапсырманың жұмысы аяқталғаннан кейін, ол жасалған клиент құрылғылары тапсырма параметрлерінде көрсетілген Басқару серверін басқаруға 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. Басты мәзірде Басқару сервері атауының жанындағы параметрлер (⚙) белгішесін басыңыз.

2. Ашылған бетте **Басқару серверлері** қойыншасына өтіңіз.

3. Жойғыңыз келетін виртуалды Басқару серверін таңдаңыз.

4. Мәзір жолында **Жою** түймесін басыңыз.

Виртуалды Басқару сервері жойылды.

Басқару серверіне Қосылымдар журналдарын қарау

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. Басты мәзірде қажетті Басқару сервері атауының жанындағы параметрлер (⚙) белгішесін 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, қолданба 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.

Қолданба дерекқорды 10 минут сайын тексереді. Оқиғалар саны көрсетілген максималды мәннен 10 000 артық болса, қолданба 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.

Басқару серверіндегі оқиғалар қоймасында сақтауға болатын оқиғалар санын шектеу үшін:

1. Басты мәзірде қажетті Басқару сервері атауының жанындағы параметрлер (⚙) белгішесін басыңыз.

   Басқару серверінің сипаттары терезесі ашылады.

2. **Жалпы** қойыншасында **Оқиғалар қоймасы** бөлімін таңдаңыз. Дерекқорда сақталатын оқиғалардың максималды санын көрсетіңіз.

3. **Сақтау** түймесін басыңыз.

Басқару серверін басқа құрылғыға тасымалдау

Егер сізге жаңа құрылғыда Басқару серверін пайдалану қажет болса, оны келесі тәсілдердің бірімен тасымалдауға болады:

- Басқару серверін мен дерекқор серверін жаңа құрылғыға жылжыту.
- 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. 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.

3. Жаңа құрылғыда басқару сервері пайдаланатын дерекқорларды басқару жүйесін (ДҚБЖ) орнатыңыз.

   ДҚБЖ таңдау кезінде Басқару сервері қызмет көрсететін құрылғылардың санын ескеріңіз.

4. 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.

5. Орнату аяқталғаннан кейін, klbackup утилитасын көмегімен жаңа құрылғыдағы Басқару сервері деректерін қалпына келтіріңіз.

6. Kaspersky Security Center Web Console бағдарламасын ашып, Басқару серверіне қосылыңыз.

7. Барлық клиент құрылғыларының Басқару серверіне қосылғанына көз жеткізіңіз.

8. Алдыңғы құрылғыдан Басқару сервері мен дерекқорлар серверін жойыңыз.

ДҚБЖ есептік деректерін өзгерту

Кейде ДҚБЖ есептік деректерін өзгерту қажет болуы мүмкін, мысалы, қауіпсіздік мақсатында есептік деректердің ротациясын орындау үшін.

klsrvconfig утилитасын пайдаланып Linux ортасында ДҚБЖ есептік деректерін өзгерту үшін:

1. Linux пәрмен жолын іске қосыңыз.

2. klsrvconfig утилитасының пәрмен жолының ашылған терезесінде мынаны көрсетіңіз:

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

3. Есептік жазбаның жаңа атауын көрсетіңіз. ДҚБЖ-да бұрыннан бар есептік жазбаның есептік деректерін көрсетуіңіз қажет.

4. Жаңа құпиясөзді енгізіңіз.

5. Растау үшін осы жаңа құпиясөзді көрсетіңіз.

ДҚБЖ 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 көшірме жасау арқылы Басқару серверінің дерекқорын басқа құрылғыға тасымалдағанда немесе Kaspersky Security Center Linux жүйесінің жаңа нұсқасына көшкен кезде деректерді қалпына келтіруге болады (Басқару сервері деректерін Kaspersky Security Center Windows басқаруына тасымалдауға қолдау көрсетілмейді).

Орнатылған басқару плагиндерінің сақтық көшірмелері сақталмайтынын ескеріңіз. Сақтық көшірмеден Басқару сервері деректерін қалпына келтіргеннен кейін, басқарылатын қолданба плагиндерін жүктеп, қайта орнату қажет.

Басқару сервер деректерінің сақтық көшірмесін жасамас бұрын, басқару тобына виртуалды Басқару серверінің 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.

Басқару сервері 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 қолданбаны 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, қолданба параметрлері);
- Басқару топтары құрылымы және клиент құрылғылары туралы конфигурациялық ақпарат;
- қашықтан орнатуға арналған қолданба дистрибутивтері қоймасы;
- Басқару сервері сертификаты.

Басқару сервері деректерін қалпына келтіру тек klbackup утилитасының көмегімен мүмкін болады.

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. Негізгі қолданба терезесінде **Активтер (құрылғылар)** → **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 15** тармағын және **Тапсырма түрі** тізімінде **Басқару сервері деректерінің резервтік қоймасы** 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.

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 BACKUP_PATH [-logfile LOGFILE] [-use_ts]|[-restore] [-password PASSWORD]
[-cert_only] [-online]
```

Егер сіз klbackup утилитасының пәрмен жолында құпиясөзді белгілемесеңіз, утилита оны интерактивті түрде енгізуді сұрайды.

Кілттердің сипаттамалары:

- `-path BACKUP_PATH` – ақпаратты BACKUP_PATH қалтасына сақтау / қалпына келтіру үшін BACKUP_PATH қалтасындағы деректерді пайдалану (міндетті параметр).

- `-logfile LOGFILE` – Басқару сервері деректерін көшіру немесе қалпына келтіру туралы есепті сақтау.

  Дерекқор серверінің есептік жазбасы және klbackup утилитасы BACKUP_PATH қалтасындағы деректерді өзгерту құқығына ие болуы керек.

- `-use_ts` – деректерді сақтау кезінде ақпаратты BACKUP_PATH қалтасына, ағымдағы жүйелік күн мен уақытты `klbackup ЖЖЖЖ-АА-КК # СС-АА-СС` пішімінде көрсететін атауы бар салынған қалтаға көшіру. Егер кілт белгіленбеген болса, ақпарат BACKUP_PATH 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, егер `-path` кілтімен `C:\KLBackups` қалтасы жасалған болса, онда `klbackup 2022-06-19 # 11-30-18` қалтасында Басқару серверінің 2022 жылғы 19 маусым, 11 сағат 30 минут 18 секундтағы күйі туралы ақпарат сақталады.

- `-restore` – Басқару сервері деректерін қалпына келтіруді орындау. Деректерді қалпына келтіру BACKUP_PATH қалтасында ұсынылған ақпарат негізінде жүзеге асырылады. Егер кілт жоқ болса, BACKUP_PATH қалтасына деректерді сақтық көшірмелеу орындалады.

- `-password PASSWORD` – Басқару сервері сертификатын сақтау немесе қалпына келтіру; сертификатты шифрлау және шифрсыздау үшін PASSWORD параметрі белгілеген құпиясөзді пайдалану.

  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. Утилитаны жаңа ғана орнатылған Басқару серверінде іске қосу ұсынылады.

- `-cert_only` – Басқару серверінің сертификаты мен жеке кілтін ғана сақтау немесе қалпына келтіру.

- `-online` – Басқару серверінің автономды күйінің уақытын барынша азайту үшін лездік сурет жасау арқылы Басқару сервері деректерінің сақтық көшірмесін жасау. Егер сіз деректерді сақтық көшірмелеу және қалпына келтіру утилитасын қолдансаңыз, бұл параметр еленбейді.

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 қолданба келесі әрекеттерді орындайды:

- Сақтау қалтасынан қажет емес қалталар мен файлдарды жояды.
- Кестелерден қажет емес жазбаларды жояды («аспалы көрсеткіштер» деп те аталады).
- Кэшті тазартады.
- Дерекқорға қызмет көрсетеді (егер сіз SQL Server немесе PostgreSQL ДҚБЖ ретінде пайдалансаңыз):
  - дерекқорды қателер тұрғысынан тексереді (тек SQL Server үшін қолжетімді);
  - 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. Негізгі қолданба терезесінде **Активтер (құрылғылар)** → **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 Әкімшілік 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. Басты мәзірде негізгі Басқару сервері атауының жанындағы параметрлер (⚙) белгішесін 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 және бұрынғы қосалқы Басқару серверлері енді бір-бірінен тәуелсіз. Серверлер иерархиясы енді жоқ.

Жалпыға қолжетімді DNS серверлеріне қатынасу

Жүйелік DNS арқылы "Лаборатория Касперского" 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 каталогті 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. Бас мәзірде өз есептік жазбаңыздың параметрлеріне өтіп, **Интерфейс опциялары** тармағын таңдаңыз.
2. Пайда болған **Интерфейс опциялары** терезесінде **Деректерді шифрлау және қорғау опциясын көрсету** параметрді қосыңыз немесе өшіріңіз.
3. **Сақтау** түймесін басыңыз.

Осыдан кейін басты мәзірде **Операциялар → Деректерді шифрлау және қорғау** бөлім пайда болады.

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 <value> -t d
   ```

   SrvUseStrictSslSettings жалаушасының <value> 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 11 жүйесімен 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 қызметі;
- Веб-сервер қызметі;
- 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 каталогті 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 <value> -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 <value> -t d
     ```

   Жалаушаның <value> параметрін көрсетіңіз:

   - `1` – TLS протоколының қолдауын қосу үшін.
   - `0` – TLS протоколының қолдауын өшіру үшін.

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:

- Kaspersky Security Center Басқару сервері және оның қосалқы Серверлері топтарындағы басқарылатын құрылғылары;
- Kaspersky Security Center Басқару сервері мен оның қосалқы Серверлері басқаратын тағайындалмаған құрылғылар.

Сценарий: желілік құрылғыларды табу

Қауіпсіздік қолданбаларын орнатпас бұрын құрылғыларды іздеу қажет. 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.

3. **Табылған құрылғыларды басқару топтарына қосу ережелерін орнату (қажет болса)**

   Желіде сауалнама өткізу кезінде олардың табылуы нәтижесінде жаңа құрылғылар пайда болады. Олар автоматты түрде **Тағайындалмаған құрылғылар** тобына кіреді. 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.

Анықталған жаңа құрылғылар белгіленген ережелерге сәйкес таратылады. Егер ережелер белгіленбесе, құрылғылар **Тағайындалмаған құрылғылар** тобында қалады.

Windows желісінің сауалнамасы

Windows желісінің сауалнамасы туралы

Жылдам сауалнама кезінде Басқару сервері желінің барлық домендері мен жұмыс топтары 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;
- SMB протоколы қосулы;
- 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.

Windows желісінің сауалнамасы параметрлерін көру және өзгерту

Windows желісінің сауалнамасы параметрлерін өзгерту үшін:

1. **Құрылғыны табу** қалтасындағы консоль шежіресінен **Домендер** салынған қалтасын таңдаңыз.

   Сіз **Қазір сауалнама өткізу** түймесі арқылы **Тағайындалмаған құрылғылар** қалтасынан **Құрылғыны табу** қалтасына ауыса аласыз.

   Домендер ішкі қалтасының жұмыс аймағында құрылғылар тізімі көрсетіледі.

2. **Қазір сауалнама өткізу** түймесін басыңыз.

   Домен сипаттары терезесі ашылады. Қажет болса, Windows желісінің сауалнамасы параметрлерін конфигурациялаңыз:

   - Windows желілік сауалнамасын қосу

     Әдепкі бойынша, осы нұсқа таңдалады. Егер сізге Windows желісінің сауалнамасын жүргізу қажет болмаса (мысалы, Active Directory сауалнамасы жеткілікті болса), сіз бұл параметрді алып тастай аласыз.

   - Жылдам сауалнама жүргізу кестесін орнату

Әдепкі бойынша уақыт аралығы 15 минутты құрайды.

Жылдам сауалнама кезінде Басқару сервері желінің барлық домендері мен жұмыс топтары құрылғыларының NetBIOS атаулары тізімі туралы ақпаратты ғана алады.

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.

  Әдепкі бойынша, сауалнама ағымдағы жүйелік уақыттан бастап бес минут сайын іске қосылады.

- **Апта күндері бойынша**

  Сауалнама жүйелі түрде, аптаның көрсетілген күндерінде, көрсетілген уақытта орындалады.

  Әдепкі бойынша, сауалнама жұма сайын, сағат 18:00:00-де іске қосылады.

- **Ай сайын, таңдалған апталардың көрсетілген күндері**

  Сауалнама жүйелі түрде, әр айдың көрсетілген күндерінде, көрсетілген уақытта орындалады.

  Әдепкі бойынша, ай күндері таңдалмаған; әдепкі бойынша басталу уақыты – 18:00:00.

- **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 қосулы.

- **Толық сауалнама жүргізу кестесін орнату**

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.

  Әдепкі бойынша, сауалнама ағымдағы жүйелік уақыттан бастап бес минут сайын іске қосылады.

- **Апта күндері бойынша**

  Сауалнама жүйелі түрде, аптаның көрсетілген күндерінде, көрсетілген уақытта орындалады.

  Әдепкі бойынша, сауалнама жұма сайын, сағат 18:00:00-де іске қосылады.

- **Ай сайын, таңдалған апталардың көрсетілген күндері**

  Сауалнама жүйелі түрде, әр айдың көрсетілген күндерінде, көрсетілген уақытта орындалады.

  Әдепкі бойынша, ай күндері таңдалмаған; әдепкі бойынша басталу уақыты – 18:00:00.

- **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 қосулы.

Желіде сауалнама өткізуді бірден іске қосу қажет болса, **Қазір сауалнама өткізу** түймесін басыңыз. Сауалнаманың екі түрі де іске қосылады.

Виртуалды Басқару серверінде Windows желісінің сауалнамасы параметрлерін қарау және өзгерту әрекеттері тарату нүктесінің сипаттары терезесінде, **Құрылғыны табу** бөлімінде жүзеге асырылады.

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.

IP ауқымдарының сауалнамасы параметрлерін көру және өзгерту

IP ауқымдарының сауалнамасы параметрлерін көру және өзгерту үшін:

1. Қолданбаның негізгі терезесінде **Табу және орналастыру** → **Табу** → **IP ауқымдары** бөліміне өтіңіз.
2. **Сипаттар** түймесін басыңыз.

   IP ауқымдарының сауалнамасы сипаттары терезесі ашылады.
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.

- **Ай сайын, таңдалған апталардың көрсетілген күндері**

  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.

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. Қолданбаның негізгі терезесінде **Табу және орналастыру** → **Табу** → **IP ауқымдары** бөліміне өтіңіз.

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.

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. Қолданбаның 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. Қолданбаның 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 жүйесі Microsoft Active Directory домен контроллері мен Samba домен контроллерлерін сұрауына қолдау көрсетеді. 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.

Сервер Microsoft Active Directory сұрауы кезінде ICMP жаңғырық сұрауларын (ping пәрменіне ұқсас) жібереді.

Алдын ала талаптар

Домен контроллерлерін сұраудан бұрын келесі протоколдар қосылғанына көз жеткізіңіз:

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

Домен контроллерлері құрылғысында келесі порттардың қолжетімді екеніне көз жеткізіңіз:

- SASL үшін 389.

- TLS үшін 636.

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.
2. **Сауалнама параметрлері** түймесін басыңыз.

   Домен контроллері сауалнамасының параметрлері терезесі ашылады.
3. **Домен контроллері сауалнамасын қосу** параметрін таңдаңыз.
4. **Көрсетілген домендер сауалнамасын жүргізу** бөлімінде **Қосу** түймесін басыңыз, домен контроллерлерінің мекенжайын және пайдаланушының тіркелгі деректерін көрсетіңіз.
5. Қажет болса, **Домен контроллері сауалнамасының параметрлері** терезесінде сауалнама кестесін көрсетіңіз. 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.

   - **Ай сайын, таңдалған апталардың көрсетілген күндері**

     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 операциялық жүйесі бар тарату нүктесі үшін Microsoft Active Directory домен контроллерлері мен Samba домен контроллерлерін сұрауға қолдау көрсетіледі.
Windows операциялық жүйесінің тарату нүктесі үшін тек Microsoft Active Directory домен контроллерлерінің сауалнамасына қолдау көрсетіледі.
Тарату нүктесі көмегімен сұрауға Mac операциялық жүйесінде қолдау көрсетілмейді.

Тарату нүктесі көмегімен домен контроллерлерінің сауалнамасын конфигурациялау үшін:

1. Тарату нүктесінің сипаттарын ашыңыз.

2. **Домен контроллерінің сауалнамасы** бөлімін таңдаңыз.

3. **Домен контроллері сауалнамасын қосу** параметрін таңдаңыз.

4. 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**

5. 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

Домен контроллеріне алғаш рет қосылған кезде, басқару сервері қосылым протоколын анықтайды. Бұл протокол домен контроллерінің болашақтағы барлық қосылымдары үшін пайдаланылады.

Домен контроллеріне бастапқы қосылу келесідей іске асады:

1. Басқару сервері домен контроллеріне TLS арқылы қосылуға әрекеттенеді.

   Әдепкі бойынша сертификатты тексеру қажет болмайды. Сертификатты мәжбүрлі түрде тексеру үшін KLNAG_LDAP_TLS_REQCERT жалаушасын 1 мәніне орнатыңыз.

   Сертификаттар тізбегіне қол жеткізу үшін әдепкі бойынша сертификаттау орталығының (CA) операциялық жүйеге тәуелді жолы қолданылады. Басқа жолды көрсету үшін KLNAG_LDAP_SSL_CACERT жалаушасын пайдаланыңыз.

2. TLS қосылымы сәтсіз болса, басқару сервері домен контроллеріне SASL (DIGEST-MD5) арқылы қосылуға әрекеттенеді.

3. SASL (DIGEST-MD5) арқылы қосылу сәтсіз болса, басқару сервері домен контроллеріне қосылу үшін шифрланбаған TCP байланысының қарапайым түпнұсқалықты тексеру (Simple Authentication) мүмкіндігін пайдаланады.

Жалаушаларды конфигурациялау үшін klscflag утилитасын пайдалануға болады.

Пәрмен жолын іске қосыңыз және ағымдағы каталогті klscflag утилитасы бар каталогке өзгертіңіз. Klscflag утилитасы Басқару сервер орнатылған каталогте орналасқан. Әдепкісінше орнату үшін: /opt/kaspersky/ksc64/sbin.
Мысалы, келесі пәрмен сертификатты мәжбүрлі түрде тексереді:

```
klscflag -fset -pv klserver -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 контроллерін дұрыс сұрағыңыз келсе, `/etc/samba/smb.conf` файлында `netbios name` және `workgroup` параметрлерін көрсетуіңіз керек.

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. Қолданбаның негізгі терезесінде **Табу және орналастыру → Орналастыру және тағайындау → 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. **Активтер (құрылғылар)** → **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.

Үздік енгізу практикалары

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 – әкімшінің негізгі құралы. Kaspersky Security Center Web Console-ін Басқару серверімен бірге бір құрылғыда орнатуға болады.
- Желілік агент – құрылғыда орнатылған қауіпсіздік қолданбасын басқару, сондай-ақ құрылғы туралы ақпаратты алу және осы ақпаратты Басқару серверіне жіберу үшін қолданылады. Желілік агенттер ұйымның құрылғыларына орнатылады.

Kaspersky Security Center Linux бағдарламасын ұйымның желісінде орналастыру келесі тәсілдермен жүзеге асырылады:

- Басқару серверін орнату;
- Әкімші құрылғысына Kaspersky Security Center Web Console орнату;
- Желілік агент пен қауіпсіздік қолданбаларын ұйымның құрылғыларына орнату.

Қорғанысты күшейту нұсқаулығы

Kaspersky Security Center Linux қолданбасы 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, "Лаборатория Касперского" 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.

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

Қорғанысты күшейту нұсқаулығы 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

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 қолданбасын 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.

Басқару серверіне қосылуға арналған рұқсат етілген IP мекенжайлары тізімін конфигурациялау

Әдепкі бойынша пайдаланушылар Kaspersky Security Center Linux жүйесіне Kaspersky Security Center Web Console орнатылған кез келген құрылғыдан кіре алады. Басқару серверін, пайдаланушылар оған тек рұқсат етілген IP мекенжайлары бар құрылғылардан қосыла алатындай етіп конфигурациялауға 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 қараңыз: PostgreSQL серверінің аутентификациясы және Сценарийі: MySQL серверінің аутентификациясы.

Есептік жазбалар және авторизация

Басқару серверін екі қадамдық тексеруді пайдалану

Kaspersky Security Center Linux бағдарламасы Kaspersky Security Center Web Console пайдаланушыларына RFC 6238 (TOTP: Time-Based One-Time Password algorithm) негізінде екі қадамдық тексеруді пайдалану мүмкіндігін береді.

Егер сіздің есептік жазбаңызға екі қадамдық тексеру қосылса, Kaspersky Security Center Web Console серверіне 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

Мүмкіндігінше, Басқару сервері бар құрылғыда түпнұсқалық растама үшін токен, смарт-карта немесе басқа тәсіл арқылы көп факторлы түпнұсқалық растаманы (MFA) пайдалану ұсынылады.

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) (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.

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 пайдаланушы Басқару сервердің қол жеткізуді басқару тізімінде (ACL) бас әкімші рөлін алады. 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 пайдаланушылардың 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.

Басқару серверін қорғауды басқару

Басқару серверін қорғау қолданбасын 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 қолданбасын 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 қолданбаны өнеркәсіптік желіге кіретін құрылғыларға орнату ұсынылады. Kaspersky Industrial Cyber Security for Nodes – әртүрлі өнеркәсіптік қолданбалық жасақтама өндірушілерімен үйлесімділік сертификаттары бар қолданба.
- Ұсынылатын қауіпсіздік қолданбалары. Басқару сервері басқа бағдарламалық жасақтамасы бар құрылғыда орнатылған болса, сіз қолданбалық жасақтама өндірушісінің антивирустық қолданбаларды пайдалану бойынша ұсыныстарын оқып шығуыңыз керек (қорғау қолданбасын таңдау бойынша ұсыныстар бұрыннан бар болуы мүмкін және сенімді аймақты конфигурациялау қажет болуы мүмкін).

Қолданбаны 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 қолданба 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 қолданбаларын және "Лаборатория Касперского" қолданбаларын 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.

Басқарылатын қолданбалар қорғанысын конфигурациялау

Басқарылатын қолданба саясаттары

Қолданылатын Kaspersky Security Center Linux қолданбасының әрбір түрі мен құрамдасы үшін саясат жасау ұсынылады (Желілік агент, Kaspersky Endpoint Security for Windows, Kaspersky Endpoint Security for Linux, Kaspersky Endpoint Agent және т.б.). 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 "Лаборатория Касперского" қауіпсіздік қолданбаларын өшірмеуі немесе жоймауы үшін, құпия сөзбен қорғауды қосу ұсынылады. Құпия сөзбен қорғауға қолдау көрсететін платформаларда, мысалы, Kaspersky Endpoint Security, Желілік агент және басқа "Лаборатория Касперского" қолданбалары үшін құпия сөз 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. Желілік агент клиент құрылғысына орнатылған кезде, утилита автоматты түрде Желілік агент орнату қалтасына көшіріледі.

Зиянкестер құрылғыларды Басқару серверіңіздің басқаруынан шығаруына жол бермеу үшін klmover утилитасын іске қосқан кезде құпия сөзбен қорғауды міндетті түрде қосу ұсынылады. Құпия сөзбен қорғауды қосу үшін желі әкімшісі саясаты параметрлерінде**Жою құпиясөзін пайдалану** параметрін таңдаңыз.

klmover утилитасына жергілікті әкімші құқықтары қажет. klmover утилитасын іске қосу үшін құпия сөзді қорғауды жергілікті әкімші құқықтарынсыз жұмыс істейтін құрылғылар үшін орнатпауға болады.

Жою құпиясөзін пайдалану параметрі қосылса, Kaspersky Security Center Web Console жою құралының (cleaner.exe) құпия сөзбен қорғау мүмкіндігі де 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, қолданба 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 қолданба келесі әрекеттерді орындайды:

- дерекқорды қателердің болуы тұрғысынан тексереді;
- 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, басқарылатын қолданбаларға орнатылған "Лаборатория Касперского" Басқару сервері мен қолданбаларының 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:
  - 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

РЕД ОС операциялық жүйесін пайдаланған кезде, РЕД ОС ресми құжаттамасында сипатталған қауіпсіздік ұсыныстарын орындау 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. Сенімді сертификаттау орталығының (CA) сертификатын қолдану ұсынылады, себебі өздігінен қол қойылған сертификат тек шектеулі қорғанысты қамтамасыз етеді.

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. **SQL Server сервері үшін өздігінен қол қойылған SSL немесе TLS сертификатын сол сертификаттың талаптарына сай жасаңыз**

   SQL Server үшін сертификатыңыз әлдеқашан бар болса, бұл қадамды өткізіп жіберіңіз.

   SSL сертификатын тек SQL Server серверінің 2016 жылдан бұрынғы нұсқаларына (13.x) ғана қолдануға болады. SQL Server 2016 (13.x) және одан жоғары нұсқаларында TLS сертификатын қолданыңыз.

2. **Сервер жалаушасының файлын жасау**

   ServerFlags каталогіне өтіп, KLSRV_MYSQL_OPT_SSL_CA сервер жалаушасына сәйкес файлды жасаңыз:

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

3. **Сервер жалаушасының файлын өзгерту**

   KLSRV_MYSQL_OPT_SSL_CA өрісінде сертификатқа жолды көрсетіңіз (ca-cert.pem файлы).

4. **Дерекқорды конфигурациялаңыз**

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

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

   ServerFlags каталогіне өтіп, сервер жалаушаларына сәйкес файлдарды жасаңыз:

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

2. **Сервер жалаушасының файлдарын өзгерту**

   Жасалған файлдарды келесідей өзгертіңіз:

   KLSRV_MYSQL_OPT_SSL_CA: ca-cert.pem файлына жолды көрсетіңіз.

   KLSRV_MYSQL_OPT_SSL_CERT: server-cert.pem файлына жолды көрсетіңіз.

   KLSRV_MYSQL_OPT_SSL_KEY: server-key.pem файлына жолды көрсетіңіз.

   Егер server-key.pem үшін құпия фраза қажет болса, ServerFlags қалтасында KLSRV_MARIADB_OPT_TLS_PASPHRASE файлын жасаңыз және ондағы құпия фразаны көрсетіңіз.

3. **Дерекқорды конфигурациялаңыз**

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

   ```
   [mysqld]
   ssl-ca="C:\mysqlCerts\ca-cert.pem"
   ssl-cert="C:\mysqlCerts\server-cert.pem"
   ssl-key="C:\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. Сенімді сертификаттау орталығының (CA) сертификатын қолдану ұсынылады, себебі өздігінен қол қойылған сертификат тек шектеулі қорғанысты қамтамасыз етеді.

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

PostgreSQL бойынша SSL аутентификациясын орнату үшін мына қадамдарды орындаңыз:

1. **PostgreSQL сервері үшін сертификат жасаңыз.**

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 сервер үшін сертификат жасаңыз.**

   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 орнатыңыз.**

   pg_hba.conf келесідей өзгертіңіз:

   ```
   hostssl all all 0.0.0.0/0 md5
   ```

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

4. **PostgreSQL сертификатын көрсетіңіз.**

   Бір жақты SSL аутентификациясы

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

   ```
   listen_addresses ='*'
   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 ='*'
   ssl = on
   ssl_ca_file = '<postgres.crt>'
   ssl_cert_file = '<psql.crt>'
   ssl_key_file = '<psql.key>'
   ```

5. **PostgreSQL демонын қайта іске қосыңыз.**

   Келесі пәрменді орындаңыз:

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

6. **Басқару сервер үшін сервер жалаушасын көрсетіңіз.**

   Бір жақты SSL аутентификациясы

ServerFlags каталогіне өтіп, KLSRV_POSTGRES_OPT_SSL_CA сервер жалаушасына сәйкес файлды жасаңыз:

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

Құрылған файлда psql.crt файлына жолды көрсетіңіз.

Екі жақты SSL аутентификациясы

ServerFlags каталогіне өтіп, сервер жалаушаларына сәйкес файлдарды жасаңыз:

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

Жасалған файлдарды келесідей өзгертіңіз:

- KLSRV_POSTGRES_OPT_SSL_CA: psql.crt файлына жолды көрсетіңіз.
- KLSRV_POSTGRES_OPT_SSL_CERT: postgres.crt файлына жолды көрсетіңіз.
- KLSRV_POSTGRES_OPT_SSL_KEY: postgres.key файлына жолды көрсетіңіз.

Егер postgres.key үшін құпия фраза қажет болса, ServerFlags қалтасында KLSRV_POSTGRES_OPT_TLS_PASPHRASE файлын жасаңыз және ондағы құпия фразаны көрсетіңіз.

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

Орналастыруға дайындық

Бұл бөлімде Kaspersky Security Center Linux орналастырудың алдында орындау қажет қадамдар сипатталған.

Kaspersky Security Center Linux орналастыруды жоспарлау

Бұл бөлім келесі өлшемшарттарға байланысты ұйымның желісінде Kaspersky Security Center Linux құрамдастарын орналастырудың оңтайлы нұсқалары туралы ақпаратты қамтиды:

- құрылғылардың жалпы санын;
- ұйымдық немесе географиялық оқшауланған бөлімшелердің (кеңселер, филиалдар) болуы;
- тар арналармен байланған оқшауланған желілердің болуы;
- интернеттен Басқару серверіне қатынасу қажеттілігі.

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. Қолданбаны 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.

  "Лаборатория Касперского" қолданбаларын 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.

  "Лаборатория Касперского" қолданбаларын 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.

Kaspersky Security Center Linux бағдарламасын ұйымның желісінде орналастыруды жоспарлау туралы

Бір Басқару сервер 20 000-нан аспайтын құрылғыға қызмет көрсете алады (MariaDB көмегімен ДҚБЖ ретінде). Егер ұйымның желісіндегі құрылғылардың жалпы саны 20 000-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. Әйтпесе, мұндай кеңселерді тар арналармен байланысқан оқшауланған желілер ретінде қарастыру керек, "Типтік конфигурация: өзіндік әкімшілері бар бірнеше ірі кеңселер" бөлімін 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. Тарату нүктелері Басқару серверінен (әдепкі жүріс-тұрыс) және интернет орналастырылған "Лаборатория Касперского" серверлерінен жаңартуларды жүктеп ала алады, "Типтік конфигурация: көптеген шағын оқшауланған кеңселер" бөлімін 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;
- сертификат өрістерінің қажетті мәндерін белгілеу үшін;
- сертификаттың қажетті криптографиялық беріктігін қамтамасыз ету үшін.

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.

Kaspersky Security Center Linux типтік конфигурациялары

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 20 000-нан аспайтын құрылғыға қызмет көрсете алады (MariaDB 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. Желілік агентті қосу профильдері тек Windows және macOS операциялық жүйелері бар құрылғыларға қолдау көрсететінін ескеріңіз.

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 "Лаборатория Касперского" 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).

Басқару сервері қашықтағы кеңседе желіні сұрай алмайтындықтан, бұл функцияның орындалуын 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. Қосымша ақпарат алу үшін мына бөлімді қараңыз: Push серверін қосу.

ДҚБЖ таңдау

Төмендегі кестеде ДҚБЖ рұқсат етілген нұсқалары және оларды ұсынымдары мен қолдану шектеулері аталған.

ДҚБЖ	Ұсынымдар және шектеулер
MySQL (қолдау көрсетілетін нұсқаларды қараңыз)	20 000-нан аз құрылғылар үшін бір Басқару серверін іске қосуды жоспарласаңыз, осы ДҚБЖ пайдаланыңыз.
MariaDB (қолдау көрсетілетін нұсқаларды қараңыз)	20 000-нан аз құрылғылар үшін бір Басқару серверін іске қосуды 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.

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.

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

Басқару серверіне интернеттен қатынасуды ұсыну

Кейбір жағдайларда интернеттен Басқару серверіне қатынасу мүмкіндігін ұсыну қажет:

- "Лаборатория Касперского" дерекқорларының, қолданба модульдердің және қолданбалардың тұрақты жаңартулары.
- Үшінші тарап қолданбаларын жаңарту

  Әдепкі бойынша, Басқару сервері Microsoft қолданбасының жаңартуларын басқарылатын құрылғыларға орнату үшін интернет байланысын қажет етпейді. Мысалы, басқарылатын құрылғылар Microsoft қолданбасының 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 қолданбаларынан басқа үшінші тарап қолданбаларының жаңартуларын орнату үшін.
- Үшінші тарап қолданбаларында осалдықтарды түзету

  Басқару серверін интернетке қосу келесі тапсырмаларды орындау үшін қажет:

  - Microsoft қолданбалық жасақтама осалдықтарының ұсынылған түзетулер тізімін жасау. Тізімді "Лаборатория Касперского" 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. Ұялы құрылғыларды басқару қажет болса, сіз 13292 TCP портын 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 қолданбасын 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).

Интернеттен қатынасу: Желілік агентті DMZ режимінде қосылым шлюзі ретінде пайдалану

Басқару сервері ұйымның ішкі желісінде орналасуы мүмкін, ал желінің демилитаризацияланған аймағында кері қосылым бағыты бар қосылым шлюзі ретінде жұмыс істейтін Желілік агенті бар құрылғы орналасуы мүмкін (Басқару сервері Желілік агентпен қосылым орнатады). Бұл жағдайда, интернеттен қатынасуды ұйымдастыру үшін келесі шарттарды орындау қажет:

- Желілік агент демилитаризацияланған аймақтағы құрылғыға орнатылуы керек. Желілік агентті орнату кезінде орнату шеберінің **Қосылым шлюзі** терезесінде **Желілік агентті DMZ режимінде қосылым шлюзі ретінде пайдалану** тармағын таңдаңыз.

- Қосылым шлюзі орнатылған құрылғысын тарату нүктесі ретінде қосуға болады. Қосылым шлюзін қоссаңыз, **Тарату нүктесін қосу** терезесінде **Таңдау → Келесі мекенжай бойынша демилитаризацияланған аймақта орналасқан қосылымдар шлюзін қосу** параметрін таңдаңыз.

- Сыртқы үстел үсті компьютерлерін Басқару серверіне қосу мақсатымен интернетті пайдалану үшін Желілік агенттің орнату пакетін өзгерту қажет. Жасалған орнату бумасының сипаттарында **Қосымша → Басқару серверіне байланыс шлюзі арқылы қосылу** параметрін таңдап, жаңадан жасалған қосылым шлюзін көрсетіңіз.

Демилитаризацияланған аймақта орналасқан қосылым шлюзі үшін Басқару сервері Басқару серверінің сертификаты қол қойған сертификатты жасайды. Егер әкімші Басқару серверіне пайдаланушы сертификатын белгілеу туралы шешім қабылдаса, онда мұны демилитаризацияланған аймақта қосылым шлюзін жасамас бұрын жасау керек.

Егер жергілікті желіден де, интернеттен де Басқару серверіне қосыла алатын ноутбуктері бар қызметкерлер болса, Желілік агент саясатында Желілік агентті ауыстыру ережесін құрған жөн.

Тарату нүктелері туралы

Желілік агенті орнатылған құрылғыларды тарату нүктесі ретінде пайдалануға болады. Бұл режимде Желілік агент Басқару серверден де, "Лаборатория Касперского" 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.

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-ден 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-ден 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-ден 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-ден 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.

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, қолданбалар тізімдемесі және т.б.) құрылғылар, топтар, оқиғалар мен нысандар көрінеді;
- виртуалды Сервер желіні тек оған қосылған тарату нүктелері арқылы сканерлей алады.

Сыртқы қызметтермен әрекеттесуге арналған желі параметрлері

Kaspersky Security Center Linux жүйесі сыртқы қызметтермен әрекеттесу үшін келесі желі параметрлерін пайдаланады.

Желі параметрлері

Желі параметрлері	Мекенжай	Сипаттамасы
Порт: 443 Протокол: HTTPS	activation-v2.kaspersky.com/activationservice/activationservice.svc	Қолданбаны белсендіру.
Порт: 443	https://s00.upd.kaspersky.com	"Лаборатория Касперского"

Протокол: HTTPS	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	"Лаборатория Касперского" дерекқорларын, қолданба модульдерін және қолданбаларын жаңарту.
Порт: 443 Протокол: HTTPS	https://downloads.upd.kaspersky.com	• "Лаборатория Касперского" дерекқорларын, қолданба модульдерін және қолданбаларын жаңарту. • "Лаборатория Касперского" серверлерінің қолжетімділігін тексеру. Kaspersky Security Center Linux қолданбасы "Лаборатория Касперского" дерекқорлары мен қолданба модульдерін жүктемес бұрын "Лаборатория Касперского" серверлерінің қолжетімділігін тексереді. Жүйелік DNS арқылы серверлерге қатынасу мүмкін болмаса, қолданба жалпыға ортақ DNS серверлерін пайдаланады.
Порт: 80 Протокол: HTTP	http://p00.upd.kaspersky.com http://p01.upd.kaspersky.com	"Лаборатория Касперского" дерекқорларын, қолданба

	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	модульдерін және қолданбаларын жаңарту.
Порт: 443 Протокол: HTTPS	ds.kaspersky.com	Kaspersky Security Network қолдану.
Порт: 443, 1443 Протокол: HTTPS	ksn-a-stat-geo.kaspersky-labs.com ksn-file-geo.kaspersky-labs.com ksn-verdict-geo.kaspersky-labs.com ksn-url-geo.kaspersky-labs.com ksn-a-p2p-geo.kaspersky-labs.com ksn-info-geo.kaspersky-labs.com ksn-cinfo-geo.kaspersky-labs.com	Kaspersky Security Network қолдану.
Протокол: HTTPS	click.kaspersky.com redirect.kaspersky.com	Интерфейстегі сілтемелерге өту.

Порт: 80 Протокол: HTTP	http://crl.kaspersky.com http://ocsp.kaspersky.com	Басқа "Лаборатория Касперского" серверлерімен TLS қосылымын орнату үшін қажет сертификаттарды тексеруге арналған серверлер.
Порт: 443 Протокол: HTTPS	https://ipm-klca.kaspersky.com	Жарнамалық хабарландырулар.

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 "Лаборатория Касперского" 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 каталогті 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
     ```

Желілік агент пен қауіпсіздік қолданбасын орналастыру

Ұйымның құрылғыларын басқару үшін құрылғыларға Желілік агентті орнату қажет. Ұйымның құрылғыларында Kaspersky Security Center Linux таратылған қолданбасын орналастыру әдетте оларға Желілік агентті орнатудан басталады.

Microsoft Windows XP желілік агенті келесі операцияларды қате орындауы мүмкін: жаңартуларды тікелей "Лаборатории Касперского" серверлерінен жүктеу (тарату нүктесі ретінде) және KSN прокси-сервері ретінде жұмыс істеу (тарату нүктесі ретінде).

Бастапқы орналастыру

Егер құрылғыда Желілік агент әлдеқашан орнатылған болса, мұндай құрылғыға қолданбаларды қашықтан орнату Желілік агенттің көмегімен жүзеге асырылады. Бұл ретте, орнатылатын қолданбаның 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. Қолданбаларды Желілік агенті орнатылған басқарылатын құрылғыларға орнату туралы толығырақ мәліметті одан әрі осы бөлімде қараңыз.

Желілік агентті Microsoft Windows платформасындағы құрылғыларға бастапқы орнатуды келесі тәсілдермен орындауға болады:

- Қолданбаларды қашықтан орнатудың үшінші тарап құралдары арқылы.
- Операциялық жүйесі және Желілік агент орнатылған қатты дисктің үлгісін клондау жолымен: дисктердің үлгілерімен немесе бөтен құралдарымен жұмыс істеу үшін Kaspersky Security Center Linux ұсынатын құралдармен.
- Microsoft Windows топтық саясат механизмі арқылы: Microsoft Windows топтық саясаттарын штаттық басқару құралдары көмегімен немесе автоматтандырылған түрде, Kaspersky Security Center Linux қолданбаларын қашықтан орнату тапсырмасында сәйкес параметрдің көмегімен.
- Kaspersky Security Center Linux қолданбаларын қашықтан орнату тапсырмасындағы тиісті параметрлердің көмегімен мәжбүрлі түрде.
- Пайдаланушыларға Kaspersky Security Center Linux қалыптастырған автономды пакеттерге сілтемелер тарату арқылы. Автономды пакеттер, параметрлері конфигурацияланған таңдалған қолданбалардың дистрибутивтерін қамтитын орындалатын модульдер болып табылады.
- Құрылғыларда қолданбалардың инсталляторларын іске қосу арқылы қолмен.

Microsoft Windows ерекшеленетін платформаларда басқарылатын құрылғыларда Желілік агентті бастапқы орнатуды қолда бар бөтен құралдармен жүргізу керек. Желілік агентті жаңа нұсқасына дейін жаңарту, сондай-ақ "Лаборатория Касперского" басқа қолданбаларын осы платформаларға қолданбаларды қашықтан орнату тапсырмаларының көмегімен, құрылғылардағы Желілік агенттерді қолдану арқылы орнату. Бұл жағдайда, орнату Microsoft Windows платформасында орнатуға ұқсас жолмен жүзеге асырылады.

Басқарылатын желіде қолданбаларды орналастыру тәсілі мен стратегиясын таңдай отырып, бірқатар факторларды назарға алған жөн (тізімі толық емес):

- ұйым желісінің конфигурациясы;
- құрылғылардың жалпы санын;
- ұйымның желісінде Active Directory домендерінің мүшесі емес құрылғылардың болуы және мұндай құрылғыларда әкімшілік 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;

- орналастыру басталған сәтте қашықтағы құрылғыларда қолданылатын қауіпсіздік параметрлері (атап айтқанда, UAC және Simple File Sharing режимін пайдалану).

Инсталляторлар параметрлерін конфигурациялау

"Лаборатория Касперского" қолданбаларын желіге орналастыруға кіріспес бұрын, орнату параметрлерін – қолданбаны орнату барысында конфигурацияланатын параметрлерді анықтап алу керек. Желілік агентті орнатқан кезде кем дегенде Басқару серверіне қосылу мекенжайын, мүмкін болса, кейбір қосымша параметрлерді белгілеу қажет. Таңдалған орнату тәсіліне байланысты, параметрлерді әртүрлі тәсілдермен белгілеуге болады. Қарапайым жағдайда (қолмен таңдалған құрылғыға интерактивті орнатқан кезде) қажетті параметрлерді инсталлятордың пайдаланушылық интерфейсі көмегімен белгілеуге болады.

Бұл параметрлерді конфигурациялау тәсілі құрылғылар топтарына қолданбаларды тыныш орнатуға қолайсыз. Әдеттегі жағдайда әкімші орталықтандырылған түрде параметрлердің мәндерін көрсетуі тиіс, олар одан әрі желідегі таңдалған құрылғыларға тыныш орнату үшін қолданылуы мүмкін.

Орнату пакеттері

Қолданбаларды орнату параметрлерін конфигурациялаудың бірінші және негізгі тәсілі әмбебап болып табылады және қолданбаларды орнатудың барлық тәсілдеріне жарамды болып келеді: Kaspersky Security Center Linux құралдарымен де, үшінші тарап құралдарының көпшілігі көмегімен де. Бұл тәсіл Kaspersky Security Center Linux-де қолданбалардың орнату пакеттерін құруды білдіреді.

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);

- инсталляторлардың немесе өзіндік пішімдегі инсталляторлардың орындалатын файлдарынан (.msi, .deb, .rpm) – стандартты немесе қолдау көрсетілетін қолданбалар үшін.

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. "Лаборатория Касперского" 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 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.

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 қолданбасын қоса, орнатылған операциялық жүйемен және жұмысқа қажетті қолданбалық 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.

- Үлгіні орналастырғаннан кейін операциялық жүйені бірінші іске қосқан кезде құрылғыларда Желілік агенттің қызметін бірінші іске қосуға дейін -dupfix кілтімен (бұл маңызды) klmover утилитасын іске қосуды қамтамасыз етіңіз. 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, Windows пәрмен жолында `klmover -cloningmode 1` пәрменін енгізіңіз.

   Желілік агент дискіні клондау режиміне ауысады.

3. Дискіні клондау режимінің ағымдағы күйін сұрау үшін, пәрмен жолында `klmover -cloningmode` пәрменін енгізіңіз.

   Нәтижесінде, утилитаның терезесінде дискіні клондау режимінің қосулы немесе өшірулі екені туралы ақпарат көрсетіледі.

4. Дискіні клондау режимін өшіру үшін, утилитаның пәрмен жолында `klmover -cloningmode 0` пәрменін енгізіңіз.

Kaspersky Security Center Linux қолданбаларын қашықтан орнату тапсырмасы арқылы мәжбүрлеп орналастыру

Егер Желілік агенттерді немесе басқа қажетті қолданбаларды дереу орналастыруды бастау қажет болса, құрылғылардың доменге кезекті кіруін күтпей немесе Active Directory доменінің мүшелері болып табылмайтын құрылғылар бар болса, Kaspersky Security Center Linux қашықтан орнату тапсырмасы көмегімен таңдалған орнату пакеттерін күштеп орнатуды қолдануға болады.

Бұл ретте, құрылғылар айқын түрде (тізіммен) немесе өздері тиесілі болып табылатын Kaspersky Security Center Linux басқару тобын таңдау немесе белгілі бір шарт бойынша құрылғы таңдауларын жасау арқылы көрсетілуі мүмкін. 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.

Бұл орнату тәсілі файлдарды құрылғылардың әрбірінің admin$ әкімшілік ресурсына көшіру жолымен және оларға қосымша қызметтерді қашықтан тіркеу арқылы жүргізіледі. Тек тағайындалған тарату нүктелері Windows басқаратын құрылғыларда әкімшілік ресурстан мәжбүрлі түрде орналастыруды жүзеге асыра алады. Бұл жағдайда, келесі шарттар орындалуы керек:

- Құрылғылар Басқару сервері жағынан немесе тарату нүктесі жағынан қосылуға қолжетімді.
- Желіде құрылғылар үшін атаулардың рұқсаты дұрыс жұмыс істеуі тиіс.
- Басқарылатын құрылғыларда admin$ жалпы қатынастың әкімшілік ресурстары сөндірілмеуі тиіс.
- Құрылғыларда Server жүйелік қызметі іске қосылуы тиіс (әдепкі бойынша бұл қызмет іске қосылған).
- Құрылғыларда Windows құралдарымен құрылғыларға қашықтан қатынасуға арналған келесі порттар ашылуы тиіс: TCP 139, TCP 445, UDP 137, UDP 138.
- Құрылғыларда Simple File Sharing режимі сөндірілуі тиіс.
- Құрылғыларда жергілікті есептік жазбалар үшін бірлескен қатынас және қауіпсіздік моделі *Кәдімгі - жергілікті пайдаланушылар өздері ретінде куәландырылады* (Classic – local users authenticate as themselves) және ешқашан *Қонақтар үшін күйінде куәландырылмайды - жергілікті пайдаланушылар қонақтар ретінде куәландырылады* (Guest only – local users authenticate as Guest).
- Құрылғылар домен мүшелері болуы тиіс немесе құрылғыларда әкімшілік құқықтары бар біріздендірілген есептік жазбалар алдын ала жасалуы тиіс.

Жұмыс топтарында орналасқан құрылғылар "Лаборатория Касперского" техникалық қолдау қызметінің веб-сайтында сипатталған riprep утилитасының көмегімен жоғарыда көрсетілген талаптарға сәйкес келтірілуі мүмкін.

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.

Қолданбаларды күшпен орнату тапсырмаларын жасаудың жеңілдетілген тәсілін қолдануға болады – автоматты түрде орнату. Бұл үшін басқару тобының сипаттарында орнату пакеттерінің тізімінен осы топтың құрылғыларына орнатылуы тиісті 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.

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. Күштеп орнатудың жұмысқа қабілеттілігі үшін мұндай әрбір оқшауланған желінің тарату нүктелерінің болуын қамтамасыз ету қажет.

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. Алайда, бұл орнату тәсілі тарату нүктелері тағайындаған құрылғыларға айтарлықтай жүктеме жасайтынын ескерген жөн. Сондықтан, тарату нүктелері ретінде жоғары өнімді тасушылары бар қуатты құрылғыларды таңдау керек. Сонымен қатар /var/opt/kaspersky/klnagent_srv/ қалтасы бар бөлімдегі бос орын көлемі орнатылатын қолданбалар дистрибутивтерінің жиынтық көлемінен бірнеше есе асып түсуі керек.

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 қолданбасынан) 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.

Желілік агенті орнатылған құрылғыларға қолданбаларды 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 Желілік агенттің көмегімен** 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, қолданбаларды 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 жою мүмкін емес. 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 жою мүмкін емес. 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 енгізу мүмкін емес. 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) қайта іске қосу қажеттілігінде әрекеттің нұсқасын 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.

Қауіпсіздік қолданбасының орнату пакетіндегі дерекқорларды жаңартудың орындылығы

Орналастыру алдында, қауіпсіздік қолданбасының 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.

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.

Инсталляторлар параметрлерін конфигурациялау

Бөлім Kaspersky Security Center Linux инсталляторлар файлдары және орнату параметрлері туралы ақпаратты, сондай-ақ Басқару серверін және Желілік агентті "тыныш" режимде орнату жөніндегі ұсынымдарды қамтиды.

Жалпы ақпарат

Windows жүйесімен жұмыс істейтін құрылғыларға арналған Kaspersky Security Center Linux компоненттерінің орнатушылары Windows Installer технологиясына ендірілген. Инсталлятордың өзегі – MSI пакеті болып саналады. Дистрибутив қаптамасының осындай пішімі Windows Installer технологиясының барлық артықшылықтарын қолдануға мүмкіндік береді: масштабталу, патчтау жүйесін, түрлендіру жүйесін қолдану мүмкіндігі, үшінші тарап шешімдерімен орталықтандырылған түрде орнату мүмкіндігі, операциялық жүйеде тіркелу айқындығы.

Тыныш режимде орнату (жауаптар файлымен)

Желілік агенттің орнату құралында пайдаланушының қатысуынсыз тыныш режимде орнатуға арналған параметрлер жазылған жауаптар файлымен (ss_install.xml) жұмыс істеу мүмкіндігі іске асырылған. ss_install.xml файлы MSI пакетімен бір қалтада орналасқан және тыныш режимде орнату кезінде автоматты түрде қолданылады. Сіз "/s" пәрмен жолының кілті арқылы автоматты түрде орнату режимін қоса аласыз.

Іске қосу мысалы:

```
setup.exe /s
```

Орнатушы қолданбасын тыныш режимде іске қоспас бұрын, Лицензиялық келісімді оқып шығыңыз. Kaspersky Security Center Linux дистрибутиві құрамына Лицензиялық келісім мәтіні бар TXT файлы кірмесе, бұл файлды "Лаборатория Касперского" сайтынан жүктеп алуға болады.

ss_install.xml файлы Kaspersky Security Center Linux инсталляторы параметрлерінің ішкі пішімі болып табылады. Дистрибутивтер құрамында әдепкі бойынша параметрлері бар ss_install.xml файлы жеткізіледі.

ss_install.xml файлын қолмен өзгертудің қажеті жоқ. Орнату пакеттерінің параметрлері Kaspersky Security Center Web Console консолінде өзгертілгенде, бұл файл Kaspersky Security Center Linux құралдары арқылы өзгертіледі.

setup.exe арқылы орнату параметрлерін ішінара конфигурациялау

setup.exe арқылы қолданбаларды орнатуды іске қосу арқылы кез келген MSI сипаттарының мәндерін MSI пакетіне жіберуге болады.

Пәрмен келесідей болады:

Мысалы:
```
/v"PROPERTY_NAME1=PROPERTY_VALUE1 PROPERTYNAME2=PROPERTYVALUE2"
```

Басқару серверін орнату параметрлері

Төмендегі кесте Kaspersky Security Center Linux жүйесін үнсіз режимде орнату кезінде конфигурациялауға болатын сипаттар берілген.

Басқару серверін тыныш режимде орнату параметрлері

Айнымалының атауы	Міндетті	Сипаттамасы	Ықт
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.	Құрылғы немесе
KLSRV_UNATT_PORT_SRV	Жоқ	Басқару серверінің порт нөмірі. Параметр міндетті емес. Әдепкі бойынша, 14000 мәні көрсетілген.	Порт нө
KLSRV_UNATT_PORT_SRV_SSL	Жоқ	Басқару сервері SSL портының нөмірі. Параметр міндетті емес.	Порт нө

		Әдепкі бойынша, 13000 мәні көрсетілген.	
KLSRV_UNATT_PORT_KLOAPI	Жоқ	Басқару сервері KLOAPI портының нөмірі. Параметр міндетті емес. Әдепкі бойынша, 13299 мәні көрсетілген.	Порт нө
KLSRV_UNATT_PORT_GUI	Жоқ	Басқару сервері GUI портының нөмірі. Параметр міндетті емес. Әдепкі бойынша, 13291 мәні көрсетілген.	Порт нө
KLSRV_UNATT_NETRANGETYPE	Жоқ	Басқаруды жоспарлап отырған құрылғылардың шамамен саны. Параметр міндетті емес. Әдепкі бойынша, 1 мәні көрсетілген.	1 1-ден желілік к 2 101-де желілік к 3 1000- желілік к
KLSRV_UNATT_DBMS_TYPE	Иә	Дерекқорды басқару жүйесінің түрі: MySQL (MariaDB) немесе Postgres.	mysql немесе postgre
KLSRV_UNATT_DBMS_INSTANCE	Иә	Дерекқор серверінің IP мекенжайы.	IP мекен
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.	kav
KLSRV_UNATT_DBMS_LOGIN	Иә	Дерекқорға рұқсаты бар пайдаланушының атауы.	
KLSRV_UNATT_DBMS_PASSWORD	Иә	Дерекқорға рұқсаты бар пайдаланушының құпиясөзі.	
KLSRV_UNATT_KLADMINSGROUP	Иә	Қызметтер үшін қауіпсіздік тобының атауы.	kladmi
KLSRV_UNATT_KLSRVUSER	Иә	Басқару сервері қызметін іске қосу үшін есептік жазбаның атауы. Учетная запись должна быть членом группы безопасности, указанной в переменной KLSRV_UNATT_KLADMINSGROUP.	ksc
KLSRV_UNATT_KLSVCUSER	Иә	Басқа қызметтерді іске қосу үшін есептік жазбаның атауы. Учетная запись должна быть членом группы безопасности, указанной в переменной KLSRV_UNATT_KLADMINSGROUP.	ksc
Басқару сервері Kaspersky Security Center Linux ақауларға төзімді кластері ретінде орналастырылатын болс келесі қосымша айнымалыларды қамтуы керек:			
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.	Virtua Немесе Externa
Егер KLFOC_UNATT_CONN_MODE айнымалысы VirtualAdapter мәніне орнатылса, жауап файлы келесі қосым айнымалыларды қамтуы керек:			
KLFOC_UNATT_CONN_MODE_VA_NAME	Осы айнымалылардың бірі қажет	Виртуалды желілік адаптердің атауы.	
KLFOC_UNATT_CONN_MODE_VA_IPV4		Виртуалды желілік адаптердің IP мекенжайы.	IP мекен
KLFOC_UNATT_CONN_MODE_VA_IPV6		Виртуалды желілік адаптердің IPv6 мекенжайы.	IPv6 мек

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 Лицензиялық келісімді толығымен оқып шыққанымды және оның шарттарын қабылдайтынымды растаймын. • 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.
UDPPORT	UDP портының нөмірі.	Сандық мән.
USEPROXY	Прокси-серверді пайдалану керек пе. Үйлесімділік себептері бойынша Желілік агент орнату пакетінің параметрлерінде прокси-серверге қосылу параметрлерін көрсету ұсынылмайды.	• 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 – бұрыннан бар сертификатты белгілеу. Егер бұл нұсқа 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.	• 1 – іске қосу; • басқа мән немесе белгіленбеген – іске қоспау.
NAGENTTAGS	Желілік агентке арналған тег (жауап файлында көрсетілген тегтен басым).	Жол мәні.

Виртуалды инфрақұрылым

Kaspersky Security Center Linux бағдарламасы виртуалды машиналармен жұмыс істеуді қолдайды. Сіз әр виртуалды машинада Желілік агент пен қауіпсіздік қолданбаларын орната аласыз, сонымен қатар виртуалды машиналарды гипервизор деңгейінде қорғай аласыз. Бірінші жағдайда, виртуалды машиналарды қорғау үшін қарапайым қауіпсіздік қолданбасын да, Kaspersky Security for Virtualization Light Agent қолданбасын 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.

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.

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.

Kaspersky Security Center Linux үшін, Желілік агенті орнатылған құрылғылардағы үшінші тарап бағдарламалық жасақтамасы %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\ қалтасына әсер ететін сценарийлер ғана маңызды. 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.

Кез келген мүмкіндік туындаған кезде, %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\ қалтасын Желілік агенті орнатылған құрылғыларға шегіндіруден аулақ болу керек, өйткені деректерді толық қайта синхрондау көп ресурстарды қажет етеді.

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.

Қолданбаларды жергілікті түрде орнату

Бұл бөлімде құрылғыларға тек жергілікті жерде орнатуға болатын қолданбаларды орнату процедурасы сипатталған.

Таңдалған клиент құрылғысында қолданбаларды жергілікті түрде орнатуды жүзеге асыру үшін сіз осы құрылғыда әкімші құқығына ие болуыңыз керек.

Қолданбаларды таңдалған клиент құрылғысына жергілікті түрде орнату үшін:

1. Клиент құрылғысына Желілік агент орнатыңыз және клиент құрылғысы мен Басқару сервері арасында байланыс орнатыңыз.

2. Осы қолданбаларға арналған Нұсқаулықтарда көрсетілген сипаттамаларға сәйкес құрылғыға қажетті қолданбаларды орнатыңыз.

3. Орнатылған қолданбалардың әрқайсысы үшін басқару плагинін әкімшінің жұмыс орнына орнатыңыз.

Сонымен қатар, Kaspersky Security Center Linux жеке орнату пакетін пайдаланып қолданбаларды жергілікті түрде орнату мүмкіндігін қолдайды. Kaspersky Security Center Linux қолданбасы "Лаборатория Касперского" қолданбаларының барлығын орнатуды қолдамайды.

Желілік агентті жергілікті орнату

Құрылғыға Желілік агентті жергілікті түрде орнату үшін:

1. Құрылғыда setup.exe файлын интернет арқылы алынған дистрибутивтен іске қосыңыз.

   Орнату үшін "Лаборатория Касперского" қолданбалары таңдалатын терезе ашылады.

2. Бағдарлама таңдау терезесінде **Kaspersky Security Center 15 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 туралы;
   - құрылғыда орнатылған қолданбалар туралы;
   - жергілікті клиент құрылғысына орнатылатын Microsoft Windows жаңартулары туралы;
   - жергілікті клиент құрылғысында табылған қолданбалардың 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.

Желілік агентті тыныш режимде орнату

Желілік агентті тыныш режимде орнатуға болады, яғни орнату параметрлерін интерактивті түрде енгізбестен. Тыныш орнату үшін Желілік агенттің орнату пакеті (MSI) қолданылады. MSI файлы Kaspersky Security Center Linux қолданбасының дистрибутивінде Packages\NetAgent\exec қалтасында орналасқан.

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 қажет. Әйтпесе, Желілік агент орнатылмайды.

Егер сіз қашықтағы құрылғыларда Kaspersky Security Center 11 және одан кейінгі нұсқасы 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, қолданба орнату оқиғаларының журналын қамтитын $klssinstlib.log файлын жасайды. Бұл файл %windir%\temp немесе %temp% қалтасында сақталады. Ақауларды жою үшін сізге немесе "Лаборатория Касперского" 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.

Қолданбаны басқару плагинін жергілікті түрде орнату

Қолданбаны басқару плагинін орнату үшін,

Басқару консолі орнатылған құрылғыда, осы қолданбаның дистрибутивіне кіретін klcfginst.exe орындалатын файлын іске қосыңыз.

klcfginst.exe файлы Kaspersky Security Center Linux басқара алатын барлық қолданбалардың құрамына кіреді. Орнату, шебер тарапынан сүйемелденеді және параметрлерді конфигурациялауды қажет етпейді.

Қолданбаларды тыныш режимде орнату

Қолданбаны тыныш режимде орнату үшін:

1. Kaspersky Security Center қолданбасының басты терезесін ашыңыз.
2. Консоль ағашының **Қашықтан орнату** қалтасында, **Орнату пакеттері** салынған қалтасында қажетті қолданбаның орнату пакетін таңдаңыз немесе бұл қолданба үшін жаңа орнату пакетін 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 қолданбаға 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.
   - "Лаборатория Касперского" қалған қолданбалары 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, қолданбаны орнату үшін немесе қолданбаның алдыңғы нұсқасын жаңарту үшін қажетті шарт болып табылады.

Қолданбаларды автономды пакеттердің көмегімен орнату

Kaspersky Security Center қолданбалардың 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. Қолданбаны Kaspersky Security Center қатысуынсыз орнату үшін, алынған файлды клиент құрылғысында жергілікті түрде іске қосуға болады.

Қолданбаны автономды орнату пакеті арқылы орнату үшін:

1. Қажетті Басқару серверіне қосыңыз.
2. **Қашықтан орнату** қалтасындағы консоль шежіресінен **Орнату пакеттері** салынған қалтасын таңдаңыз.
3. Жұмыс аймағында қажетті қолданбаның орнату пакетін таңдаңыз.
4. Автономды орнату пакетін жасау процесін келесі тәсілдердің көмегімен іске қосыңыз:
   - Орнату пакетінің мәнмәтіндік мәзірінде **Жеке орнату пакетін жасау** тармағын таңдаңыз.
   - Орнату пакетінің жұмыс аймағындағы **Жеке орнату пакетін жасау** сілтемесі бойынша өтіңіз.

Нәтижесінде, автономды орнату пакетін жасау шебері іске қосылады. Содан кейін, шебердің нұсқауларын орындаңыз.

Шебердің соңғы қадамында автономды орнату пакетін клиент құрылғысына жіберу тәсілін таңдаңыз.

5. Қолданбаның жеке орнату пакетін клиент құрылғысына жіберіңіз.

6. Жеке орнату пакетін клиент құрылғысында іске қосыңыз.

Нәтижесінде, қолданба 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.

Желілік агенттің орнату пакетінің параметрлері

Желілік агенттің орнату пакетінің параметрлерін конфигурациялау үшін:

1. **Қашықтан орнату** қалтасындағы консоль шежіресінен **Орнату пакеттері** салынған қалтасын таңдаңыз.

   Қашықтан орнату қалтасы әдепкі бойынша **Кеңейтілген** қалтасына салынған.

2. Желілік агенттің орнату пакетінің мәнмәтіндік мәзірінде **Сипаттар** тармағын таңдаңыз.

Желілік агенттің орнату пакетінің сипаттары терезесі ашылады.

Жалпы

Жалпы бөлімінде орнату пакеті туралы жалпы ақпарат келтірілген:

- орнату пакетінің атауы;
- орнату пакеті жасалған қолданбаның атауы және нұсқасы;
- орнату пакетінің өлшемі;
- орнату пакетін жасау күні;
- орнату пакетін орналастыру қалтасына апаратын жол.

Параметрлер

Бұл бөлімде Желілік агент орнатылғаннан кейін, оның жұмысын қамтамасыз ету үшін қажетті параметрлерді конфигурациялауға болады. Осы бөлімнің параметрлері тек Windows басқаратын құрылғылар үшін ғана қолжетімді.

Мақсатты қалта параметрлер блогында Желілік агент орнатылатын клиент құрылғысындағы қалтаны таңдауға болады.

- **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.

Төмендегі параметрлер блогында, Желілік агентті қашықтан жою тапсырмасы үшін құпиясөз белгілеуге болады:

- **Жою құпиясөзін пайдалану**

  Параметр қосулы болса, онда **Өзгерту** түймесін басқан кезде қолданбаны жою үшін құпиясөзді енгізуге болады (тек Windows отбасының операциялық жүйелері басқаратын құрылғылардағы Желілік агент үшін қолжетімді).

  Әдепкі бойынша, параметр өшірулі.

- **Күйі**

  Құпиясөз күйі: **Құпия орнатылды** немесе **Құпиясөз орнатылмаған**.

  Әдепкі бойынша, құпиясөз орнатылмаған.

- **Желілік агент қызметін рұқсатсыз өшіруден немесе тоқтатудан қорғау және параметрлердегі өзгерістердің алдын алу**

  Желілік агент басқарылатын құрылғыға орнатылғаннан кейін, осы параметр қосылса, компонентті 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**

  Егер бұл параметр қосулы болса, Басқару серверіне, Желілік агентке, Kaspersky Security Center Web Console консолінe, Exchange ActiveSync ұялы құрылғылар серверіне және iOS MDM серверіне жүктелген барлық жаңартулар мен патчтар 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

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 сервері**

  Басқару сервері орнатылған құрылғының мекенжайы.

- **Порт**

  Қосылым орындалатын порт нөмірі.

- **SSL порты**

  SSL протоколының көмегімен қосылым орындалатын порт нөмірі.

- **Сервер сертификатын пайдалану**

  Егер бұл параметр қосулы болса, Желілік агенттің Басқару серверіне қатынасуын түпнұсқалық растамадан өткізу үшін **Шолу** түймесін басқан кезде көрсетуге болатын сертификат файлы пайдаланылады.

  Егер бұл параметр өшірулі болса, сертификат файлы, Желілік агентті **Сервер мекенжайы** өрісінде көрсетілген мекенжайға алғаш қосқан кезде Басқару серверінен алынады.

  Параметрді өшіру ұсынылмайды, себебі Серверге қосылған кезде Желілік агентпен Басқару серверінің сертификатын автоматты түрде алу қауіпсіз емес болып табылады.

  Әдепкі бойынша, жалауша қойылған.

- **SSL 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 портының нөмірі**

  Өрісте Басқару серверін UDP протоколы бойынша Желілік агентке қосу портының нөмірін көрсетуге болады.

  Әдепкі бойынша, UDP портының нөмірі – 15000.

- Microsoft Windows брандмауэрінде желілік агенттің порттарын ашу

  Параметр қосылса, Желілік агент пайдаланатын UDP порттары Microsoft Windows брандмауэрінің ерекшеліктер тізіміне қосылады.

  Әдепкі бойынша, параметр қосулы.

- Прокси-серверді пайдалану

  Бұл параметр өшірілсе, құрылғыны Басқару серверіне қосу үшін тікелей қосылым пайдаланылады.

  Бұл параметр қосылса, прокси сервер параметрлерін көрсетіңіз:

  - **Прокси-сервердің мекенжайы**
  - **Прокси-сервердің порты**

  Прокси-серверіңіз аутентификацияны қажет етсе, **Прокси-сервердегі түпнұсқалық растама** параметрін қосып, прокси -сервермен қосылым орнатылған есептік жазбаның **Пайдаланушы аты** мен **Құпиясөз** көрсетіңіз. Прокси-сервердегі түпнұсқалық растама үшін ғана талап етілетін ең аз құқықтарға ие есептік жазба деректерін беру ұсынылады.

Үйлесімділік себептері бойынша Желілік агент орнату пакетінің параметрлерінде прокси-серверге қосылу параметрлерін көрсету ұсынылмайды.

Қосымша

Кеңейтілген бөлімінде қосылым шлюзін қалай қолдануға болатынын конфигурациялауға болады. Бұл үшін келесі әрекеттерді орындауға болады:

- Желілік агентті, деректер жіберу уақытында Басқару серверіне қосылу, онымен байланысу және деректерді Желілік агентте қауіпсіз жерде сақтау үшін демилитаризацияланған аймақтағы қосылым шлюзі (DMZ) ретінде қолданыңыз.
- Басқару серверіне қосылу санын азайту үшін Басқару серверіне қосылым шлюзі арқылы қосылыңыз. Бұл жағдайда, қосылым шлюзі ретінде қолданылатын құрылғының мекенжайын **Қосылым шлюзі мекенжайы** өрісіне енгізіңіз.
- Желіңізде виртуалды машиналар болса, Virtual Desktop Infrastructure (VDI) үшін қосылымды конфигурациялаңыз. Бұл үшін келесі әрекеттерді орындаңыз:

  - 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.

  - VDI 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.

Қосымша құрамдастар

Бұл бөлімде Желілік агентпен бірге орнатылатын қосымша құрамдастарды таңдауға болады.

Тегтер

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.

Тексерістер журналы

Бұл бөлімде 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.

Желілік агенттің орнату пакетінің параметрлері, төмендегі кестеде келтірілген нақты операциялық жүйе үшін қолжетімді.

Желілік агенттің орнату пакетінің параметрлері

Сипаттар бөлімі	Windows	Mac	Linux
Жалпы	✓	✓	✓
Параметрлер	✓	–	–
Қосылым	✓	✓ (**Microsoft Windows брандмауэрінде желілік агенттің порттарын ашу** және **Тек прокси-серверді автоматты түрде анықтауды пайдалану** параметрлерінен бөлек)	✓ (**Microsoft Windows брандмауэрінде желілік агенттің порттарын ашу** және **Тек прокси-серверді автоматты түрде анықтауды пайдалану** параметрлерінен бөлек)
Кеңейтілген	✓	✓	✓

Қосымша құрамдастар	✓	✓	✓
Тегтер	✓	✓ (автоматты түрде тег қою ережелерінен бөлек)	✓ (автоматты түрде тег қою ережелерінен бөлек)
Тексерістер журналы	✓	✓	✓

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.

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.

Клиент құрылғыларын басқару

Бұл бөлімде басқару топтарындағы құрылғыларды қалай басқару керектігі сипатталған.

Басқарылатын құрылғының параметрлері

Басқарылатын құрылғының параметрлерін қарап шығу үшін:

1. Қолданбаның негізгі терезесінде **Активтер (құрылғылар)** → **Басқарылатын 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 қолданбаларды соңғы рет жаңарту күні.

  - Басқару серверіне қосылған уақыты

    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-те 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.

- **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:

  - **Операциялық жүйе**
  - **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 қолданбасын орнатқан сәттен бастап (құрылғыны бірінші рет тексеру) немесе қауіп есептегіші соңғы нөлденген сәттен бастап клиент құрылғысында анықталған қауіптердің жалпы саны.

  - **Зарарсыздандырудан 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 Windows жүйесіне арналған Kaspersky Endpoint Security анықтамасында берілген.

Файлдарды тек Kaspersky Endpoint Security for Windows орнатылған басқарылатын құрылғыларда шифрлауға болады.

- **Бағдарлама анықтаған құрылғы күйі** бөлімінде клиент құрылғысында орнатылған басқарылатын қолданба анықтаған құрылғының күйі туралы ақпарат көрсетіледі. Құрылғының бұл күйі Kaspersky Security Center Linux анықтағаннан өзгеше болуы мүмкін.

- **Бағдарламалар**

  Осы қойындыда клиент құрылғысында орнатылған "Лаборатория Касперского" қолданбаларының тізімі көрсетіледі. Қолданба туралы жалпы ақпаратты, құрылғыда болған оқиғалар тізімін және қолданба параметрлерін көру үшін қолданба атауын басуға болады.

- **Белсенді саясаттар мен профильдері**

  Осы қойындыда басқарылатын құрылғыда белсенді 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. Байланыс болмаған жағдайда, күй көрсетілмейді.

- **Оқиғалар**

  Оқиғалар қойыншасында таңдалған клиент құрылғысы үшін Басқару серверінде тіркелген оқиғалар көрсетіледі.

- **Қауіпсіздік мәселелері**

Қауіпсіздік мәселелері қойындысында клиенттік құрылғы үшін қауіпсіздік мәселелерін көруге, өңдеуге және жасауға болады. Қауіпсіздік мәселелері клиент құрылғысында орнатылған "Лаборатория Касперского" басқарылатын қолданбаларының көмегімен автоматты түрде де, әкімші тарапынан қолмен де жасалуы мүмкін. Мысалы, егер пайдаланушы зиянды қолданбаларды құрылғыға жеке алынбалы дискіден үнемі тасымалдап отырса, әкімші қауіпсіздік мәселесін жасауы мүмкін. 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 "Лаборатория Касперского" 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 қолданбалар мен оларға арналған жаңартулардың тізімдемесін көруге, сондай-ақ қолданбалар тізімдемесінің көрсетілуін конфигурациялауға болады.

  Орнатылған қолданбалар 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.

  Қолданба атауын басқан кезде қолданба туралы мәліметтері және сол қолданба 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 экспортталуда

    Файлға экспорттау түймесі арқылы сіз құрылғы өзара әрекеттесетін тарату нүктелерінің тізімін файлға сақтай аласыз. Әдепкі бойынша, қолданба 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.

- **Қолжетімді жаңартулар**. Бұл бөлімде құрылғыда орнатылмаған бағдарламалық жасақтама жаңартуларының тізімін көруге болады.

- **Бағдарламалық жасақтама осалдықтары**. Осы бөлімде клиент құрылғыларында орнатылған үшінші тарап қолданбаларының 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

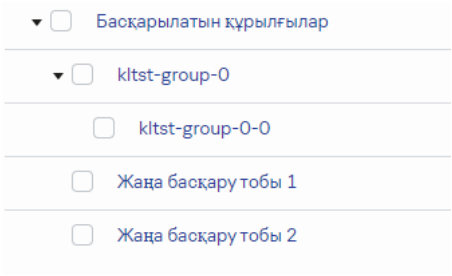
Қолданбаларда таңдалған осалдықтың сипаттарын бөлек терезеде көру үшін тізімдегі қолданбалардағы осалдықтың атын басыңыз. Сипаттар терезесінде келесі әрекеттерді орындауға болады:

- Осы басқарылатын құрылғыдағы қолданбаларда (Басқару консолінде немесе Kaspersky Security Center Web Console веб-консолінде) осалдықты өткізіп жіберу.
- Осалдық үшін ұсынылған түзетулер тізімін қарап шығу.
- Осалдықты түзету үшін бағдарламалық жасақтама жаңартуын қолмен көрсету (Басқару консолінде немесе Kaspersky Security Center Web Console веб-консолінде).
- 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.

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. Қолданбаның негізгі терезесінде **Активтер (құрылғылар)** → **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. Қолданбаның негізгі терезесінде **Активтер (құрылғылар)** → **Топтардың иерархиясы** бөліміне өтіңіз.

2. **Импорттау** түймесін басыңыз.

Нәтижесінде, басқару топтарының құрылымын жасау шебері іске қосылады. Содан кейін, шебердің нұсқауларын орындаңыз.

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 **Активтер (құрылғылар)** → **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 *Қолданбаны 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 таңдау үшін тапсырмаларды қолдану, әдістемеге сәйкес Желілік агенттерді тағайындау керек және т.с.с.

Құрылғыны жылжыту ережелерін жасау

Құрылғыларды басқару топтары бойынша таратылатын құрылғыны жылжыту ережелерін конфигурациялауға болады.

Құрылғыны жылжыту ережесін жасау үшін:

1. Қолданбаның негізгі терезесінде **Активтер (құрылғылар)** → **Жылжыту ережелері** бөліміне өтіңіз.
2. **Қосу** түймесін басыңыз.
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.

- **Белсенді ереже**

  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.

- **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** укажите қойыншасында құрылғылар басқару тобына жылжытылатын кемінде бір өлшемшартті көрсетіңіз.

5. **Сақтау** түймесін басыңыз.

Жылжыту ережелері жасалды. Ол жылжыту ережелерінің тізімінде пайда болады.

Тізімдегі ереже неғұрлым жоғары болса, оның басымдығы да соғұрлым жоғары болады. Жылжыту ережесінің басымдылығын арттыру немесе азайту үшін ережені сәйкесінше тізімде жоғары немесе төмен жылжыту үшін тінтуірді пайдаланыңыз.

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:

   - Қолданбаның негізгі терезесінде **Активтер (құрылғылар)** → **Жылжыту ережелері** бөліміне өтіңіз.

   - Қолданбаның 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.

   - **Белсенді ереже**

     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.

   - **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.
- Желілік агент немесе Басқару сервері сияқты клиент құрылғыларында орнатылған басқарылатын қолданбалар.
- Клиент құрылғылары болып табылатын виртуалды машиналар.

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 қойындысы

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 қойындысы

Бұл қойыншада құрылғыларды жылжыту ережесін ескеретін құрылғылардың желілік деректерін көрсетуге болады:

- **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.

- **Байланыс профилі өзгертілді**

  Келесі мәндердің бірін таңдаңыз:

  - **Иә**. Құрылғыларды жылжыту ережесі тек қосылым профилі өзгертілген клиент құрылғыларына қатысты қолданылады.
  - **Жоқ**. Құрылғыларды жылжыту ережесі тек қосылым профилі өзгермеген клиент құрылғыларына қатысты 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 клиент құрылғыларына 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.

- **Құрылғы иесінің Active Directory қауіпсіздік тобындағы мүшелігі**

  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 қойындысы

Бұл қойындыда клиент құрылғыларында орнатылған басқарылатын қолданбалар 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 тек Желілік агент орнатылмаған клиент құрылғыларына қолданылады.
  - **Мән таңдалмаған**. Шарт қолданылмайды.

- **Бағдарламалар**

Бұл құрылғыларға құрылғыларды жылжыту ережесі қолданылуы үшін клиент құрылғыларында қандай басқарылатын қолданбалар орнатылуы керек екенін көрсетіңіз. Мысалы, **Kaspersky Security Center 15 Желілік агенті** немесе **Kaspersky Security Center 15 Басқару сервері** тармағын таңдаңыз.

Егер сіз басқарылатын қолданбаны таңдамасаңыз, шарт қолданылмайды.

- **Операциялық жүйенің 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.

- **Операциялық жүйенің биттік өлшемі**

  Сіз клиент құрылғыларын операциялық жүйенің бит өлшеміне қарай таңдай аласыз. **Операциялық жүйенің биттік өлшемі** өрісінде келесі мәндердің бірін таңдауға болады:

  - **Белгісіз**
  - **x86**
  - **AMD64**
  - **IA64**

  Клиент құрылғыларының операциялық жүйесінің бит өлшемін тексеру үшін:

  1. Қолданбаның негізгі терезесінде **Активтер (құрылғылар)** → **Басқарылатын құрылғылар** бөліміне өтіңіз.
  2. Оң жақтағы **Бағандар параметрлері** түймесін ( ) басыңыз.
  3. **Операциялық жүйенің биттік өлшемі** параметрін таңдап, **Сақтау** түймесін басыңыз.

     Осыдан кейін, әрбір басқарылатын құрылғы үшін операциялық жүйенің бит өлшемі көрсетіледі.

- **Операциялық жүйенің қызметтік бума нұсқасы**

  Өрісте орнатылған операциялық жүйе пакетінің нұсқасын көрсетуге болады (*X.Y* пішімінде), оның болуы бойынша құрылғыға құрылғыны жылжыту ережесі қолданылады. 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.

- **Операциялық жүйе құрастырылымы**

  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.

- **Операциялық жүйе 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 қойындысы

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**. Жылжытылатын құрылғылар виртуалды машиналар болмауы керек.
  - **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**. Жылжытылатын құрылғылар VDI бөлігі болмауы керек.
  - **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 сақтау орындарына 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.

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. Қолданбаның негізгі терезесінде **Активтер (құрылғылар)** → **Басқарылатын құрылғылар** бөліміне өтіңіз.
2. Тізімнің үстіндегі **Ағымдағы жол:** `<ағымдағы_жол>` сілтемесінен өтіңіз.
3. Ашылған терезеде құрылғыларды қосуды қажет ететін басқару тобын таңдаңыз.
4. **Құрылғылар қосу** түймесін басыңыз.

   Нәтижесінде, құрылғыларды жылжыту шебері іске қосылады.
5. 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.
  - 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: , \ / * ' " ; : & ` ~ ! @ # $ ^ ( ) = + [ ] { } | < > %

6. Басқару тобына қосылатын құрылғылар тізімін қараңыз. Сіз құрылғыларды қосу немесе жою арқылы тізімді өңдей аласыз.
7. 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 мәзірдегі **Активтер (құрылғылар)** → **Басқарылатын құрылғылар** бөлімге өтіңіз, **Ағымдағы жол** өрістегі сілтеме бойынша өтіңіз және сол жақта ашылған панельде басқару тобын таңдаңыз.

- **Тағайындалмаған құрылғылар** тобын ашу үшін негізгі мәзірде **Табу және орналастыру → Тағайындалмаған құрылғылар** бөліміне өтіңіз.

2. Басқару топта кластерлер немесе сервер массивтері болса, **Басқарылатын 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 қолданба сервер массивінің бөлігі екені туралы ақпарат берсе, онда клиент құрылғысы кластер түйініне айналады.

Басқару топта серверлердің кластерлері немесе массивтері болса, **Басқарылатын 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 әрекеттерді орындауға болады, бірақ кластер түйінін жою немесе оны кластерден бөлек басқа басқару топқа 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 "Лаборатория Касперского" 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. Қолданбаның негізгі терезесінде **Активтер (құрылғылар)** → **Басқарылатын 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. Аталған тапсырмалар кластер түйіндерінде орнатылған "Лаборатория Касперского" 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.

"Лаборатория Касперского" қолданбалары

Сипаттар терезесінде кластер түйіндерінде орнатылған "Лаборатория Касперского" қолданбасына қатысты ақпарат пен параметрлері бар қосымша қойындылар 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 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:

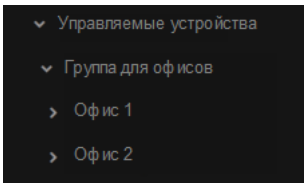
- Желі топологиясын ескере отырып, басқару тобының құрылымын құру. Басқару топтарының құрылымы желінің топологиясын нақты түрде көрсетуге міндетті емес. Желінің бөлектенген бөліктеріне қандай да бір басқару топтарының сай келуі жеткілікті. Тарату нүктелерін автоматты түрде тағайындауды қолдануға немесе 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-ден 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-ден 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-ден 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-ден 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.

Тарату нүктелерін автоматты түрде тағайындау үшін:

1. Басты мәзірде қажетті Басқару сервері атауының жанындағы параметрлер (⚙) белгішесін 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.

Құрылғыны қолмен тарату нүктесі етіп тағайындау үшін:

1. Басты мәзірде қажетті Басқару сервері атауының жанындағы параметрлер (⚙) белгішесін 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.

  - **Көп мекенжайлық жіберуді пайдалану**

    Егер параметр қосулы болса, орнату пакеттерін топ шегіндегі клиент құрылғыларына автоматты түрде тарату үшін көп мекенжайлы IP таратылымы қолданылады.

    Көп мекенжайлы IP таратылымы қолданбаларды орнату пакетінен клиент құрылғылары тобына орнатуға кететін уақытты азайтады, бірақ қолданбаны 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 IPv4 мекенжайы.

  - **Жаңартуларды тарату**

Жаңартулар келесі көздерден басқарылатын құрылғыларға қолданылады:

- Бұл параметр қосулы болса, бұл тарату нүктесі болады.
- Егер параметр өшірулі болса, басқа тарату нүктелері, Басқару сервері немесе "Лаборатория Касперского" 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.

- **Орнату пакеттерін тарату**

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 "Лаборатория Касперского" 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.

- **Push-серверді іске 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.

- **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.

- **Интернетке қосылу параметрлері** бөлімінде интернетке қатынасу параметрлерін конфигурациялауға болады:
  - **Прокси-серверді пайдалану**

    Егер жалауша қойылса, енгізу өрістерінде прокси-серверге қосылу параметрлерін конфигурациялауға 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 түпнұсқалық растама**

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 қолданбаны 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 "Лаборатория Касперского" 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 15111 HTTPS порты арқылы жүзеге асырылады.

- **Порт арқылы HTTPS**

  Басқарылатын құрылғылар KSN прокси-серверіне қосылу үшін қолдана алатын HTTPS портының нөмірі. Әдепкі бойынша, KSN прокси-серверіне қосылу 15111 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.

- Ұялы құрылғылар үшін портты ашу (тек Басқару серверінің SSL түпнұсқалық растамасы)

  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. Байланыс орнатылған кезде, тек Басқару сервері түпнұсқалық растамасын орындайды.

- Ұялы құрылғылар үшін портты ашу (екі жақты SSL түпнұсқалық растамасы)

  Қосылым шлюзінің Басқару сервері мен ұялы құрылғылардың екі жақты түпнұсқалық растамасы үшін пайдаланылатын портты ашуын қаласаңыз, осы параметрді қосыңыз. 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.

- Тарату нүктесі көмегімен домен контроллері сауалнамасын орнатыңыз.

  - Домен контроллерінің сауалнамасы

    Домен контроллері үшін құрылғыларды табу мүмкіндігін қосуға болады.

    Домен контроллері сауалнамасын қосу параметрін таңдасаңыз, сауалнама үшін домен контроллерлерін таңдап, кестені орнатуға 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.

    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.

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. Қолданбаның негізгі терезесінде **Активтер (құрылғылар)** → **Басқарылатын құрылғылар** бөліміне өтіңіз.
2. Басқарылатын құрылғылар тізімінің үстіндегі **Ағымдағы жол** өрісінде сілтеме бойынша өтіңіз.
3. Сол жағында ашылған панельде тағайындалған тарату нүктелерін көргіңіз келетін басқару тобын таңдаңыз.

   Ол үшін **Тарату нүктелері** мәзір тармағын пайдаланыңыз.
4. Қолданбаның негізгі терезесінде **Активтер (құрылғылар)** → **Тарату нүктелері** бөліміне өтіңіз.

5. Басқару тобына тарату нүктелерін қосу үшін **Белгілеу** түймені басыңыз.

6. 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 қолданбаның 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. Басты мәзірде қажетті Басқару сервері атауының жанындағы параметрлер (⚙) белгішесін 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 **Push-серверді іске қосу** 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. **ОК** түймесін басыңыз.

Push сервері таңдалған тарату нүктесінде қосылған.

Құрылғы күйлері туралы

Kaspersky Security Center Linux бағдарламасы әрбір басқарылатын құрылғыға күй тағайындайды. Нақты күйі, пайдаланушы анықтаған шарттардың орындалғанына байланысты. Кейбір жағдайларда Kaspersky Security Center Linux құрылғысына күй тағайындау кезінде құрылғының желіде көрінуін ескереді (төмендегі кестені қараңыз). 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 қолданбасы 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 бағдарлама сканерлеуі ұзақ уақыт орындалмады	Құрылғы желіде көрінеді және құрылғыда қауіпсіздік қолданбасы 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 қолданбасы 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 іске қосу керек	Құрылғы желіде көрінеді, бірақ қолданба таңдалған себептердің біріне байланысты құрылғыны белгіленген	0 минуттан көбірек.

	уақыттан ұзағырақ қайта жүктеуді талап етеді.	
Үйлесімді емес бағдарламалар орнатылды	Құрылғы желіде көрінеді, бірақ Желілік агент орындаған қолданбалық жасақтаманы түгендеу кезінде, құрылғыда үйлесімсіз қолданбалардың 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 қолданбаларда осалдықтар анықталды.	• Критикалық. • Жоғары. • Орташа. • Осалдықты жабу мүмкін болмаса, 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.
Windows Update жаңартуларын іздеу ұзақ уақыт бойы орындалмады	*Windows Update жаңартуларын синхрондау* тапсырмасы көрсетілген уақыттан артық 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.
Ұялы 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 клиент құрылғысында орнатылған "Лаборатория Касперского" басқарылатын қолданбаларының көмегімен автоматты түрде де, әкімші тарапынан қолмен де жасалуы мүмкін.	• Қосқыш өшірулі. • Қосқыш қосулы.
Бағдарлама анықтаған құрылғы күйі	Құрылғының күйін басқарылатын қолданба анықтайды.	• 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 қолданбасы көрсетілген уақыттан артық өшірулі. Бұл жағдайда қауіпсіздік қолданбасының 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 қолданбасы 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 Дерекқорлар ескірген күйін тағайындау үшін *Databases are outdated* шартының мәні өзгермейді.

Kaspersky Security Center Linux қолданбасы құрылғыға күй тағайындаған кезде, кейбір шарттар үшін (жоғарыдағы кестеде "Шарттар сипаттамасы" бағанын қараңыз) құрылғылардың көзге көрінуі ескеріледі. Мысалы, басқарылатын құрылғыға *Критикалық* күйі берілген болса, Дерекқорлар ескірген шарты орындалғандықтан, құрылғы үшін көзге көрінетін болғандықтан, құрылғыға *OK* күйі беріледі.

Құрылғылардың күйлерін ауыстыруды конфигурациялау

Құрылғыға *Критикалық* немесе *Ескерту* күйлерін тағайындау шарттарын өзгерте аласыз.

Құрылғының күйін Критикалық деп өзгерту үшін:

1. Сипаттар терезесін келесі тәсілдердің бірімен ашыңыз:

   - Басқару сервері саясатының мәнмәтіндік мәзіріндегі **Саясаттар** қалтасында **Сипаттар** тармағын таңдаңыз.
   - Басқару тобының мәнмәтіндік мәзірінде **Сипаттар** тармағын таңдаңыз.

2. **Бөлімдер** панелінде ашылған **Сипаттар** терезесінде **Құрылғының күйі** таңдаңыз.
3. **Осы кезде Критикалыққа орнату** бөлімінде тізімнен шартқа жалауша қойыңыз.

   Алайда, сіз ата-ана саясатында бұғатталмаған параметрлерді өзгерте аласыз.

4. Таңдалған шарт үшін өзіңізге қажетті мәнді белгілеңіз.

   Барлық шарттар емес, тек кейбірі үшін мәндерді орнатуыңызға болады.

5. **OK** түймесін басыңыз.

Белгіленген шарттарды орындамаған жағдайда, басқарылатын құрылғыға *Критикалық* күйі тағайындалады.

Құрылғының күйін Ескерту деп өзгерту үшін:

1. Сипаттар терезесін келесі тәсілдердің бірімен ашыңыз:

   - Басқару сервері саясатының мәнмәтіндік мәзіріндегі **Саясаттар** қалтасында **Сипаттар** тармағын таңдаңыз.
   - Басқару тобының мәнмәтіндік мәзірінде **Сипаттар** тармағын таңдаңыз.

2. **Бөлімдер** панелінде ашылған **Сипаттар** терезесінде **Құрылғының күйі** бөлімін таңдаңыз.
3. **Осы кезде Ескертуге орнату** бөлімінде тізімдегі шарт үшін жалауша қойыңыз.

   Алайда, сіз ата-ана саясатында бұғатталмаған параметрлерді өзгерте аласыз.

4. Таңдалған шарт үшін өзіңізге қажетті мәнді белгілеңіз.

   Барлық шарттар емес, тек кейбірі үшін мәндерді орнатуыңызға болады.

5. **OK** 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, **Критикалық күйі бар құрылғылар**, **Қорғаныс өшірілген**, **Белсенді қауіптер анықталды**). Алдын ала анықталған таңдауды жою мүмкін емес. Сондай-ақ, сіз қосымша *оқиғалардың пайдаланушы таңдауларын* жасап, конфигурациялай аласыз.

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 қолданбаның атауы белгіленген болса, онда құрылғы таңдауларына бір уақытта көрсетілген қолданба 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. Қолданбаның негізгі терезесінде **Активтер (құрылғылар)** → **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 **тапсырманыЖаңа тапсырма**Жаңа тапсырма түймесін басуға болады.

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. Қолданбаның негізгі терезесінде **Активтер (құрылғылар)** → **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. Қолданбаның негізгі терезесінде **Активтер (құрылғылар)** → **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** қойындысында **Жаңа шарт** сілтемесіне 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

Егер бұл параметр қосулы болса, белгіленген таңдау шарты кері қайтарылады. Шартқа сәйкес келмейтін барлық құрылғылар таңдауға кіреді.

Әдепкі бойынша, параметр өшірулі.

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 клиент құрылғыларына 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 болып табылатын құрылғылар таңдауға қосылмайды.
  - **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.

- Қосылым 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 ауыстырып қосу 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**. Қолданба 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 қолданбадан құрылғы күйінің сипаттамасы бойынша таңдауға құрылғыларды қосу өлшемшарттарын конфигурациялауға болады:

- Құрылғының күйі

Құрылғы күйлерінің бірін таңдауға болатын ашылмалы тізім: *OK*, *Критикалық* немесе *Ескерту*.

- Нақты уақыт режимінде қорғау 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 шарттар үшін жалаушалар қоюға болады, оларды ұстанған кезде құрылғыға таңдалған күй тағайындалатын болады: *OK, Критикалық* немесе *Ескерту*.

Басқарылатын бағдарламалардың құрамдастарының күйі бөлімінде, басқарылатын қолданбалардың 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 қолданба анықтаған ықтимал мәселелер тізіміне сәйкес құрылғыларды таңдауға қосу өлшемшарттарын конфигурациялауға болады. Егер сіз таңдаған құрылғыда кем дегенде бір мәселе болса, құрылғы таңдауға қосылады. Бірнеше қолданба үшін көрсетілген мәселені таңдағанда, сізде барлық тізімдерде осы мәселені автоматты түрде таңдау мүмкіндігі болады.

Сіз басқарылатын қолданбалар күйлерінің сипаттамасы үшін жалаушаларды қоя аласыз, оларды алған кезде құрылғылар таңдауға қосылады. Бірнеше қолданба үшін көрсетілген күйді таңдағанда, сізде барлық тізімдерде осы күйді автоматты түрде таңдау мүмкіндігі болады.

Жүйе мәліметтері

Операциялық жүйе 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.

- **Операциялық жүйенің қызметтік бума нұсқасы**

  Өрісте орнатылған операциялық жүйе пакетінің нұсқасын көрсетуге болады (*X.Y* пішімінде), оның болуы бойынша құрылғыға құрылғыны жылжыту ережесі қолданылады. Әдепкі бойынша, нұсқаның мәндері белгіленбеген.

- **Операциялық жүйенің биттік өлшемі**

  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.

- **Операциялық жүйе құрастырылымы**

  Бұл параметр тек Windows операциялық жүйелері үшін қолданылады.

  Операциялық жүйенің жинақ нөмірі. Таңдалған операциялық жүйеде тең, анағұрлым ерте немесе анағұрлым кеш жинақ нөмірі болуы керек пе екенін көрсетуге болады. Сондай-ақ, көрсетілгеннен басқа барлық жинақ нөмірлерін іздеуді конфигурациялауға болады.

- **Операциялық жүйе 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**. Ізделетін құрылғылар виртуалды машиналар болмауы керек.
  - **Иә**. Ізделетін құрылғылар виртуалды машиналар болуы керек.

- **Виртуалды машинаның түрі**

  Ашылмалы тізімнен виртуалды машина өндірушісін таңдауға болады.

  Бұл 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**. Ізделетін құрылғылар Virtual Desktop Infrastructure бөлігі болмауы тиіс.
  - **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.

- **Жедел жад өлшемі, МБ түрінде, келесіден бастап**

  Құрылғыдағы жедел жадының ең аз көлемі. Енгізу өрістеріндегі (қоса алғанда) мәндер ауқымына сәйкес келетін жедел жады бар құрылғылар таңдау құрамына енгізіледі.

- **Жедел жад өлшемі, МБ түрінде, келесіге дейін**

  Құрылғыдағы жедел жадының ең көп көлемі. Енгізу өрістеріндегі (қоса алғанда) мәндер ауқымына сәйкес келетін жедел жады бар құрылғылар таңдау құрамына енгізіледі.

Үшінші тарап бағдарламалық жасақтамасы туралы мәліметтер

Бағдарламалар тізімдемесі бөлімінде қандай бағдарламалар орнатылғанына байланысты құрылғыларды таңдауға қосу өлшемшарттарын конфигурациялауға болады:

- **Бағдарлама атауы**

  Қолданбаны таңдауға болатын ашылмалы тізім. Көрсетілген қолданба орнатылған құрылғылар таңдауға қосылады.

- **Бағдарламаның нұсқасы**

  Таңдалған қолданбаның нұсқасын көрсететін енгізу өрісі.

- **Өндіруші**

  Құрылғыда орнатылған қолданбаның өндірушісін таңдауға болатын ашылмалы тізім.

- **Бағдарлама күйі**

  Қолданба күйін таңдауға болатын ашылмалы тізім (*Орнатылған*, *Орнатылмаған*). Таңдалған күйге байланысты, аталған қолданба орнатылған немесе орнатылмаған құрылғылар таңдауға қосылады.

- **Жаңарту бойынша іздеу**

  Егер бұл параметр қосулы болса, іздеу сіз іздеген құрылғыларда орнатылған қолданбаларды 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 қолданбаларын таңдауға болатын ашылмалы тізім. Іздеу кезінде, таңдалған қолданба орнатылған құрылғылар таңдауға қосылады.

- **Бағдарлама тегі**

  Ашылмалы тізімнен қолданба тегін таңдауға болады. Сипаттамада таңдалған тегі бар қолданбалар 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**. Егер бұл нұсқа таңдалса, нәтижелерге Windows Update жаңартуларын басқа көзден алатын құрылғылар кіреді.

«Лаборатория Касперского» бағдарламалары туралы мәліметтер

«Лаборатория Касперского» бағдарламалары бөлімінде құрылғыларды таңдалған басқарылатын қолданбаның негізінде таңдауға қосу өлшемшарттарын конфигурациялауға болады:

- **Бағдарлама атауы**

  Ашылмалы тізімде, "Лаборатория Касперского" қолданбасының атауы бойынша іздеу кезінде құрылғыларды таңдау құрамына қосу өлшемшартын таңдауға болады.

  Тізімде, әкімшінің жұмыс станциясында басқару плагиндері орнатылған қолданбалардың атаулары ғана берілген.

  Егер қолданба таңдалмаса, онда өлшемшарт қолданылмайды.

- **Бағдарламаның нұсқасы**

  Енгізу өрісінде "Лаборатория Касперского" қолданбасы нұсқасының нөмірі бойынша іздеу кезінде құрылғыларды таңдау құрамына қосу өлшемшартын көрсетуге болады.

  Егер нұсқа нөмірі көрсетілмесе, онда өлшемшарт қолданылмайды.

- **Критикалық жаңартудың атауы**

  Енгізу өрісінде қолданба үшін белгіленген жаңарту пакетінің атауы немесе нөмірі бойынша іздеу кезінде құрылғыларды таңдау құрамына қосу өлшемшартын көрсетуге болады.

  Егер өріс толтырылмаса, онда өлшемшарт қолданылмайды.

- **Қолданба күйі**

  Қолданба күйін таңдауға болатын ашылмалы тізім (*Орнатылған*, *Орнатылмаған*). Таңдалған күйге байланысты, аталған қолданба орнатылған немесе орнатылмаған құрылғылар таңдауға қосылады.

- **Модульдердің соңғы жаңарту мерзімін таңдау**

  Бұл параметрдің көмегімен құрылғыларда орнатылған қолданба модульдерінің соңғы рет жаңартылған уақыты бойынша құрылғыларды іздеу өлшемшартын белгілеуге болады.

  Егер жалауша қойылса, енгізу өрістерінде құрылғыларда орнатылған қолданба 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**. Қолданба Kaspersky Security Center Linux басқаратын құрылғыларды таңдауды қамтиды.
  - **Жоқ**. Қолданба Kaspersky Security Center Linux басқармайтын құрылғыларды таңдауды қамтиды.
  - **Мән таңдалмаған**. Өлшемшарт қолданылмайды.

- **Қауіпсіздік бағдарламасы орнатылған**

  Ашылмалы тізімде қауіпсіздік қолданбасы орнатылған құрылғыны таңдау құрамына қосуға болады:

  - **Иә**. Қолданба, қауіпсіздік қолданбасы орнатылған құрылғыларды таңдауға қосады.
  - **Жоқ**. Қолданба, қауіпсіздік қолданбасы орнатылмаған құрылғыларды 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 құрамдастары бөлікшесі Kaspersky Security Center Web Console веб-консолінде сәйкес басқару плагиндері орнатылған қолданба құрамдастарының тізімін қамтиды.

Бағдарлама құрамдастары бөлімінде, таңдалған қолданбаға қатысты құрамдастар нұсқаларының нөмірлеріне сәйкес құрылғыларды іріктеуге қосу өлшемшартын белгілеуге болады:

- **Күйі**

Басқарылатын қолданба 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 қолданбаның таңдалған құрамдасы көрсетілген күйге ие болса, құрылғы құрылғыны таңдауға кіреді.

Қолданбалар жіберген күйлер:

- *Тоқтатылды* – құрамдас өшірілген және қазіргі уақытта жұмыс істемейді.
- *Кідіртілді* – құрамдас, мысалы, пайдаланушы басқарылатын қолданбада 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 қолданбаны іріктеп орнату кезінде орнату құрамдасын таңдамады.
- *Лицензия қолдау көрсетпейді* - Лицензия таңдалған құрамдасқа қолданылмайды.

Басқа күйлерден айырмашылығы, *Құрылғыдан деректер жоқ* күйін басқарылатын қолданба жібермейді. Бұл параметр, қолданбаларда таңдалған құрамдас күйі туралы ақпарат жоқ екенін көрсетеді. Мысалы, бұл жағдай, таңдалған құрамдас құрылғыда орнатылған қолданбалардың 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.

- **Болуы керек**

  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.

- **Болмауы керек**

  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.

- **Құрылғы иесінің Active Directory қауіпсіздік тобындағы мүшелігі**

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. Қолданбаның негізгі терезесінде **Активтер (құрылғылар)** → **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

Бұл бөлімде құрылғы тегтері сипатталған, оларды жасау және өзгерту, сондай-ақ құрылғыларға тегтерді қолмен және автоматты түрде тағайындау бойынша нұсқаулар келтірілген.

Құрылғы тегтері туралы

Kaspersky Security Center Linux құрылғыларға *тегтерді* тағайындауға мүмкіндік береді. Тег дегеніміз – құрылғыларды топтау, сипаттау, іздеу үшін пайдалануға болатын құрылғы идентификаторы. 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 құрылғыларды белгілеу қажет болса, тегтерді қолмен тағайындауға болады. Тегтерді автоматты түрде тағайындау, белгіленген тегтерді тағайындау ережелеріне сәйкес Kaspersky Security Center Linux тарапынан орындалады.

Құрылғыларға тегтерді автоматты түрде тағайындау, белгілі бір ережелерді орындау кезінде жүзеге асырылады. Әрбір тегке бөлек ереже сай келеді. Ережелер құрылғының желілік сипаттарына, операциялық жүйеге, құрылғыда орнатылған қолданбаларға 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.

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. Қолданбаның негізгі терезесінде **Активтер (құрылғылар)** → **Тегтер** → **Құрылғы тегтері** бөліміне өтіңіз.

2. **Қосу** түймесін басыңыз.

   Тег жасау терезесі көрсетіледі.

3. **Тег** өрісінде тег атауын енгізіңіз.

4. Өзгерістерді сақтау үшін **Сақтау** түймесін басыңыз.

Жаңа жасалған тег құрылғы тегтерінің тізімінде пайда болады.

Құрылғы тегтерін өзгерту

Құрылғының тегін қайта атау үшін:

1. Қолданбаның негізгі терезесінде **Активтер (құрылғылар)** → **Тегтер** → **Құрылғы тегтері** бөліміне өтіңіз.

2. Қайта атау қажет болған тегті бөлектеңіз.

   Тегтің сипаттары терезесі ашылады.

3. **Тег** өрісінде тегтің атауын өзгертіңіз.

4. Өзгерістерді сақтау үшін **Сақтау** түймесін басыңыз.

Жаңартылған тег құрылғы тегтері тізімінде пайда болады.

Құрылғы тегтерін жою

Құрылғы тегтерін жою үшін:

1. Қолданбаның негізгі терезесінде **Активтер (құрылғылар)** → **Тегтер** → **Құрылғы тегтері** бөліміне өтіңіз.

2. Тізімнен 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.

Сіз жойған тег, автоматты түрде тег қою ережелерінен автоматты түрде жойылмайды. Тегті жойғаннан кейін, ол құрылғының параметрлері тегтерді белгілеу ережелерінің шарттарына бірінші рет сай келген кезде жаңа құрылғыға тағайындалатын болады.

Егер бұл тег құрылғыға қолданба немесе Желілік агент арқылы тағайындалса, жойылған тег құрылғыдан автоматты түрде жойылмайды. Құрылғыдан тегті жою үшін klscflag утилитасын пайдаланыңыз.

Тег тағайындалған құрылғыларды қарап шығу

Тегтері тағайындалған құрылғыларды қарап шығу үшін:

1. Қолданбаның негізгі терезесінде **Активтер (құрылғылар)** → **Тегтер** → **Құрылғы тегтері** бөліміне өтіңіз.
2. Тағайындалған құрылғылар тізімін қарағыңыз келетін құрылғы үшін тег атауының жанындағы **Құрылғыларды көру** сілтемесінен өтіңіз.

   Құрылғылар тізімінде тек тегтер тағайындалған құрылғылар көрсетіледі.

Құрылғы тегтерінің тізіміне оралу үшін браузердегі **Артқа** түймесін басыңыз.

Құрылғыға тағайындалған тегтерді қарап шығу

Құрылғыға тағайындалған тегтерді қарап шығу үшін:

1. Қолданбаның негізгі терезесінде **Активтер (құрылғылар)** → **Басқарылатын құрылғылар** бөліміне өтіңіз.
2. Тегтерін қарап шығу қажет құрылғыны таңдаңыз.
3. Ашылған құрылғының сипаттар терезесінде **Тегтер** бөлімін таңдаңыз.

   Таңдалған құрылғыға тағайындалған тегтер тізімі көрсетіледі.

Құрылғыға басқа тег тағайындауға немесе бұрын тағайындалған тегті жоюға болады. Сондай-ақ, Басқару серверінде бар барлық құрылғы тегтерін қарап шығуға болады.

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. Өзгерістерді сақтау үшін **Сақтау** түймесін басыңыз.

Таңдалған тег құрылғыға тағайындалады.

Тағайындалған тегті құрылғыдан жою

Құрылғыдан тағайындалған тегті алып тастау үшін:

1. Қолданбаның негізгі терезесінде **Активтер (құрылғылар)** → **Басқарылатын құрылғылар** бөліміне өтіңіз.
2. Тегтерін қарап шығу қажет құрылғыны таңдаңыз.
3. Ашылған құрылғының сипаттар терезесінде **Тегтер** бөлімін таңдаңыз.
4. Алып тастау қажет тегке қарама қарсы жалауша қойыңыз.
5. Тізімнің жоғарғы жағындағы **Тегті белгілеуден бас тарту** түймесін басыңыз.
6. Пайда болған терезеде **Иә** түймесін басыңыз.

Тег құрылғыдан алып тасталады.

Құрылғыдан алынған тег жойылмайды. Қажет болса, оны қолмен жоюға болады.

Қолданбалар немесе Желілік агент арқылы құрылғыға тағайындалған тегтерді қолмен жою мүмкін емес. Бұл тегтерді жою 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:

- Қолданбаның негізгі терезесінде **Активтер (құрылғылар)** → **Тегтер** → **Автоматты түрде тег қою ережелері** бөліміне өтіңіз.
- Қолданбаның негізгі терезесінде **Активтер (құрылғылар)** → **Тегтер** → **Құрылғы тегтері**, содан соң **Автоматты түрде тег қою ережелерін орнату** сілтемесінен өтіңіз.
- Құрылғыға тағайындалған тегтерді қарауға өтіңіз және **Параметрлер** 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 **OK** түймесін басыңыз.
6. Өзгерістерді 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. Ережені келесі шарттар бойынша конфигурациялаңыз: бірнеше шартты 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. Өзгерістерді 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 **Жою** түймесін тағы да басыңыз.

Таңдалған ереже жойылады. Осы ереженің сипаттарында көрсетілген тег тағайындалған барлық құрылғылардан алынады.

Құрылғыдан алынған тег жойылмайды. Қажет болса, оны қолмен жоюға 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 қолданбалардың деректерге қол жеткізуіне жол бермейді.

Желіңізде Kaspersky Endpoint Security for Windows қолданбасы орнатылған Windows операциялық жүйесі бар басқарылатын құрылғылар болса, деректерді шифрлау функциясын пайдалана аласыз. Бұл жағдайда шифрлаудың келесі түрлерін басқаруға болады:

- Windows Server операциялық жүйесі жұмыс істейтін құрылғыларда BitLocker дискісін шифрлау;
- Windows for Workstations операциялық жүйесі жұмыс істейтін құрылғыларда Kaspersky дискісін шифрлау.

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 Windows жүйесіне арналған Kaspersky Endpoint Security анықтамасында берілген.

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,

Қолданбаның 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;

- қолданбаға шифрланған файлға қатынасуға тыйым салынған;
- белгісіз қателер.

Құрылғыларда деректерді шифрлау кезінде туындаған оқиғалар тізімін қарап шығу үшін:

Қолданбаның 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. Қолданбаның негізгі терезесінде **Активтер (құрылғылар) → Басқарылатын 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 қолданбалардың шифрланған файлдарға қатынасуын бұғаттау туралы ақпарат бар. Бұл есеп, авторизацияланбаған пайдаланушы немесе қолданба шифрланған файлдарға немесе қатты дискілерге қатынас алуға әрекеттеніп жатса, пайдалы болады.

Сіз **Бақылау және есеп беру → 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. Қолданбаның негізгі терезесінде **Операциялар → Деректерді шифрлау және қорғау** бөліміне өтіңіз.
3. 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.
4. 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 for Windows бағдарламасы басқарылатын құрылғыға орнатылмаған болса. Сұрауды алғаннан кейін сіз қатынасу кілті файлын жасап, оны пайдаланушыға жібере аласыз. Барлық қолдану нұсқалары және толық нұсқаулар Windows жүйесіне арналған Kaspersky Endpoint Security анықтамасында берілген.

Шифрланған қатты дискіге автономды режимде қатынасу мүмкіндігін ұсыну үшін:

1. Пайдаланушыдан қатынасты сұрау файлын алыңыз (FDERTC кеңейтімі бар файл). Windows жүйесіне арналған Kaspersky Endpoint Security бағдарламасында файлды жасау үшін Windows жүйесіне арналған Kaspersky Endpoint Security анықтамасындағы нұсқауларды орындаңыз.
2. Қолданбаның 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 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.

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 15** қолданбасын 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.

   - **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 қолданбаны 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.

Тапсырманың жұмысы аяқталғаннан кейін, ол жасалған клиент құрылғылары тапсырма параметрлерінде көрсетілген Басқару серверін басқаруға 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.

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. Қолданбаның негізгі терезесінде **Активтер (құрылғылар)** → **Топтардың иерархиясы** бөліміне өтіңіз.
2. Қажетті басқару тобының атауын таңдаңыз.

   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.
5. **Құрылғы 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.

6. **Сақтау** түймесін басыңыз.

Сіздің өзгертулеріңіз сақталды және қолданылды.

Құрылғылардың пайдаланушыларына хабар жіберу

Құрылғылардың пайдаланушыларына хабар жіберу үшін:

1. Негізгі қолданба терезесінде **Активтер (құрылғылар)** → **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.

Тапсырманың жұмысы 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. Негізгі қолданба терезесінде **Активтер (құрылғылар)** → **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. Қажет болса, пайдаланушыға жіберілетін хабарды және өшіру және қайта іске қосу пәрмендері үшін **Бұғатталған сессияларда бағдар. келесі уақыттан кейін мәжбүрлеп жабу (мин)** параметрін көрсетуге болады.

6. Жасалған тапсырманы іске қосыңыз.

Тапсырманың жұмысы аяқталғаннан кейін, пәрмен (қосу, өшіру немесе қайта іске қосу) таңдалған құрылғыларда орындалатын болады.

"Лаборатория Касперского" қолданбаларын орналастыру

Бұл бөлімде Kaspersky Security Center Web Console көмегімен ұйымыңыздағы клиент құрылғыларында "Лаборатория Касперского" қолданбаларын қалай орналастыру керектігі сипатталған.

Сценарий: "Лаборатория Касперского" қолданбаларын орналастыру

Бұл сценарийде Kaspersky Security Center Web Console көмегімен "Лаборатория Касперского" қолданбаларын орналастыру рәсімі сипатталған. Бағдарламаны жылдам іске қосу шеберін және қорғанысты орналастыру шеберін қолдануға немесе барлық қажетті қадамдарды қолмен орындауға болады.

Келесі қолданбалар Kaspersky Security Center Web Console көмегімен орналастыру үшін қолжетімді:

- Kaspersky Endpoint Security for Linux;
- Kaspersky Endpoint Security for Windows.

Кезеңдер

"Лаборатория Касперского" қолданбаларын орналастыру келесі кезеңдерден тұрады:

1. **Қолданбаны 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.

   "Лаборатория Касперского" қолданбаларын Kaspersky Security Center Linux көмегімен кейбір құрылғыларда, мысалы, қашықтағы қызметкерлердің құрылғыларында орната алмасаңыз, қолданбалар үшін жеке орнату пакеттерін жасай аласыз. "Лаборатория Касперского" қолданбаларын 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, "Лаборатория Касперского" сайтынан Желілік агенттің және қауіпсіздік қолданбаларының дистрибутивтерін жүктеп алуға болады. Егер қандай да бір себептермен қолданбаларды қашықтан орнату мүмкін болмаса, қолданбаларды 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 қолданбаның 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.

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. Әдепкі бойынша орнатылған саясат параметрлерін қолдануға болады. Сондай-ақ, сіз әдепкі бойынша белгіленген саясат параметрлерін кез келген уақытта өз талаптарыңызға сай өзгерте аласыз.

6. **Нәтижелерді тексеру**

   Орналастырудың сәтті орындалғанына көз жеткізіңіз: әрбір қолданба үшін саясаттар мен тапсырмалар жасалған және осы қолданбалар басқарылатын құрылғыларға орнатылған.

Нәтижелер

Сценарийдің аяқталуы арқасында:

- Таңдалған қолданбалар үшін барлық қажетті саясаттар мен тапсырмалар жасалады.
- Тапсырмаларды іске қосу кестесі өз талаптарыңызға сай конфигурацияланады.
- Таңдалған клиент құрылғыларында таңдалған қолданбалар орналастырылған немесе орналастырылуға жоспарланған.

"Лаборатория Касперского" қолданбаларын басқаруға арналған плагинін қосу

Kaspersky Endpoint Security for Linux немесе Kaspersky Endpoint Security for Windows сияқты "Лаборатория Касперского" қолданбасын орналастыру үшін сол қолданба үшін басқарудың веб-плагинін жүктеп алуыңыз керек.

"Лаборатория Касперского" қолданбаларының веб-плагиндерін жүктеу үшін:

1. Қолданбаның негізгі терезесінде **Параметрлер** → **Веб-плагиндер** бөліміне өтіңіз.
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 "Лаборатория Касперского" Техникалық қолдау қызметі веб-сайтынан жүктеп ала аласыз.

Файлдағы басқару веб-плагинді жүктеу 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.

"Лаборатория Касперского" қолданбаларына арналған орнату пакеттерін жүктеп алу және жасау

Басқару сервері интернетке қатынаса алса, сіз "Лаборатория Касперского" веб-серверлерінен "Лаборатория Касперского" қолданбаларының орнату пакеттерін жасай аласыз.

"Лаборатория Касперского" қолданбаларына арналған орнату пакеттерін жүктеп алу және жасау үшін:

1. Келесі әрекеттердің бірін орындаңыз:

   - Қолданбаның негізгі терезесінде **Табу және орналастыру** → **Орналастыру және тағайындау** → **Орнату пакеттері** бөліміне өтіңіз.
   - Қолданбаның негізгі терезесінде **Операциялар** → **Қоймалар** → **Орнату пакеттері** бөліміне өтіңіз.

   Сондай-ақ, "Лаборатория Касперского" қолданбаларына 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.

2. **Қосу** түймесін басыңыз.

   Орнату пакетін жасау шебері іске қосылады. Шебердің жұмысын жалғастыру үшін **Келесі** түймесін басыңыз.

3. **«Лаборатория Касперского» бағдарламасы үшін орнату пакетін жасаңыз** таңдаңыз.

"Лаборатория Касперского" веб-серверлерінде қолжетімді орнату пакеттерінің тізімі көрсетіледі. Тізімде тек Kaspersky Security Center Linux қолданбасының ағымдағы нұсқасымен үйлесімді қолданбалардың орнату пакеттері бар.

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.

5. Ақпаратпен танысып, **Орнату пакетін жүктеп алу және жасау** түймесін басыңыз.

   Дистрибутив орнату пакетіне түрлендіре алмаса, онда **Орнату пакетін жүктеп алу және жасау** түймесінің орнына **Дистрибутивті жүктеп алу** түймесі көрсетіледі.

   Орнату пакетін Басқару серверіне жүктеп салу басталады. Шебер терезесін жабуға немесе нұсқаулықтың келесі қадамына өтуге болады. Шеберді жапсаңыз, жүктеу процесі фондық режимде жалғасады.

   Орнату пакетін жүктеп салу процесін қадағалағыңыз келсе:

   a. Қолданбаның негізгі терезесінде **Операциялар → Қоймалар → Орнату пакеттері → Орындалып жатыр ()** бөліміне өтіңіз.

   b. Кестенің **Жүктеп алудың орындалу барысы** және **Жүктеп алу күйі** бағандарында әрекеттің орындалу барысын бақылаңыз.

   Процесс аяқталғаннан кейін, орнату пакеті **Жүктеп алынды** қойыншасындағы тізімге қосылады. Егер жүктеу процесі тоқтап, жүктеу күйі **Түпкі пайдаланушының лицензиялық келісімін қабылдау** болып өзгерсе, орнату пакетінің атауын басып, нұсқаулықтың келесі қадамына өтіңіз.

   > 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. Кейбір "Лаборатория Касперского" қолданбаларын жүктеу процесі 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.

7. 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.

Файлдан орнату пакетін жасау

Сіз конфигурацияланған орнату пакеттерін пайдалана аласыз:

- клиент құрылғыларына кез келген қолданбаны (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, қолданбаны тыныш режимде орнату үшін.

Пайдаланушы орнату пакетін жасау үшін:

1. Келесі әрекеттердің бірін орындаңыз:
   - Қолданбаның негізгі терезесінде **Табу және орналастыру** → **Орналастыру және тағайындау** → **Орнату пакеттері** бөліміне өтіңіз.
   - Қолданбаның негізгі терезесінде **Операциялар** → **Қоймалар** → **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. **Файлдан орнату пакетін жасау** тармағын таңдаңыз.
4. Орнату пакетінің 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.
6. Егер сіз "Лаборатория Касперского" қолданбасының файлын көрсеткен болсаңыз, сізге сол қолданбаның Лицензиялық келісімін оқып, қабылдау ұсынылуы мүмкін. Жалғастыру үшін Лицензиялық келісімнің шарттарын қабылдауыңыз қажет. **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 қажет. 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.

   Қолданбаны орнату пакетінен тыныш режимде орнату үшін пәрмен жолының параметрлерін көрсетуге болады. Пәрмен жолының параметрлерін көрсету міндетті емес.

   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.
  - **Көзі**. Қолданба өндірушісінің атауы.
  - **Бағдарлама**. Пайдаланушы орнату пакетіне қапталған қолданбаның атауы.
  - **Нұсқа**. Қолданба нұсқасы.
  - **Тіл**. Пайдаланушы орнату пакетіне қапталған қолданбаның тілі.
  - **Өлшемі (МБ)**. Орнату пакетінің өлшемі.
  - **Операциялық жүйе**. 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 қолданбаларды 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 (installer.exe) болып саналады. Қолданбаны Kaspersky Security Center Linux қатысуынсыз орнату үшін, алынған файлды клиент құрылғысында жергілікті түрде іске қосуға болады. "Лаборатория Касперского" қолданбалары үшін де, үшінші тарап қолданбалары үшін де жеке орнату пакетін жасауға болады. Үшінші тарап қолданбалары үшін жеке орнату пакетін жасау үшін, пайдаланушы орнату пакетін жасау керек.

Жеке орнату пакетінің үшінші тұлғаларға қолжетімсіз болғанына көз жеткізіңіз.

Жеке орнату пакетін жасау үшін:

1. Келесі әрекеттердің бірін орындаңыз:

- Қолданбаның негізгі терезесінде **Табу және орналастыру** → **Орналастыру және тағайындау** → **Орнату пакеттері** бөліміне өтіңіз.
- Қолданбаның негізгі терезесінде **Операциялар** → **Қоймалар** → **Орнату пакеттері** бөліміне өтіңіз.

Басқару серверінде қолжетімді орнату пакеттерінің тізімі көрсетіледі.

2. Орнату пакеттері тізімінен пакетті таңдап, тізімнің үстінде **Орналастыру** түймесін басыңыз.
3. **Автономды пакетті пайдалану** параметрін таңдаңыз.

   Нәтижесінде, автономды орнату пакетін жасау шебері іске қосылады. Шебердің жұмысын жалғастыру үшін **Келесі** түймесін басыңыз.
4. Таңдалған қолданбамен бірге Желілік агентті орнату керек болса, **Желілік агентті осы бағдарламамен бірге орнату** параметрі қосылғанына көз жеткізіңіз.

   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 қолданба үшін жеке орнату пакеті Басқару серверінде бұрыннан бар болса, шебер бұл туралы хабарды көрсетеді. Бұл жағдайда, келесі әрекеттердің бірін таңдауыңыз қажет:

   - **Жеке орнату пакетін жасау**. Қолданбаның жаңа нұсқасы үшін жеке орнату пакетін жасағыңыз келсе және сіз бұған дейін жасаған қолданбаның 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 қолданба 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 ешбір басқару тобына жылжытқыңыз келмесе, осы параметрді өзгертпеңіз.

   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.
6. Жеке орнату пакетін жасау процесі аяқталғаннан кейін, **Дайын** түймесін басыңыз.

   Жеке 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.

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.

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.

Linux үшін Желілік агентті тыныш режимде орнату мақсатында:

1. Linux операциялық жүйесі бар қажетті құрылғыны қашықтан орнату үшін дайындап қойыңыз. Кез келген лайықты пакеттерді басқару жүйесінің көмегімен .deb немесе .rpm Желілік агент пакетін қолдана отырып, қашықтан орнату пакетін жүктеңіз және жасаңыз.

2. SUSE Linux Enterprise Server 15 операциялық жүйесі бар құрылғыларға Желілік агентті орнатқыңыз келсе, алдымен Желілік агентті орнату үшін insserv-compat пакетін орнатыңыз.

3. Лицензиялық келісімді оқып шығыңыз. Лицензиялық келісімнің шарттарын түсініп, қабылдаған жағдайда ғана төмендегі қадамдарды орындаңыз.

4. Жауап файлының толық атауын (жолды қоса) енгізу арқылы KLAUTOANSWERS ортасының айнымалы мәнін белгілеңіз, мысалы:

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

5. Ортаның айнымалысында көрсетілген каталогта жауап файлын (TXT пішімінде) 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 қажет:

- 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	Ықтим
KLNAGENT_SERVER	Иә	Толық домендік атау (FQDN) немесе IP мекенжайы ретінде ұсынылған Басқару сервері атауын қамтиды.	Құрылғын немесе IP
KLNAGENT_AUTOINSTALL	Иә	Тыныш орнату режимі қосылғанын анықтайды.	1 – тыныш қосулы; ор пайдалану ешқандай ұсынылма Басқасы – режим өш кезінде па әрекеттер мүмкін.
EULA_ACCEPTED	Иә	Пайдаланушы Желілік агенттің Лицензиялық келісімін қабылдап-қабылдамайтынын анықтайды; егер айнымалы көрсетілмесе, оны Лицензиялық келісімді қабылдамау деп түсіндіруге болады.	1 – Мен Ли келісімді т оқып шық оның шарт қабылдайт растаймы Басқа мән белгіленбе Лицензиял шарттары келіспейм жүзеге ас
KLNAGENT_PROXY_USE	Жоқ	Басқару серверімен орнатылған қосылым прокси-сервердің параметрлерін қолданады ма екенін анықтайды. Әдепкі бойынша, 0 мәні көрсетілген.	1 – прокси параметрл қолданыла Басқасы – сервер па қолданылм
KLNAGENT_PROXY_ADDR	Жоқ	Басқару серверімен байланыс орнату үшін қолданылатын прокси-сервер мекенжайын анықтайды.	Құрылғын немесе IP
KLNAGENT_PROXY_LOGIN	Жоқ	Прокси-серверге кіру үшін қолданылатын пайдаланушы атын анықтайды.	Кез келген қолданыст пайдалану
KLNAGENT_PROXY_PASSWORD	Жоқ	Прокси-серверге кіру үшін қолданылатын пайдаланушы құпиясөзін анықтайды.	Операция әріптер ме пішіммен р

			құпиясөзд жиынтығы
KLNAGENT_VM_VDI	Жоқ	Динамикалық виртуалды машиналарды жасау үшін кескінге Желілік агенттің орнатылып-орнатылмағанын анықтайды.	1 – Желілік динамикал машинала үшін қолда кескінге о Басқасы – барысынд қолданылм
KLNAGENT_VM_OPTIMIZE	Жоқ	Желілік агенттің параметрлері гипервизор үшін оңтайлы ма екенін анықтайды.	1 – Желілік әдепкі бой жергілікті гипервизо қолдануды оңтайланд алатындай өзгертілге
KLNAGENT_TAGS	Жоқ	Желілік агенттің үлгісіне тағайындалған тегтерді атап көрсетеді.	Нүктелі үт бөлінген б бірнеше т
KLNAGENT_UDP_PORT	Жоқ	Желілік агент қолданатын UDP портын анықтайды. Әдепкі бойынша, 15000 мәні көрсетілген.	Кез келген қолданыст нөмірі.
KLNAGENT_PORT	Жоқ	Желілік агент қолданбайтын портты (TLS емес) анықтайды. Әдепкі бойынша, 14000 мәні көрсетілген.	Кез келген қолданыст нөмірі.
KLNAGENT_SSLPORT	Жоқ	Желілік агент қолданбайтын портты (TLS емес) анықтайды. Әдепкі бойынша, 13000 мәні көрсетілген.	Кез келген қолданыст нөмірі.
KLNAGENT_USESSL	Жоқ	Қосылу үшін тасымал деңгейінің (TLS) қауіпсіздігі қолданылады ма екенін анықтайды.	1 (әдепкі б TLS қолда Басқасы – қолданылм
KLNAGENT_GW_MODE	Жоқ	Қосылым шлюзі пайдаланылады ма екенін анықтайды.	1 (әдепкі б ағымдағы өзгертілме қоңырау к қосылым ш көрсетілм 2 – қосыль қолданылм

			3 – қосыль қолданыла 4 – Желілі демилитар аймақта (D шлюзі рет пайдаланы
KLNAGENT_GW_ADDRESS	Жоқ	Қосылым шлюзінің мекенжайын анықтайды. Мән, KLNAGENT_GW_MODE = 3 болса ғана қолданылады.	Құрылғыны немесе IP
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 – Желілік орнатқанн пайдалану құрылғы ие тіркеуге ар утилита іс Басқа – өш

6. Желілік агентті орнату:

- 32 биттік операциялық жүйесі бар құрылғыға RPM пакетінен Желілік агентті орнату үшін келесі пәрменді орындаңыз:
  `# rpm -i klnagent-<build number>.i386.rpm`
- 64 биттік операциялық жүйесі бар құрылғыда RPM пакетінен Желілік агент орнату үшін келесі пәрменді орындаңыз:
  `# rpm -i klnagent64-<build number>.x86_64.rpm`
- 64 биттік операциялық жүйесі бар ARM архитектурасы құрылғысында RPM пакетінен Желілік агентті орнату үшін келесі пәрменді орындаңыз:
  `# rpm -i klnagent64-<build number>.aarch64.rpm`
- 32 биттік операциялық жүйесі бар құрылғыға DEB пакетінен Желілік агентті орнату үшін келесі пәрменді орындаңыз:
  `# apt-get install ./klnagent_<build number>_i386.deb`
- 64 биттік операциялық жүйесі бар құрылғыда DEB пакетінен Желілік агент орнату үшін келесі пәрменді орындаңыз:
  `# apt-get install ./klnagent64_<build number>_amd64.deb`
- 64 биттік операциялық жүйесі бар DEB архитектурасы құрылғысында RPM пакетінен Желілік агентті орнату үшін келесі пәрменді орындаңыз:
  `# apt-get install ./klnagent64_<build number>_arm64.deb`

Linux үшін Желілік агентті орнату тыныш режимде басталады; пайдаланушыдан процесс кезінде ешқандай әрекеттерді орындау сұралмайды.

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.

Алдын ала шарттар:

- Linux Желілік агентін орнатқыңыз келетін құрылғыда қолдау көрсетілетін Linux дистрибутивтерінің бірі жұмыс істейтініне көз жеткізіңіз.
- "Лаборатория Касперского" сайтынан Желілік агентті орнату файлын жүктеп алыңыз.

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. Қолданба кілті үшін директория жасаңыз:

   ```
   mkdir -p /etc/digsig/keys/legacy/kaspersky/
   ```

4. Қолданба кілтін алдыңғы қадамда жасалған /opt/kaspersky/ksc64/share/kaspersky_astra_pub_key.gpg каталогына 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.

5. Дискілердің жедел жадын жаңартыңыз:

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

   Жүйені қайта жүктеңіз.

6. Linux операциялық жүйесі бар кез келген құрылғыға ортақ дайындық қадамдарын орындаңыз.

Құрылғы дайындалды. Енді желілік агентті орнатуды бастауға болады.

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 қолданбаның атауынан және нұсқасынан автоматты түрде жасалатын жеке орнату пакетінің атауы.
- **Бағдарлама атауы**. Жеке орнату пакетіне кіретін қолданбаның 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.

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.

Орнату пакеттерін қосалқы Басқару серверлеріне тарату

Kaspersky Security Center Linux қолданбасы сізге "Лаборатория Касперского" қолданбалары үшін және үшінші тарап қолданбалары үшін орнату пакеттерін жасауға, сондай-ақ орнату пакеттерін клиент құрылғыларына таратуға және пакеттерден қолданбалар 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 қолданбаларды қашықтан орната аласыз.

Орнату пакеттерін қосалқы Басқару серверлеріне тарату үшін:

1. Қосалқы Басқару серверлері негізгі Басқару серверіне қосылғанына көз жеткізіңіз.
2. Негізгі қолданба терезесінде **Активтер (құрылғылар)** → **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.

Linux операциялық жүйесімен жұмыс істейтін құрылғыны дайындау және Linux операциялық жүйесі бар құрылғыға Желілік агентті қашықтан орнату

Желілік агентті орнату екі қадамнан тұрады:

- Linux операциялық жүйесі бар құрылғыны дайындау
- Желілік агентті қашықтан орнату

Linux операциялық жүйесі бар құрылғыны дайындау

Linux операциялық жүйесі бар құрылғыны Желілік агентті қашықтан орнатуға дайындау үшін:

1. Linux операциялық жүйесі бар мақсатты құрылғыда келесі бағдарламалық жасақтама орнатылғанына көз жеткізіңіз:
   - Sudo.
   - Perl тілі интерпретаторының 5.10 немесе одан жоғары нұсқасы.
2. Құрылғының конфигурациясын тексеріңіз:
   a. Құрылғыға SSH арқылы қосылуға болатындығын тексеріңіз (мысалы, PuTTY қолданбасы).

      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. Құрылғыға қосылу үшін пайдаланылатын пайдаланушы есептік жазбасы үшін sudo сұрауы құпиясөзін өшіріңіз.

   c. sudoers конфигурациялық файлын ашу үшін sudo `visudo` пәрменін қолданыңыз.

      Ашылған файлда, `%sudo` (немесе CentOS операциялық жүйесін қолдансаңыз, `%wheel`) мәнінен басталатын жолды табыңыз. Осы жолдың астында келесіні көрсетіңіз: `<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`

   d. sudoers файлын сақтаңыз және жабыңыз.

e. SSH арқылы құрылғыға қайта қосылыңыз және `sudo whoami` пәрменінің көмегімен, sudo қызметі құпиясөзді қажет етпейтінін тексеріңіз.

3. `/etc/systemd/logind.conf` файлын ашыңыз және 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`.

   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.

   Өзгертілген параметрді қолдану үшін, Linux басқаруымен жұмыс істейтін құрылғыны қайта іске қосыңыз немесе келесі пәрменді іске қосыңыз:

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

4. SUSE Linux Enterprise Server 15 операциялық жүйесі бар құрылғыларға Желілік агентті орнатқыңыз келсе, алдымен Желілік агентті орнату үшін insserv-compat пакетін орнатыңыз.

5. 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.

Желілік агентті қашықтан орнату

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 (қолданбалар, 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. Қолданба интерфейсін пайдаланып немесе "Лаборатории Касперского" веб-сайтынан Желілік агентті орнату пакетін жүктеп алыңыз.

   c. Қашықтан орнату пакетін жасау үшін келесі файлдарды пайдаланыңыз:

      - klnagent.kpd;
      - akinstall.sh;
      - Желілік агенттің deb немесе rpm пакеті.

2. Қолданбаны 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. Қолданбаны қашықтан орнату тапсырмасын іске қосыңыз. Қоршаған ортаны сақтау үшін `su` пәрменіне арналған параметрді пайдаланыңыз: `-m, -p, --preserve-environment`.

SSH протоколын пайдалану арқылы Желілік агентті 20-шы нұсқадан төмен емес Fedora операциялық жүйесі бар құрылғыларға орнатып жатсаңыз, орнату сәтсіз аяқталуы мүмкін. Бұл жағдайда, Желілік агентті /etc/sudoers файлына сәтті орнату үшін Defaults requiretty параметріне түсініктеме беріңіз (оны талданған кодтан жою үшін түсініктеме синтаксисіне салыңыз). Defaults requiretty параметрі SSH арқылы қосылу кезінде неліктен мәселе тудыруы мүмкін екендігі туралы толық сипаттаманы Bugzilla мәселелерін қадағалау жүйесінің сайтынан таба аласыз.

Қашықтан орнату тапсырмасын пайдаланып қолданбаларды орнату

Kaspersky Security Center Linux қашықтан орнату тапсырмаларын пайдаланып құрылғыларға қолданбаларды қашықтан орнатуға мүмкіндік береді. Тапсырмалар шебердің көмегімен жасалады және құрылғыларға тағайындалады. Құрылғыларға 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.

Қашықтан орнату тапсырмасы Желілік агент орнатылмаған құрылғыда дұрыс жұмыс істеуі үшін TCP 139 және 445, UDP 137 және 138 порттарын ашу қажет. Бұл порттар әдепкі бойынша доменге қосылған барлық құрылғыларда ашық. Олар Құрылғыларды орнатуға дайындау утилитасы көмегімен автоматты түрде ашылады.

Қолданбаларды қашықтан орнату

Бұл бөлімде басқару тобындағы құрылғыларға, белгілі бір мекенжайлары бар құрылғыларға немесе құрылғы таңдауларына қолданбаны қашықтан орнату туралы ақпарат бар.

Қолданбаны таңдалған құрылғыларға орнату үшін:

1. Негізгі қолданба терезесінде **Активтер (құрылғылар)** → **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.

- **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 қолданбаны 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.

Қолданбаны қашықтан орнату тапсырмасы көрсетілген құрылғылар үшін жасалды. **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. **Орнату пакеттері** қадамында келесі параметрлерді көрсетіңіз:

   - Орнатылуы қажет қолданбаның орнату пакетін **Орнату пакетін таңдау** өрісінен таңдаңыз.

   - **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 қолданбаны (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 қолданбаны 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 қолданбасын 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 қолданбасын іске қоспайды. *Қолданбаны қашықтан орнату* тапсырмасын қайта іске қосу үшін **Орнату әрекеттерінің максималды саны** параметрінің мәнін арттырыңыз және тапсырманы орындаңыз. Сондай-ақ, сіз *Қолданбаны қашықтан орнату* тапсырмасының басқасын жасай аласыз.

- Деректерді бір "Лаборатория Касперского" қолданбасынан екіншісіне тасымалдап жатсаңыз және ағымдағы қолданбаңыз құпиясөзбен қорғалған болса, **Ағымдағы Kaspersky қолданбасын жоюға арналған құпиясөз** өрісіне құпиясөзді енгізіңіз. Ағымдағы "Лаборатория Касперского" қолданбасы деректерді тасымалдау кезінде жойылатынын ескеріңіз.

  Ағымдағы Kaspersky қолданбасын жоюға арналған құпиясөз өрісі, **Орнату пакетін мәжбүрлеп жүктеп алу** параметрлер тобында **Желілік агенттің көмегімен** параметрін таңдаған жағдайда ғана қолжетімді болады.

  Жою құпиясөзін тек *Қолданбаны 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 қолданбаларды 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 қолданба клиент құрылғысында орнатылған болса, қайта орнатылмайды.

    Егер бұл параметр өшірулі болса, қолданба 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 қолданбасы файлдарды жібермейді және қолданбаны орнатуға тырыспайды. Мысалы, әртүрлі операциялық жүйелері бар құрылғыларды қамтитын басқару тобының құрылғыларынан кейбір қолданбаларды орнату үшін басқару тобына орнату тапсырмасын тағайындауға болады, содан кейін қажеттіден басқа операциялық жүйесі бар құрылғыларды өткізіп жіберу үшін осы параметрді қосуға болады.

  - **Active Directory топтық саясаттарында бума 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 қолданбалар клиент құрылғысын қайта жүктеуге мүмкіндік бермеуі мүмкін. Мысалы, егер мәтіндік редакторда құжатпен жұмыс жасалса және өзгертулер сақталмаса, қолданба құрылғыны қайта жүктеуге мүмкіндік бермейді.

    Егер бұл параметр қосулы болса, құрылғыны қайта іске қоспас бұрын бұғатталған құрылғылардағы мұндай қолданбалар 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 қолданбаларды қолмен жауып, сол құрылғыларды қайта іске қосуы керек.

    Әдепкі бойынша, параметр өшірулі.

- Қолданбаны орнатқыңыз келетін құрылғыларды таңдаңыз:

- **Барлық құрылғыларда орнату**

  Қолданба 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**

  Қолданба 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.

7. Шебердің осы қадамында қолданбаларды орнату кезінде құрылғыны қайта жүктеу талап етілетін көрсетіңіз:

   - **Құрылғыны қайта іске қоспау**

     Осы нұсқа таңдалған болса, онда қауіпсіздік қолданбасы орнатылғаннан кейін, құрылғы қайта іске қосылмайды.

   - **Құрылғыны қайта іске қосу**

     Осы нұсқа таңдалған болса, онда қауіпсіздік қолданбасы орнатылғаннан кейін, құрылғы қайта іске қосылады.

8. Қажет болса, кезең-кезеңімен **Құрылғыларға қатынасу үшін есептік жазбаларды таңдау** қадамында *Қолданбаны қашықтан орнату* тапсырмасын орындау үшін пайдаланылатын есептік жазбаларды қосыңыз:

   - **Есептік жазба қажет емес (Желілік агент орнатылды)**

     Егер бұл нұсқа таңдалса, қолданба 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, қолданбаны орнату үшін пайдаланушы есептік жазбасын көрсетуге болады.

Орнату қолданбасы іске қосылатын пайдаланушы есептік жазбасын көрсету үшін **Қосу** түймесін басыңыз, **Жергілікті есептік жазба** таңдаңыз және пайдаланушы есептік жазбасының есептік 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.

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 қолданба көрсетілген құрылғылар жиынтығына орнатылады.

Қосалқы Басқару серверлеріне қолданбаларды орнату

Қолданбаны қосалқы Басқару серверлеріне орнату үшін:

1. Өзіңізге қажетті қосалқы Басқару серверлерін басқаратын Басқару серверіне қосылыңыз.

2. Орнатылған қолданбаға 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**Орнату пакетін таратутапсырманы жасаңыз**.

3. Қосалқы Басқару серверлеріне қолданбаны қашықтан орнату тапсырмасын жасаңыз. **Қосалқы Басқару серверіне бағдарламаны қашықтан орнату** тапсырма түрін таңдаңыз.

   Жаңа тапсырма жасау шебері жұмысының нәтижесінде таңдалған қосалқы Басқару серверлеріне таңдалған қолданбаны 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 қолданба қосалқы Басқару серверлеріне орнатылады.

Unix басқаруымен жұмыс істейтін құрылғыларда қашықтан орнату параметрлерін көрсету

Қолданбаны 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. Негізгі қолданба терезесінде **Активтер (құрылғылар)** → **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 қолдану мүмкін 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. Қолданба орнату пакетін қалтаға орналастырады және орнату процедурасын бастайды.
5. **Сақтау** түймесін басыңыз.

Көрсетілген тапсырма параметрлері сақталған.

Үшінші тарап қауіпсіздік қолданбаларын алмастыру

"Лаборатория Касперского" қауіпсіздік қолданбаларын Kaspersky Security Center Linux құралдарымен орнату үшін, орнатылатын қолданбамен үйлеспейтін үшінші тарап қолданбасын жою қажет болуы мүмкін. Kaspersky Security Center Linux, үшінші тарап қолданбаларын жоюдың бірнеше тәсілін ұсынады.

Қолданбаны қашықтан орнатуды кезінде үйлесімсіз қолданбаларды жою

Қорғанысты орналастыру шеберінде қауіпсіздік қолданбасын қашықтан орнату кезінде **Үйлесімді емес бағдарламаларды автоматты түрде жою** параметрін қосуға болады. Егер бұл параметр қосулы болса, Kaspersky Security Center Linux қолданбасы басқарылатын құрылғыға қауіпсіздік қолданбасын орнатпас бұрын, үйлесімсіз қолданбаларды жояды.

Үйлесімсіз қолданбаларды бөлек тапсырма арқылы жою

Үйлесімсіз қолданбаларды жою үшін *Бағдарламаны қашықтан жою* тапсырмасы қолданылады. Тапсырма қауіпсіздік қолданбасын 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 қолданбасы инсталляторы үйлесімсіз қолданбалардың ешқайсысын сәтті жоя алмаған жағдайда қолданылғаны жөн.

Қолданбаларды немесе бағдарламалық жасақтама жаңартуларын қашықтан жою

Сіз тек Желілік агент көмегімен Linux жұмыс істейтін басқарылатын құрылғылардағы қолданбаларды немесе қолданбалық жасақтама жаңартуларын қашықтан жоюға болады.

Қолданбаларды немесе қолданбалық жасақтама жаңартуларын қашықтан жою үшін:

1. Қолданбаның негізгі терезесінде **Активтер (құрылғылар)** → **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 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.
6. Тапсырмалар тағайындалатын құрылғыларды таңдаңыз.

   Шебердің келесі қадамына өтіңіз.
7. Қандай қолданбаны жойғыңыз келетінін таңдаңыз, содан кейін жойғыңыз келетін қолданбаларды, жаңартуларды немесе патчтарды таңдаңыз:

   - **Басқарылатын бағдарламаны жою**

     "Лаборатория Касперского" қолданбалары тізімі көрсетіледі. Жойғыңыз келетін қолданбаларды таңдаңыз.

   - **Үйлесімсіз бағдарламаны жою**

"Лаборатория Касперского" немесе Kaspersky Security Center Linux қауіпсіздік қолданбаларына сәйкес келмейтін қолданбалардың тізімі көрсетіледі. Жойғыңыз келетін қолданбаларға қарама-қарсы жалаушалар қойыңыз.

- Бағдарламаны бағдарламалар тізімдемесінен жою

Әдепкі бойынша, Желілік агенттер басқарылатын құрылғыларда орнатылған қолданбалар туралы ақпаратты Басқару серверіне жібереді. Орнатылған қолданбалар тізімі қолданбалар тізімдемесінде сақталады.

Қолданбалар тізілімінен қолданбаны таңдау үшін:

a. **Жойылатын бағдарлама** өрісіне басып, жойғыңыз келетін қолданбаны таңдаңыз.

b. Жою параметрлерін көрсетіңіз:

- Жою режимі

Қолданбаны қалай жойғыңыз келетінін таңдаңыз:

- **Жою пәрменін автоматты түрде анықтау**

  Егер қолданбада қолданба өндірушісі белгілеген жою пәрмені болса, Kaspersky Security Center Linux бұл пәрменді пайдаланады. Осы нұсқаны таңдау ұсынылады.

- **Жою пәрменін белгілеу**

  Қолданбаны жою үшін пәрменіңізді көрсеткіңіз келсе, осы нұсқаны таңдаңыз.

  Алдымен қолданбаны **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 қолданбасы таңдалған қолданбада қолданба 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 қолданбаны 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 қолданбаларының тізімі көрсетіледі. Жойғыңыз келетін нысанды таңдаңыз.

Көрсетілетін тізім, қолданбалар мен жаңартулардың жалпы тізімі болып табылады және ол басқарылатын құрылғыларда орнатылған қолданбалар мен жаңартуларға сәйкес келмейді. Нысанды таңдамас бұрын, тапсырманың әрекет ету ауқымында анықталған құрылғыларда қолданбаның немесе жаңартудың орнатылғанына көз жеткізген жөн. Сипаттар терезесінде қолданба немесе жаңарту орнатылған құрылғылардың тізімін көруге болады.

Құрылғылар тізімін көру үшін:

a. Қолданбаның немесе жаңартулардың атын басыңыз.

Сипаттар терезесі ашылады.

b. **Құрылғылар** бөлімін ашыңыз.

Сондай-ақ, құрылғы сипаттары терезесінде орнатылған қолданбалар 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, қолданба 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 қолданбаны жоюға дайын болса, сіз **Жою әрекеттерінің максималды саны** параметрінің мәнін арттырып, қолданбаны 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 қолданбасы файлдарды жібермейді және қолданбаны орнатуға тырыспайды. Мысалы, әртүрлі операциялық жүйелері бар құрылғыларды қамтитын басқару тобының құрылғыларынан кейбір қолданбаларды орнату үшін басқару тобына орнату тапсырмасын тағайындауға болады, содан кейін қажеттіден басқа операциялық жүйесі бар құрылғыларды өткізіп жіберу үшін осы параметрді қосуға болады.

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)**
  - **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, қолданба құрылғыны қайта жүктеуге мүмкіндік бермейді.

  Егер бұл параметр қосулы болса, құрылғыны қайта іске қоспас бұрын бұғатталған құрылғылардағы мұндай қолданбалар 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 қолданбаларды 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, қолданба 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 *Қолданбаны қашықтан жою* тапсырмасын тағайындайтын құрылғыларда Желілік агент орнатылмаған болса, осы нұсқаны таңдаңыз.

Қолданба инсталляторын іске қосуға негіз болып саналатын есептік жазбаны көрсетіңіз. **Қосу** түймесін басыңыз, **Есептік жазба** тармағын 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.

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 жасалады, тең шеледі және тапсырмалар тізімінде, **Активтер (құрылғылар)** → **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 қолданба таңдалған құрылғыларда жойылады.

SUSE Linux Enterprise Server 15 басқаратын құрылғыны Желілік агентті орнатуға дайындау

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.

SUSE Linux Enterprise Server 15 операциялық жүйесімен құрылғыны дайындағандан кейін Желілік агентті орнатыңыз.

Windows құрылғысын қашықтан орнатуға дайындау. riprep утилитасы

Клиент құрылғысына қолданбаны 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, қолданбаны қашықтан орнату кезінде келесі мәселелер туындауы мүмкін:
  - клиент құрылғысында **Файлдарға қарапайым жалпы қатынасты өшіру** орнатылған;
  - клиент құрылғысында Server қызметі жұмыс істемейді;
  - клиент құрылғысында қажетті порттар жабық;
  - тапсырма орындалып жатқан есептік жазбаның құқықтары жеткіліксіз.

  Қолданбаны Желілік агенті орнатылмаған клиент құрылғысына орнату кезінде туындаған мәселелерді шешу үшін, құрылғыны қашықтан орнатуға дайындау утилитасын (riprep) пайдалануыңызға болады.

Windows басқаруындағы құрылғыны қашықтан орнатуға дайындау үшін riprep утилитасын пайдаланыңыз. Утилитаны жүктеп алу үшін мына сілтемені басыңыз:
https://media.kaspersky.com/utilities/CorporateUtilities/KSC/riprep.exe

Құрылғыны қашықтан орнатуға дайындау утилитасы Microsoft Windows XP Home Edition операциялық жүйесінің басқаруымен жұмыс істемейді.

Windows басқаруындағы құрылғыны интерактивті режимде қашықтан орнатуға дайындау

Windows басқаруындағы құрылғыны интерактивті режимде қашықтан орнатуға дайындау үшін:

1. Клиент құрылғысында riprep.exe файлын іске қосыңыз.
2. Қашықтан орнатуға дайындау утилитасының ашылған басты терезесінде келесі параметрлерді таңдаңыз:
   - **Файлдарға қарапайым жалпы қатынасты өшіру**
   - **Басқару серверінің қызметін іске қосу**
   - **Порттарды ашу**
   - **Есептік жазба қосу**
   - **Пайдаланушы есептік жазбаларды бақылауды өшіру** (параметр Microsoft Windows Vista, Microsoft Windows 7 және Microsoft Windows Server 2008 операциялық жүйелері үшін қолжетімді)
3. **Іске қосу** түймесін басыңыз.

   Нәтижесінде, утилитаның басты терезесінің төменгі жағында құрылғыны қашықтан орнатуға дайындау кезеңдері көрсетіледі.

Есептік жазба қосу параметрін таңдаған болсаңыз, есептік жазбаны жасау кезінде есептік жазбаның атауы мен құпиясөзді енгізуге арналған сұрау пайда болады. Нәтижесінде, жергілікті әкімшілер тобына тиесілі жергілікті есептік жазба жасалады.

Пайдаланушы есептік жазбаларды бақылауды өшіру параметрін таңдаған болсаңыз, есептік жазбаларды бақылауды ажырату әрекеті, утилитаны іске қосуға дейін есептік жазбаларды бақылау өшірулі болған жағдайда да орындалады. Есептік жазбаны бақылау өшірілгеннен кейін, құрылғыны қайта іске қосуға арналған сұрау пайда болады.

Windows басқаруындағы құрылғыны дыбыссыз режимде қашықтан орнатуға дайындау

Windows басқаруындағы құрылғыны дыбыссыз режимде қашықтан орнатуға дайындау үшін:

клиент құрылғысында қажетті кілттер жиынтығы бар пәрмен жолынан riprep.exe файлын іске қосыңыз.

Утилитаның пәрмен жолының синтаксисі:

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

Кілттердің сипаттамалары:

- `-silent` – утилитаны дыбыссыз режимде іске қосу.

- `-cfg CONFIG_FILE` – утилитаның конфигурациясын анықтау, мұндағы `CONFIG_FILE` – конфигурация файлына апарар жол (.ini кеңейтімі бар файл).

- `-tl traceLevel` – трассалау деңгейін белгілеу, мұндағы `traceLevel` – 0-ден 5-ке дейінгі сан. Кілт белгіленбесе, 0 мәні қолданылады.

Утилитаны дыбыссыз режимде іске қосу нәтижесінде сіз келесі тапсырмаларды орындай аласыз:

- файлдарға қарапайым ортақ қатынасты өшіру;

- клиент құрылғысында Server қызметін іске қосу;

- порттарды ашу;

- жергілікті есептік жазбаны жасау;

- пайдаланушының есептік жазбасын басқаруды (UAC) өшіру.

Құрылғыны қашықтан орнатуға дайындау параметрлерін `-cfg` кілтінде көрсетілген конфигурациялық файлда белгілей аласыз. Бұл параметрлерді белгілеу үшін конфигурациялық файлға келесі ақпаратты қосу керек:

- `Common` бөлімінде қандай тапсырмаларды орындау керектігін көрсетіңіз:

  - `DisableSFS` – файлдарға қарапайым ортақ қатынасты өшіру (0 – тапсырма өшірулі; 1 – тапсырма қосулы).

  - `StartServer` – Server қызметін іске қосу (0 – тапсырма өшірулі; 1 – тапсырма қосулы).

  - `OpenFirewallPorts` – қажетті порттарды ашу (0 – тапсырма өшірулі; 1 – тапсырма қосулы).

  - `DisableUAC` – есептік жазбаларды басқаруды өшіру (0 – тапсырма өшірулі; 1 – тапсырма қосулы).

  - `RebootType` – пайдаланушының есептік жазбасын басқару (UAC) өшірілгенде қайта іске қосу қажет болған кездегі жүріс-тұрысты анықтау. Келесі параметр мәндерін пайдалануыңызға болады:

    - 0 – құрылғыны ешқашан қайта іске қоспау;

    - 1 – егер утилитаны іске қоспас бұрын пайдаланушы есептік жазбаны басқару қосулы болса, құрылғыны қайта іске қосу;

    - 2 – егер утилитаны іске қоспас бұрын пайдаланушы есептік жазбаны басқару қосулы болса, құрылғыны күштеп қайта іске қосу;

    - 4 – құрылғыны әрқашан қайта іске қосу;

    - 5 – құрылғыны әрқашан күштеп қайта іске қосу.

- `UserAccount` бөлімінде есептік жазба атауын (`user`) және оның құпиясөзін (`Pwd`) көрсету.

Конфигурациялық файл мазмұнының мысалы:

```
[Common]
DisableSFS=0
StartServer=1
OpenFirewallPorts=1
[UserAccount]
```

```
user=Admin
Pwd=Pass123
```

Утилитаның жұмысы аяқталғаннан кейін, іске қосу қалтасында келесі файлдар жасалады:

- riprep.txt – утилитаның жұмыс істеу кезеңдері мен оларды жүргізу себептері атап көрсетілген жұмыс туралы есеп;
- riprep.log – трассирлеу файлы (белгіленген трассирлеу деңгейі 0-ден үлкен болса жасалады).

Скрипттерді қашықтан орындау тапсырмасын жасау

Клиенттік құрылғыда орнату пакетін орындау және қолданбаны қашықтан орнату үшін *Сценарийлерді қашықтан іске қосу* 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.

Сценарийлерді қашықтан іске қосу тапсырмасын іске қосу үшін:

1. **Жаңа тапсырма жасау шебері** өтіңіз және **Сценарийлерді қашықтан іске қосу** 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.

   Сценарийлерді қашықтан іске қосу 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. Келесі әрекеттердің бірін орындаңыз:

   - Қолданбаның негізгі терезесінде **Табу және орналастыру** → **Орналастыру және тағайындау** → **Орнату пакеттері** бөліміне өтіңіз.
   - Қолданбаның негізгі терезесінде **Операциялар** → **Қоймалар** → **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. Орнату пакетінің 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.** Қолданба өндірушісінің атауы.
  - **Нұсқа.** Қолданба 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 "Лаборатория Касперского" қолданбалары негізінде жасалмаған пакеттер үшін қолжетімді.

Скрипттерді қашықтан орындау тапсырмасы үшін мұрағатты дайындау

manifest.json файлына негізделген *Сценарийлерді қашықтан іске қосу* 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

  <файл1>

<файл2>

<папка1>/<файл3>

<папка2>/<папка3>/<файл4>

...

<файлX>

manifest.json – тапсырма манифест файлы.

<файл1>, ..., <файлX> – орындалуы қажет скрипттері бар файлдар жинағы.

Скрипттерді қашықтан орындау тапсырмасын пайдаланып құрылғыларға қолданбаларды қашықтан орнату

Сценарийлерді қашықтан іске қосу 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 dpkg -I <package_name>.deb
  ```

- manifest.json

  Қашықтағы қолданбаны орнатуға арналған JSON схемасы

  ```
  {
    "version": 1,
    "actions": [
      {
        "type": "execute",
        "path": "install.sh",
        "args": "<enter the arguments, if necessary>",
        "results": [
          {
            "code": 0,
            "next": "continue"
          }
        ],
        "default_next": "break"
      }
    ]
  }
  ```

1.

Сценарийлерді қашықтан іске қосу 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.

Сценарийлерді қашықтан іске қосу тапсырмасы аяқталғаннан кейін қолданба клиент құрылғысына орнатылады.

Скрипттерді қашықтан орындау тапсырмасы үшін хабарландыруларды конфигурациялау және бақылау

Сценарийлерді қашықтан іске қосу тапсырмасы үшін оқиғаны сақтау кезіндегі бақылауды, жүріс-тұрысты және хабарландыруларды конфигурациялауға болады.

Сценарийлерді қашықтан іске қосу тапсырмасының күйін көру үшін:

1. Негізгі қолданба терезесінде **Құрылғылар** → **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 деректорында, Басқару серверіндегі оқиғалар журналында немесе құрылғыда сақтағыңыз келсе, сәйкес параметрді қосыңыз.

Хабарландыруларды конфигурациялау туралы қосымша ақпарат алу үшін осы мақаланы қараңыз.

Лицензиялау

Бұл бөлімде келесі ақпарат бар:

- Kaspersky Security Center Linux лицензиясына қатысты жалпы түсініктер.
- "Лаборатория Касперского" басқарылатын қолданбаларына арналған лицензияларды басқару нұсқаулары.

Kaspersky Security Center Linux лицензиялау туралы

Бұл бөлімде Kaspersky Security Center Linux лицензиялаумен байланысты негізгі түсініктер туралы ақпарат бар.

Лицензиялық келісім туралы

Лицензиялық келісім – қолданбаны қандай шарттарда пайдалана алатыныңыз көрсетілген, сіз бен "Лаборатория Касперского" АҚ арасында жасалған заңды келісім.

Қолданбамен 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.
- "Лаборатория Касперского" сайтынан license.txt файлын жүктеп алу арқылы.

Сіз Linux үшін Желілік агентке арналған Лицензиялық келісімнің шарттарымен келесі тәсілдер арқылы таныса аласыз:

- Желілік агенттің дистрибутивін "Лаборатория Касперского" 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;
- "Лаборатория Касперского" сайтынан license.txt файлын жүктеп алу арқылы.

Сіз қолданбаны орнату кезінде Лицензиялық келісімнің мәтінімен келіскеніңізді растай отырып, Лицензиялық келісімнің шарттарын қабылдайсыз. Егер сіз Лицензиялық келісімнің шарттарымен келіспесеңіз, қолданбаны орнатуды тоқтатып, қолданбаны пайдаланбауыңыз қажет.

Лицензия туралы

Лицензия – бұл Лицензиялық келісім негізінде сізге берілген Kaspersky Security Center Linux бағдарламаны пайдалану үшін уақыт бойынша шектелген құқық.

Көрсетілетін қызметтердің көлемі және қолданбаны пайдалану мерзімі қолданба қолданылатын лицензияға байланысты.

Лицензиялардың келесі түрлері қарастырылған:

- *Сынақ*.

  Қолданбамен танысуға арналған тегін лицензия. Сынақ лицензиясының жарамдылық мерзімі қысқа.

  Сынақ лицензиясының мерзімі аяқталғаннан кейін, Kaspersky Security Center Linux бағдарламасы өзінің барлық функцияларын орындауды тоқтатады. Қолданбаны пайдалануды жалғастыру үшін сізге коммерциялық лицензия сатып алу қажет.

  Қолданбаны сынақ лицензиясы бойынша тек бір сынақ мерзімінде пайдалануға болады.

- *Коммерциялық*.

  Ақылы лицензия.

  Коммерциялық лицензияның қолданылу мерзімі аяқталған кезде қолданбаның негізгі функциялары өшіріледі. Kaspersky Security Center бағдарламасын пайдалануды жалғастыру үшін коммерциялық лицензияның жарамдылық мерзімін ұзарту қажет. Коммерциялық лицензияның мерзімі аяқталғаннан кейін, қолданбаны 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:

- лицензиялық кілт немесе тапсырыс нөмірі;
- лицензия берілетін пайдаланушы туралы ақпарат;
- берілетін лицензия бойынша белсендіруге болатын қолданба туралы ақпарат;
- лицензиялау бірліктерінің санына қойылатын шектеу (мысалы, берілетін лицензия бойынша қолданбаны 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 қолданбаны белсендіріп, пайдалануға мүмкіндік беретін биттер тізбегі. Лицензиялық кілтті "Лаборатория Касперского" мамандары жасайды.

Қолданбаға лицензиялық кілтті келесі тәсілдердің бірімен қосуға болады: *кілт файлын* қолдану немесе *белсендіру кодын* енгізу. Лицензиялық кілт қолданбаның интерфейсінде, оны қолданбаға қосқаннан кейінгі бірегей әріптік-цифрлық реттілік түрінде көрсетіледі.

Лицензиялық келісімнің шарттары бұзылған жағдайда, лицензиялық кілтті "Лаборатория Касперского" бұғаттауы мүмкін. Егер лицензиялық кілт бұғатталған болса, қолданба жұмыс істеуі үшін басқа лицензиялық кілтті қосу қажет.

Лицензиялық кілт белсенді және қосымша (резервтік) болуы мүмкін.

Белсенді лицензиялық кілт – ағымдағы сәтте қолданбаның жұмыс істеуі үшін қолданылатын лицензиялық кілт. Белсенді кілт ретінде, сынақ немесе коммерциялық лицензия үшін лицензиялық кілтті қосуға болады. Қолданбада бірден артық белсенді лицензиялық кілт болуы мүмкін емес.

Қосымша (резервттегі) лицензиялық кілт – қолданбаны 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, қолданба іске қосылғанша немесе коммерциялық лицензияның қолданылу мерзімі аяқталғанға дейін осы режимде жұмыс істейді. Басқару консолінің негізгі функциясын қолдайтын Kaspersky Security Center қолданбасы ұйымның желісін қорғауға арналған "Лаборатория Касперского" қолданбаларының құрамында жеткізіледі. Бұдан бөлек, ол "Лаборатория Касперского" 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 "Лаборатория Касперского" сайтынан таба аласыз. Әрбір шешім бетінде осы шешімге енгізілген қолданбалардың 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 функцияларды ұсынбайды.

Функция немесе сипат	Kaspersky Security Center Linux қолданбасының 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; • қолданбаларды қашықтан орнату; • клиент құрылғыларында орнатылған қолданба параметрлерін орталықтандырылған конфигурациялау; • ұйымның антивирустық қауіпсіздігінің күйін бақылау; • пайдаланушы рөлдерін басқару; • қолданбалардың 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; • қолданыстағы лицензиялы қолданбалар топтарын қарау және өзгерту; • желі сауалнамасы нәтижесінде табылған жабдықтар тізімін қолмен қарау және өңдеу; • қашықтан орнатуға болатын операциялық жүйе кескіндерінің тізімін қарау.		
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 қолданбалары үшін табылған осалдықтар мен қажетті жаңартулар тізімдерін алады. • *Осалдықтарды түзету* тапсырмасы *Осалдықтарды түзету* тапсырмасы үшінші тарап қолданбалары үшін ұсынылған Microsoft қолданбаларының түзетулері мен пайдаланушылық түзетулерді пайдаланады. Бұл тапсырманы пайдалану мақсатында, тапсырма параметрлерінде көрсетілген осалдықтарды түзету үшін пайдаланушылық түзетулерді қолмен көрсету қажет.	✓	✓

Осалдықтар мен патчтарды басқару: кеңейтілген функционалдылық Бағдарламалық жасақтама жаңартуларын автоматты түрде қашықтан орнату 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 Syslog пішімі арқылы SIEM жүйелеріне экспорттау Syslog протоколы бойынша Kaspersky Security Center Басқару серверінде және басқарылатын құрылғыларды орнатылған "Лаборатория Касперского" қолданбаларында 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.	✓	✓
Оқиғаларды SIEM жүйелеріне экспорттау: IBM ұсынған QRadar және Micro Focus ұсынған ArcSight	–	✓

Оқиғалар экспорты, қауіпсіздік жүйелерінің мониторингін қамтамасыз ететін және әртүрлі шешімдерден деректерді шоғырландыратын ұйымдастырушылық және техникалық деңгейлерде қауіпсіздік мәселелерімен жұмыс істейтін орталықтандырылған жүйелерде қолданылуы мүмкін. 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.

Арнайы протокол бойынша CEF және LEEF протоколдарын, SIEM жүйесіне жалпы оқиғаларды, сондай-ақ "Лаборатория Касперского" қолданбалары Басқару серверіне жіберген оқиғаларды экспорттау үшін пайдалануға болады.

LEEF (Log Event Extended Format) – бұл IBM Security QRadar SIEM үшін оқиғалардың мамандандырылған пішімі. QRadar жүйесі LEEF протоколы арқылы берілетін оқиғаларды қабылдай алады, анықтай алады және 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. ArcSight және Splunk SIEM жүйелері осы протоколды қолданады.

Кілт файлы туралы

Кілт файлы – "Лаборатория Касперского" сізге ұсынатын key кеңейтімі бар файл. Кілт файлы қолданбаны 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.

Қолданбаны кілт файлы арқылы белсендіру үшін "Лаборатория Касперского" 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 "Лаборатория Касперского" веб-сайтынан кілт файлын алыңыз.

Деректерді беру туралы

Жергілікті түрде өңделетін деректер

Kaspersky Security Center Linux қолданбасы 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 "Лаборатория Касперского" қолданбалары 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 "Лаборатория Касперского" қолданбаларын орнату;
- орнатылған қолданбалардың жұмыс параметрлері мен тапсырмаларын басқару;
- "Лаборатория Касперского" және басқа өндірушілер қолданбаларының жаңартуларын басқару, осалдықтарды іздеу және түзету;
- құрылғыларда "Лаборатория Касперского" қолданбаларын белсендіру;
- пайдаланушы есептік жазбаларын басқару;
- құрылғылардағы "Лаборатория Касперского" қолданбаларының жұмысы туралы ақпаратты қарау;
- есептерді қарау.

Өзінің негізгі функцияларын орындау үшін Kaspersky Security Center Linux қолданбасы келесі ақпаратты қабылдай алады, сақтай алады және өңдей алады:

- Ұйым желісіндегі құрылғылар туралы ақпарат Active Directory немесе Samba домен контроллерлерін сұрау немесе IP ауқымдарын сұрау арқылы алынады. Басқару сервері деректерді өз бетінше алады немесе Желілік агентке жібереді.
- Ұйымдық бөлімшелер, домендер, пайдаланушылар және топтар туралы Active Directory және Samba ақпараты. 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, атауы мен түрі (Windows доменіне тиесілі құрылғылар үшін), 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 "Лаборатория Касперского" қолданбасы туралы ақпарат, дамп файлдары, оқиғалар журналдары, "Лаборатория Касперского" 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.

- Құрылғыда орнатылған "Лаборатория Касперского" қолданбалары туралы деректер. Басқарылатын қолданба деректерді құрылғыдан Басқару серверіне Желілік агент арқылы жібереді:

  - Басқарылатын құрылғыда орнатылған "Лаборатория Касперского" қолданбаларының параметрлері: "Лаборатория Касперского" қолданбасының атауы мен нұсқасы, күйі, тұрақты қорғау күйі, құрылғыны соңғы тексеру күні мен уақыты, анықталған қауіптер саны, зарарсыздандыру орындалмаған нысандар саны, қолданба компоненттерінің болуы және күйі, "Лаборатория Касперского" қолданбасының параметрлері мен тапсырмалары туралы ақпарат, белсенді және резервтегі лицензиялық кілттер туралы ақпарат, қолданбаны орнату күні мен идентификаторы.

  - Қолданба жұмысының статистикасы: басқарылатын құрылғыдағы "Лаборатория Касперского" қолданбасының құрамдастары күйінің өзгерістерімен және қолданба құрамдастары бастаған тапсырмаларды орындаумен байланысты оқиғалар.

  - "Лаборатория Касперского" қолданбасы айқындаған құрылғының күйі.

  - "Лаборатория Касперского" қолданбасы беретін тегтер.

- Kaspersky Security Center Linux құрамдастары және "Лаборатория Касперского" басқарылатын қолданбалары 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 Басқару консольдеріне Kaspersky Security Center Web Console веб-консолінен енгізеді.

- Саясат және саясат профильдері түрінде ұсынылған Kaspersky Security Center Linux құрамдастарының және "Лаборатория Касперского" басқарылатын қолданбаларының конфигурациялары. Пайдаланушы деректерді Kaspersky Security Center Web Console интерфейсінде енгізеді.

- Kaspersky Security Center Linux құрамдастары және "Лаборатория Касперского" басқарылатын қолданбалары 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).
- Басқарылатын құрылғыларда орнатылған қолданбалар мен патчтар туралы деректер (Қолданбалар 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 қолданбалары үшін қолжетімді жаңарту туралы деректер.

- Басқарылатын құрылғылардағы үшінші тарап қолданбаларындағы осалдықтарды түзету үшін жаңартуларды оқшауланған Басқару серверіне жүктеу үшін қажетті деректер. Пайдаланушы Басқару серверінің klscflag утилитасын пайдаланып, деректерді енгізеді және жібереді.
- Реттелмелі қолданбалар санаттары. Пайдаланушы деректерді Kaspersky Security Center Web Console интерфейсінде енгізеді.
- Қолданбаны басқару функциясы арқылы басқарылатын құрылғыларда анықталған орындалатын файлдар туралы деректер. Басқарылатын қолданба деректерді құрылғыдан Басқару серверіне Желілік агент арқылы жібереді. Деректердің толық тізімі тиісті қолданбаның анықтамасында келтірілген.
- Windows операциялық жүйесі бар құрылғыларды шифрлау және шифрлау күйлері туралы ақпарат. Басқарылатын қолданба деректерді құрылғыдан Басқару серверіне Желілік агент арқылы жібереді.
- "Лаборатория Касперского" қолданбаларының деректерін шифрлау функциясы орындайтын Windows операциялық жүйесі бар құрылғылардағы деректерді шифрлау қателері туралы ақпарат. Басқарылатын қолданба деректерді құрылғыдан Басқару серверіне Желілік агент арқылы жібереді. Деректердің толық тізімі тиісті қолданбаның анықтамасында келтірілген.
- Сақтық көшірмелеуге орналастырылған файлдар туралы деректер. Басқарылатын қолданба деректерді құрылғыдан Басқару серверіне Желілік агент арқылы жібереді. Деректердің толық тізімі тиісті қолданбаның анықтамасында келтірілген.
- Карантинге орналастырылған файлдар туралы деректер. Басқарылатын қолданба деректерді құрылғыдан Басқару серверіне Желілік агент арқылы жібереді. Деректердің толық тізімі тиісті қолданбаның анықтамасында келтірілген.
- Егжей-тегжейлі талдау үшін "Лаборатория Касперского" мамандары сұраған файлдар туралы деректер. Басқарылатын қолданба деректерді құрылғыдан Басқару серверіне Желілік агент арқылы жібереді. Деректердің толық тізімі тиісті қолданбаның анықтамасында келтірілген.
- Аномалияларды бейімделумен басқару ережелерінің күйі және іске қосылуы туралы деректер. Басқарылатын қолданба деректерді құрылғыдан Басқару серверіне Желілік агент арқылы жібереді. Деректердің толық тізімі тиісті қолданбаның 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 қолданба деректерді құрылғыдан Басқару серверіне Желілік агент арқылы жібереді. Деректердің толық тізімі тиісті қолданбаның анықтамасында келтірілген.
- Шифрленген құрылғыларды шифрлау және шифрлау күйі туралы ақпарат. Басқарылатын қолданба деректерді құрылғыдан Басқару серверіне Желілік агент арқылы жібереді.
- Құрылғылардағы деректерді шифрлау қателері туралы ақпарат. Шифрлау "Лаборатория Касперского" қолданбаларын деректерді шифрлау функциясы арқылы орындалады. Басқарылатын қолданба деректерді

құрылғыдан Басқару серверіне Желілік агент арқылы жібереді. Деректердің толық тізімі тиісті қолданбаның анықтамасында келтірілген.

- Басқарылатын бағдарламаланатын логикалық контроллерлер (БЛК) тізімі. Басқарылатын қолданба деректерді құрылғыдан Басқару серверіне Желілік агент арқылы жібереді. Деректердің толық тізімі тиісті қолданбаның анықтамасында келтірілген.

- Қауіптердің даму тізбегін жасауға арналған деректер. Басқарылатын қолданба деректерді құрылғыдан Басқару серверіне Желілік агент арқылы жібереді. Деректердің толық тізімі тиісті қолданбаның анықтамасында келтірілген.

- Ұйым қызметкерлерінің бұлттық сервистерге қол жеткізу әрекеттері туралы ақпарат. Басқарылатын қолданба деректерді құрылғыдан Басқару серверіне Желілік агент арқылы жібереді. Деректердің толық тізімі тиісті қолданбаның 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.

- Енгізілген белсендіру кодтары немесе кілт файлдары туралы толық ақпарат. Пайдаланушы деректерді Басқару консолі интерфейсіне немесе Kaspersky Security Center Web Console веб-консоліне енгізеді.

- Пайдаланушылардың есептік жазбалары: атауы, сипаттамасы, толық атауы, электрондық пошта мекенжайы, негізгі телефон нөмірі, құпиясөзі, Басқару сервері жасаған құпия кілті және екі қадамдық тексеру 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.

- "Лаборатория Касперского" 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 қолданба плагиндерінің жұмыс істеуі үшін қажетті және күнделікті жұмыс барысында Басқару сервері дерекқорында плагиндер сақтайтын деректер. Сипаттама және деректерді беру тәсілдері тиісті қолданбаның 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 "Лаборатория Касперского" 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 "Лаборатория Касперского" басқарылатын қолданбасынан деректерді алады және оны Басқару серверіне береді. "Лаборатория Касперского" басқарылатын қолданбалары өңдейтін деректер тізбесі тиісті қолданбалардың анықтамаларында келтірілген.
- Басқару сервері желілік құрылғылар туралы ақпаратты өз бетінше алады немесе оны тарату нүктесі ретінде әрекет ететін желілік агент жібереді.

Атап көрсетілген деректер Басқару сервері дерекқорында сақталады. Пайдаланушы аттары және құпиясөздер шифрланған түрде сақталады.

Жоғарыда аталған барлық деректерді "Лаборатория Касперского" 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 "Лаборатория Касперского" бағдарламасына автоматты түрде берілмейді, алайда, әкімші осы файлдарды "Лаборатория Касперского" бағдарламасына Техникалық қолдау қызметінің сұрауы бойынша Kaspersky Security Center Linux жұмысындағы мәселелерді шешу үшін қолмен жібере алады.

"Лаборатория Касперского" барлық алынған деректерді заңнамаға және "Лаборатория Касперского" қолданыстағы ережелеріне сәйкес қорғауды қамтамасыз етеді. Деректер қауіпсіз байланыс арналары бойынша беріледі.

Сілтемелер арқылы Басқару консоліне немесе 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.

"Лаборатория Касперского" 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 қолданбаны 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 қолданбаның 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 қолданбаның 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 қолданбасын пайдалану кезінде, Kaspersky Security Center Linux қолданбасы автоматты түрде белсендіру серверіне жазылымның аяқталу күніне дейін белгілі бір уақыт аралығында жүгінеді. Жүйелік DNS арқылы серверге қатынасу мүмкін болмаса, қолданба 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. Басты мәзірде қажетті Басқару сервері атауының жанындағы параметрлер (⚙) белгішесін басыңыз.

   Басқару серверінің сипаттары терезесі ашылады.

2. **Жалпы** қойындысында **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 **Резервтегі 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.

"Лаборатория Касперского" басқарылатын қолданбаларын лицензиялау

Бұл бөлімде Kaspersky Security Center қолданбасының "Лаборатория Касперского" басқарылатын қолданбаларының лицензиялық кілттерімен жұмыс істеу мүмкіндіктері сипатталған.

Kaspersky Security Center Linux қолданбасы "Лаборатория Касперского" қолданбаларының 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 қолданба 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 қолданбаларды лицензиялау

Басқарылатын құрылғыларда орнатылған "Лаборатория Касперского" қолданбалары, қолданбалардың әрқайсысына кілт файлын немесе белсендіру кодын қолдану арқылы іске қосылуы керек. Кілт файлы немесе белсендіру коды келесі тәсілдермен таратылуы мүмкін:

- автоматты тарату арқылы;
- басқарылатын қолданбаның орнату пакетін пайдалану;
- басқарылатын қолданбаның Лицензиялық кілтін қосу тапсырмасы арқылы;
- басқарылатын қолданбаны қолмен белсендіру.

Жоғарыда аталған тәсілдердің кез келгенімен белсенді немесе сақтық лицензиялық кілтті қосуға болады. "Лаборатория Касперского" қолданбасы қазіргі уақытта белсенді болып саналатын кілтті пайдаланады және белсенді кілттің әрекет ету мерзімі аяқталғаннан кейін қолданылатын резерттегі лицензиялық кілтті сақтайды. Лицензиялық кілті қосылып жатқан қолданба кілттің белсенді немесе резервтік екенін анықтайды. Кілтті анықтау лицензиялық кілтті қосу үшін қолданылатын тәсілге байланысты емес.

Автоматты түрде тарату

Егер сіз әртүрлі басқарылатын қолданбаларды 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 қажет. Ұйымның құрылғыларында "Лаборатория Касперского" қауіпсіздік қолданбасы, мысалы, Kaspersky Endpoint Security for Linux орнатылған. Лицензиялық кілтті таратуды қажет ететін жаңа құрылғы табылды. Қолданба 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 қолданба 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 қолданбаның 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 қолданбаны орнату пакеті арқылы орнатқан жағдайда, белсендіру кодын немесе кілт файлын орнату пакетінде немесе сол қолданбаның саясатында көрсетуге болады. Лицензиялық кілт, құрылғыны Басқару серверімен кезекті рет синхрондау кезінде басқарылатын құрылғыларға қолданылады.

Нұсқаулар: Лицензиялық кілтті орнату пакетіне қосу

Басқарылатын қолданбаның лицензиялық кілтін қосу тапсырмасы арқылы тарату

Басқарылатын қолданбаның 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 "Лаборатория Касперского" қолданбасын жергілікті түрде қосу үшін қолданба құралдарын пайдалануға болады. Кеңейтілген ақпаратты орнатылған қолданбаларға арналған құжаттамадан қараңыз.

Лицензиялық кілтті Басқару серверінің қоймасына қосу

Басқару сервері қоймасына лицензиялық кілтті қосу үшін:

1. Қолданбаның негізгі терезесінде **Операциялар** → **Лицензиялау** → **«Лаборатория Касперского» лицензиялары** бөліміне өтіңіз.
2. **Қосу** түймесін басыңыз.
3. Қосқыңыз келетін нәрсені таңдаңыз:
   - **Кілт файлын қосу**

     Кілт файлын таңдаңыз түймесін басып, қосқыңыз келетін .key файлын таңдаңыз.
   - **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 лицензиялық кілтті қосу тапсырмасы арқылы таратуға мүмкіндік береді.

Таратпас бұрын лицензиялық кілтті Басқару серверінің қоймасына қосыңыз.

Лицензиялық кілтті клиент құрылғыларына кілтті қосу тапсырмасы арқылы тарату үшін:

1. Негізгі қолданба терезесінде **Активтер (құрылғылар)** → **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 қолданбаны таңдаңыз.

4. **Тапсырма түрі** тізімде **кілт қосу** тапсырмасын таңдаңыз.

5. **Тапсырманың атауы** өрісіне жаңа тапсырманың атын енгізіңіз.

6. Тапсырмалар тағайындалатын құрылғыларды таңдаңыз.

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:

   Кілтті қосу 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.

10. Бұл кілтті резервтегі кілт ретінде қолданғыңыз келсе, **Лицензия туралы ақпарат** шеберінің қадамында **Резервтегі кілт ретінде пайдалану** параметрін қосыңыз.

    Бұл жағдайда резервтік кілт белсенді кілттің мерзімі аяқталғаннан кейін пайдаланылады.

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 жасалып, орнатылып, тапсырмалар тізімінде 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 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. Қолданбаның негізгі терезесінде **Операциялар → Лицензиялау → «Лаборатория Касперского» лицензиялары** бөліміне өтіңіз.

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.

4. **Сақтау** түймесін басыңыз.

Лицензиялық кілт сай келетін құрылғыларға автоматты түрде таратылатын болады.

Лицензиялық кілтті тарату Желілік агенттің құралдарымен орындалады. Бұл арада, қолданба 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 қолданба 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. Осы параметрді таңдамасаңыз, лицензиялық кілтті кейінірек қолмен тарата аласыз.

Қолданылатын лицензиялық кілттер туралы ақпаратты қарап шығу

Басқару сервері қоймасына қосылған лицензиялық кілттердің тізімін көру үшін:

Қолданбаның негізгі терезесінде **Операциялар → Лицензиялау → «Лаборатория Касперского» лицензиялары** бөліміне өтіңіз.

Басқару сервері қоймасына қосылған кілт файлдары мен белсендіру кодтарының тізімі көрсетіледі.

Лицензиялық кілт туралы толық ақпаратты көру үшін:

1. Қолданбаның негізгі терезесінде **Операциялар → Лицензиялау → «Лаборатория Касперского» лицензиялары** бөліміне өтіңіз.
2. Қажетті лицензиялық кілттің атын басыңыз.

Ашылған лицензиялық кілттің сипаттары терезесінде сіз келесіні көре аласыз:

- **Жалпы** қойындысында – лицензиялық кілт туралы негізгі ақпарат.
- **Құрылғылар** қойыншасында – орнатылған "Лаборатория Касперского" қолданбасын белсендіру үшін лицензиялық кілт қолданылған клиент құрылғыларының тізімі.

Таңдалған клиент құрылғысында қандай лицензиялық кілттердің жиі кездесетінін көру үшін:

1. Қолданбаның негізгі терезесінде **Активтер (құрылғылар) → Басқарылатын құрылғылар** бөліміне өтіңіз.
2. Қажетті құрылғының атауын басыңыз.

3. Ашылған құрылғының сипаттар терезесінде **Бағдарламалар** бөлімін таңдаңыз.

4. Таратылған лицензиялық кілт туралы ақпаратты көргіңіз келетін қолданбаның атауын басыңыз.

5. Ашылған қолданба 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 "Лаборатория Касперского" белсендіру серверлеріне сұрау жібереді. Жүйелік DNS арқылы серверлерге қатынасу мүмкін болмаса, қолданба жалпыға ортақ DNS серверлерін пайдаланады.

Лицензиялық шектеуден асып кету оқиғалары

Kaspersky Security Center Linux, клиент құрылғыларында орнатылған "Лаборатории Касперского" қолданбаларының лицензиялық шектеулерінен асып кету оқиғалары туралы ақпарат алуға мүмкіндік береді.

Лицензиялық 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, қолданбалар 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. Басты мәзірде Басқару сервердің жанындағы параметрлер (⚙) белгішесін басыңыз.

      Басқару серверінің сипаттары терезесі ашылады.

   b. **Жалпы** қойындысында **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. Қолданбаның негізгі терезесінде **Операциялар → Лицензиялау → «Лаборатория Касперского» лицензиялары** бөліміне өтіңіз.

3. Қажетті кілт файлын немесе белсендіру кодын таңдап, **Жою** түймесін басыңыз.

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, "Лаборатория Касперского" кез келген басқарылатын қолданбасы үшін Лицензиялық келісімді кері қайтарып ала аласыз. Лицензиялық келісімді қайтарып алмас бұрын таңдалған қолданбаны жою керек.

"Лаборатория Касперского" басқарылатын қолданбалары үшін Лицензиялық келісімді кері қайтарып алу үшін:

1. Басқару сервер сипаттары терезесін ашыңыз және **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.

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 "Лаборатория Касперского" қолданбасын 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; қолданба енді орнатылмайды.

"Лаборатория Касперского" қолданбалары лицензиясының әрекет ету мерзімін ұзарту

Сіз мерзімі біткен немесе жақын арада аяқталатын (30 күннен аз) "Лаборатория Касперского" қолданбасының лицензиясының жарамдылық мерзімін ұзарта аласыз.

Жарамдылық мерзімі жақын арада аяқталатын немесе аяқталған лицензияның мерзімін ұзарту үшін:

1. Келесі әрекеттердің бірін орындаңыз:

   - Қолданбаның негізгі терезесінде **Операциялар → Лицензиялау → «Лаборатория Касперского» лицензиялары** бөліміне өтіңіз.

   - Қолданбаның негізгі терезесінде **Бақылау және есеп беру → Бақылау тақтасы** бөліміне өтіңіз және хабарландырудың жанындағы **Жарамдылық мерзімі өтіп кеткен лицензияларды қарау** сілтемесінен өтіңіз.

   «Лаборатория Касперского» лицензиялары 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 "Лаборатория Касперского" 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 – "Лаборатория Касперского" бизнес-шешімдерінің барлық спектрін көруге, өзіңізге қажет шешімдерді таңдауға және "Лаборатория Касперского" 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 "Лаборатория Касперского" 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 "Лаборатория Касперского" 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 сервистер.
  - **Желі**: жергілікті желі, АТ инфрақұрылымы.

- **Қызмет**: "Лаборатория Касперского" ұсынатын қауіпсіздікпен байланысты қызметтер.

"Лаборатория Касперского" бизнес шешімін табу және сатып алу үшін:

1. Қолданбаның негізгі терезесінде **Marketplace** бөліміне өтіңіз.
   Әдепкі бойынша, бөлімде "Лаборатория Касперского" 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.

"Лаборатория Касперского" 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. **"Лаборатория Касперского" қолданбалары үшін саясаттар мен саясат профильдерін конфигурациялау және тарату**

   Басқарылатын құрылғыларда орнатылған "Лаборатория Касперского" қолданбаларының параметрлерін конфигурациялау және тарату үшін қауіпсіздікті басқарудың екі түрлі тәсілдемесін қолдануға болады: пайдаланушыға бағытталған және құрылғыға бағытталған. Осы екі тәсілдемені біріктіруге болады.

2. **"Лаборатория Касперского" қолданбаларын 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 "Лаборатория Касперского" қолданбаларын басқарудың қосымша тапсырмаларын жасаңыз.

3. **Дерекқорға оқиғаларды жүктеуді бағалау және шектеу**

   Басқарылатын қолданбалардың жұмысындағы 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: Оқиғалар қоймасындағы оқиғалар санын конфигурациялау.

Нәтижелер

Осы сценарий аяқталғаннан кейін, сіздің желіңіз "Лаборатория Касперского" қолданбаларын, Басқару сервері алатын тапсырмалар мен оқиғаларды конфигурациялау арқылы қорғалады:

- "Лаборатория Касперского" қолданбалары саясаттар мен саясат профильдеріне сай конфигурацияланған.
- Қолданбаларды басқару тапсырмалар жиынтығының көмегімен жүзеге асырылады.
- Дерекқорда сақталуы мүмкін оқиғалардың ең көп саны белгіленген.

Желі қорғанысын конфигурациялап болғаннан кейін, сіз "Лаборатория Касперского" қолданбалары 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 қолданбасының әртүрлі параметрлерін қолдануға мүмкіндік береді. Мысалы, әртүрлі басқару топтарында орналасқан құрылғыларға әртүрлі параметрлерді қолдануға болады.

Пайдаланушыға бағытталған қауіпсіздікті басқару қауіпсіздік қолданбаларының 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 қолданба параметрлерін анықтай аласыз. Мысалы, қолданбалардың 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 – "Лаборатория Касперского" қолданбаларымен жұмыс істеуге арналған параметрлердің өзіндік конфигурациясын алады. Параметрлер конфигурациясы қолданбаның 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, қолданбаның 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 "Лаборатория Касперского" қолданбаларын басқару сценарийі келесі қадамдарды қамтиды:

1. **Қолданбалар саясаттарын конфигурациялау**

   Әр қолданба үшін саясат жасау арқылы басқарылатын құрылғыларда орнатылған "Лаборатория Касперского" қолданбаларының параметрлерін конфигурациялаңыз. Бұл саясат жиынтығы клиент құрылғыларына қолданылады.

   Қолданбаны жылдам іске қосу шебері арқылы желі қорғанысын конфигурациялау кезінде Kaspersky Security Center Linux қолданбасы келесі қолданбалар 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 қолданба 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 "Лаборатория Касперского" қолданбалары 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, "Лаборатория Касперского" белгіленген қолданбаларына 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, "Лаборатория Касперского" қолданбалары саясат иерархиясы арқылы көрсетілген және таралған параметрлерге сәйкес конфигурацияланады.

Қолданба саясаттары мен саясат профильдері басқару топтарына қосылған жаңа құрылғыларға автоматты түрде қолданылады.

Саясаттарды конфигурациялау және тарату: пайдаланушыларға бағытталған тәсілдеме

Бұл бөлімде басқарылатын құрылғыларда орнатылған "Лаборатория Касперского" қолданбаларын орталықтандырылған конфигурациялауға арналған пайдаланушыға бағытталған сценарий сипатталған. 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 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 "Лаборатория Касперского" қолданбаларын басқару сценарийі келесі қадамдарды қамтиды:

1. **Қолданбалар саясаттарын конфигурациялау**

   Әр қолданба үшін саясат жасау арқылы басқарылатын құрылғыларда орнатылған "Лаборатория Касперского" қолданбаларының 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 қолданба 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 құрылғыларға тиісті рөлдерді 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 қажет. 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 қолданба 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 қолданба 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 профильдерін жасау**

   Ұйымыңыздың әрбір пайдаланушы рөлі үшін саясат профилін жасаңыз. Саясат профильдері әр пайдаланушының рөліне байланысты пайдаланушы құрылғыларында орнатылған қолданбаларға 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 "Лаборатория Касперского" қолданбаларына 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, "Лаборатория Касперского" белгіленген қолданбаларына 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, "Лаборатория Касперского" қолданбалары 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. Қолданба саясаттары мен саясат профильдері сол пайдаланушының құрылғыларына автоматты түрде қолданылады.

Саясаттар және профильдер

Kaspersky Security Center Web Console қолданбасында "Лаборатория Касперского" қолданбаларына 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 "Лаборатория Касперского" қолданбасының параметрлері жиынтығы. "Лаборатория Касперского" қолданбаларының бірнешеуін басқару тобының құрылғыларына орната аласыз. Kaspersky Security Center бағдарламасы басқару тобындағы "Лаборатория Касперского" қолданбасының әрқайсысы үшін бір саясаттан ұсынады. Саясат келесі мәртебелердің біріне ие:

Саясат күйі	

Күй	Сипаттамасы
Белсенді	Бұл, құрылғыға қатысты қолданылатын ағымдағы саясат. "Лаборатория Касперского" қолданбасы үшін әрбір басқару тобында тек бір саясат белсенді болуы мүмкін. "Лаборатория Касперского" қолданбасының 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 қолданба үшін түрлі мәндері бар бірнеше саясатты конфигурациялауға болады.
- Бір қолданба 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 қолданба 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
🔒 Не определено	Егер параметрдің жанында ашық құлып белгішесі пайда болса және қосқыш өшірулі болса, параметр саясатта көрсетілмейді. Пайдаланушы бұл параметрлерді басқарылатын қолданба 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

	қолданба 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 "Лаборатория Касперского" қолданбасының параметрлерімен қайта тағайындалуы мүмкін.

Келесі әрекеттерді орындау үшін құлып белгішесін пайдалануға болады:

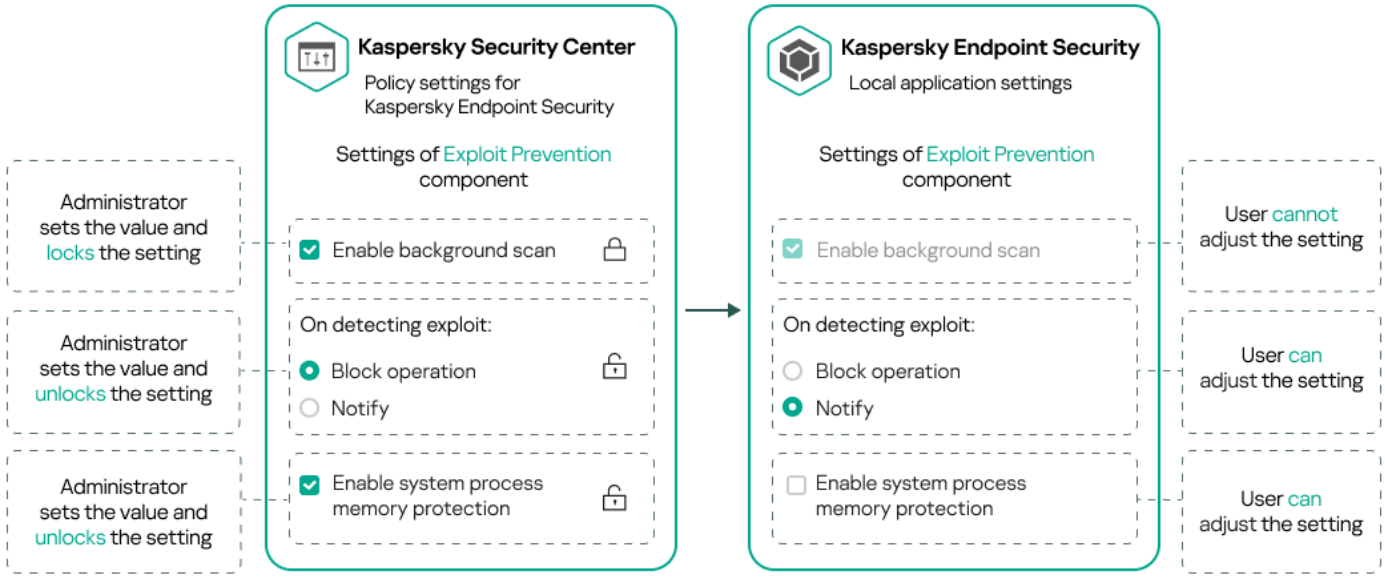
- Басқару ішкі тобы саясаты үшін параметрлерді құлыптау.
- Басқарылатын құрылғыдағы "Лаборатория Касперского" қолданбасының параметрлерін құлыптау.

Осылайша, құлыпталған параметр басқарылатын құрылғыдағы тиімді параметрлерде қолданылады.

Тиімді параметрлерді қолдану келесі әрекеттерді қамтиды:

- Басқарылатын құрылғы "Лаборатория Касперского" қолданбасының параметрлерінің мәндерін қолданады.
- Басқарылатын құрылғы саясат параметрлерінің құлыпталған мәндерін қолданады.

Саясат және "Лаборатория Касперского" басқарылатын қолданбасы бірдей параметрлер жиынтығын қамтиды. Саясат параметрлерін конфигурациялау кезінде "Лаборатория Касперского" қолданбасының параметрлері басқарылатын құрылғыдағы мәндерді өзгертеді. Басқарылатын құрылғыда құлыпталған параметрлерді өзгерту мүмкін емес (төмендегі суретті қараңыз):



"Лаборатория Касперского" қолданбасының құлыптары мен параметрлері

Саясат пен саясат профильдерін иелену

Бұл бөлімде, саясаттар және профильдер иерархиясы және оларды иелену туралы ақпарат келтірілген.

Саясаттар иерархиясы

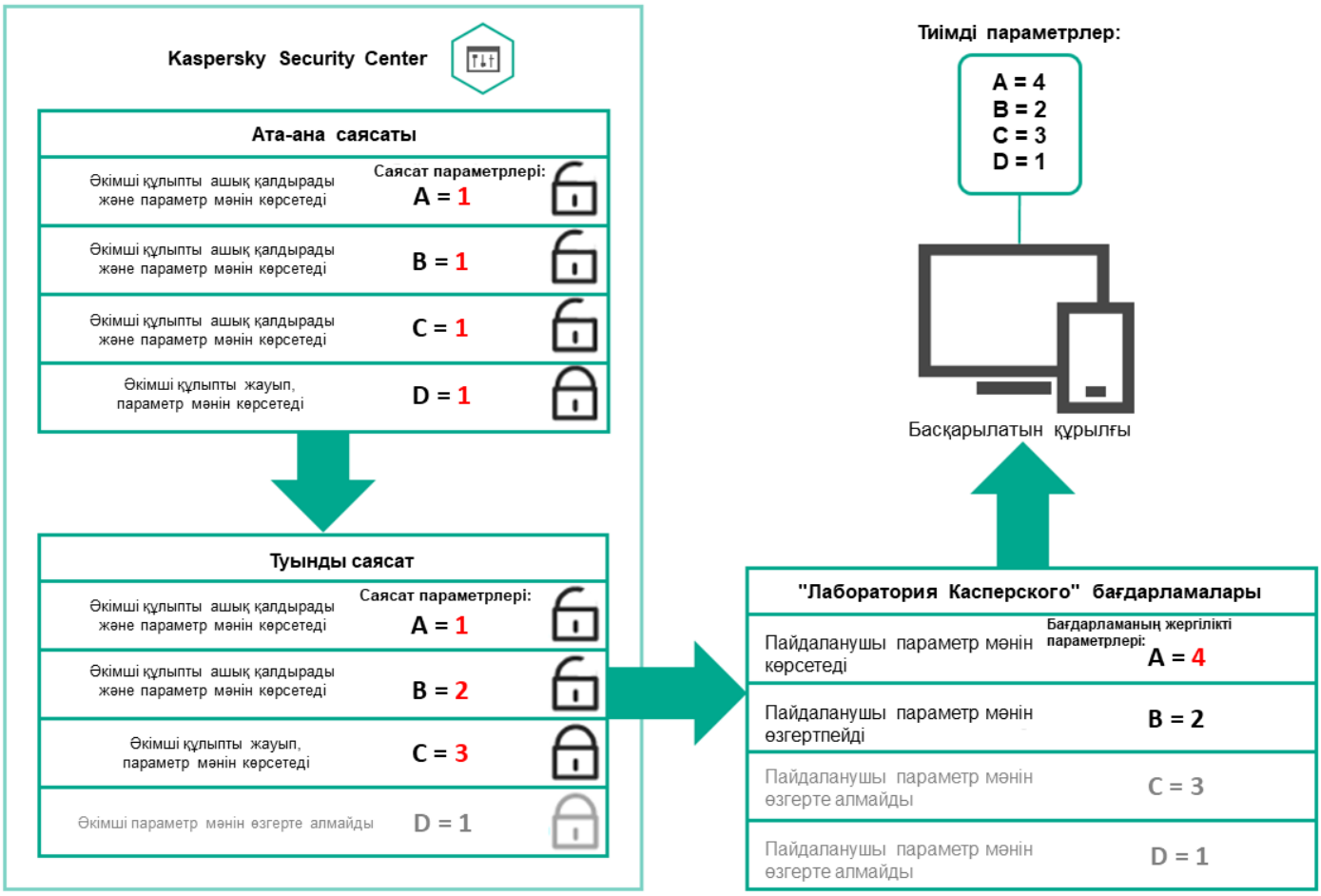
Түрлі құрылғылар үшін түрлі параметрлер керек болса, сіз құрылғыларды басқару топтарына біріктіре аласыз.

Сіз бөлек басқару тобына арналған саясатты көрсете аласыз. Саясат параметрлерін *иеленуге 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 қолданбаның 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).

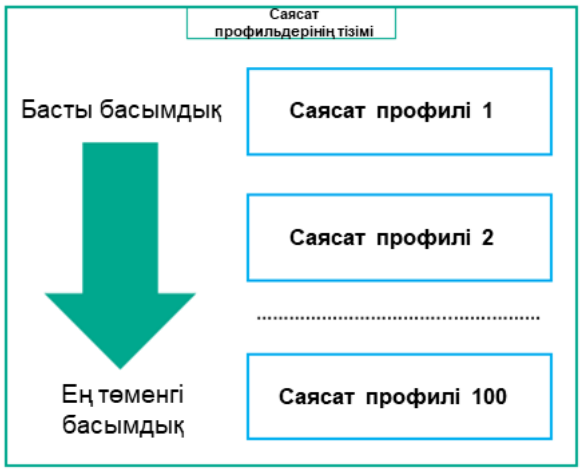


Саясаттар иерархиясы

Саясаттар иерархиясындағы саясат профильдері

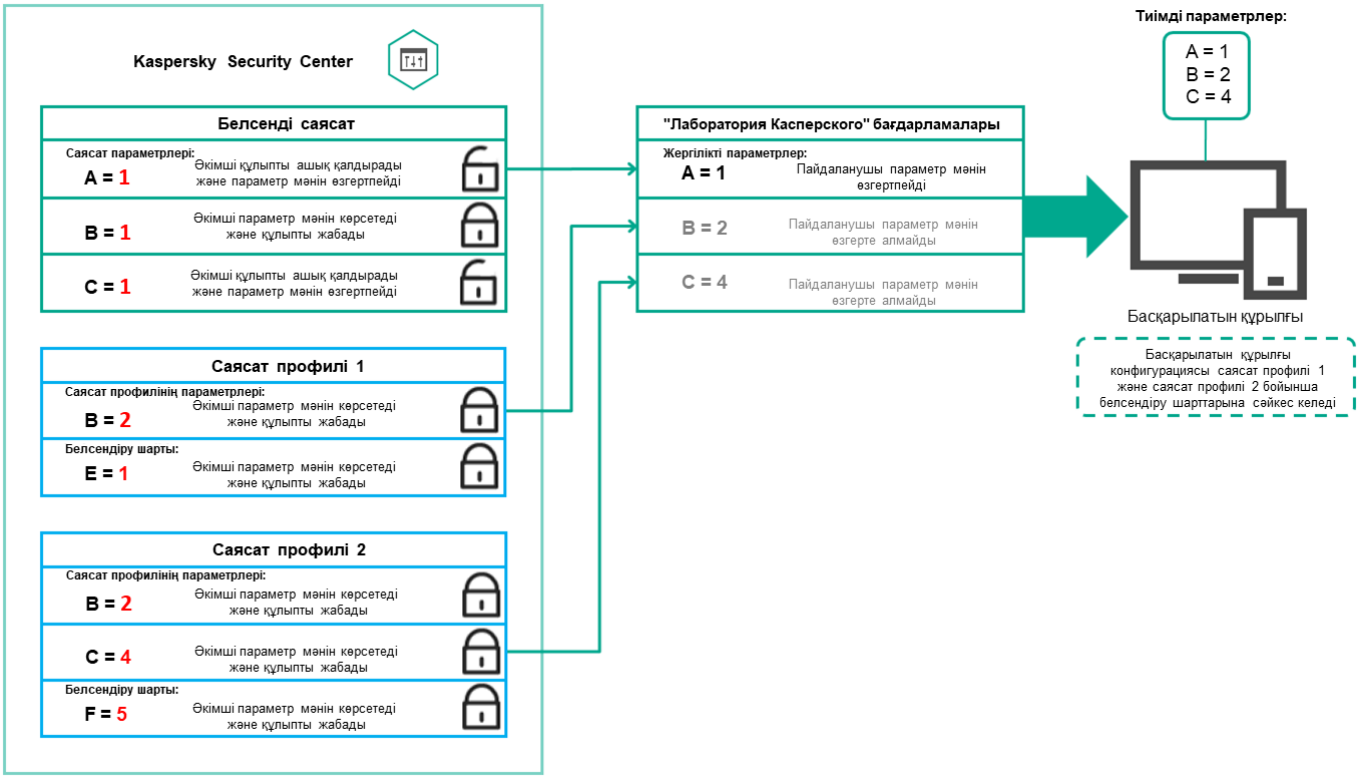
Саясат профильдерінде басымдықты тағайындаудың келесі шарттары бар:

- 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).



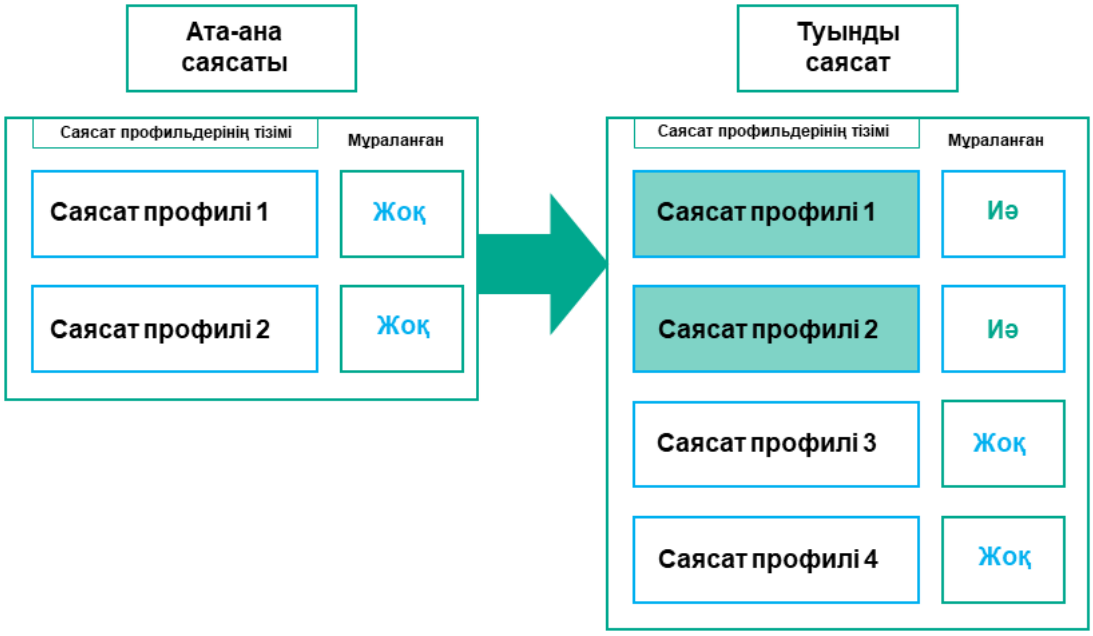
Басқарылатын құрылғының конфигурациясы бірнеше саясат профильдерін белсендіру шарттарына сәйкес келеді

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).

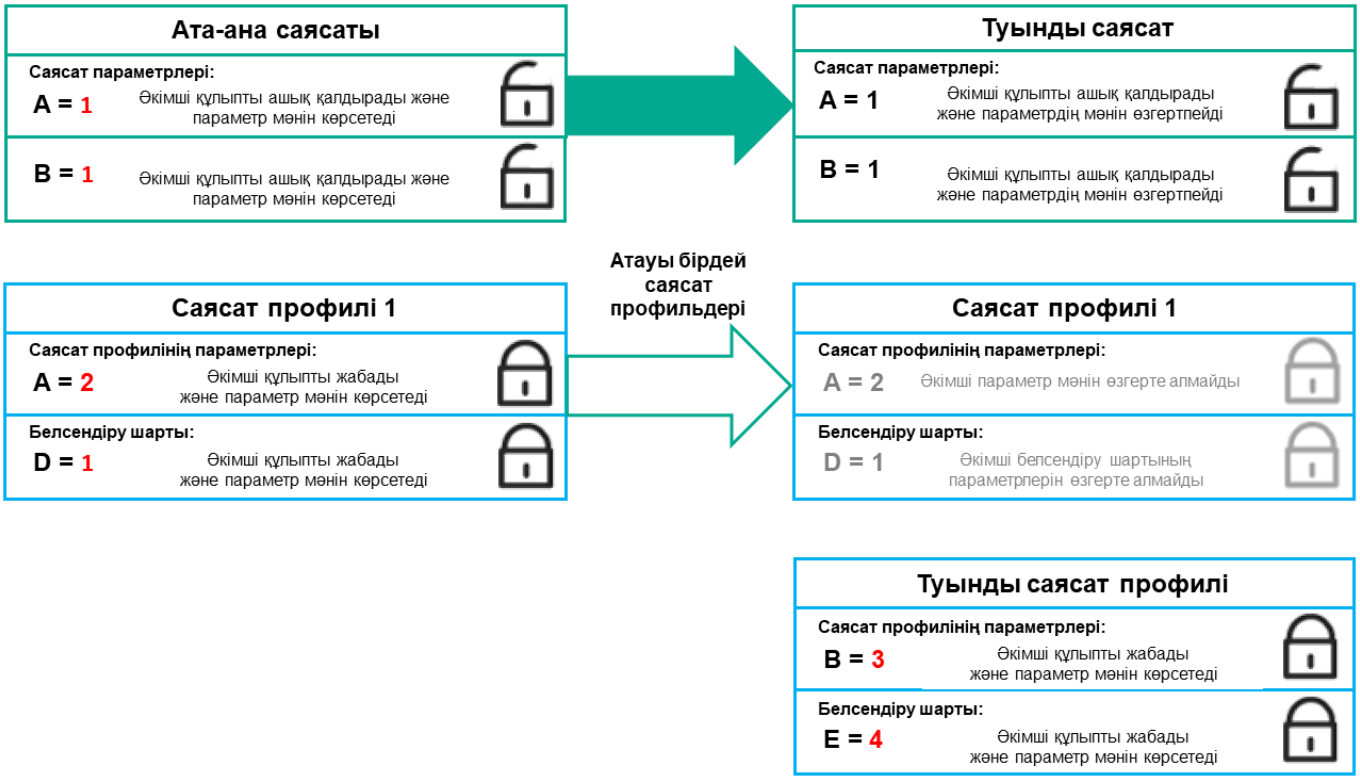


Саясат профильдерінің параметрлерін иелену

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 құрылғыда параметрлер қалай жүзеге асырылады?

Басқарылатын құрылғыда тиімді параметрлердің қолданылуын келесідей сипаттауға болады:

- Барлық құлыпталмаған параметрлердің мәндері саясаттан алынады.
- Содан кейін, олар басқарылатын қолданба 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. Қолданбаның негізгі терезесінде **Активтер (құрылғылар)** → **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. Қолданбаның негізгі терезесінде **Активтер (құрылғылар)** → **Саясат және профильдер** бөліміне өтіңіз.
2. **Қосу** түймесін басыңыз.

   Бағдарламаны таңдаңыз терезесі ашылады.
3. Саясат жасауды қажет ететін қолданбаны таңдаңыз.
4. **Келесі** түймесін басыңыз.

Жалпы қойыншасында жаңа саясат параметрлері терезесі ашылады.

5. Қаласаңыз, әдепкі бойынша белгіленген келесі саясат параметрерін өзгерте аласыз: атауы, күйі және иелену.

6. **Бағдарлама параметрлері** қойындысын таңдаңыз.

   Не болмаса, шығу үшін **Сақтау** түймесін басыңыз. Саясат саясаттар тізіміне пайда болып, сіз оның сипаттарын кейінірек өзгерте аласыз.

7. **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 қолданбаға байланысты. Толығырақ ақпарат келесі дереккөздерде келтірілген:

   - Басқару серверін конфигурациялау
   - Желілік агент саясатының параметрлері
   - Kaspersky Endpoint Security for Linux анықтамасы
   - Kaspersky Endpoint Security for Windows анықтамасы

   Басқа қауіпсіздік қолданбаларының параметрлері туралы толығырақ білу үшін тиісті қолданбаның құжаттамасын қараңыз.

   Өзгерістерді болдырмау үшін **Бас тарту** түймесін басуға болады.

8. Саясат өзгерістерін сақтау үшін **Сақтау** түймесін басыңыз.

Нәтижесінде, қосылған саясат саясаттар тізімінде көрсетіледі.

Саясаттардың жалпы параметрлері

Жалпы

Жалпы қойындысында 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 негізгі 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.

Оқиғаны конфигурациялау

Оқиғаны конфигурациялау қойыншада оқиғаларды тіркеуді және оқиғалар туралы хабарлауды конфигурациялауға болады. Оқиғалар қойыншалардағы маңыздылық деңгейлері бойынша бөлінген:

- **Критикалық**

  Критикалық 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). Қажет болса, бұл параметрлерді **Электрондық пошта**, **SMS** және **Іске қосылатын орындалатын файл** қойындыларында өзгертуге болады.

Тексерістер журналы

Тексерістер журналы қойыншада сіз саясатты тексеру тізімін және кері қайтарылған өзгерістерді көре аласыз.

Саясатты өзгерту

Саясатты өзгерту үшін:

1. Қолданбаның негізгі терезесінде **Активтер (құрылғылар)** → **Саясат және профильдер** бөліміне өтіңіз.
2. Өзгертуді қажет ететін саясатты таңдаңыз.

   Саясат сипаттары терезесі ашылады.
3. Сіз саясатты жасайтын жалпы параметрлер мен қолданба параметрлерін көрсетіңіз. Толығырақ ақпарат келесі дереккөздерде келтірілген:

   - Басқару серверін конфигурациялау
   - Желілік агент саясатының параметрлері
   - Kaspersky Endpoint Security for Linux анықтамасы
   - Kaspersky Endpoint Security for Windows анықтамасы

   Басқа қауіпсіздік қолданбаларының параметрлері туралы толығырақ білу үшін осы қолданбалардың құжаттамасын қараңыз.
4. **Сақтау** түймесін басыңыз.

Саясат өзгерістері саясаттың сипаттарында сақталып, **Тексерістер журналы** бөлімінде көрсетіледі.

Саясатты иелену параметрін қосу және өшіру

Саясатта иелену параметрін қосу немесе өшіру үшін:

1. Қажетті саясатты ашыңыз.

2. **Жалпы** қойындысын ашыңыз.

3. Саясатты иеленуді қосу немесе өшіру:

   - Егер еншілес топ үшін **Параметрлерді негізгі саясаттан иелену** параметрін қосқан болсаңыз және әкімші тектік саясаттағы кейбір параметрлерді бұғаттаған болса, еншілес саясат үшін бұл саясат параметрлерін өзгерте алмайсыз.

   - Егер еншілес саясат үшін **Параметрлерді негізгі саясаттан иелену** опциясын өшірген болсаңыз, кейбір параметрлер тектік саясатта "бұғатталған" болса да, еншілес саясаттағы барлық параметрлерді өзгертуге болады.

   - Тектік топта **Еншілес саясаттардағы параметрлерді мәжбүрлеп иелену** параметрі қосылса, бұл әрбір еншілес саясат үшін **Параметрлерді негізгі саясаттан иелену** параметрін қосады. 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.

4. Өзгерістерді сақтау үшін **Сақтау** түймесін басыңыз немесе өзгерістерді қабылдамау үшін **Бас тарту** түймесін басыңыз.

Әдепкі бойынша, **Параметрлерді негізгі 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. Қолданбаның негізгі терезесінде **Активтер (құрылғылар)** → **Саясат және профильдер** бөліміне өтіңіз.

2. Жалаушаны, көшірілетін саясатқа (немесе саясаттарға) қарама-қарсы қойыңыз.

3. **Көшіру** түймесін басыңыз.

   Экранның оң жағында басқару топтарының ағашы көрсетіледі.

4. Ағашта 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 жылжыту үшін:

1. Қолданбаның негізгі терезесінде **Активтер (құрылғылар)** → **Саясат және профильдер** 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. Қолданбаның негізгі терезесінде **Активтер (құрылғылар)** → **Саясат және профильдер** 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.
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. Қолданбаның негізгі терезесінде **Активтер (құрылғылар)** → **Саясат және профильдер** 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. Қолданбаның негізгі терезесінде **Активтер (құрылғылар)** → **Басқарылатын құрылғылар** бөліміне өтіңіз.

2. Басқару серверімен синхрондау қажет құрылғының атауын таңдаңыз.

   Ашылған сипаттар терезесінде **Жалпы** бөлімін таңдаңыз.

3. **Мәжбүрлеп синхрондау** түймесін басыңыз.

Қолданба 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:

   - Негізгі мәзірде **Активтер (құрылғылар)**→ **Басқарылатын құрылғылар** бөліміне өтіңіз, басқарылатын құрылғылар тізімінің үстінде **Ағымдағы жол** өрістегі сілтемеден өтіңіз және синхрондалатын құрылғыларды қамтитын басқару тобын таңдаңыз.

   - Құрылғылар тізімін қарау үшін құрылғы таңдауларын іске қосыңыз.

2. Басқару серверімен синхрондауды қажет ететін құрылғылардың жанында жалауша қойыңыз.

3. Басқарылатын құрылғылар тізімі үстінде көп нүктелі (...) түймесін басып, **Мәжбүрлеп синхрондау** түймесін басыңыз.

   Қолданба 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 "Лаборатория Касперского" қолданбасының 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 қолданба саясатын жеткізу күні мен уақытын көру үшін:

1. Қолданбаның негізгі терезесінде **Активтер (құрылғылар)** → **Басқарылатын құрылғылар** бөліміне өтіңіз.

2. Басқару серверімен синхрондау қажет құрылғының атауын таңдаңыз.

   Ашылған сипаттар терезесінде **Жалпы** бөлімін таңдаңыз.

3. **Бағдарламалар** қойындысына өтіңіз.

4. Саясатты синхрондау күнін көру қажет қолданбаны таңдаңыз.

   Қолданба 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. Қолданбаның негізгі терезесінде **Активтер (құрылғылар)** → **Саясат және профильдер** бөліміне өтіңіз.
2. Құрылғыдағы қолдану күйін көргіңіз келетін саясат атауының жанына жалаушаны қойыңыз.
3. Пайда болған мәзірден **Тарату** тармағын таңдаңыз.

   <саясат атауы> тарату нәтижесі терезесі ашылады.
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. Бас мәзірде өз есептік жазбаңыздың параметрлеріне өтіп, **Интерфейс опциялары** тармағын таңдаңыз.
2. **Саясатты үлестіру нәтижесінде көрсетілетін құрылғылардың максималды саны** өрісінде құрылғылар санын енгізіңіз (100 000-ға дейін).

   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. Басты мәзірде қажетті Басқару сервері атауының жанындағы параметрлер (⚙) белгішесін басыңыз.

   Жалпы қойындысында Басқару сервері сипаттары терезесі ашылады.
2. **Вирустық шабуыл** 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. Қолданбаның негізгі терезесінде **Активтер (құрылғылар)** → **Саясат және профильдер** 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 **ОК** түймесін басыңыз.

Саясат және оның саясат профильдерінің барлығы жойылған.

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 және саясат профилін жою туралы ақпарат береді.

Саясат профильдерін қарау

Саясат профильдерін қарау үшін:

1. Қолданбаның негізгі терезесінде **Активтер (құрылғылар)** → **Саясат және профильдер** бөліміне өтіңіз.

2. Профильдерін қарау қажет саясатты таңдаңыз.

   Жалпы қойыншасында саясат сипаттары терезесі ашылады.

3. **Саясат профильдері** қойындысын ашыңыз.

Саясат профильдері кесте түрінде көрсетіледі. Саясатта саясат профильдері болмаса, бос кесте көрсетіледі.

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.

4. **Бағдарлама параметрлері** қойындысын 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.

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** қойындысында көшіргіңіз келетін 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, саясат профилінің параметрлерін, оның аты мен басымдылығын 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** қойындысында **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.

- **Бұл құрылғыда Басқару сервері байланысының ережесі белсенді**

  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 саясат профилін белсендіру шартын конфигурациялау үшін жалаушаны қойыңыз.

  Бұл параметр үшін келесі қадамда мынаны көрсетіңіз:

  - **Жедел жадтың 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.

Шебер терезелерінің кейінгі саны осы қадамдағы параметрлерді таңдауға байланысты. Саясат профилін белсендіру ережелерін кейінірек өзгертуге болады.

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 қолданбалардың параметрлерінде өзгерістерді азайтуға мүмкіндік береді.

Желілік агент саясатының параметрлері

Желілік агент саясаты параметрлерін конфигурациялау үшін:

1. Қолданбаның негізгі терезесінде **Активтер (құрылғылар)** → **Саясат және профильдер** бөліміне өтіңіз.

2. Желілік агент саясатының атауын басыңыз.

   Желілік агент саясатының сипаттары терезесі ашылады. Сипаттар терезесі төменде сипатталған қойындылар мен параметрлерді қамтиды.

Linux және Windows басқаратын құрылғылары үшін әртүрлі параметрлер қолжетімді екенін ескеріңіз.

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 негізгі 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 (қолданбаларды 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 қолданбалары әрбір қауіпсіздік қолданбасы 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 қолданбасына жібереді (мысалы, Kaspersky Endpoint Security for Linux). Берілетін ақпарат қауіпсіздік қолданбасының интерфейсінде көрсетіледі.

  Желілік агент келесі ақпаратты береді:

  - саясатты басқарылатын құрылғыға жеткізу уақыты;
  - саясатты басқарылатын құрылғыға жеткізу кезінде белсенді саясат пен автономды пайдаланушылар саясатының атауы;
  - саясатты басқарылатын құрылғыға жеткізу кезінде басқарылатын құрылғыға тиесілі басқару тобының атауы және толық жолы;
  - 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, осы параметр қосылса, компонентті 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

  Егер параметр қосулы болса, **Өзгерту** түймесін басқан кезде, желілік агентті қашықтан жою тапсырмасы үшін klmover утилитасына арналған құпия сөзді көрсетуге болады.

  Әдепкі бойынша, параметр өшірулі.

Қоймалар

Қоймалар бөлімінде Желілік агент Басқару серверіне жіберетін нысандардың түрлерін таңдауға болады. Желілік агент саясатында, осы бөлімде көрсетілген параметрлерді өзгертуге тыйым салынса, бұл параметрлерді өзгерту мүмкін емес. Қоймалар бөлімінің параметрлері тек Windows басқаратын құрылғылар үшін ғана қолжетімді:

- Орнатылған бағдарламалардың мәліметтері

  Егер бұл параметр қосылса, клиент құрылғыларында орнатылған қолданбалар туралы ақпарат Басқару серверге жіберіледі.

  Әдепкі бойынша, параметр қосулы.

- Патчтар туралы ақпаратты қамту

  Клиент құрылғыларында орнатылған қолданба 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

  Егер параметр орнатылған болса, Windows Update жаңартулары туралы ақпарат клиент құрылғыларына орнатылуы керек Басқару серверіне жіберіледі.

  Әдепкі бойынша, параметр қосулы. Тек Windows үшін қолжетімді.

- Бағдарламалық жасақтама осалдықтары мен сәйкес жаңартулар туралы мәліметтер

  Егер бұл параметр қосылса, басқарылатын құрылғыларда табылған үшінші тарап қолданбаларындағы (Microsoft қолданбалық жасақтамасын қоса) осалдықтар туралы ақпарат және осалдықтарды түзету қолданбалық жасақтамасының жаңартулары (Microsoft қолданбалық 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 қолданбаларының 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

Бағдарламалық жасақтаманың жаңартулары мен осалдықтары

Бағдарламалық жасақтаманың жаңартулары мен осалдықтары бөлімінде орындалатын файлдарды осалдықтардың бар-жоғы тұрғысынан тексеруді қосуыңызға 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 қосуды басқару

Өшіріп қайта қосуды басқару бөлімінде қолданбаның жұмыс істеуі, оны орнату немесе жою кезінде басқарылатын құрылғының операциялық жүйесін қайта іске қосу қажет болса, әрекетті таңдауға және конфигурациялауға болады. **Өшіріп қайта қосуды басқару** бөлімінің параметрлері тек Windows басқаратын құрылғылар үшін ғана қолжетімді:

- **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 қолданба 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, қолданба 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, қолданба құрылғыны қайта жүктеуге мүмкіндік бермейді.

  Егер бұл параметр қосулы болса, құрылғыны қайта іске қоспас бұрын бұғатталған құрылғылардағы мұндай қолданбалар 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 қолданбаларды 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 "Лаборатория Касперского" патчтары жаңарту серверлерінен жүктелгеннен кейін автоматты түрде басқарылатын құрылғыларға орнатылады.

  Егер жалауша алынып тасталса, *Анықталмаған* мәртебесі бар "Лаборатория Касперского" жүктелген патчтары, әкімші олардың мәртебесін *Расталды* деп өзгерткеннен кейін орнатылады.

  Әдепкі бойынша, параметр қосулы.

- **Басқару серверінен жаңартулар мен антивирустық дерекқорды алдын ала жүктеп алыңыз (ұсынылған)**

Егер жалауша алынып тасталса, жаңартуларды алудың офлайн моделі өшіріледі. Басқару сервері жаңартуларды алған кезде, ол Желілік агентті (ол орнатылған құрылғыларда) басқарылатын қолданбалар 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 қолданбалар үшін қолжетімді болады.

Клиент құрылғысындағы басқарылатын қолданба жаңартуларды алу үшін Желілік агентке жүгінген кезде, Агент өзінде қажетті жаңартулардың бар ма екенін тексереді. Жаңартулар басқарылатын қолданба сұрау салған сәттен бастап 25 сағаттан ерте болмайтын мерзімнің ішінде Басқару серверінен алынған болса, онда Желілік агент Басқару серверіне қосылмайды және басқарылатын қолданбаға жергілікті кэштегі жаңартуларды ұсынады. Желілік агент қолданбаларға 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.

    Егер синхрондау кезеңі 15 минуттан аз болып белгіленсе, синхрондау 15 минут сайын орындалады. Егер синхрондау кезеңі 15 минутқа немесе одан да көп уақытқа орнатылса, синхрондау көрсетілген кезеңмен орындалады.

  - 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 брандмауэрінде Желілік агенттің порттарын ашу

  Егер параметр қосулы болса, Желілік агент жұмыс істеуі үшін қажетті UDP порты Microsoft Windows желілік экранының 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) байланыс шлюзін пайдаланыңыз

  Егер параметр қосулы болса, онда параметрлері басқару тобының сипаттарында белгіленген тарату нүктесінің қосылым шлюзі қолданылады.

  Әдепкі бойынша, параметр қосулы.

- UDP портын пайдалану

  Басқарылатын құрылғының KSN прокси-серверіне UDP порты арқылы қосылуы үшін **UDP портын пайдалану** жалаушасын қойып, **UDP порты нөмірін** көрсетіңіз. Әдепкі бойынша, параметр қосулы. Әдепкі бойынша, KSN прокси-серверіне қосылу 15111 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 бөлікшесінде Желілік орналасудың параметрлерін белгілеуге және Басқару сервері қолжетімсіз болғанда автономды пайдаланушы режиміне ауысуға болады. **Байланыс профильдері** бөлімінің параметрлері тек Windows басқаратын құрылғылар үшін ғана қолжетімді:

- 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 қосылу профильдері

Қосылым профильдеріне тек Windows басқаратын құрылғылар үшін ғана қолдау көрсетіледі.

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 қолданбасында орнатылған қолданбалар автономды режимдегі құрылғыларға арналған саясат профильдерін және автономды пайдаланушыларға арналған саясаттарды қолданатын болады. Қолданба үшін автономды пайдаланушыларға арналған саясат анықталмаған болса, қолданба белсенді саясатты қолданатын болады.

  Параметр өшірулі болса, қолданбалар 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:

- **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

Бұл параметр қосылса, тарату нүктесі **Сауалнама кестесін орнату** түймесі арқылы орнатылған 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 түпнұсқалық растама**

  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 қолданбаны 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 "Лаборатория Касперского" 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**

  Басқарылатын құрылғының KSN прокси-серверіне UDP порты арқылы қосылуы үшін **UDP портын пайдалану** жалаушасын қойып, **UDP порты нөмірін** көрсетіңіз. Әдепкі бойынша, параметр қосулы. Әдепкі бойынша, KSN прокси-серверіне қосылу 15111 UDP порты арқылы жүзеге асырылады.

- **Порт арқылы HTTPS**

Басқарылатын құрылғылардың KSN прокси-серверіне HTTPS порты арқылы қосылуын қаласаңыз, **HTTPS пайдалану** параметрін қосыңыз және **Порт арқылы HTTPS** өрісінде порт нөмірін көрсетіңіз. Әдепкі бойынша, параметр өшірулі. Әдепкі бойынша, KSN прокси-серверіне қосылу 15111 HTTPS порты арқылы жүзеге асырылады.

Жаңартулар (тарату нүктелері)

Жаңартулар (тарату нүктелері) бөлімінде айырмашылық файлдарын жүктеу функциясын қосуыңызға болады, себебі тарату нүктелері жаңартуларды "Лаборатория Касперского" жаңартулар серверлерінен айырмашылық файлдары түрінде алып тұрады.

Жергілікті есептік жазбаны басқару (тек Linux)

Жергілікті есептік жазбаны басқару (тек Linux) бөлімі үш бөлікшеден тұрады:

- **Пайдалану сертификаттарын басқару**
- **Қолданылатын жергілікті әкімші топтарын қосу не өңдеу**
- **Пайдаланушы құрылғысындағы sudoer файлдарын өзгерістерден қорғау үшін сілтемелік файл жүктеп салу**

Пайдалану 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.

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	✓	✓	✓
Қолданбаларды қашықтан орнатудың үшінші тарап құралдары арқылы қолданбалар орнату	✓	✓	✓
Құрылғыларда қолданба 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	✓	✓	✓

Тарату нүктесі			
Тарату нүктесін қолдану	✓	✓	✓
Тарату нүктелерін автоматты түрде тағайындау	✓	✓ Network Location Awareness (NLA) қолданбай.	✓ Network Location Awareness (NLA) қолданбай.
Жаңартуларды алудың офлайн-моделі	✓	✓	✓
Желіде сауалнама өткізу	✓ • IP ауқымдарының сауалнамасы • Домен контроллері сауалнамасы	✓ • IP ауқымдарының сауалнамасы • Zeroconf сауалнамасы • Домен контроллерлерінің сауалнамасы (Microsoft Active Directory, Samba 4 Active Directory)	–
KSN прокси-сервері қызметін тарату нүктесінің жағында іске қосу	✓	✓	–
Жаңартуларды басқарылатын құрылғыларға тарататын тарату нүктесі қоймаларына "Лаборатория Касперского" жаңарту серверлері арқылы жүктеп алу	✓	✓	– 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.
Қолданбаларды күшпен орнату	✓	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	✓	✓	–
Үшінші тарап өндірушілердің қолданбаларымен жұмыс істеу			
Қолданбаларды	✓	✓	✓

құрылғыларға қашықтан орнату			
Желілік агент саясатында операциялық жүйенің жаңартуларын конфигурациялау	✓	–	–
Қолданба осалдықтары туралы ақпаратты қарау	✓	–	–
Қолданба осалдықтарын іздеу	✓	–	–
Бағдарламалық жасақтама жаңартуы	✓	–	–
Құрылғыларда орнатылған бағдарламалық жасақтаманы түгендеу	✓	✓	–
Виртуалды машиналар			
Виртуалды машиналарға Желілік агент орнату	✓	✓	✓
VDI үшін параметрлерді оңтайландыру	✓	✓	✓
Динамикалық виртуалды машиналарды қолдау	✓	✓	✓
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	✓	✓	✓
Желілік агентті бір	✓	–	✓

Басқару серверінен екіншісіне ауыстырып қосу (автоматты түрде желілік орналасуы бойынша)			
Клиент құрылғысы мен Басқару сервері арасындағы қосылымды сканерлеу. klnagchk утилитасы	✓	✓	✓
Клиент құрылғысының жұмыс үстеліне қашықтан қосылу	✓	–	✓ Virtual Network Computing (VNC) жүйесін пайдалану.
Деректерді тасымалдау шебері арқылы жеке орнату пакетін жүктеу	✓	✓	✓

Желілік агенттің параметрлерін операциялық жүйелер бойынша салыстыру

Төмендегі кестеде желілік агент орнатылған, басқарылатын құрылғының операциялық жүйесіне байланысты қандай Желілік агент параметрлері қолжетімді екені көрсетілген.

Желілік агенттің параметрлері: операциялық жүйелер бойынша салыстыру

Параметрлер бөлімі	Windows	Linux	macOS
Жалпы	✓	✓	✓
Оқиғаны 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** параметрі қолжетімді.

		• **Жабдық тізімдемесі туралы ақпарат**	
Қосылым мүмкіндігі → Желі	✓	✓ **Microsoft Windows брандмауэрінде Желілік агенттің порттарын ашу** параметрлерінен басқа.	✓
Қосылым мүмкіндігі → Байланыс профильдері	✓	–	✓
Қосылым мүмкіндігі → Байланыс кестесі	✓	✓	✓
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.

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. Төмендегі пәрменді пайдаланып, ресурстарды аз тұтыну режимі қосылған ба екенін тексеріңіз:

   ```
   $ sudo service klnagent64 status
   ```

   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
   ```

3. Төмендегі пәрменді пайдаланып, ресурстарды аз тұтыну режимі өшірілген бе екенін тексеріңіз:

   ```
   $ sudo service klnagent64 status
   ```

   Ресурстарды аз тұтыну режимі өшірулі.

Сондай-ақ, *Скрипттерді қашықтан орындау* тапсырмасының көмегімен ресурстарды аз тұтыну режимін қашықтан қосуға болады.

Kaspersky Endpoint Security саясатын қолмен конфигурациялау

Бұл бөлімде Kaspersky Endpoint Security саясатының параметрлерін конфигурациялау бойынша ұсыныстар бар. Саясат сипаттары терезесінде конфигурациялауды орындауға болады. Параметрді өзгерткен кезде, көрсетілген мәндерді жұмыс станциясына қолдану үшін тиісті параметрлер тобының оң жағындағы құлып белгішесін түртіңіз.

Kaspersky Security Network конфигурациялау

Kaspersky Security Network (KSN) – файлдардың, веб-ресурстардың және бағдарламалық жасақтаманың беделі туралы ақпараты бар бұлтты қызметтер инфрақұрылымы. Kaspersky Security Network бағдарламасы Kaspersky Endpoint Security for Windows бағдарламасына әртүрлі қауіп түрлеріне тезірек жауап беруге, кейбір қорғаныс құрамдастарының тиімділігін арттыруға, сондай-ақ жалған іске қосылудың ықтималдығын азайтуға мүмкіндік береді. Kaspersky Security Network туралы толық ақпарат алу үшін Kaspersky Endpoint Security for Windows құжаттамасын қараңыз.

Ұсынылатын KSN параметрлерін белгілеу үшін:

1. Қолданбаның негізгі терезесінде **Активтер (құрылғылар)** → **Саясат және профильдер** бөліміне өтіңіз.
2. Kaspersky Endpoint Security for Windows саясатын басыңыз.

   Таңдалған саясаттың сипаттар терезесі ашылады.
3. Саясат сипаттары терезесінде **Бағдарлама параметрлері** → **Кеңейтілген қорғаныс** → **Kaspersky Security Network** бөліміне өтіңіз.
4. **KSN прокси-серверін қолдану** параметрі қосулы екеніне көз жеткізіңіз. Бұл параметрді пайдалану желі трафигін қайта таратуға және оңтайландыруға көмектеседі.

   > Managed Detection and Response пайдаланып жатсаңыз, тарату нүктесі және **KSN кеңейтілген режимі үшін** KSN прокси-сервері параметрін қосу керек.
5. KSN прокси-сервері қызметі қолжетімді болмаса, KSN серверлерін қолдануды қосуға болады. KSN серверлері "Лаборатория Касперского" жағында (KPSN пайдаланған кезде) және үшінші тараптарда (KPSN пайдаланған кезде) орналасуы мүмкін.
6. **OK** түймесін басыңыз.

Ұсынылған KSN параметрлері конфигурацияланды.

Желілік экранды қорғайтын желілер тізімін тексеру

Kaspersky Endpoint Security for Windows желілік экраны барлық желілеріңізді қорғайтынына көз жеткізіңіз. Әдепкі бойынша желілік экран келесі қосылым түрлері бар желілерді қорғайды:

- **Жалпыға ортақ желі**. Антивирустық қолданбалар, желілік экрандар немесе сүзгілер мұндай желідегі құрылғыларды қорғамайды.
- **Жергілікті желі**. Бұл желідегі құрылғылар үшін файлдар мен принтерлерге қатынас шектеулі.
- **Сенімді желі**. Мұндай желідегі құрылғылар шабуылдардан және файлдар мен деректерге рұқсатсыз кіруден қорғалған.

Егер сіз пайдаланушы желісін орнатқан болсаңыз, оны желілік экран қорғайтынына көз жеткізіңіз. Ол үшін Kaspersky Endpoint Security for Windows саясатының сипаттарындағы желілер тізімін тексеріңіз. Тізімде кейбір желілер көрсетілмеуі мүмкін.

Желілік экран туралы көбірек білу үшін Kaspersky Endpoint Security for Windows құжаттамасын қараңыз.

Желілер тізімін тексеру үшін:

1. Қолданбаның негізгі терезесінде **Активтер (құрылғылар)** → **Саясат және профильдер** бөліміне өтіңіз.
2. Kaspersky Endpoint Security for Windows саясатын басыңыз.

   Таңдалған саясаттың сипаттар терезесі ашылады.
3. Саясат сипаттарында **Бағдарлама параметрлері** → **Базалық қорғаныс** → **Желілік экран** бөліміне өтіңіз.
4. **Қолжетімді желілер** блогында **Желі параметрлері** сілтемесінен өтіңіз.

   Желілік қосылымдар терезесі көрсетіледі. Бұл терезеде желілер тізімі көрсетіледі.
5. Егер тізімде желі болмаса, оны қосыңыз.

Желілік құрылғыларды тексеруді өшіру

Kaspersky Endpoint Security for Windows қолданбасымен желілік дискілерді тексеру арқасында оларға жүктеме айтарлықтай төмендеуі мүмкін. Тікелей файл серверлерінде тексеруді жүзеге асырған жөн.

Kaspersky Endpoint Security for Windows саясатының сипаттарында желілік дискіні тексеруді өшіруге болады. Осы саясат параметрлерінің сипаттамасын Kaspersky Endpoint Security for Windows құжаттамасынан қараңыз.

Желілік дискіні тексеруді өшіру үшін:

1. Қолданбаның негізгі терезесінде **Активтер (құрылғылар)** → **Саясат және профильдер** бөліміне өтіңіз.
2. Kaspersky Endpoint Security for Windows саясатын басыңыз.

   Таңдалған саясаттың сипаттар терезесі ашылады.
3. Саясаттың сипаттарында **Бағдарлама параметрлері** → **Базалық қорғаныс** → **Файл қауіптерінен қорғаныс** бөліміне өтіңіз.
4. **Қорғаныс аумағы** блогында **Барлық желілік дискілер** параметрін өшіріңіз.
5. **ОК** түймесін басыңыз.

Желілік дискілерді тексеру өшірілген.

Басқару серверінің жадынан бағдарламалық жасақтама туралы мәліметтерді алып тастау

Басқару серверін желілік құрылғыларда іске қосылған қолданба модульдері туралы ақпаратты сақтамайтындай етіп конфигурациялау ұсынылады. Нәтижесінде, Басқару серверінің жады толып кетпейді.

Kaspersky Endpoint Security for Windows саясаты сипаттарында осы ақпаратты сақтауды өшіре аласыз.

Орнатылған қолданба модульдері туралы ақпаратты сақтауды өшіру үшін:

1. Қолданбаның негізгі терезесінде **Активтер (құрылғылар)** → **Саясат және профильдер** бөліміне өтіңіз.
2. Kaspersky Endpoint Security for Windows саясатын басыңыз.

   Таңдалған саясаттың сипаттар терезесі ашылады.
3. Саясат сипаттарында **Бағдарлама параметрлері** → **Жалпы параметрлер** → **Есептер және қоймалар** тармағына өтіңіз.
4. **Басқару серверін хабарландыру** блогында, егер жоғарғы деңгейдегі саясатта **Іске қосылатын қолданбалар туралы** жалаушасы қойылған болса, оны алып тастаңыз.

   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.

Орнатылған қолданба модульдері туралы ақпарат бұдан былай Басқару сервері дерекқорында сақталмайды.

Жұмыс станцияларында Kaspersky Endpoint Security for Windows интерфейсіне қатынасуды конфигурациялау

Егер ұйымның желісіндегі антивирустық қорғанысты Kaspersky Security Center Linux арқылы орталықтан басқару қажет болса, Kaspersky Endpoint Security for Windows саясатының сипаттарындағы интерфейс параметрлерін төменде сипатталғандай көрсетіңіз. Нәтижесінде, сіз жұмыс станцияларында Kaspersky Endpoint Security for Windows бағдарламасына рұқсатсыз қатынасуға және Kaspersky Endpoint Security for Windows параметрлерін өзгертуге жол бермейсіз.

Осы саясат параметрлерінің сипаттамасын Kaspersky Endpoint Security for Windows құжаттамасынан қараңыз.

Ұсынылатын интерфейс параметрлерін белгілеу үшін:

1. Қолданбаның негізгі терезесінде **Активтер (құрылғылар)** → **Саясат және профильдер** бөліміне өтіңіз.
2. Kaspersky Endpoint Security for Windows саясатын басыңыз.

   Таңдалған саясаттың сипаттар терезесі ашылады.
3. Саясат сипаттарында **Бағдарлама параметрлері** → **Жалпы параметрлер** → **Интерфейс** бөліміне өтіңіз.
4. **Пайдаланушымен өзара әрекеттесу** блогында **Интерфейссіз** параметрін таңдаңыз. Жұмыс станцияларында Kaspersky Endpoint Security for Windows пайдаланушы интерфейсін көрсету өшіріледі және олардың пайдаланушылары Kaspersky Endpoint Security for Windows параметрлерін өзгерте алмайды.
5. **Құпиясөзбен қорғауды қосу** блогында қосқышты қосыңыз. Бұл әрекет, жұмыс станцияларында Kaspersky Endpoint Security for Windows параметрлерін рұқсатсыз немесе байқаусызда өзгерту қаупін азайтады.

Kaspersky Endpoint Security for Windows интерфейсінің ұсынылған параметрлері белгіленген.

Басқару сервері дерекқорында маңызды саясат оқиғаларын сақтау

Басқару сервері дерекқорының толып кетуіне жол бермеу үшін дерекқорға тек маңызды оқиғаларды сақтау ұсынылады.

Басқару сервері дерекқорында маңызды оқиғаларды тіркеуді конфигурациялау үшін:

1. Қолданбаның негізгі терезесінде **Активтер (құрылғылар)** → **Саясат және профильдер** бөліміне өтіңіз.
2. Kaspersky Endpoint Security for Windows саясатын басыңыз.

   Таңдалған саясаттың сипаттар терезесі ашылады.
3. Саясат сипаттары терезесінде **Оқиғаны конфигурациялау** қойындысына өтіңіз.
4. **Критикалық** бөлімінде **Оқиғаны қосу** түймесін басып, келесі оқиғаның жанында жалауша қойыңыз:
   - *Лицензиялық келісім бұзылған.*
   - *Қолданбаның автоматты іске қосылуы өшірілген.*
   - *Белсендіру қатесі.*
   - *Белсенді қауіп анықталды. Зарарсыздандыру процедурасын іске қосу керек.*
   - *Зарарсыздандыру мүмкін емес.*
   - *Бұрын ашылған қауіпті сілтеме табылды.*
   - *Процесс үзілді.*
   - *Желілік белсенділікке тыйым салынған.*
   - *Желілік шабуыл анықталды.*
   - *Қолданбаны іске қосуға тыйым салынады.*
   - *Қатынасуға тыйым салынған (жергілікті параметрлер негізінде).*
   - *Қатынасуға тыйым салынған (KSN).*
   - *Жаңартудың жергілікті қатесі.*
   - *Бір уақытта екі тапсырманы орындау мүмкін емес.*
   - *Kaspersky Security Center-мен өзара әрекеттесу қатесі.*
   - *Кейбір құрамдастар жаңартылмаған.*
   - *Файлдарды шифрлау / шифрсыздау ережелерін қолдану қатесі.*
   - *Ықшам режимді белсендіру қатесі.*
   - *Ықшам режимді өшіру қатесі.*

- *Шифрлау модулін жүктеу мүмкін болмады.*
- *Саясатты қолдану мүмкін емес.*
- *Қолданба құрамдастарын өзгерту кезіндегі қате.*

5. **ОК** түймесін басыңыз.
6. **Функционалдық ақау** бөлімінде **Оқиғаны қосу** түймесін басып, келесі оқиғаның жанында ғана жалаушаны қойыңыз: *Тапсырма параметрлері дұрыс емес. Тапсырманың параметрлері қолданылмаған*.
7. **ОК** түймесін басыңыз.
8. **Ескерту** бөлімінде **Оқиғаны қосу** түймесін басып, тек келесі оқиғалардың жанындағы жалаушаларды белгілеңіз:
   - *Қолданбаның өзін-өзі қорғауы өшірілген.*
   - *Қорғаныс құрамдастары өшірулі.*
   - *Резервттегі лицензиялық кілт жарамсыз.*
   - *Қаскүнемдер компьютерге немесе жеке деректерге зиян келтіру үшін пайдалануы мүмкін заңды БҚ табылды (жергілікті параметрлер негізінде).*
   - *Қаскүнемдер компьютерге немесе жеке деректерге зиян келтіру үшін пайдалануы мүмкін заңды БҚ табылды (KSN).*
   - *Нысан жойылды.*
   - *Нысан зарарсыздандырылды.*
   - *Пайдаланушы шифрлау саясатынан бас тартты.*
   - *Файлды әкімші Kaspersky Anti Targeted Attack Platform серверіндегі карантиннен қалпына келтірді.*
   - *Әкімші файлды Kaspersky Anti Targeted Attack Platform серверінде карантинге қойды.*
   - *Әкімшіге қолданбаны іске қосуға тыйым салу туралы хабар жіберу.*
   - *Әкімшіге құрылғыға қатынасу тыйым салу туралы хабар жіберу.*
   - *Әкімшіге веб-бетке қатынасу тыйым салу туралы хабар жіберу.*
9. **ОК** түймесін басыңыз.
10. **Ақпараттық** бөлімінде **Оқиғаны қосу** түймесін басып, тек келесі оқиғалардың жанындағы жалаушаларды белгілеңіз:
    - *Нысанның сақтық көшірмесі жасалды.*
    - *Қолданбаны сынақ режимінде іске қосуға тыйым салынады.*
11. **ОК** түймесін басыңыз.

Басқару сервері дерекқорында маңызды оқиғаларды тіркеу конфигурацияланған.

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 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.

KSN туралы

Kaspersky Security Network (KSN) – файлдардың, веб-ресурстардың және бағдарламалық жасақтаманың беделі туралы "Лаборатория Касперского" жедел білім базасына қатынасуды ұсынатын онлайн-қызметтер инфрақұрылымы. Kaspersky Security Network деректерін пайдалану "Лаборатория Касперского" қолданбаларының қауіптерге реакциясының жоғары жылдамдығын қамтамасыз етеді, кейбір қорғаныс құрамдастарының тиімділігін арттырады, сондай-ақ жалған іске қосылудың ықтималдығын азайтады. KSN қолданбасы "Лаборатория Касперского" беделдік дерекқорларынан басқарылатын құрылғыларға орнатылған қолданбалар туралы ақпаратты алуға мүмкіндік береді.

KSN қолданбасына қатыса отырып, сіз автоматты режимде "Лаборатория Касперского" ұйымына Kaspersky Security Center Linux басқаратын клиент құрылғыларына орнатылған "Лаборатория Касперского" қолданбаларының 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 қолданбасына қатыса отырып, сіз автоматты режимде "Лаборатория Касперского" ұйымына Kaspersky Security Center Linux басқаратын клиент құрылғыларына орнатылған "Лаборатория Касперского" қолданбаларының жұмысы туралы ақпарат беруге келісесіз. Ақпаратты беру, конфигурацияланған KSN бағдарламасына қатынасу параметрлеріне сәйкес орындалады. "Лаборатория Касперского" 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 "Лаборатория Касперского" қолданбалары орнатылған құрылғыларды пайдаланушыларға өз құрылғыларынан 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-прокси параметрлері**KSN-прокси параметрлеріқатынасу параметрлерін конфигурациялай** аласыз.

Қолданба, қолданбаны бастапқы орнату шеберінің жұмысы барысында KSN қолданбасына қосылуға ұсынады. Сіз KSN қолдана бастай аласыз немесе қолданбамен 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 жаңарту кезінде немесе 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 қосулы болған кезде, Kaspersky Security Center Linux бағдарламасы KSN серверлерінің қолжетімді болуын тексереді. Жүйелік DNS арқылы серверлерге қатынасу мүмкін болмаса, қолданба жалпыға ортақ DNS серверлерін пайдаланады. Бұл, қауіпсіздік деңгейіне басқарылатын құрылғылар үшін қолдау көрсетілетіндігіне көз жеткізу үшін керек.

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 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 сипаттарыKSN-прокси параметрлері**KSN-прокси параметрлері 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. Басты мәзірде қажетті Басқару сервері атауының жанындағы параметрлер (⚙) белгішесін басыңыз.

   Басқару серверінің сипаттары терезесі ашылады.

2. **Жалпы** қойындысында **KSN-прокси параметрлері** бөлімін таңдаңыз.

3. Қосқышты **Басқару серверіндегі KSN Проксиді қосу Қосулы** күйіне жылжытыңыз.

   KSN-де клиент құрылғыларынан деректерді беру клиент құрылғыларында жұмыс істейтін Kaspersky Endpoint Security саясатымен реттеледі. Егер жалауша алынып тасталса, KSN бағдарламасына Басқару серверінен және клиент құрылғыларынан Kaspersky Security Center Linux арқылы деректерді 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. Қосқышты **Kaspersky Security Network пайдалану Қосулы** күйіне ауыстырыңыз.

   Егер параметр қосулы болса, клиент құрылғылары патчтарды орнату нәтижелерін "Лаборатория Касперского" бағдарламасына жібереді. Бұл параметрді қосқан кезде KSN мәлімдемесі шарттарын оқып, қабылдағаныңызға көз жеткізіңіз.

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 ақпарат бар хабар пайда болады.

KPSN келесі "Лаборатория Касперского" 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 KSN қолдауы туралы ақпарат алады. Қолданба сипаттары терезесіндегі **Кеңейтілген қорғаныс** бөлімінің **Kaspersky Security Network** бөлімшесінде KSN: KSN немесе KPSN жеткізушісі көрсетіледі.

KSN-прокси параметрлері бөліміндегі Басқару сервер сипаттары терезесінде KSN орнатылмаған болса, Kaspersky Security Center Linux жүйесі Kaspersky Security Network статистикасын жібермейді.

5. Егер прокси-сервер параметрлері Басқару сервер сипаттарында орнатылса, бірақ желі архитектурасы KPSN-ді тікелей пайдалануды талап ететін болса, **KPSN желісіне қосылған кезде прокси-сервер параметрлерін елемеу** жалаушасын белгілеңіз. 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, **Порт арқылы HTTPS** 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-прокси параметрлері** 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 "Лаборатория Касперского" бағдарламасына жібереді.

Тарату нүктесінің Kaspersky Security Network (KSN) бағдарламасына қатынасуын конфигурациялау үшін:

1. Тарату нүктесі қолмен тағайындалғанына көз жеткізіңіз.
2. Басты мәзірде қажетті Басқару сервері атауының жанындағы параметрлер () белгішесін басыңыз.

   Басқару серверінің сипаттары терезесі ашылады.
3. **Жалпы** қойындысында **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 қосу және өшіру

KSN қосу үшін:

1. Басты мәзірде қажетті Басқару сервері атауының жанындағы параметрлер () белгішесін басыңыз.

   Басқару серверінің сипаттары терезесі ашылады.
2. **Жалпы** қойындысында **KSN-прокси параметрлері** бөлімін таңдаңыз.
3. Қосқышты **Басқару серверіндегі KSN Проксиді қосу Қосулы** күйіне жылжытыңыз.

   Нәтижесінде, KSN прокси-сервері қызметі қосылады.
4. Қосқышты **Kaspersky Security Network пайдалану Қосулы** күйіне ауыстырыңыз.

   Нәтижесінде, KSN қосулы болады.

   Егер қосқыш қосулы болса, клиент құрылғылары патчтарды орнату нәтижелерін "Лаборатория Касперского" бағдарламасына жібереді. Қосқышты қоса отырып, сіз KSN мәлімдемесін оқып, оның шарттарын қабылдауыңыз қажет.
5. **Сақтау** түймесін басыңыз.

KSN өшіру үшін:

1. Басты мәзірде қажетті Басқару сервері атауының жанындағы параметрлер (⚙) белгішесін басыңыз.

   Басқару серверінің сипаттары терезесі ашылады.

2. **Жалпы** қойындысында **KSN-прокси параметрлері** бөлімін таңдаңыз.

3. KSN прокси-сервер қызметін өшіру үшін қосқышты **Басқару серверіндегі KSN Проксиді қосу Өшірулі** күйіне қойыңыз немесе қосқышты **Kaspersky Security Network пайдалану Өшірулі** күйіне қойыңыз.

   Осы қосқыштардың бірі өшірулі болса, клиент құрылғылары патчтарды орнату нәтижелерін "Лаборатория Касперского" бағдарламасына жібермейді.

   KPSN пайдалансаңыз, қосқышты **Kaspersky Private Security Network пайдалану Өшірулі** күйіне қойыңыз.

   Нәтижесінде, KSN өшірулі болады.

4. **Сақтау** түймесін басыңыз.

Қабылданған KSN мәлімдемесін қарау

Kaspersky Security Network (KSN) қосқан кезде сіз KSN мәлімдемесін оқып, қабылдауыңыз қажет. Сіз қабылданған KSN мәлімдемесін кез келген уақытта көре аласыз.

Қабылданған KSN мәлімдемесін қарап шығу үшін:

1. Басты мәзірде қажетті Басқару сервері атауының жанындағы параметрлер (⚙) белгішесін басыңыз.

   Басқару серверінің сипаттары терезесі ашылады.

2. **Жалпы** қойындысында **KSN-прокси параметрлері** 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 жаңарту кезінде немесе 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 жаңартқаннан немесе 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. Қолданбаның 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 ретінде әрекет ететін құрылғыда іске қосылған процестердің тізімі көрсетіледі.
2. Іске қосылған процестер тізімінде `/opt/kaspersky/ksc64/sbin/ksnproxy` процесінің іске қосылғанын тексеріңіз.

Егер `/opt/kaspersky/ksc64/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 қолданбалар** → **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.

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 "Лаборатория Касперского" қауіпсіздік қолданбаларының жұмысын басқарады. Тапсырмалардың көмегімен қолданбаларды орнату, іске қосу және тоқтату, файлдарды сканерлеу, қолданбалардың дерекқорлары мен модульдерін жаңарту, қолданбалармен басқа әрекеттер орындалады.

Kaspersky Security Center Web Console серверінде осы қолданба үшін басқару плагині орнатылған жағдайда ғана Kaspersky Security Center Web Console серверінде осы қолданба 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 деректерін сақтық көшірмелеу;
- 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 қолданбасының 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 қолданба 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 қолданба 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 – бұл тапсырма орындалатын құрылғылардың ішкі жиынтығы. 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.

- 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. Негізгі қолданба терезесінде **Активтер (құрылғылар)** → **Тапсырмалар** бөліміне өтіңіз.
2. **Қосу** түймесін басыңыз.

Жаңа тапсырма жасау шебері іске қосылады. Шебердің қадамдарын орындаңыз.

3. **Тапсырманы жасауды аяқтау** бетінде **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.

4. **Аяқтау** түймесін басыңыз.

Тапсырма жасалып, тапсырмалар тізімінде көрсетіледі.

Таңдалған құрылғыларға тағайындалған тапсырманы жасау үшін:

1. Қолданбаның негізгі терезесінде **Активтер (құрылғылар)** → **Басқарылатын 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.

Қолданба әр тапсырманың сипаттарында белгіленген кестеге сәйкес тапсырмаларды орындайды. Тапсырманы кез келген уақытта тапсырмалар тізімінен қолмен іске қосуға болады. Сондай-ақ, **Басқарылатын құрылғылар** тізімінен құрылғыларды таңдап, олар үшін бар тапсырманы орындауға болады.

Тапсырманы қолмен іске қосу үшін:

1. Негізгі қолданба терезесінде **Активтер (құрылғылар)** → **Тапсырмалар** бөліміне өтіңіз.

2. Көрсетілген тапсырмалар тізімінде іске қосқыңыз келетін тапсырманың жанына жалауша қойыңыз.

3. **Іске қосу** түймесін басыңыз.

Тапсырма іске қосылды. Тапсырма күйін **Күйі** бағанында немесе **Нәтиже** түймесін басу арқылы тексере аласыз.

Тапсырмалар тізімін қарап шығу

Сіз Kaspersky Security Center Linux бағдарламасында жасалған тапсырмалар тізімін көре аласыз.

Тапсырмалар тізімін көру үшін,

Негізгі қолданба терезесінде **Активтер (құрылғылар)** → **Тапсырмалар** бөліміне өтіңіз.

Тапсырмалар тізімі көрсетіледі. Тапсырмалар, өздері қатысты болып табылатын қолданбалардың 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 Жалпы** қойындысында, ал тапсырмалар 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, қолданба құрылғыны қайта жүктеуге мүмкіндік бермейді.

Егер бұл параметр қосулы болса, құрылғыны қайта іске қоспас бұрын бұғатталған құрылғылардағы мұндай қолданбалар 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 қолданбаларды қолмен жауып, сол құрылғыларды қайта іске қосуы керек.

Әдепкі бойынша, параметр өшірулі.

- Тапсырма кестесі параметрлері:
  - **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 қолданба 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.

    - **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.

    - **Күн сайын (жазғы уақытқа өтуге қолдау көрсетілмейді)**

Тапсырма, күндер түрінде белгіленген аралықпен жүйелі түрде орындалады. Бұл кесте жазғы уақытты сақтауды қолдамайды. Демек, уақыт жаздың басында немесе соңында бір сағатқа алға немесе артқа ауысқанда, тапсырманың нақты іске қосылу уақыты өзгермейді.

Бұл кестені пайдалану ұсынылмайды. Бұл, Kaspersky Security Center Linux кері үйлесімділігі үшін қажет.

Әдепкі бойынша, тапсырма күн сайын, ағымдағы жүйелік уақытта іске қосылады.

- **Апта сайын**

  Тапсырма апта сайын, көрсетілген күні және көрсетілген уақытта 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.

- **Ай сайын, таңдалған апталардың көрсетілген күндері**

  Тапсырма жүйелі түрде, әр айдың көрсетілген күндерінде, көрсетілген уақытта орындалады.

  Әдепкі бойынша ай күндері таңдалмаған. Әдепкі бойынша басталу уақыты – 18:00.

- **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 "Лаборатория Касперского" қолданбасын 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 қолданбаны 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.

- Есептік жазба параметрлері:
  - **Әдепкі бойынша есептік жазба.**

    Тапсырма, сол тапсырманы орындайтын қолданба 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, құрылғыларды автоматты түрде өшіру қажет болса, **Тапсырманы орындағаннан кейін құрылғыларды өшіру** параметрін 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 қолданба 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, қолданба 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 қолданба 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:

  - **Құрылғылар**

    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 таңдаулары.**

  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. Негізгі қолданба терезесінде **Активтер (құрылғылар)** → **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.

Тапсырманы импорттау үшін:

1. Негізгі қолданба терезесінде **Активтер (құрылғылар)** → **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.

   - **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 қолданбаны 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. Негізгі қолданба терезесінде **Активтер (құрылғылар)** → **Тапсырмалар** бөліміне өтіңіз.
2. **Тапсырмаларды іске қосу үшін есептік жазбалардың сәйкестендіру 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 келетіндігін 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 **Сәйкестендіру 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. Жергілікті тапсырмаларды орындау нәтижелерін қарау мүмкін емес.

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.

Қолданба тегтері

Бұл бөлімде қолданба тегтері сипатталған, оларды жасау және өзгерту, сондай-ақ үшінші тарап қолданбаларына тегтерді тағайындау бойынша нұсқаулар берілген.

Қолданба тегтері туралы

Kaspersky Security Center Linux, үшінші тарап қолданбаларына ("Лаборатории Касперского" компаниясынан басқа өндірушілер шығарған қолданбалар) тегтер тағайындауға мүмкіндік береді. Тег, қолданбаларды топтастыру және іздеу үшін пайдалануға болатын қолданба белгісі болып саналады. Қолданбаға 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.

Қолданба тегтерін жасау

Қолданба тегін жасау үшін:

1. Қолданбаның негізгі терезесінде **Операциялар → Үшінші тарап бағдарламалары → Бағдарлама тегтері** бөліміне өтіңіз.
2. **Қосу** түймесін басыңыз.

   Тег жасау терезесі көрсетіледі.
3. Тегті көрсетіңіз.
4. Өзгерістерді сақтау үшін **OK** түймесін басыңыз.

Жасалған тег қолданба тегтерінің тізімінде пайда болады.

Қолданба тегтерін өзгерту

Қолданба тегін қайта атау үшін:

1. Қолданбаның негізгі терезесінде **Операциялар → 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. Өзгерістерді сақтау үшін **OK** түймесін басыңыз.

Жаңартылған тег қолданба тегтері тізімінде пайда болады.

Қолданбаларға тегтер тағайындау

Қолданбаға тегтер тағайындау үшін:

1. Қолданбаның негізгі терезесінде **Операциялар → Үшінші тарап бағдарламалары → Бағдарламалар тізімдемесі** бөліміне өтіңіз.

2. Тегтерді белгілеу қажет қолданбаны таңдаңыз.

3. **Тегтер** қойындысын таңдаңыз.

   Қойыншада Басқару серверінде бар барлық қолданба тегтері пайда болады. Таңдалған қолданбаға тағайындалған тегтер **Тег белгіленді** бағанындағы жалаушалармен белгіленеді.

4. Тағайындау қажет тегтер үшін **Тег белгіленді** бағанындағы жалаушаларды қойыңыз.

5. Өзгерістерді сақтау үшін **Сақтау** түймесін басыңыз.

Қолданбаға тегтер белгіленді.

Қолданбаларға тағайындалған тегтерді алып тастау

Қолданбадан тегтерді алып тастау үшін:

1. Қолданбаның негізгі терезесінде **Операциялар** → **Үшінші тарап бағдарламалары** → **Бағдарламалар тізімдемесі** бөліміне өтіңіз.

2. Тегтерді алып тастау қажет қолданбаны таңдаңыз.

3. **Тегтер** қойындысын таңдаңыз.

   Қойыншада Басқару серверінде бар барлық қолданба тегтері пайда болады. Таңдалған қолданбаға тағайындалған тегтер **Тег белгіленді** бағанындағы жалаушалармен белгіленеді.

4. Алып тастау қажет тегтер үшін **Тег белгіленді** бағанындағы жалаушаларды алып тастаңыз.

5. Өзгерістерді сақтау үшін **Сақтау** түймесін басыңыз.

Тегтер қолданбадан алынады.

Қолданбалардан алынған тегтер жойылмайды. Қажет болса, оларды қолмен жоюға болады.

Қолданба тегтерін жою

Қолданба тегін жою үшін:

1. Қолданбаның негізгі терезесінде **Операциялар** → **Үшінші тарап бағдарламалары** → **Бағдарлама тегтері** бөліміне өтіңіз.

2. Тізімнен жойғыңыз келетін қолданба тегтерін таңдаңыз.

3. **Жою** түймесін басыңыз.

4. Пайда болған терезеде **OK** түймесін басыңыз.

Таңдалған қолданба тегі жойылды. Жойылған тег, ол тағайындалған барлық қолданбалардан автоматты түрде алынып тасталады.

Құрылғыны басқару құрамдасы бұғаттаған сыртқы құрылғыға автономды қатынас ұсыну

Kaspersky Endpoint Security саясатының Құрылғыны басқару құрамдасында сіз пайдаланушылардың клиент құрылғысына орнатылған немесе қосылған сыртқы құрылғыларға (мысалы, қатты дискілер, камералар немесе Wi-Fi модульдері) қатынасуын басқара аласыз. Бұл клиент құрылғысын сыртқы құрылғылар қосылған кезде жұқтырудан қорғауға және деректердің жоғалуын немесе ағып кетуін болдырмауға мүмкіндік береді.

Егер сізге Құрылғыны басқару құрамдасы бұғаттаған сыртқы құрылғыға уақытша қатынас беру қажет болса, бірақ құрылғыны сенімді құрылғылар тізіміне қосу мүмкін болмаса, сіз сыртқы құрылғыға уақытша офлайн қатынас ұсына аласыз. Офлайн қатынас клиент құрылғысының желіге қатынаса алмайтындығын білдіреді.

Kaspersky Endpoint Security саясатының параметрлерінде, **Бағдарлама параметрлері → Қауіпсіздікті басқару → Құрылғыны басқару** бөлімінде **Уақытша қатынасты сұрауға рұқсат беру** параметрі қосулы болса ғана, құрылғыны басқару бұғаттаған сыртқы құрылғыға офлайн қатынас ұсына аласыз.

Құрылғыны басқару құрамдасы бұғаттаған сыртқы құрылғыға офлайн қатынасты қамтамасыз ету келесі қадамдарды қамтиды:

1. Kaspersky Endpoint Security тілқатысу терезесінде құлыпталған сыртқы құрылғыға қатынас алғысы келетін құрылғының пайдаланушысы қатынасқа сұрау салу файлын жасап, оны Kaspersky Security Center Linux әкімшісіне жібереді.

2. Осы сұрау салуды алғаннан кейін, Kaspersky Security Center Linux әкімшісі қатынас кілті файлын жасап, оны құрылғы пайдаланушысына жібереді.

3. Kaspersky Endpoint Security тілқатысу терезесінде құрылғы пайдаланушысы қатынас кілті файлын іске қосады және сыртқы құрылғыға уақытша қатынас алады.

Құрылғыны басқару құрамдасы бұғаттаған сыртқы құрылғыға уақытша қатынас ұсыну үшін:

1. Қолданбаның негізгі терезесінде **Активтер (құрылғылар) → Басқарылатын құрылғылар** бөліміне өтіңіз.

   Басқарылатын құрылғылардың тізімі көрсетіледі.

2. Бұл тізімде, Құрылғыны басқару құрамдасы бұғаттаған сыртқы құрылғыға қатынас сұрайтын пайдаланушы құрылғысын таңдаңыз.

   Тек бір құрылғыны ғана таңдауға болады.

3. Басқарылатын құрылғылар тізімі үстінде көп нүктелі (...) түймесін басып, **Құрылғыға офлайн режимде қатынасуға рұқсат беру** түймесін басыңыз.

4. Ашылған **Бағдарлама параметрлері** терезесінде, **Құрылғыны басқару** бөлімінде **Шолу** түймесін басыңыз.

5. Пайдаланушыдан алған қатынасқа сұрау салу файлын таңдап, **Ашу** түймесін басыңыз. Файлдың пішімі AKEY болуы тиіс.

   Пайдаланушы қатынасқа сұрау салған бұғатталған құрылғы туралы ақпарат көрсетіледі.

6. **Құрылғыға қосылу ұзақтығы** параметрінің мәнін көрсетіңіз.

Бұл параметр, сіз пайдаланушыға құлыпталған құрылғыға қатынасу мүмкіндігін ұсынатын уақыт ұзақтығын анықтайды. Әдепкі бойынша мәні, пайдаланушы қатынасқа сұрау салу файлын жасау кезінде көрсеткен мән болып табылады.

7. **Белсендіру кезеңі** параметрінің мәнін көрсетіңіз.

   Бұл параметр, пайдаланушы ұсынылған қатынасу кілті арқылы құлыпталған құрылғыға қатынасты белсендіре алатын кезеңді анықтайды.

8. **Сақтау** түймесін басыңыз.

9. Құлыпталған құрылғыға қатынасу кілті бар файлды сақтағыңыз келетін тағайындалған қалтаны таңдаңыз.

10. **Сақтау** түймесін басыңыз.

Нәтижесінде, пайдаланушыға қатынасу кілті файлын жібергенде және оны Kaspersky Endpoint Security тілқатысу терезесінде белсендіргенде, пайдаланушы құлыпталған құрылғыға белгілі бір кезеңге уақытша қатынас алады.

13291-портты ашу үшін klscflag утилитасын пайдалану

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 Linux 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 қолданбаларын 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:

   - Сіз 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-мен өзара әрекеттесу орнатылады және қосылады. Толық ақпарат Kaspersky Industrial CyberSecurity for Networks анықтамасында келтірілген.

2. Kaspersky Industrial CyberSecurity for Networks сервері орнатылған құрылғыны Тағайындалмаған құрылғылар тобынан Басқарылатын құрылғылар тобына жылжытыңыз:

   a. Қолданбаның негізгі терезесінде **Құрылғыны табу және орналастыру → 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. Қолданбаның 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. Қолданбаның негізгі терезесінде **Бақылау және есеп беру → 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-мен 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 екі түрін қолдайды:

- Ұйым қызметкерлерінің есептік жазбалары. Басқару сервер ұйымның желісінде сауалнама жүргізу кезінде осы жергілікті пайдаланушылардың есептік жазбалары туралы мәліметтерді алады.
- Kaspersky Security Center Linux ішкі пайдаланушы есептік жазбалары. Порталда ішкі пайдаланушы есептік жазбаларын жасауға болады. Бұл есептік жазбалар тек Kaspersky Security Center Linux жүйесінде пайдаланылады.

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, **Ішкі түр** сүзгісін **Ішкі** немесе **Жергілікті** өлшемшартына орнатыңыз.

Пайдаланушы рөлдері туралы

Пайдаланушы рөлі (бұдан әрі *рөл* деп те аталады) – бұл құқықтар мен рұқсаттар жиынтығын қамтитын нысан. Рөл, пайдаланушының құрылғысында орнатылған "Лаборатория Касперского" қолданбаларының 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 "Лаборатория Касперского" әр қолданбасы үшін бөлек құрылған саясаттың сипаттары. Рөл әртүрлі қолданбалар үшін жасалған көптеген саясат профильдерімен байланысты. Осылайша, рөл – белгілі бір пайдаланушы түріне арналған параметрлерді біріктіру әдісі болып табылады.

Қол жеткізу құқықтарын басқарудың қолданба функцияларына қол жеткізуді рөлдер негізінде орнату

Kaspersky Security Center Linux қолданбасы рөлдер негізінде Kaspersky Security Center Linux функцияларына және "Лаборатория Касперского" басқарылатын қолданбаларының функцияларына қатынасуды қамтамасыз етеді.

Сіз Kaspersky Security Center Linux пайдаланушылары үшін қолданба 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 қолданбаға 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. Қолданбада 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.

Қолданба 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.

Жалпы функциялар : **ACL тізімдеріне қарамастан нысандарға қол жеткізу** функционалдық аймағы аудитке арналған. Пайдаланушыларға осы функционалды аймақта **Оқу** құқығы берілгенде, олар барлық нысандарға толық **Оқу** рұқсатын алады және жергілікті әкімші құқықтарымен (Linux жүйесіне арналған root) Желілік агент арқылы Басқару серверіне қосылған таңдалған құрылғыларда кез келген жасалған тапсырмаларды орындай алады. Бұл құқықтарды қызметтік міндеттерін орындау үшін қажет пайдаланушылардың шектеулі санына беру ұсынылады.

Кестеде жоқ барлық тапсырмалар, есептер, параметрлер және орнату пакеттері **Жалпы функционал: Базалық функционалдылық** аймағы аймағына жатады.

Қолданба функцияларына қатынасу құқықтары

Функционалдық аймақ	Құқық	Пайдаланушының әрекеті: әрекетті орындауға қажетті құқық	Тапсырма	Есеп
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.
Жалпы функциялар: **ACL тізімдеріне қарамастан, нысандарға қатынасу**	**Оқу.**	Барлық нысандарға қатысты оқуға қатынас алу: **Оқу**.	Жоқ.	Жоқ.
Жалпы функционал: **Базалық функционал**	• **Оқу.** • **Жазу.**	• Виртуалды сервер үшін құрылғыны жылжыту ережелері (жасау, өзгерту немесе	• Жаңартуларды Басқару серверінің қоймасына жүктеп алу.	• Қорғаныс жағдайы ту есеп.

	• **Орындау.** • **Құрылғы таңдаулары бойынша әрекеттерді орындау.**	жою): **Жазу**, **Құрылғы таңдаулары бойынша әрекеттерді орындау**. • Пайдаланушы сертификатының мобильді протоколын (LWNGT) алу: **Оқу**. • Пайдаланушы сертификатының мобильді протоколын (LWNGT) орнату: **Жазу**. • NLA анықтаған желілер тізімін алу: **Оқу**. • NLA анықтаған желілер тізімін қосу, өзгерту немесе жою: **Жазу**. • Топтардың қатынасын бақылау тізімін қарау: **Оқу**. • Операциялық жүйе журналын көру: **Оқу** .	• Есептерді жеткізу. • Орнату пакеттерін тарату. • Қосалқы Басқару серверлеріне қолданбаларды орнату.	• Қауіп-қатер туралы есе • Ең көп зақымдалға құрылғылар туралы есе • Антивирус дерекқорды туралы есе • Қателер тур есеп. • Желілік шабуылдар туралы есе • Пошталық жүйелерді қорғауға ар қолданбала туралы жиы есеп. • Жұмыс станциялар және Windo серверлері қорғау бағдарлама туралы жиы есеп. • Периметрд қорғайтын бағдарлама туралы жиы есеп. • Орнатылған қолданба ту туралы жиы есеп. • Вирус жұққ құрылғылар пайдаланыш туралы есе • Қауіпсіздік мәселелері туралы есе • Оқиғалар ту есеп.

				• Тарату нүктелерінің әрекетінде • Қосалқы Ба серверлері туралы есе • Құрылғылар басқару оқиғалары т есеп. • Осалдықтар туралы есе • Рұқсат берілмеген бағдарлама бойынша ес • Веб-бақыла туралы есе • Басқарылат құрылғылар шифрлауды туралы есе • Жаппай сақ құрылғылар шифрлау кү туралы есе • Шифрланға құрылғыға қатынасу құқықтары т есеп. • Файлдарды шифрлау қа туралы есе • Шифрланға файлдарға қатынасты бұғаттау ту есеп. • Пайдаланы тиімді құқық туралы есе • Құқықтар ту есеп.

Жалпы функциялар: **Жойылған нысандар**	• **Оқу.** • **Жазу.**	• Себетте жойылған нысандарды қарау: **Оқу**. • Себеттен нысандарды жою: **Жазу**.	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.
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**.	• Басқару сервері деректерін сақтық көшірмелеу. • Дерекқорларға қызмет көрсету.	Жоқ.

		• 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 жібере алатын оқиғалардың максималды санын көрсетіңіз: **Жазу**. • Басқару сервері оқиғаларды жібере алатын кезеңді өзгерту: **Жазу**.		
Жалпы функциялар: **"Лаборатория Касперского" қолданбаларын орналастыру**	• **"Лаборатория Касперского" патчтарын басқару.** • **Оқу.** • **Жазу.** • **Орындау.** • **Құрылғы таңдаулары бойынша әрекеттерді орындау.**	Патчты орнатуды растау немесе қабылдамау: **"Лаборатория Касперского" патчтарын басқару**.	Жоқ.	• Виртуалды Басқару серверінің лицензияль кілтін пайда туралы есе • "Лаборатор Касперског қолданбала нұсқалары т есеп. • Үйлесімсіз қосымшала туралы есе • "Лаборатор Касперског қолданба м

				жаңартулар нұсқалары есеп. • Қорғаныс орналастыр туралы есе
Жалпы функциялар: **Лицензиялық кілттерді басқару**	• **Кілт файлын экспорттау.** • **Жазу.**	• Кілт файлын экспорттау: **Кілт файлын экспорттау**. • Басқару серверінің лицензиялық кілтінің параметрлерін өзгерту: **Жазу**.	Жоқ.	Жоқ.
Жалпы функциялар: **Есептерді басқару**	• **Оқу.** • **Жазу.**	• ACL тізімдеріне қарамастан, нысандар үшін есептер жасау: **Жазу**. • ACL тізімдеріне қарамастан, есептерді орындау: **Оқу**.	Жоқ.	Жоқ.
Жалпы функционал: **Басқару серверлері иерархиясы**	**Басқару серверлерінің иерархиясын конфигурациялау**	• Қосалқы Басқару серверлерін қосу, жаңарту немесе жою: **Басқару серверлерінің иерархиясын конфигурациялау**.	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**. • Ішкі пайдаланушыларды басқару:	Жоқ.	Жоқ.

		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.
Жалпы функционал: **Шифрлау кілттерін басқару**	**Жазу.**	Шифрлау кілттерін импорттау: **Жазу**.	Жоқ.	Жоқ.
Жүйені басқару: **Осалдықтар мен патчтарды басқару**	• **Оқу.** • **Жазу.** • **Орындау.**	• Үшінші тарап патчтарының сипаттарын көру: **Оқу**.	• Осалдықтарды түзету. • Қажетті жаңартуларды	Бағдарламалы жасақтаманың жаңартулары т есеп.

	• **Құрылғы таңдаулары бойынша әрекеттерді орындау.**	• Үшінші тарап патчтарының сипаттарын өзгерту: **Жазу**.	орнату және осалдықтарды түзету.	
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 **Іске қосу** арқылы тапсырманы іске қоса алады немесе оны іске қосу үшін жоспарлауы мүмкін. Пайдаланушы **Таңдалған құрылғыларда әрекеттерді орындау** арқылы таңдалған құрылғыларда тапсырманы іске қоса алады.	"Скрипттерді қашықтан орындау"	Жоқ.

Алдын ала анықталған пайдаланушы рөлдері

Kaspersky Security Center Linux пайдаланушыларына тағайындалған пайдаланушы рөлдері оларға қолданбаның функцияларына қатынасу құқықтарының жиынтығын береді.

Виртуалды серверде жасалған пайдаланушыларға басқару серверінде рөлдерді тағайындау мүмкін емес.

Сіз алдын ала анықталған пайдаланушы рөлдерін бұрыннан конфигурацияланған құқықтар жиынтығымен бірге пайдалана аласыз немесе рөлдер жасай аласыз және қажетті құқықтарды өзіңіз конфигурациялай аласыз. 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	Есептердің барлық түрлерімен, сондай-ақ қашықтағы нысандарды қарауды қоса алғанда, барлық қарау операцияларымен кез келген операцияларды орындауға рұқсат етілген (**Жойылған нысандар** аймағы үшін **Оқу** және **Жазу** құқықтары берілген). Басқа операцияларға рұқсат берілмеді. Сіз бұл рөлді ұйымыңыздың аудитін жүргізетін қызметкерге тағайындай аласыз.
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.

Мобильді құрылғыларды басқару: Жалпы және **Жүйені басқару** функционалдық аймағының мүмкіндіктері Kaspersky Security Center Linux-те қолжетімді емес. **Жүйені басқару әкімшісі/операторы** және **Мобильді құрылғыларды басқару әкімшісі/операторы** рөлдері бар пайдаланушының тек **Жалпы функционал**: **Базалық функционал** функционалды аймақта кіру құқықтары бар.

Пайдаланушылардың алдын ала анықталған рөлдерінің құқықтары

Рөл	Сипаттамасы
Басқару серверінің әкімшісі	Келесі функционалдық аймақтарда барлық операцияларға рұқсат береді: **Жалпы функционал**: • **Базалық функционалдылық.** • **Оқиғаларды өңдеу.** • **Басқару серверлерінің иерархиясы.** • **Виртуалды Басқару серверлері.** **Жалпы функционал: Шифрлау кілтін басқару** аймағында **Оқу** және **Жазу** құқықтарын ұсынады.
Басқару серверінің операторы	Барлық келесі функционалдық аймақтарда **Оқу** және **Орындау** құқықтарын ұсынады: **Жалпы функционал**: • **Базалық функционалдылық.** • **Виртуалды Басқару серверлері.**
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.
Қолданбаларды орнату әкімшісі	Келесі функционалдық аймақтарда барлық операцияларға рұқсат береді: **Жалпы функционал**: • **Базалық функционалдылық.** • **"Лаборатория Касперского" қолданбаларын орналастыру.** • **Лицензиялық кілттерді басқару.**

	Жалпы функционал: Виртуалды Басқару серверлері аймағында **Оқу** және **Орындау** құқықтарын ұсынады.
Қолданбаларды орнату операторы	Барлық келесі функционалдық аймақтарда **Оқу** және **Орындау** құқықтарын ұсынады: **Жалпы функционал**: • **Базалық функционалдылық.** • **"Лаборатория Касперского" қолданбаларын орналастыру** (сондай-ақ, осы аймақта **"Лаборатория Касперского" патчтарын басқару** құқықтарын ұсынады). • **Виртуалды Басқару серверлері.**
Kaspersky Endpoint Security әкімшісі	Келесі функционалдық аймақтардағы барлық операцияларға рұқсат береді: • **Жалпы функционал: Базалық функционал.** • Барлық функцияларды қоса алғанда, Kaspersky Endpoint Security аймағы. **Жалпы функционал: Шифрлау кілтін басқару** аймағында **Оқу** және **Жазу** құқықтарын ұсынады.
Kaspersky Endpoint Security операторы	Барлық келесі функционалдық аймақтарда **Оқу** және **Орындау** құқықтарын ұсынады: • **Жалпы функционал: Базалық функционал.** • Барлық функцияларды 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.** **Жалпы функционал: Шифрлау кілтін басқару** аймағында **Оқу** және **Жазу** құқықтарын ұсынады.
Бас оператор	Барлық келесі функционалдық аймақтарда **Оқу** және **Орындау** (қолданылса) құқықтарын ұсынады: • **Жалпы функционал**: • **Базалық функционалдылық.** • **Жойылған нысандар.** • **Басқару серверіне қатысты әрекеттер.** • **"Лаборатория Касперского" қолданбаларын орналастыру.** • **Виртуалды Басқару серверлері.** • Барлық функцияларды қоса алғанда, Kaspersky Endpoint Security аймағы.
Ұялы құрылғыларды басқару әкімшісі	**Жалпы функционал: Базалық функционал** аймағынаймағындағы барлық әрекеттерге рұқсат береді.

Қауіпсіздік қызметінің офицері	Келесі функционалдық аймақтарда барлық операцияларға рұқсат береді: **Жалпы функционал**: • **ACL тізіміне қарамастан, нысандарға қатынасу.** • **Есептерді басқару.** **Жүйені басқару: Қосылымдар** аймағында **Оқу**, **Жазу**, **Орындау**, **Құрылғылардағы файлдарды әкімшінің жұмыс орнында сақтау** және **Құрылғылардың таңдауларында әрекеттерді орындау** құқықтарын ұсынады. 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. Бұл функцияға Kaspersky Security Center 11 және қолданбаның одан жоғары нұсқаларында қолдау көрсетілмейді.
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.

Нысандар жиынтығына қатынасу құқықтарын тағайындау

Сервер деңгейінде қатынасу құқықтарын тағайындауға қосымша ретінде, сіз нақты нысандарға, мысалы, қажетті тапсырмаға қатынасу мүмкіндігін тағайындай аласыз. Қолданба 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:
   - **Активтер (құрылғылар) → Топтардың иерархиясы**.
   - **Активтер (құрылғылар) → Тапсырмалар**.
   - **Бақылау және есеп беру → Есептер**.
   - **Активтер (құрылғылар) → Құрылғы таңдаулары**.
   - **Бақылау және есеп беру → 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 пайдаланушылар топтарына құқықтарды тағайындау

Kaspersky Endpoint Security for Linux сияқты басқару плагиндеріңіз бар "Лаборатория Касперского" Басқару сервері мен қолданбаларының әртүрлі мүмкіндіктерін пайдалану үшін пайдаланушыларға немесе пайдаланушы топтарына құқықтарды тағайындауға болады.

Пайдаланушыға немесе пайдаланушылар тобына рөл тағайындау үшін келесі әрекеттерді орындаңыз:

1. Басты мәзірде қажетті Басқару сервері атауының жанындағы параметрлер (⚙) белгішесін басыңыз.

   Басқару серверінің сипаттары терезесі ашылады.

2. **Қол жеткізу құқықтары** қойындысында құқық тағайындағыңыз келетін пайдаланушы немесе қауіпсіздік тобы атының жанындағы жалаушаны белгілеп, **Қол жеткізу құқықтары** түймесін басыңыз.

   Бір уақытта бірнеше пайдаланушыны немесе қауіпсіздік тобын таңдау мүмкін емес. Бірнеше нысанды таңдасаңыз, **Қол жеткізу құқықтары** түймесі өшірулі болады.

3. Пайдаланушы немесе топ үшін құқықтар жинағын орнатыңыз:

   a. Түйінді Басқару сервер немесе басқа "Лаборатория Касперского" қолданбасының функцияларымен кеңейтіңіз.

   b. Қажетті функцияның немесе қол жеткізу құқығының жанындағы **Рұқсат** немесе **Тыйым салу** жалаушасын белгілеңіз.

1-мысал: пайдаланушыға немесе топқа қолданбаны біріктіру функциясына (**Оқу**, **Жазу** және **Орындау**) барлық қолжетімді қол жеткізу құқықтарын беру үшін **Қолданба 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 функциялар:
  - Басқару топтарын басқару (тек Kaspersky Security Center Linux 11 және одан да жоғары нұсқа үшін).
  - ACL тізіміне қарамастан, нысандарға қатынасу (тек Kaspersky Security Center Linux 11 және одан да жоғары нұсқа үшін).
  - Базалық функционалдылық.
  - Жойылған нысандар (тек Kaspersky Security Center Linux 11 және одан да жоғары нұсқа үшін).
  - Шифрлау кілтін басқару.
  - Оқиғаларды өңдеу.
  - Басқару серверіне қатысты әрекеттер (тек Басқару сервері сипаттары терезесінде).
  - "Лаборатория Касперского" қолданбаларын орналастыру.
  - Лицензиялық кілттерді басқару.
  - Қолданбаларды біріктіру.
  - Есептерді басқару.
  - Басқару серверлерінің иерархиясы.
  - Пайдаланушы рұқсаттары.
  - Виртуалды Басқару серверлері.
- Ұялы құрылғыларды басқару:
  - Жалпы.
  - Self Service Portal.
- Жүйені басқару:
  - Қосылымдар.
  - Жабдықты түгендеу.

- Желіге қатынасуды басқару.
- Операциялық жүйені орналастыру.
- Қашықтан орнату.
- Қолданбалар түгендемесі.

Құқық үшін не **Рұқсат**, не **Тыйым салу** 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 **Тыйым салу** жалаушасы қойылған), онда бұл құқық басқа құқықтар жиынтығында рұқсат етілген немесе анықталмаған болса да, пайдаланушы үшін тыйым салынған болып саналады.

Ішкі пайдаланушының есептік жазбасын қосу

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) (a-z);
       - сандар (0-9);
       - арнайы таңбалар (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;).

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

Енгізген құпиясөзді қарау үшін **Көрсету** түймесін басып тұрыңыз.

Пайдаланушының құпиясөз енгізу әрекеттерінің саны шектеулі. Әдепкі бойынша, енгізу әрекеттерінің максималды саны 10-ға тең. Енгізу әрекеттерінің максималды санын "Құпиясөз енгізу әрекеттерінің санын енгізу" бөлімінде сипатталғандай, өзгертуге болады.

Егер пайдаланушы құпиясөзді бірнеше рет қате енгізсе, пайдаланушы есептік жазбасы бір сағатқа бұғатталады. Сіз есептік жазбаны тек құпиясөзді ауыстыру арқылы бұғаттан босата аласыз.

4. Өзгерістерді сақтау үшін **Сақтау** түймесін басыңыз.

Пайдаланушының есептік жазбасы пайдаланушылар тізіміне қосылды.

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. Өзгерістерді сақтау үшін **Сақтау** түймесін басыңыз.

Қауіпсіздік тобы топтар тізіміне қосылды.

Ішкі пайдаланушының есептік жазбасын өзгерту

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:

- **Сипаттама**
- **Толық атауы**
- **Электрондық пошта мекенжайы**
- **Негізгі телефон нөмірі**
- **Жаңа құпиясөз орнату** 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) (a-z);
    - сандар (0-9);
    - арнайы таңбалар (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;).
  - Құпиясөзде бос орындар, Юникод таңбалары немесе "." таңбасы "@" алдында тұрған кезде "." және "@" тіркесімі болмауы тиіс.

  Енгізілген құпиясөзді қарау үшін, **Көрсету** түймесін басып, оны қажетті уақыт бойы ұстап тұрыңыз.

  > Пайдаланушының құпиясөз енгізу әрекеттерінің саны шектеулі. Әдепкі бойынша, енгізу әрекеттерінің максималды саны 10-ға тең. Сіз рұқсат етілген амалдар санын өзгерте аласыз; алайда, қауіпсіздік тұрғысынан, бұл санды азайтпаған жөн. Егер пайдаланушы құпиясөзді бірнеше рет қате енгізсе, пайдаланушы есептік жазбасы бір сағатқа бұғатталады. Сіз есептік жазбаны тек құпиясөзді ауыстыру арқылы бұғаттан босата аласыз.

- Қажет болса, пайдаланушының қолданбаға қосылуына тыйым салу үшін қосқышты **Өшірулі** күйіне ауыстырыңыз. Мысалы, қызметкер компаниядан жұмыстан шыққаннан кейін, есептік жазбаны өшіруге болады.

4. **Аутентификация қауіпсіздігі** 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. Өзгерістерін сақтау үшін **Сақтау** түймесін басыңыз.

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. Өзгерістерді 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. Қолданбаның 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 ұялы құрылғының иесі етіп тағайындау туралы ақпаратты Kaspersky Security for Mobile анықтамасында 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. Қолданбаның 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** қойындысын таңдаңыз.
5. **Қосу** түймесін басыңыз.
6. Құрылғылар тізімінен пайдаланушыға тағайындағыңыз келетін құрылғыны таңдаңыз.
7. **OK** 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 **Активтер (құрылғылар)** → **Басқарылатын 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, егер сіз 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 шифрін шешеді және пайдаланушы құрылғының иесі ретінде тіркеледі.

Сондай-ақ, Желілік агентті жауап файлымен тыныш режимде орнатқан кезде пайдаланушыны құрылғы иесі ретінде тағайындауға болады. Жауап файлы арқылы тыныш режимде орнату туралы қосымша ақпарат алу үшін мақаланы қараңыз.

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.

Пайдаланушы үшін екі қадамдық тексеру қосылса, сізге қолданбадан уақытша бір реттік құпиясөзді (TOTP) енгізу қажет болады. Екі қадамдық тексеру туралы қосымша ақпарат алу үшін мақаланы қараңыз.

Желілік агентті орнатқаннан кейін пайдаланушыны құрылғы иесі ретінде тағайындау

Пайдаланушыға құрылғы иесі ретінде тіркелуге рұқсат беру үшін:

1. Kaspersky Security Center Web Console веб-консолінде **Табу және орналастыру** → **Орналастыру және тағайындау** → **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 құрылғы иесі ретінде тіркеу үшін:

1. Клиент құрылғысындағы пәрмен желісінде келесі пәрменді іске қосыңыз:
   ```
   $ /opt/kaspersky/klnagent64/bin/nagregister -set_owner
   ```

2. Сұралса, есептік жазбаңыз бен құпиясөзіңізді 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.

Пайдаланушы үшін екі қадамдық тексеру қосылса, сізге қолданбадан уақытша бір реттік құпиясөзді (TOTP) енгізу қажет болады. Екі қадамдық тексеру туралы қосымша ақпарат алу үшін мақаланы қараңыз.

Пайдаланушы құрылғының иесі ретінде тіркелген.

Пайдаланушыны құрылғының иесі етіп тағайындаудың күшін жою

Пайдаланушыны клиент құрылғысында құрылғы иесі ретінде тағайындаудан шығару үшін:

1. Клиент құрылғысындағы пәрмен желісінде келесі пәрменді іске қосыңыз:
   `$ /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.

Пайдаланушы үшін екі қадамдық тексеру қосылса, сізге қолданбадан уақытша бір реттік құпиясөзді (TOTP) енгізу қажет болады. Екі қадамдық тексеру туралы қосымша ақпарат алу үшін мақаланы қараңыз.

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. Қолданбаның 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. Ашылатын пайдаланушы сипаттары терезесінде **Аутентификация қауіпсіздігі** қойындысын таңдаңыз.

4. Есептік жазба параметрлерін өзгерткен кезде есептік деректерді әрбір рет сұрағыңыз келсе, **Аутентификация қауіпсіздігі** қойыншасында **Пайдаланушы есептік жазбасын өзгерту рұқсатын тексеру үшін аутентификацияны сұрау** параметрін таңдаңыз. Не болмаса **Пайдаланушыларға осы есептік жазбаны қосымша аутентификациясыз өзгертуге рұқсат беріңіз** нұсқасын таңдаңыз.

5. **Сақтау** түймесін басыңыз.

Екі қадамдық тексеру

Бұл бөлімде Kaspersky Security Center Web Console серверіне рұқсатсыз кіру қаупін азайту үшін екі қадамдық тексеруді қолдану сипатталған.

Сценарий: барлық пайдаланушылар үшін екі қадамдық тексеруді конфигурациялау

Бұл сценарий, барлық пайдаланушылар үшін екі қадамдық тексеруді қалай қосу керектігін және екі қадамдық тексеруден пайдаланушы есептік жазбаларын қалай алып тастау керектігін сипаттайды. Егер сіз өзіңіздің есептік жазбаңызды басқа пайдаланушылар үшін қоспас бұрын екі қадамдық тексеруді қоспаған болсаңыз, қолданба алдымен сіздің есептік жазбаңыз үшін екі қадамдық тексеруді қосу терезесін ашады. Бұл сценарий сіздің есептік жазбаңыз үшін екі қадамдық тексеруді қалай қосу керектігін де сипаттайды.

Егер сіз өзіңіздің есептік жазбаңыз үшін екі қадамдық тексеруді қосқан болсаңыз, барлық пайдаланушылар үшін екі қадамдық тексеруді қосуға болады.

Алдын ала талаптар

Бастамас бұрын:

- Басқа пайдаланушылардың есептік жазбаларының қауіпсіздік параметрлерін өзгерту үшін есептік жазбаңызда **Жалпы функционал: Пайдаланушы рұқсаттары** функционалдық аймағындағы Нысан ACL параметрлерін өзгерту құқығы бар екеніне көз жеткізіңіз.
- Басқару серверінің басқа пайдаланушылары өз құрылғыларына аутентификация қолданбасын орнатқанына көз жеткізіңіз.

Кезеңдер

Барлық пайдаланушылар үшін екі қадамдық тексеруді қосу келесі кезеңдерден тұрады:

1. **Құрылғыда аутентификация қолданбасы орнатылуда**

   Уақытқа негізделген бір реттік құпиясөз (TOTP) алгоритмін қолдайтын кез келген түпнұсқалықты тексеру қолданбасын орнатуға болады, мысалы:

   - Google Authenticator.
   - Microsoft Authenticator.
   - Bitrix24 OTP.
   - Яндекс кілт.
   - Avanpost Authenticator.
   - Aladdin 2FA.

   Kaspersky Security Center Linux өзіңіз пайдаланғыңыз келетін аутентификация қолданбасын қолдайтынын тексеру үшін, барлық пайдаланушылар немесе белгілі бір пайдаланушы үшін екі факторлы растауды қосыңыз.

   Қадамдардың бірі аутентификация қолданбасы жасаған қауіпсіздік кодын беруді болжайды. Бәрі сәтті болса, Kaspersky Security Center Linux таңдалған түпнұсқалықты тексеру қолданбасын қолдайды.

2. **Аутентификация қолданбасының уақытын және Басқару сервері орнатылған құрылғының уақытын синхрондау**

   Аутентификация қолданбасы бар құрылғыдағы уақыт пен Басқару сервері бар құрылғыдағы уақыт сыртқы уақыт көздері көмегімен UTC-пен синхрондалғанына көз жеткізіңіз. Әйтпесе, түпнұсқалықты тексеру және екі қадамдық тексеруді белсендіру сәтсіз болуы мүмкін.

3. **Екі қадамдық тексеруді қосу және есептік жазбаңызға құпия кілт алу**

   Есептік жазбаңыз үшін екі қадамдық тексеруді қосқаннан кейін, барлық пайдаланушылар үшін екі қадамдық тексеруді қосуға болады.

4. **Барлық пайдаланушылар үшін екі қадамдық тексеруді қосу**

   Екі қадамдық тексеру қосылған пайдаланушылар оны Басқару серверіне кіру үшін пайдалануы керек.

5. **Жаңа пайдаланушыларға өздері үшін екі сатылы растауды орнатуға тыйым салу**

   Kaspersky Security Center Web Console веб-консоліне кіру қауіпсіздігін одан әрі жақсарту үшін жаңа пайдаланушылардың өздері үшін екі сатылы растауды орнатуына тыйым салуға болады.

6. **Қауіпсіздік кодын шығарушының атын өзгерту**

   Аттары ұқсас бірнеше Басқару серверіңіз болса, бәлкім, әртүрлі Басқару серверлерін жақсырақ тану үшін қауіпсіздік кодын шығарушыларын аттарын өзгертуіңізге тура келеді.

7. **Екі қадамдық тексеруді қосуды қажет етпейтін пайдаланушы есептік жазбаларын алып тастау**

   Қажет болса, екі қадамдық тексеруден пайдаланушылардың есептік жазбаларын алып тастаңыз. Есептік жазбалары алынып тасталған пайдаланушыларға Басқару серверіне кіру үшін екі қадамдық тексеруді пайдаланудың қажеті жоқ.

8. **Сіздің есептік жазбаңыз үшін екі қадамдық тексеруді баптау**

   Егер пайдаланушылар екі қадамдық тексеруден алынып тасталмаса және екі қадамдық тексеру әлі есептік жазбалары үшін конфигурацияланбаған болса, олар оны Kaspersky Security Center Web Console веб-консоліне кірген кезде ашылатын терезеде конфигурациялауы керек. Әйтпесе, олар құқықтарына сәйкес Басқару серверіне қол жеткізе алмайды.

Нәтижелер

Бұл сценарийді орындағаннан кейін:

- Сіздің есептік жазбаңыз үшін екі қадамдық тексеру қосулы.
- Жойылған пайдаланушы есептік жазбаларынан басқа Басқару серверінің барлық пайдаланушыларының есептік жазбалары үшін екі қадамдық тексеру кіреді.

Есептік жазбаны екі қадамдық тексеру туралы

Kaspersky Security Center Linux бағдарламасы Kaspersky Security Center Web Console пайдаланушылары туралы екі қадамдық тексеруді ұсынады. Егер сіздің есептік жазбаңызға екі қадамдық тексеру қосылса, Kaspersky Security Center Web Console серверіне 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.

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. Шығарушы аты, аутентификация қолданбасында Басқару сервері идентификаторы ретінде қолданылады. Қауіпсіздік кодын шығарушының атын өзгерткен болсаңыз, жаңа құпия кілтті шығарып, оны аутентификация қолданбасына беру керек. Қауіпсіздік коды бір реттік болып табылады және 90 секундқа дейін жарамды (нақты уақыты әртүрлі болуы мүмкін).

Екі қадамдық тексеру қосылған кез келген пайдаланушы өзінің құпия кілтін қайта енгізе алады. Пайдаланушы қайта берілген құпия кілтпен түпнұсқалық растаманы жасағанда және қолданбаға кіру үшін осы кілтті пайдаланғанда, Басқару сервері пайдаланушы есептік жазбасы үшін жаңа құпия кілтті сақтайды. Егер пайдаланушы жаңа құпия кілтті дұрыс енгізбеген болса, Басқару сервері жаңа құпия кілтті сақтамайды және ағымдағы құпия кілтті алдағы түпнұсқалық растама үшін жарамды күйде қалдырады.

Уақытқа негізделген бір реттік құпия сөз (TOTP) алгоритмін қолдайтын кез келген түпнұсқалық растама бағдарламалық жасақтамасын аутентификация қолданбасы ретінде пайдалануға болады. Мысалы, Google Authenticator. Қауіпсіздік кодын жасау үшін аутентификация қолданбасында орнатылған уақытты Басқару сервері үшін орнатылған уақытпен синхрондау керек.

Kaspersky Security Center Linux өзіңіз пайдаланғыңыз келетін аутентификация қолданбасын қолдайтынын тексеру үшін, барлық пайдаланушылар немесе белгілі бір пайдаланушы үшін екі факторлы растауды қосыңыз.

Қадамдардың бірі аутентификация қолданбасы жасаған қауіпсіздік кодын беруді болжайды. Бәрі сәтті болса, Kaspersky Security Center Linux таңдалған түпнұсқалықты тексеру қолданбасын қолдайды.

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.

Аутентификация қолданбасын бірнеше ұялы құрылғыларға орнату ұсынылады. Құпия кілтті (немесе QR кодын) сақтап қойыңыз және оны қауіпсіз жерде сақтаңыз. Бұл ұялы құрылғыға қатысу мүмкіндігі жоғалған жағдайда Kaspersky Security Center Web Console серверіне қатынасуды қалпына келтіруге көмектеседі.

Kaspersky Security Center Linux бағдарламасын пайдалануды қамтамасыз ету үшін сіз өзіңіздің есептік жазбаңызға екі қадамдық тексеруді қосып, барлық пайдаланушылар үшін екі қадамдық тексеруді қоса аласыз.

Сіз екі қадамдық тексеруден есептік жазбаларды алып тастай аласыз. Бұл түпнұсқалық растама үшін қауіпсіздік кодын ала алмайтын қызметтік есептік жазбалар үшін қажет болуы мүмкін.

Екі қадамдық тексеру келесі ережелерге сәйкес жұмыс істейді:

- Тек **Жалпы функционал: Пайдаланушы рұқсаттары** функционалдық аймағының Нысан ACL параметрлерін өзгерту құқығы бар пайдаланушы ғана барлық пайдаланушылар үшін екі қадамдық тексеруді қоса аласыз.
- Есептік жазбалар үшін екі қадамдық тексеруді қосқан пайдаланушы ғана барлық пайдаланушылар үшін екі қадамдық тексеруді қоса алады.

- Өз есептік жазбасы үшін екі қадамдық тексеруді қосқан пайдаланушы ғана барлық пайдаланушылар үшін қосылған екі қадамдық тексеру тізімінен басқа пайдаланушы есептік жазбаларын алып тастай алады.
- Пайдаланушы екі қадамдық тексеруді тек өзінің есептік жазбасы үшін ғана қоса алады.
- **Жалпы функционал: Пайдаланушы рұқсаттары** функционалдық аймағының Нысан ACL параметрлерін өзгерту құқығы бар және Kaspersky Security Center Web Console серверінде екі қадамдық тексеру арқылы авторизацияланған пайдаланушы: барлық пайдаланушыларға арналған екі қадамдық тексеру өшірулі болса ғана, кез келген басқа пайдаланушы үшін; барлық пайдаланушылар үшін қосылған екі қадамдық тексеру тізімінен алынып тасталған пайдаланушы үшін.
- Екі қадамдық тексеру арқылы Kaspersky Security Center Web Console серверіне кірген кез келген пайдаланушы құпия кілтті қайта ала алады.
- Сіз қазір жұмыс істеп жатқан Басқару серверінің барлық пайдаланушылары үшін екі қадамдық тексеруді қосуға болады. Егер сіз бұл параметрді Басқару серверінде қоссаңыз, оның виртуалды Басқару серверлерінің пайдаланушы есептік жазбалары үшін де осы параметрді қосасыз және қосалқы Басқару серверлерінің пайдаланушы есептік жазбалары үшін екі қадамдық тексеруді қоспайсыз.

Сіздің есептік жазбаңыз үшін екі қадамдық тексеруді қосу

Сіз өзіңіздің есептік жазбаңыз үшін ғана екі қадамдық тексеруді қоса аласыз.

Есептік жазбаңыз үшін екі қадамдық тексеруді қоспас бұрын, ұялы құрылғыда аутентификация қолданбасы орнатылғанына көз жеткізіңіз. Аутентификация қолданбасында орнатылған уақыт Басқару сервері орнатылған құрылғының уақытымен синхрондалғанына көз жеткізіңіз.

Пайдаланушы есептік жазбасы үшін екі қадамдық тексеруді қосу үшін:

1. Қолданбаның негізгі терезесінде **Пайдаланушылар және рөлдер** → **Пайдаланушылар және топтар** бөліміне өтіп, **Пайдаланушылар** қойындысын таңдаңыз.
2. Есептік жазбаңыздың атын басыңыз.
3. Ашылатын пайдаланушы сипаттары терезесінде **Аутентификация қауіпсіздігі** қойындысын таңдаңыз:
   a. **Пайдаланушының атын, құпиясөзін және қауіпсіздік кодын сұрау (екі қадамдық тексеру)** параметрін таңдаңыз. **Сақтау** түймесін басыңыз.
   b. Ашылған екі кезеңді тексеру терезесінде **Екі қадамдық тексеруді орнату жолын қараңыз** түймесін басыңыз.

      Аутентификация қолданбасында құпия кілтті енгізіңіз немесе **QR кодын қарау** түймесін басыңыз және бір реттік қауіпсіздік кодын алу үшін мобильді құрылғыдағы аутентификация қолданбасымен QR кодын сканерлеңіз.
   c. Екі қадамдық тексеру терезесінде аутентификация қолданбасы жасаған қауіпсіздік кодын көрсетіп, **Тексеру және қолдану** түймесін басыңыз.
4. **Сақтау** түймесін басыңыз.

Сіздің есептік жазбаңыз үшін екі қадамдық тексеру қосулы.

Барлық пайдаланушылар үшін екі қадамдық тексеруді қосу

Есептік жазбаңыздың **Жалпы функционал: Пайдаланушы рұқсаттары** функционалдық аймағының Нысан ACL параметрлерін өзгерту құқығы бар болса және сіз екі қадамдық тексеру арқылы түпнұсқалық растаманы орындаған болсаңыз, Басқару серверінің барлық пайдаланушылары үшін екі қадамдық тексеруді қоса аласыз.

Барлық пайдаланушылар үшін екі қадамдық тексеруді қосу үшін:

1. Басты мәзірде қажетті Басқару сервері атауының жанындағы параметрлер (⚙) белгішесін басыңыз.

   Басқару серверінің сипаттары терезесі ашылады.

2. Сипаттар терезесінің **Аутентификация қауіпсіздігі** қойыншасында **барлық пайдаланушылар үшін екі қадамдық** тексеруді қосыңыз.

3. Егер сіз өзіңіздің есептік жазбаңыз үшін екі кезеңді тексеруді қоспаған болсаңыз, қолданба сіздің есептік жазбаңыз үшін екі қадамдық тексеруді қосу терезесін ашады.

   a. Ашылған екі кезеңді тексеру терезесінде **Екі қадамдық тексеруді орнату жолын қараңыз** түймесін басыңыз.

   b. Аутентификация қолданбасында құпия кілтті қолмен енгізіңіз немесе **QR кодын қарау** түймесін басыңыз және бір реттік қауіпсіздік кодын алу үшін мобильді құрылғыдағы аутентификация қолданбасымен QR кодын сканерлеңіз.

   c. Екі қадамдық тексеру терезесінде аутентификация қолданбасы жасаған қауіпсіздік кодын көрсетіп, **Тексеру және қолдану** түймесін басыңыз.

Екі кезеңді тексеру барлық пайдаланушылар үшін қосылған. Басқару сервері пайдаланушылары, соның ішінде барлық пайдаланушылар үшін екі қадамдық тексеруді қосқаннан кейін қосылған пайдаланушылар, есептік жазбалары екі қадамдық тексеруден алынып тасталған пайдаланушылардан басқа, өз есептік жазбалары үшін екі қадамдық тексеруді орнатуы керек.

Пайдаланушы есептік жазбасы үшін екі қадамдық тексеруді өшіру

Есептік жазбаңыз үшін, сондай-ақ кез келген басқа пайдаланушының есептік жазбасы үшін екі қадамдық тексеруді өшіруге болады.

Жалпы функционал: Пайдаланушы рұқсаттары функционалдық аймағының Нысан ACL параметрлерін өзгерту құқығы бар есептік жазбаңыз болса, пайдаланушылардың басқа есептік жазбалары үшін екі қадамдық тексеруді өшіруге болады.

Пайдаланушы есептік жазбасы үшін екі қадамдық тексеруді өшіру үшін:

1. Қолданбаның негізгі терезесінде **Пайдаланушылар және рөлдер** → **Пайдаланушылар және топтар** бөліміне өтіп, **Пайдаланушылар** қойындысын таңдаңыз.

2. Екі қадамдық тексеруді өшіргіңіз келетін ішкі пайдаланушы есептік жазбасын басыңыз. Бұл сіздің жеке есептік жазбаңыз немесе кез келген басқа пайдаланушының есептік жазбасы болуы мүмкін.

3. Ашылатын пайдаланушы сипаттары терезесінде **Аутентификация қауіпсіздігі** қойындысын таңдаңыз.

4. Пайдаланушының есептік жазбасы үшін екі сатылы растауды өшіргіңіз келсе, **Тек пайдаланушының аты мен құпиясөзін сұрау** параметрін таңдаңыз.

5. **Сақтау** түймесін басыңыз.

Сіздің есептік жазбаңыз үшін екі қадамдық тексеру өшірулі.

Барлық пайдаланушылар үшін екі қадамдық тексеруді өшіру

Сіздің есептік жазбаңыз үшін екі қадамдық тексеру қосулы болса және сіздің есептік жазбаңызда **Жалпы функционал: Пайдаланушы рұқсаттары** функционалдық аймағының Нысанның ACL тізіміндерін өзгерту құқығы болса, сіз барлық пайдаланушылар үшін екі қадамдық тексеруді өшіре аласыз. Егер сіздің есептік жазбаңыз үшін екі қадамдық тексеру қосылмаған болса, оны барлық пайдаланушылар үшін өшірмес бұрын, есептік жазбаңыз үшін екі қадамдық тексеруді қосу қажет.

Барлық пайдаланушылар үшін екі қадамдық тексеруді өшіру үшін:

1. Басты мәзірде қажетті Басқару сервері атауының жанындағы параметрлер (⚙) белгішесін басыңыз.

   Басқару серверінің сипаттары терезесі ашылады.

2. Сипаттар терезесінің **Аутентификация қауіпсіздігі** қойындысында **барлық пайдаланушылар үшін екі сатылы растау** қосқышын өшіріңіз.

3. Түпнұсқалық растама терезесінде өзіңіздің есептік жазбаңыздың есептік деректерін енгізіңіз.

Барлық пайдаланушылар үшін екі қадамдық тексеру өшірулі.

Есептік жазбаларды екі қадамдық тексеруден алып тастау

Жалпы функциялар: Пайдаланушы рұқсаттары функционалдық аймағының Нысанның ACL тізімдерін өзгерту құқығыңыз бар болса, пайдаланушылардың есептік жазбаларын екі қадамдық тексеруден алып тастай аласыз.

Егер пайдаланушы есептік жазбасы барлық пайдаланушылар үшін екі сатылы тексеру тізімінен алынып тасталса, бұл пайдаланушыға екі қадамдық тексеруді пайдаланудың қажеті жоқ.

> Екі қадамдық тексеруден есептік жазбаларды алып тастау түпнұсқалық растама кезінде қауіпсіздік кодын бере алмайтын қызметтік есептік жазбалар үшін қажет болуы мүмкін.

Егер сіз кейбір пайдаланушы есептік жазбаларын екі қадамдық тексеруден алып тастағыңыз келсе:

1. Басты мәзірде қажетті Басқару сервері атауының жанындағы параметрлер (⚙) белгішесін басыңыз.

   Басқару серверінің сипаттары терезесі ашылады.

2. Екі қадамдық тексеру үшін ерекшеліктер кестесіндегі сипаттар терезесінің **Аутентификация қауіпсіздігі** қойыншасында **Қосу** түймесін басыңыз.

3. Ашылған терезеде:

   a. Жойғыңыз келетін пайдаланушы есептік жазбасын таңдаңыз.

   b. **OK** түймесін басыңыз.

Таңдалған пайдаланушы есептік жазбалары екі қадамдық тексеруден шығарылады.

Сіздің есептік жазбаңыз үшін екі қадамдық тексеруді баптау

Екі сатылы растауды қосқаннан кейін, Kaspersky Security Center Linux жүйесіне алғаш рет кірген кезде есептік жазбаңызға арналған екі сатылы растау параметрлері терезесі ашылады.

Есептік жазбаңыз үшін екі қадамдық тексеруді конфигурацияламас бұрын, ұялы құрылғыда аутентификация қолданбасы орнатылғанына көз жеткізіңіз. Аутентификация қолданбасы бар құрылғыдағы уақыт пен Басқару сервері бар құрылғыдағы уақыт сыртқы уақыт көздері көмегімен UTC-пен синхрондалғанына көз жеткізіңіз.

Есептік жазба үшін екі қадамдық тексеруді конфигурациялау үшін:

1. Ұялы құрылғыдағы аутентификация қолданбасын пайдаланып бір реттік қауіпсіздік кодын жасаңыз. Ол үшін келесі әрекеттердің бірін орындаңыз:

   - Құпия кілтті аутентификация қолданбасына қолмен енгізіңіз.
   - **QR кодын қарау** түймесін басып, QR кодын аутентификация қолданбасымен сканерлеңіз.

   Қауіпсіздік коды ұялы құрылғыңызда көрсетіледі.

2. Екі қадамдық тексеру параметрі терезесінде аутентификация қолданбасы жасаған қауіпсіздік кодын көрсетіп, **Тексеру және қолдану** түймесін басыңыз.

Сіздің есептік жазбаңыз үшін екі қадамдық тексеру конфигурацияланған. Сіздің құқықтарыңызға сәйкес Басқару серверіне қатынасу мүмкіндігі бар.

Жаңа пайдаланушыларға өздері үшін екі сатылы растауды орнатуға тыйым салу

Kaspersky Security Center Web Console веб-консоліне кіру қауіпсіздігін одан әрі жақсарту үшін жаңа пайдаланушылардың өздері үшін екі сатылы растауды орнатуына тыйым салуға болады.

Бұл параметр қосылса, жаңа домен әкімшісі сияқты екі сатылы растауды өшірген пайдаланушы өзі үшін екі сатылы растауды орната алмайды. Демек мұндай пайдаланушыны басқару серверінде аутентификациялау мүмкін емес және ол екі сатылы растау қосылған басқа Kaspersky Security Center Linux әкімшісінің рұқсатынсыз Kaspersky Security Center Web Console жүйесіне кіре алмайды.

Бұл параметр екі сатылы растау барлық пайдаланушылар үшін қосылған болса қолжетімді болады.

Жаңа пайдаланушылардың өздері үшін екі сатылы растауды орнатуына тыйым салу үшін:

1. Басты мәзірде қажетті Басқару сервері атауының жанындағы параметрлер (⚙) белгішесін басыңыз.

   Басқару серверінің сипаттары терезесі ашылады.

2. Сипаттар терезесіндегі **Аутентификация қауіпсіздігі** қойындысында **Жаңа пайдаланушыларға екі сатылы растау параметрлерін өз бетінше орнатуға тыйым салу** қосқышын қосыңыз.

Бұл параметр екі сатылы растау ерекшеліктеріне қосылған пайдаланушы есептік жазбаларына әсер етпейді.

Екі сатылы растау өшірілген пайдаланушыға Kaspersky Security Center Web Console консоліне кіру рұқсатын беру үшін **Жаңа пайдаланушыларға екі сатылы растау параметрлерін өз бетінше орнатуға тыйым салу** параметрін уақытша өшіріңіз, пайдаланушыдан екі сатылы растауды қосуды сұраңыз, содан кейін параметрді қайтадан қосыңыз.

Жаңа құпия кілтті жасау

Есептік жазбаңызды екі қадамдық тексеру үшін, екі қадамдық тексеру арқылы авторизацияланған болсаңыз ғана жаңа құпия кілт жасай аласыз.

Пайдаланушы есептік жазбасы үшін жаңа құпия кілт жасау үшін:

1. Қолданбаның негізгі терезесінде **Пайдаланушылар және рөлдер** → **Пайдаланушылар және топтар** бөліміне өтіп, **Пайдаланушылар** қойындысын таңдаңыз.

2. Екі қадамдық тексеру үшін жаңа құпия кілт жасағыңыз келетін пайдаланушы есептік жазбасын басыңыз.

3. Ашылатын пайдаланушы сипаттары терезесінде **Аутентификация қауіпсіздігі** қойындысын таңдаңыз.

4. **Аутентификация қауіпсіздігі** қойыншасында **Жаңа құпия кілтті жасау** сілтемесінен өтіңіз.

5. Ашылған екі қадамдық тексеру терезесінде аутентификация қолданбасы жасаған жаңа қауіпсіздік кілтін көрсетіңіз.

6. **Тексеру және қолдану** түймесін басыңыз.

Пайдаланушы үшін жаңа құпия кілт жасалды.

Егер сіз ұялы құрылғыңызды жоғалтсаңыз, аутентификация қолданбасын басқа ұялы құрылғыға орнатуға және Kaspersky Security Center Web Console сервисіне қатынасуды қалпына келтіру үшін жаңа құпия кілт жасауға болады.

Қауіпсіздік кодын шығарушының атын өзгерту

Сізде әртүрлі Басқару серверлері үшін бірнеше идентификаторлар болуы мүмкін (оларды шығарушылар деп те атайды). 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 атын өзгерткеннен кейін, жаңа құпия кілтті қайта шығарып, оны аутентификация қолданбасына беру керек.

Қауіпсіздік кодын шығарушының жаңа атын көрсету үшін:

1. Басты мәзірде қажетті Басқару сервері атауының жанындағы параметрлер (⚙) белгішесін басыңыз.

   Басқару серверінің сипаттары терезесі ашылады.

2. Ашылатын пайдаланушы сипаттары терезесінде **Аутентификация қауіпсіздігі** қойындысын таңдаңыз.

3. **Аутентификация қауіпсіздігі** қойындысында **Өңдеу** сілтемесіне өтіңіз.

   Қауіпсіздік кодын шығарушыны өңдеу бөлімі ашылады.

4. Қауіпсіздік кодын шығарушының жаңа атын көрсетіңіз.

5. **OK** түймесін басыңыз.

Басқару сервері үшін қауіпсіздік кодын шығарушының жаңа аты көрсетілген.

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.

3. **Жою** түймесін басыңыз.

4. Пайда болған терезеде **OK** түймесін басыңыз.

Пайдаланушы немесе қауіпсіздік тобы жойылды.

Пайдаланушы рөлін жасау

Пайдаланушы рөлін жасау үшін:

1. Қолданбаның 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** қойындысында рөл атауын өзгертіңіз.

     Алдын ала анықталған рөл атауларын өзгерте алмайсыз.
   - **Параметрлер** қойыншасында рөлдің әрекет ету ауқымын, сондай-ақ рөлмен байланысты саясаттар мен саясат профильдерін өзгертіңіз.
   - **Қатынасу құқықтары** қойыншасында "Лаборатория Касперского" қолданбаларына қатынасу құқықтарын өзгертіңіз.
6. Өзгерістерді сақтау үшін **Сақтау** түймесін басыңыз.

Жасалған рөл пайдаланушы рөлдері тізімінде пайда болады.

Пайдаланушы рөлін өзгерту

Пайдаланушы рөлін өзгерту үшін:

1. Қолданбаның негізгі терезесінде **Пайдаланушылар және рөлдер** → **Рөлдер** бөліміне өтіңіз.
2. Өзгерту қажет рөлді таңдаңыз.
3. Ашылған терезеде рөл параметрлерін өзгертіңіз:
   - **Жалпы** қойындысында рөл атауын өзгертіңіз.

     Алдын ала анықталған рөл атауларын өзгерте алмайсыз.
   - **Параметрлер** қойыншасында рөлдің әрекет ету ауқымын, сондай-ақ рөлмен байланысты саясаттар мен саясат профильдерін өзгертіңіз.
   - **Қатынасу құқықтары** қойыншасында "Лаборатория Касперского" қолданбаларына қатынасу құқықтарын өзгертіңіз.

4. Өзгерістерді 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. Қолданбаның 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. Сипаттар терезесін жабу үшін **Жабу** (⨯) түймесін басыңыз.

Таңдалған пайдаланушылар, қауіпсіздік топтары және басқару топтары рөл аймағына қосылды.

Пайдаланушы рөлін жою

Пайдаланушы рөлін жою үшін:

1. Қолданбаның 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 қолданбаларды іске қосуға тыйым салады. Қалалық навигация қолданбалары "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 қолданбаларын қолдануға рұқсат беретін саясат профилін жасауға болады. Барлық басқа саясат параметрлері өзгеріссіз қалады. Тек "Курьер" рөлі бар пайдаланушыларға қалалық навигация қолданбаларын пайдалануға рұқсат етіледі. Содан кейін, басқа қызметкерге "Курьер" рөлі тағайындалса, онда бұл қызметкер сіздің ұйымыңызға тиесілі құрылғыда қалалық навигациялық қолданбаларды қолдана алады. Алайда, осы басқару тобының басқа құрылғыларында қалалық навигациялық қолданбаларды пайдалануға тыйым салынады.

Рөлді саясат профилімен байланыстыру үшін:

1. Қолданбаның негізгі терезесінде **Пайдаланушылар және рөлдер** → **Рөлдер** бөліміне өтіңіз.
2. Саясат профилімен байланыстырылатын рөлді таңдаңыз.

   Жалпы қойыншасында рөл сипаттары терезесі ашылады.
3. **Параметрлер** қойындысына өтіп, **Саясат және профильдер** бөліміне төмен жылжыңыз.
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.

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. Негізгі қолданба терезесінде **Активтер (құрылғылар)** → **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.

   - **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 қолданбаны 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. Негізгі қолданба терезесінде **Активтер (құрылғылар)** → **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.

   - **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 қолданбаны 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.

"Лаборатория Касперского" дерекқорлары мен қолданбаларын жаңарту

Бұл бөлімде тұрақты жаңартулар үшін орындау қажет қадамдар сипатталған:

- "Лаборатория Касперского" дерекқорлары мен қолданба модульдері;
- Kaspersky Security Center Linux құрамдастары мен қауіпсіздік қолданбаларын қоса алғанда, "Лаборатория Касперского" орнатылған қолданбалары.

Сценарий: "Лаборатория Касперского" қолданбалары мен дерекқорларын үнемі жаңартып тұру

Бұл бөлімде "Лаборатория Касперского" дерекқорлары, қолданба модульдері мен қолданбаларын 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 қолдауға тиіссіз.

Желі қорғанысына, келесіні үнемі жаңартып тұру арқылы қолдау көрсетіледі:

- "Лаборатория Касперского" дерекқорлары мен қолданба модульдері;
- Kaspersky Security Center Linux құрамдастары мен қауіпсіздік қолданбаларын қоса алғанда, "Лаборатория Касперского" орнатылған қолданбалары.

Сіз осы сценарийді аяқтағаннан кейін, келесіге сенімді бола аласыз:

- Сіздің желіңіз Kaspersky Security Center Linux құрамдастары мен қауіпсіздік қолданбаларын қоса алғанда, "Лаборатория Касперского" ең соңғы бағдарламалық жасақтамасымен қорғалған.
- Желі қауіпсіздігі үшін критикалық тұрғыдан маңызды болып саналатын "Лаборатория Касперского" антивирустық дерекқорлары мен басқа да дерекқорлары, әрдайым өзекті.

Алдын ала талаптар

Басқарылатын құрылғылардың Басқару серверімен қосылымы болуы тиіс. Құрылғылардың қосылымы болмаса, "Лаборатория Касперского" дерекқорлары, қолданба модульдері мен қолданбаларын қолмен немесе тікелей "Лаборатория Касперского" 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 "Лаборатория Касперского" қолданбаларын орналастыру сценарийіне сәйкес басқарылатын құрылғыларда "Лаборатория Касперского" қауіпсіздік қолданбалары 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.

"Лаборатория Касперского" қолданбалары мен дерекқорларын жаңарту келесі кезеңдерден тұрады:

1. **Жаңарту схемасын таңдау**

   Қауіпсіздік қолданбаларына 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 "Лаборатория Касперского" жаңартулар серверлерінен Басқару сервері қоймасына, сондай-ақ Kaspersky Security Center Linux үшін дерекқорлар мен қолданба модульдерінің 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 "Лаборатория Касперского" жаңарту серверлерінен жүктейтін етіп конфигурациялай аласыз. Басқару сервері мен тарату нүктелері арасындағы трафик "Лаборатория Касперского" 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 орындарының қоймаларына жүктеп алу* тапсырмасы жасалған кезде, тарату нүктелері жаңартуларды Басқару сервері қоймасынан емес, "Лаборатория Касперского" жаңарту серверлерінен жүктейді.

   Нұсқаулар: Жаңартуларды тарату орындарының қоймаларына жүктеп алу тапсырмасын жасау

4. **Тарату нүктелерін конфигурациялау**

   Сіздің желіңізге тарату нүктелері тағайындалған болса, **Жаңартуларды тарату** 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 "Лаборатория Касперского" бүкіл дерекқор файлдарының немесе қолданба модульдерінің орнына айырмашылық файлдарын жүктейді. Айырмашылықтар файлы дерекқор немесе қолданба модульдері файлдарының екі нұсқасы арасындағы айырмашылықтарды сипаттайды. Сондықтан, айырмашылық файлдары бүкіл файлдарға қарағанда аз орын алады. Нәтижесінде, Басқару сервері мен басқарылатын құрылғылар арасындағы трафик азаяды. Бұл мүмкіндікті пайдалану үшін *Жаңартуларды Басқару серверінің қоймасына жүктеп алу* және/немесе *Жаңартуларды тарату орындарының қоймаларына жүктеп алу* тапсырмасының сипаттарындағы **diff файлдарды жүктеп алу** параметрін қосыңыз.

   Нұсқаулар: "Лаборатория Касперского" дерекқорлары мен қолданба модульдерін жаңарту үшін айырмашылық файлдарын пайдалану

6. **Қауіпсіздік қолданбалары үшін жаңартуларды автоматты түрде орнатуды конфигурациялау**

"Лаборатория Касперского" қолданба модульдерін және дерекқорларын, соның ішінде антивирустық базаларды уақтылы жаңартуды қамтамасыз ету мақсатында, басқарылатын қолданбалар үшін *Жаңарту* тапсырмасын жасаңыз. Уақтылы жаңартуды қамтамасыз ету үшін тапсырма кестесін конфигурациялау кезінде **Қоймаға жаңартуларды жүктеу кезінде** нұсқасын таңдау ұсынылады.

Егер сіздің желіңізде тек IPv6 қолдайтын құрылғылар болса және сіз осы құрылғыларда орнатылған қауіпсіздік қолданбаларын үнемі жаңартып отырғыңыз келсе, басқарылатын құрылғыларда 13.2 нұсқасындағы Басқару сервері және 13.2 нұсқасындағы Желілік агент орнатылғанына көз жеткізіңіз.

Егер жаңарту Лицензиялық келісімнің шарттарын қабылдауды талап етсе, алдымен Лицензиялық келісімнің шарттарын оқып, қабылдауыңыз қажет. Осыдан кейін, жаңартулар басқарылатын құрылғыларға таратылуы мүмкін.

7. **"Лаборатория Касперского" 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. "Лаборатория Касперского" басқаратын қолданбаны 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 құрылғыларында орнатылған "Лаборатория Касперского" 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.

Нәтижелер

Сценарий аяқталғаннан кейін Kaspersky Security Center Linux жүйесі жаңартулар Басқару серверінің қоймасына жүктелгеннен кейін "Лаборатория Касперского" дерекқорларын жаңарту үшін конфигурацияланды. Енді сіз желі жұмысын бақылауға кірісе аласыз.

Дерекқорларды, қолданба модульдерін және "Лаборатория Касперского" қолданбаларын жаңарту туралы

Басқару серверлері мен басқарылатын құрылғыларды қорғау жаңартылған күйде екеніне көз жеткізу үшін келесі жаңартуларды уақтылы ұсыну қажет:

- "Лаборатория Касперского" дерекқорлары мен қолданба модульдері.

  Kaspersky Security Center Linux қолданбасы "Лаборатория Касперского" дерекқорлары мен қолданба модульдерін жүктемес бұрын "Лаборатория Касперского" серверлерінің қолжетімділігін тексереді. Жүйелік DNS арқылы серверлерге қатынасу мүмкін болмаса, қолданба жалпыға ортақ DNS серверлерін пайдаланады. Бұл антивирустық дерекқорларды жаңарту және басқарылатын құрылғылардың қауіпсіздік деңгейін сақтау үшін қажет.

- Kaspersky Security Center Linux құрамдастары мен қауіпсіздік қолданбаларын қоса алғанда, "Лаборатория Касперского" орнатылған қолданбалары.

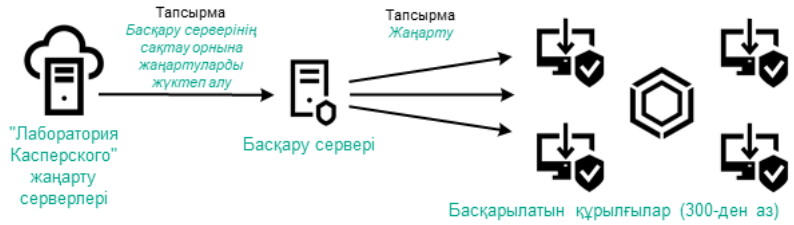
Kaspersky Security Center Linux сізге Windows жүйесімен жұмыс істейтін клиенттік құрылғыларда орнатылған Желілік агент пен "Лаборатория Касперского" қолданбаларын автоматты түрде жаңартуға мүмкіндік береді. Басқару серверін, Kaspersky Security Center Web Console веб-консолін және веб-басқару плагиндерін үздіксіз жаңартуға қолдау көрсетілмейді. Бұл компоненттерді жаңарту үшін, олардың соңғы нұсқаларын "Лаборатория Касперского" 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* тапсырмасы.
  - *Жаңартуларды тарату орындарының қоймаларына жүктеп алу* тапсырмасы.
- Жергілікті қалта, ортақ қатынасы бар қалта немесе FTP сервері арқылы қолмен
- Басқарылатын құрылғылардағы Kaspersky Endpoint Security үшін "Лаборатория Касперского" 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).



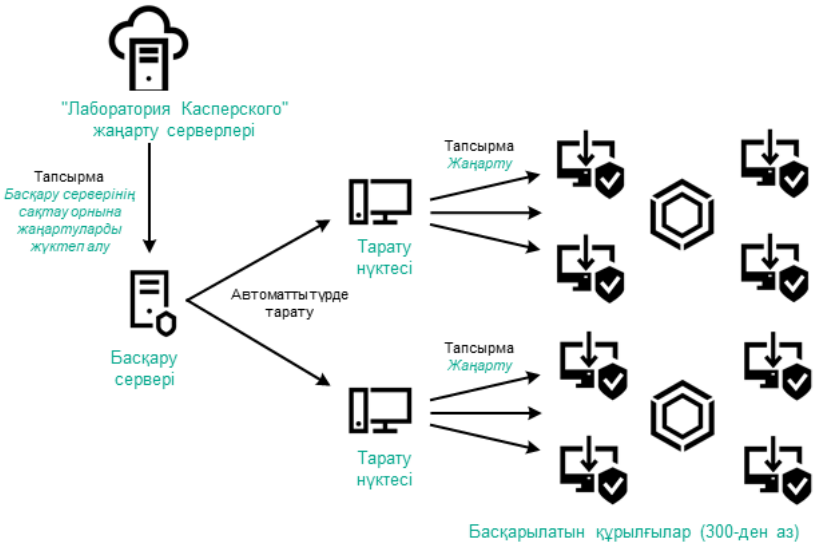
Жаңартуларды Басқару серверінің қоймасына жүктеп алу тапсырмасын қолдану арқылы және тарату нүктелерінсіз жаңарту

Жаңарту көзі ретінде сіз "Лаборатория Касперского" жаңарту серверлерін ғана емес, сонымен қатар жергілікті немесе желілік қалтаны да пайдалана аласыз.

Әдепкі бойынша, Басқару сервері "Лаборатория Касперского" 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 "Лаборатория Касперского" дерекқорларының жаңартулары және Kaspersky Endpoint Security үшін қолданба 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.

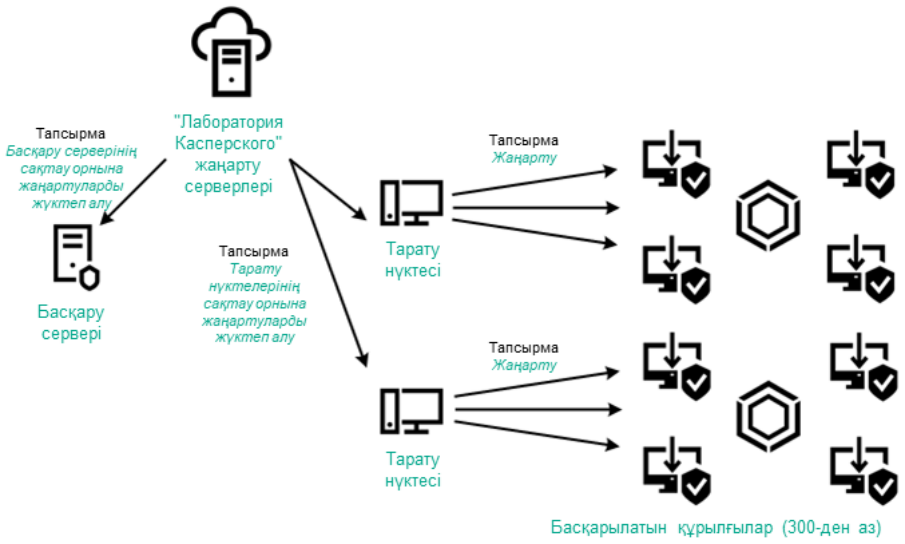
Әрбір басқарылатын "Лаборатория Касперского" қолданбасы Басқару серверінен қажетті жаңартуларды сұрайды. Басқару сервері осы сұрауларды біріктіреді және тек қолданбалар сұрайтын жаңартуларды жүктейді. Осылайша, тек қажетті жаңартулар және тек бір рет қана жүктелетіні қамтамасыз етіледі. *Жаңартуларды Басқару серверінің қоймасына жүктеп алу* тапсырмасын орындау кезінде "Лаборатория Касперского" дерекқорлары мен қолданба модульдерінің қажетті нұсқаларының жүктелуін қамтамасыз ету үшін "Лаборатория Касперского" жаңарту серверлеріне автоматты түрде Басқару сервері мынадай ақпаратты жібереді:

- қолданбаның идентификаторы және нұсқасы;
- қолданбаны 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. "Лаборатория Касперского" АҚ алынған ақпаратты заңда белгіленген талаптарға сәйкес қорғайды.

Екі тапсырманы пайдалану: Жаңартуларды Басқару серверінің қоймасына жүктеп алу және Жаңартуларды тарату орындарының қоймаларына жүктеп алу

Тарату нүктелерінің қоймаларына жаңартуларды Басқару сервері қоймасының орнына тікелей "Лаборатория Касперского" жаңарту серверлерінен жүктеп алуға болады, содан кейін жаңартуларды басқарылатын құрылғыларға таратуға болады (төмендегі суретті қараңыз). Басқару сервері мен тарату нүктелері арасындағы трафик "Лаборатория Касперского" 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 орындарының қоймаларына жүктеп алу*

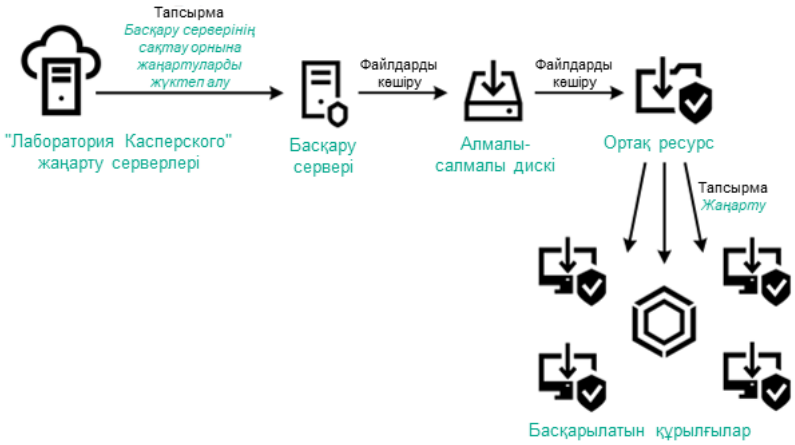
Әдепкі бойынша, Басқару сервері мен тарату нүктелері "Лаборатория Касперского" жаңарту серверлерімен өзара әрекеттеседі және HTTPS жаңартуларын жүктейді. Басқару серверін және/немесе тарату нүктелерін HTTPS орнына HTTP протоколын пайдалану үшін конфигурациялауға болады.

Бұл схеманы іске асыру үшін *Жаңартуларды Басқару серверінің қоймасына жүктеп алу* тапсырмасына қосымша ретінде *Жаңартуларды тарату орындарының қоймаларына жүктеп алу* тапсырмасын жасаңыз. Осыдан кейін, тарату нүктелері жаңартуларды Басқару серверінің қоймасынан емес, "Лаборатория Касперского" жаңарту серверлерінен жүктейді.

Бұл схема үшін де *Жаңартуларды Басқару серверінің қоймасына жүктеп алу* тапсырмасы керек, себебі бұл тапсырма Kaspersky Security Center Linux үшін "Лаборатория Касперского" дерекқорлары мен қолданба 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 "Лаборатория Касперского" дерекқорларын, қолданба модульдерін және қолданбаларын 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).



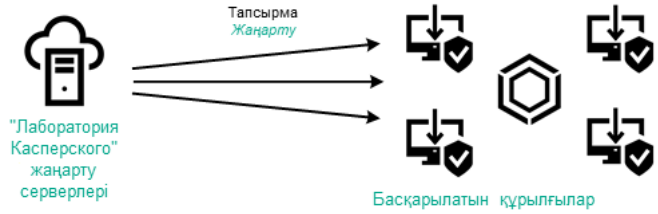
Жергілікті қалта, ортақ қатынасы бар қалта немесе FTP сервері арқылы жаңарту

Kaspersky Endpoint Security бағдарламасындағы жаңарту көздері туралы қосымша ақпарат алу үшін келесі анықтамаларды қараңыз:

- Kaspersky Endpoint Security for Linux анықтамасы
- Kaspersky Endpoint Security for Windows анықтамасы

Басқарылатын құрылғылардағы Kaspersky Endpoint Security үшін "Лаборатория Касперского" жаңарту серверлерінен тікелей

Басқарылатын құрылғыларда сіз Kaspersky Endpoint Security бағдарламасын "Лаборатория Касперского" жаңарту серверлерінен тікелей жаңартуларды алу үшін конфигурациялай аласыз (төмендегі суретті қараңыз).



Қауіпсіздік қолданбаларын тікелей "Лаборатория Касперского" жаңарту серверлерінен жаңарту

Бұл схемада қауіпсіздік қолданбасы Kaspersky Security Center Linux ұсынған қойманы пайдаланбайды. Жаңартуларды тікелей "Лаборатория Касперского" жаңарту серверлерінен алу үшін қауіпсіздік қолданбасында жаңарту көзі ретінде "Лаборатория Касперского" жаңарту серверлерін көрсетіңіз. Осы параметрлер туралы қосымша ақпарат алу үшін анықтаманың келесі бөлімдерін қараңыз:

- Kaspersky Endpoint Security for Linux анықтамасы
- Kaspersky Endpoint Security for Windows анықтамасы

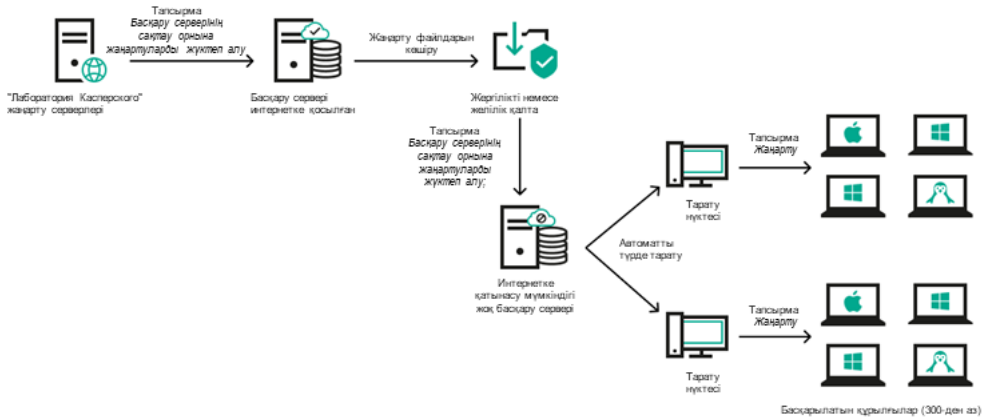
Басқару сервері интернетке қатынаса алмаса, жергілікті немесе желілік қалта арқылы

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 қолданбалары сұрайтын жаңартуларды жүктейтіндіктен, Басқару серверлері басқаратын қауіпсіздік қолданбаларының 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.

Жаңартуларды Басқару серверінің қоймасына жүктеп алу тапсырмасын жасау

Жаңартуларды Басқару серверінің қоймасына жүктеп алу тапсырма "Лаборатория Касперского" қауіпсіздік қолданбасының дерекқорлары мен қолданба модульдерінің жаңартуларын "Лаборатория Касперского" 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 бір ғана *Жаңартуларды Басқару серверінің қоймасына жүктеп алу* тапсырма болуы мүмкін. 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. Негізгі қолданба терезесінде **Активтер (құрылғылар)** → **Тапсырмалар** бөліміне өтіңіз.
2. **Қосу** түймесін басыңыз.

Жаңа тапсырма жасау шебері іске қосылады. Содан кейін, шебердің нұсқауларын орындаңыз.

3. Kaspersky Security Center қолданбасы 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.

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.

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 сіз "Лаборатория Касперского" жаңарту серверлерін, жергілікті немесе желілік қалтаны немесе негізгі Басқару серверін пайдалана аласыз.

     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**

     Егер параметр қосулы болса, жаңартуларды алғаннан кейін Басқару сервері қосалқы Басқару серверлері тарапынан жаңартуларды алу тапсырмаларын іске қосатын болады. Әйтпесе, 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 "Лаборатория Касперского" 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.

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 Linux қолданбасы дерекқорлар мен қолданба модульдері жаңартуларын жаңа схема бойынша жүктеп алады. Қолданба 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 қолданбалардың 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.

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 қолданба 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.

  - Күн сайын (жазғы уақытқа өтуге қолдау көрсетілмейді)

    Тапсырма, күндер түрінде белгіленген аралықпен жүйелі түрде орындалады. Бұл кесте жазғы уақытты сақтауды қолдамайды. Демек, уақыт жаздың басында немесе соңында бір сағатқа алға немесе артқа ауысқанда, тапсырманың нақты іске қосылу уақыты өзгермейді.

    Бұл кестені пайдалану ұсынылмайды. Бұл, Kaspersky Security Center Linux кері үйлесімділігі үшін қажет.

    Әдепкі бойынша, тапсырма күн сайын, ағымдағы жүйелік уақытта іске қосылады.

  - Апта сайын

Тапсырма апта сайын, көрсетілген күні және көрсетілген уақытта 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.

- **Ай сайын, таңдалған апталардың көрсетілген күндері**

  Тапсырма жүйелі түрде, әр айдың көрсетілген күндерінде, көрсетілген уақытта орындалады.

  Әдепкі бойынша ай күндері таңдалмаған. Әдепкі бойынша басталу уақыты – 18:00.

- **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 "Лаборатория Касперского" қолданбасын 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.

10. **Сақтау** түймесін басыңыз.

Тапсырма жасалды және конфигурацияланды.

Жаңартуларды Басқару серверінің қоймасына жүктеп алу тапсырмасын орындау нәтижесінде, дерекқорлар мен қолданба модульдерінің 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.

Егер *Жаңартуларды тексеру* тапсырмасын орындау нәтижелері бойынша уақытша қоймада орналастырылған жаңартулар дұрыс емес деп танылса немесе тапсырма қатемен аяқталса, жаңартуларды ортақ қатынасы бар қалтаға көшіру жүргізілмейді. 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 қолданбасының тұрақты қорғаныс күйі өзгерді;
- талап бойынша тексеру тапсырмасын орындау барысында жұқтырған нысан табылды;
- "Лаборатория Касперского" қолданбасының 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 қолданба 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. Негізгі қолданба терезесінде **Активтер (құрылғылар)** → **Тапсырмалар** бөліміне өтіңіз.
2. **Жаңартуларды Басқару серверінің қоймасына жүктеп алу** тапсырмасының атын басыңыз.
3. Ашылатын тапсырма сипаттары терезесінде **Бағдарлама параметрлері** қойындысына өтіп, **Жаңарту тексерісін іске қосу** параметрін қосыңыз.
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.
   c. Бұрын жасалған сынақ құрылғылары бар басқару тобын таңдаңыз.
   d. Kaspersky Security Center Linux қолдайтын қажетті қолданбаны жаңарту тапсырмасын таңдаңыз, содан кейін зиянды БҚ іздеу тапсырмасын таңдаңыз.

      Осыдан кейін, келесі параметрлер пайда болады. Оларды қосулы күйде қалдыру ұсынылады:

      - **Дерекқорларды жаңартудан кейін құрылғыны өшіріп қайта 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 қорғау 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.

   e. *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* түймесін басып, **Сақтау** тапсырмасы сипаттары терезесін жабыңыз.

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 "Лаборатория Касперского" жаңарту серверлері мен тарату нүктелері арасындағы трафиктен қымбатырақ болса немесе Басқару серверіңізде интернетке қатынасу мүмкіндігі болмаса пайдалана аласыз.

Бұл тапсырма "Лаборатория Касперского" жаңарту серверлерінен тарату нүктелері қоймалары жаңартуларды жүктеу үшін қажет. Жаңартулардың тізіміне мыналар кіреді:

- "Лаборатория Касперского" қауіпсіздік қолданбаларына арналған дерекқорлар мен қолданба модульдері жаңартулары;
- Kaspersky Security Center құрамдастарын жаңарту;
- "Лаборатория Касперского" қауіпсіздік қолданбалары жаңартулары.

Жаңартуларды жүктегеннен кейін, оларды басқарылатын құрылғыларға таратуға болады.

*Таңдалған басқару тобына **Жаңартуларды тарату орындарының қоймаларына жүктеп алу** тапсырмасын жасау үшін:*

1. Негізгі қолданба терезесінде **Активтер (құрылғылар)** → **Тапсырмалар** бөліміне өтіңіз.
2. **Қосу** түймесін басыңыз.

   Жаңа тапсырма жасау шебері іске қосылады. Содан кейін, шебердің нұсқауларын орындаңыз.
3. Kaspersky Security Center қолданбасы үшін **Task type** өрісінен **Жаңартуларды тарату орындарының қоймаларына жүктеп алу** тармағын таңдаңыз.
4. Жасап жатқан тапсырманың атын көрсетіңіз. Тапсырма атауы 100 таңбадан асуы және арнайы таңбаларды ("*<>?\:|) қамтуы мүмкін емес.
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:

  - "Лаборатория Касперского" жаңарту серверлері

    "Лаборатория Касперского" қолданбаларына дерекқорлар мен модульдердің жаңартуларын жіберетін "Лаборатория Касперского" HTTP серверлері мен HTTPS серверлері.

    Әдепкі бойынша, осы нұсқа таңдалады.

  - 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 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 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.

- **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 Linux қолданбасы дерекқорлар мен қолданба модульдері жаңартуларын жаңа схема бойынша жүктеп алады. Қолданба 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 қолданбалардың 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** параметрін 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 қолданба 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.

- **Күн сайын (жазғы уақытқа өтуге қолдау көрсетілмейді)**

  Тапсырма, күндер түрінде белгіленген аралықпен жүйелі түрде орындалады. Бұл кесте жазғы уақытты сақтауды қолдамайды. Демек, уақыт жаздың басында немесе соңында бір сағатқа алға немесе артқа ауысқанда, тапсырманың нақты іске қосылу уақыты өзгермейді.

  Бұл кестені пайдалану ұсынылмайды. Бұл, Kaspersky Security Center Linux кері үйлесімділігі үшін қажет.

  Әдепкі бойынша, тапсырма күн сайын, ағымдағы жүйелік уақытта іске қосылады.

- **Апта сайын**

  Тапсырма апта сайын, көрсетілген күні және көрсетілген уақытта 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.

- **Ай сайын, таңдалған апталардың көрсетілген күндері**

  Тапсырма жүйелі түрде, әр айдың көрсетілген күндерінде, көрсетілген уақытта орындалады.

  Әдепкі бойынша ай күндері таңдалмаған. Әдепкі бойынша басталу уақыты – 18:00.

- **Вирустық шабуылды анықтағанда**

Тапсырманы *Вирустық шабуыл* оқиғасы туындағаннан кейін іске қосуға болады. Вирустық шабуылдарды қадағалайтын қолданба түрлерін таңдаңыз. Қолданбалардың 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, қолданбалардың барлық түрлері таңдалған.

Вирустық шабуыл туралы хабарлайтын қауіпсіздік қолданбасының түріне байланысты әртүрлі тапсырмаларды іске қосуға болады. Бұл жағдайда, сізге қажет емес қолданба 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 "Лаборатория Касперского" қолданбасын 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 орындарының қоймаларына жүктеп алу тапсырмасын орындау нәтижесінде, дерекқорлар мен қолданба модульдерінің 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:

- "Лаборатория Касперского" 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.

"Лаборатория Касперского" 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 "Лаборатория Касперского" жаңарту серверлерінен жаңартуларды қолмен жүктеп алуға және жүктелген файлдарды қажетті қалтаға орналастыруға болады.

Жергілікті немесе желілік қалтаға бір ғана жолды көрсетуге болады. Басқару сервері жергілікті қалта ретінде орнатылған құрылғыдағы қалтаны көрсетуіңіз керек. Желі қалтасы ретінде FTP серверін немесе HTTP серверін немесе SMB ортақ ресурсын пайдалануға болады. Егер SMB үлесі аутентификацияны қажет етсе, ол қажетті есептік деректерімен жүйеге алдын ала қосылуы керек. SMB1 протоколын пайдалану ұсынылмайды, себебі ол қауіпті.

"Лаборатория Касперского" жаңарту серверлерін және жергілікті немесе желілік қалтаны қоссаңыз, алдымен қалтадағы жаңартулар жүктеледі. Жүктеп алу кезінде қате орын алған жағдайда, "Лаборатория Касперского" жаңарту серверлері пайдаланылады.

Егер жаңартулары бар ортақ қатынасы бар қалтасы құпиясөзбен қорғалған болса, **Жаңарту көзінің ортақ қалтасына қатынасу үшін есептік жазбаны көрсетіңіз (болған жағдайда)** параметрін қосып, қатынасу үшін қажетті есептік деректерді енгізіңіз.

Жаңарту көздерін қосу үшін:

1. Негізгі қолданба терезесінде **Активтер (құрылғылар)** → **Тапсырмалар** бөліміне өтіңіз.
2. **Жаңартуларды Басқару серверінің қоймасына жүктеп алу** түймесін басыңыз.
3. **Бағдарлама параметрлері** қойындысына өтіңіз.
4. **Жаңартулардың көздері** жанындағы **Конфигурациялау** түймесін басыңыз.
5. Пайда болған терезеде **Қосу** түймесін басыңыз.
6. Жаңарту көздерінің тізімінде қажетті көздерді қосыңыз. Егер сіз **Жергілікті немесе желілік қалта** жалаушасын орнатсаңыз, қалтаға жолды көрсетіңіз.
7. **OK** түймесін басыңыз, содан кейін жаңарту көзінің сипаттары терезесін жабыңыз.
8. Қашықтан диагностикалау терезесінде **OK** түймесін басыңыз.
9. Тапсырма терезесінде **Сақтау** түймесін басыңыз.

Жаңартулар енді Басқару серверінің қоймасына көрсетілген көздерден жүктеледі.

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 "Лаборатория Касперского" сайтынан жүктеп алу және қолмен орнату керек.

Бір немесе бірнеше жаңартуды растау немесе болдырмау үшін:

1. Қолданбаның негізгі терезесінде **Операциялар → «Лаборатория Касперского» бағдарламалары → Байқалмайтын жаңартулар** бөліміне өтіңіз.

   Қолжетімді жаңартулар тізімі көрсетіледі.

   Басқарылатын қолданбаларды жаңарту үшін Kaspersky Security Center қолданбасының 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.

"Лаборатория Касперского" қолданбаларына 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 қолданбасының дерекқорлары мен модульдерін автоматты түрде жаңартуды конфигурациялауға болады.

Kaspersky Endpoint Security for Windows жаңартуларын құрылғыларға жүктеуді және автоматты түрде орнатуды конфигурациялау үшін:

1. Негізгі қолданба терезесінде **Активтер (құрылғылар)** → **Тапсырмалар** бөліміне өтіңіз.
2. **Қосу** түймесін басыңыз.

   Жаңа тапсырма жасау шебері іске қосылады. Содан кейін, шебердің нұсқауларын орындаңыз.
3. Kaspersky Endpoint Security for Windows қолданбасы 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** қойындысында 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 қойындысының 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. Қолданба модульдерінің жаңартуларын қолданба дерекқорларымен бірге жүктеу және орнату үшін **Қолданба модульдерінің жаңартуларын орнату** параметрін қосыңыз.

Егер параметр қосулы болса, Kaspersky Endpoint Security for Windows бағдарламасы пайдаланушыға қолданба модульдерінің қолжетімді жаңартулары туралы хабарлайды және жаңарту тапсырмасы орындалған кезде қолданба 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, **Қолданба модулінің критикалық жаңартуларын автоматты түрде орнату** параметрін қосуға да болады. Қолданба модульдерінің жаңартулары болған кезде, Kaspersky Endpoint Security for Windows қолданбасы *Критикалық* күйі бар жаңартуларды автоматты түрде орнатады; бағдарлама модульдерінің қалған жаңартуларын – әкімші оларды орнатуды мақұлдағаннан кейін.

Егер қолданба модульдерін жаңарту Лицензиялық келісімнің және Құпиялылық саясатының ережелерімен танысуды және келісуді көздейтін болса, онда пайдаланушы Лицензиялық келісімнің және Құпиялылық саясатының ережелерімен келіскеннен кейін, қолданба жаңартуды белгілейді.

13. Қолданба 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, қолданба "Лаборатория Касперского" жаңартулар серверлеріне сұрау салады.

Кейбір жаңартулар басқарылатын қолданба плагиндерінің соңғы нұсқаларын орнатуды талап етеді.

"Лаборатория Касперского" дерекқорлары мен қолданба модульдерін жаңарту үшін айырмашылық файлдарын пайдалану туралы

Kaspersky Security Center Linux бағдарламасы "Лаборатория Касперского" 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 қолданба модульдері файлдарының екі нұсқасы арасындағы айырмашылықтарды сипаттайды. Айырмашылық файлдарын пайдалану трафикті ұйымыңыздың желісінде сақтайды, өйткені айырмашылық файлдары бүкіл дерекқор және қолданба модульдері 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 қолданба 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: сценарий

Кезеңдер

1. **Басқару серверіндегі функцияны қосу**

   Жаңартуларды Басқару серверінің қоймасына жүктеу тапсырмасының сипаттарында функцияны іске қосыңыз.

2. **Тарату нүктесі үшін функцияны қосу**

   Жаңартуларды тарату орындарының қоймаларына жүктеу тапсырмасының көмегімен жаңартуларды алып тұратын тарату нүктесі үшін функцияны іске қосу.

   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 сипаттарында және (тарату нүктелері қолмен тағайындалған болса және саясат параметрлерін қайта анықтағыңыз келсе) Басқару серверінің сипаттарында **Тарату нүктелері** бөлімінде іске 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, "Лаборатория Касперского" серверлерінен, жергілікті немесе желілік қалтадан жаңартулар алып тұруға мүмкіндік береді.

Тарату нүктесі үшін жаңартулар алуды конфигурациялау үшін келесі әрекеттерді орындаңыз:

1. Басты мәзірде қажетті Басқару сервері атауының жанындағы параметрлер (⚙) белгішесін 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 "Лаборатория Касперского" дерекқорлары мен қолданба модульдеріне арналған жаңартулар

Басқарылатын құрылғыларда "Лаборатория Касперского" дерекқорлары мен қолданба 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 қолданба модульдерін 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 қолданбасына қажетті жаңартулар болуы үшін, басқарылатын желілік құрылғылардың кем дегенде біреуінде осы қауіпсіздік қолданбасы орнатылуы керек. Бұл қолданба Жаңартуларды Басқару серверінің қоймасына жүктеп алу тапсырмасы арқылы *Жаңартуларды Басқару серверінің қоймасына жүктеп алу* үшін конфигурациялануы керек.

- Бірдей қауіпсіздік қолданбасы орнатылған және Басқару сервері қоймасынан, тарату нүктесі қоймасынан немесе тікелей "Лаборатория Касперского" жаңарту серверлерінен жаңартулар алуға конфигурацияланған кез келген құрылғы.

Төменде Басқару сервері қоймасынан көшіру арқылы дерекқорлар мен қолданба модульдері жаңартуларын орнатудың мысалы келтірілген.

Автономды құрылғылардағы "Лаборатория Касперского" дерекқоры мен қолданба модульдерін жаңарту үшін:

1. Алынбалы жетекті Басқару сервері орнатылған құрылғыға қосыңыз.

2. Жаңарту файлдарын алынбалы жетекке көшіріңіз.

   Жаңартулар әдепкі бойынша мына мекенжайда орналасқан: \\<server name>\KLSHARE\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 анықтамасы
   - Kaspersky Endpoint Security for Windows 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, "Лаборатория Касперского" дерекқорлары мен қолданба модульдері құрылғыда жаңартылады.

Веб-плагиндерді сақтық көшірмелеу және қалпына келтіру

Kaspersky Security Center Web Console веб-консолі сізге сақталған күйді қалпына келтіру үшін веб-плагиннің ағымдағы күйінің деректерін сақтық көшірмелеуге мүмкіндік береді. Мысалы, веб-плагин деректерін жаңа нұсқаға жаңартпас бұрын, оның сақтық көшірмесін жасауға болады. Жаңартудан кейін, егер ең жаңа нұсқа сіздің талаптарыңызға немесе дәмелеріңізге сәйкес келмесе, деректердің сақтық көшірмесінен веб-плагиннің алдыңғы нұсқасын қалпына келтіруге болады.

Веб-плагин деректерінің сақтық көшірмесін жасау үшін:

1. Қолданбаның негізгі терезесінде **Параметрлер** → **Веб-плагиндер** бөліміне өтіңіз.

2. **Веб-плагиндер** бөлімінде деректердің сақтық көшірмесін жасау қажет веб-плагиндерді таңдап, **Сақтық көшірмені жасау** түймесін басыңыз.

Таңдалған веб-плагиндердің деректерін сақтық көшірмелеу. Сіз деректердің жасалған сақтық көшірмелерін **Резервтік қоймалар** қойыншасында қарап шыға аласыз.

Деректердің сақтық көшірмесінен веб-плагинді қалпына келтіру үшін:

1. Қолданбаның негізгі терезесінде **Параметрлер** → **Резервтік қоймалар** бөліміне өтіңіз.

2. **Резервтік қоймалар** бөлімінде қалпына келтіргіңіз келетін веб-плагин деректерінің сақтық көшірмесін таңдаңыз, содан соң **Сақтық көшірмеден қалпына келтіру** түймесін басыңыз.

Веб-плагин таңдалған деректердің сақтық көшірмесінен қалпына келтіріледі.

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.
- Қорғанысты орналастыру туралы есеп есебін жасау және қарау.

6. **Клиент құрылғылары қорғанысын тексеру**

   Нұсқаулар:

   - Қорғаныс күйі және Қауіптер статистикасы санаттарынан есепті жасау және қарау.
   - Критикалық оқиғалар таңдауын іске қосу және қарау.

7. **Дерекқорға оқиғаларды жүктеуді бағалау және шектеу**

   Басқарылатын қолданбалар 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: **Критикалық оқиғалар**, **Функциялық 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. Бұл ақпарат **Қоймалар** қалтасына салынған **Смарт оқыту күйіндегі ережелерді іске қосу** қалтасында тізім түрінде сақталады. 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 тізімін қарау

Аномалияларды бейімделумен басқару ережелері арқылы орындалған анықтау тізімін қарау үшін:

1. Консоль ағашында Басқару серверінің қажетті түйінін таңдаңыз.

2. **Смарт оқыту күйіндегі ережелерді іске қосу** ішкі қалтасын таңдаңыз (әдепкі бойынша ол **Кеңейтілген** → **Қоймалар** қалтасында орналасқан).

   Тізімде Аномалияларды бейімделумен басқару ережелері арқылы орындалатын келесі анықтау ақпарат көрсетіледі:

   - **Басқару тобы**

     Құрылғы қосылған басқару тобының атауы.

   - **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.

   - **Жалпы уақыт ережелері іске қосылды**

     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.

Әрбір элементтің сипаттарын қарау үшін:

1. Консоль ағашында Басқару серверінің қажетті түйінін таңдаңыз.
2. **Смарт оқыту күйіндегі ережелерді іске қосу** ішкі қалтасын таңдаңыз (әдепкі бойынша ол **Кеңейтілген** → **Қоймалар** қалтасында орналасқан).
3. **Смарт оқыту күйіндегі ережелерді іске қосу** қалтасының жұмыс аймағында қажетті нысанды таңдаңыз.
4. Келесі әрекеттердің бірін орындаңыз:
   - Экранның оң жағындағы жұмыс аймағында **Сипаттар** сілтемесінен өтіңіз.
   - Нысанның контекстік мәзірінде **Сипаттар** тармағын таңдаңыз.

Ашылған нысан сипаты терезесінде нысан туралы ақпарат көрсетіледі.

Сіз Аномалияларды бейімделумен басқару ережелері анықтаған тізімдегі кез келген нысанды растай аласыз немесе ерекшеліктерге қоса аласыз.

Нысанды растау үшін,

анықтау тізімінен бір немесе бірнеше элементті таңдап, **Растау** түймесін басыңыз.

Элементтер күйі **Расталуда** болып өзгереді.

Сіздің растауыңыз ережелер қолданатын статистикаға әсер етеді (толық ақпаратты Kaspersky Endpoint Security 11 for Windows анықтамасынан қараңыз).

Нысанды ерекшеліктерге қосу үшін,

Анықтау тізімі нысанының (немесе бірнеше нысанының) контекстік мәзірінде **Ерекшеліктерге қосу** тармағын таңдаңыз.

Нәтижесінде, ерекшелікті қосу шебері іске қосылады. Шебердің нұсқауларын орындаңыз.

Егер сіз нысанды қабылдамасаңыз немесе растасаңыз, ол клиент құрылғысы Басқару серверімен келесі рет синхрондалғаннан кейін анықтау тізімінен шығарылады және бұдан былай тізімде көрсетілмейді.

Аномалияларды бейімделумен басқару ережесіне ерекшеліктер қосу

Ерекшелікті қосу шебері Kaspersky Endpoint Security үшін Аномалияларды бейімделумен басқару ережелерінен ерекшеліктерді қосуға мүмкіндік береді.

Төмендегі тәсілдердің бірін пайдаланып, шеберді іске қосуға болады.

Аномалияларды бейімделумен басқару қалтасындағы ерекшелікті қосу шеберін іске қосу үшін:

1. Консоль ағашында өзіңізге қажетті Басқару серверінің атауы бар торапты таңдаңыз.
2. **Смарт оқыту күйіндегі ережелерді іске қосу** ішкі қалтасын таңдаңыз (әдепкі бойынша ол **Кеңейтілген → Қоймалар** қалтасында орналасқан).
3. Жұмыс аймағында нысанның (немесе бірнеше нысанның) контекстік мәзіріндегі анықтау тізімінен **Ерекшеліктерге қосу** тармағын таңдаңыз.

   Бір уақытта 1000-ға дейін ерекшелік қосуға болады. Егер сіз көбірек элементтерді таңдап, оларды ерекшеліктерге қосуға тырыссаңыз, қате туралы хабар пайда болады.

Нәтижесінде, ерекшелікті қосу шебері іске қосылады. Шебердің жұмысын жалғастыру үшін **Келесі** түймесін басыңыз.

Консоль ағашындағы басқа түйіндерден ерекшелікті қосу шеберін іске қосу үшін:

- Басқару серверінің негізгі терезесінің **Оқиғалар** қойындысын ашып, **Пайдаланушылардың сұраулары** немесе **Соңғы оқиғалар** тармағын таңдаңыз.
- **Аномалияларды бейімделумен басқару ережелерінің күйі туралы есеп** терезесінде **Анықтамалар саны** бағанын таңдаңыз.

Ерекшелікті қосу шеберін пайдаланып, Аномалияларды бейімделумен басқару ережелеріне ерекше жағдайларды қосу үшін:

1. Шебердің бірінші қадамында басқару плагиндері осы қолданбаларға арналған саясаттарға ерекшеліктерді қосуға мүмкіндік беретін "Лаборатория Касперского" қолданбаларының тізімінен қолданбаны таңдаңыз.

   Егер сізде тек Windows жүйесіне арналған Kaspersky Endpoint Security қолданбасы болса және Аномалияларды бейімделумен басқару ережелерін қолдайтын басқа қолданбалар болмаса, бұл қадамды өткізіп жіберуге болады.

2. Ерекшеліктер қосқыңыз келетін саясаттар мен саясат профильдерін таңдаңыз.

   Келесі қадам саясатты өңдеу барысын көрсетеді. **Бас тарту** түймесін басып, саясатты өңдеуді доғаруға болады.

   Иеленген саясаттарды жаңарту мүмкін емес. Саясатты өзгертуге құқықтарыңыз болмаса, мұндай саясат та жаңартылмайды.

   Барлық саясаттар өңделгеннен (немесе саясаттарды өңдеу доғарылғаннан) кейін, есеп жасалады. Есеп, қандай саясаттардың сәтті жаңартылғанын (жасыл белгіше), қандай саясаттардың жаңартылмағанын (қызыл белгіше) көрсетеді.

3. Шебердің жұмысын аяқтау үшін **Дайын** түймесін басыңыз.

   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 **Бақылау және есеп беру → 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. Негізгі қолданба терезесінде **Бақылау және есеп беру → Бақылау тақтасы** бөліміне өтіңіз.
2. **Веб-виджетті қосу не қалпына келтіру** түймесін басыңыз.
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.
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. Негізгі қолданба терезесінде **Бақылау және есеп беру → Бақылау тақтасы** бөліміне өтіңіз.
2. Жою қажет веб-виджеттің жанындағы параметрлер (⚙) белгішесін басыңыз.
3. **Веб-виджетті жасыру** таңдаңыз.
4. Пайда болған **Ескерту** терезеде **OK** 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. Негізгі қолданба терезесінде **Бақылау және есеп беру → 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.

Веб-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. Негізгі қолданба терезесінде **Бақылау және есеп беру → 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. Негізгі қолданба терезесінде **Бақылау және есеп беру → 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. Өзгерістерді сақтау үшін **Сақтау** түймесін басыңыз.

Таңдалған веб-виджеттің параметрлері өзгертіледі.

Параметрлер жиынтығы нақты веб-виджетке байланысты. Төменде кейбір жалпы параметрлер берілген:

- **Веб-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.
- **Осы кезде Критикалыққа орнату** және **Осы кезде Ескертуге орнату** – күй графигінде түстер тағайындалатын ережелер.

Веб-виджет параметрлерін өзгерткеннен кейін веб-виджет деректерін қолмен жаңартуға болады.

Веб-виджет деректерін жаңарту үшін:

1. Негізгі қолданба терезесінде **Бақылау және есеп беру → 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** қойындысында **Бақылау және есеп беру** → **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 "Лаборатория Касперского" қолданбаларының статистикасын көргісі келсе және оған қатынасу құқығы қажет болса, сол пайдаланушыға құқықтарды конфигурациялаңыз. Осыдан кейін, "Лаборатория Касперского" қолданбаларының деректері пайдаланушыда осы қолданбалардың 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.

Есептер

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 **Бақылау және есеп беру → 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. Қолданбаның негізгі терезесінде **Бақылау және есеп беру** → **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.
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).
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.
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.

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. Қолданбаның негізгі терезесінде **Бақылау және есеп беру** → **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.
4. Есеп үлгісі сипаттарын өзгертіңіз:

   - **Жалпы** қойындысы:
     - 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, құрылғыда мұндай есепті қалыптастыру кезінде жад таусылуы мүмкін. Бұл, есепті қалай алмауыңызға әкелуі мүмкін.

       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 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 белгіленген уақыт аралықтарында (сағат түрінде көрсетілген) деректерді 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 сол есепті тек сол үшін жасай аласыз.

Әдепкі бойынша, параметр өшірулі.

- **Өрістер** қойындысы

  Есепте көрсетілетін өрістерді таңдаңыз. **Жоғары жылжыту** және **Төменге жылжыту** түймелерінің көмегімен өрістерді көрсету тәртібін өзгертіңіз. **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. Өзгерістерді 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. Қолданбаның негізгі терезесінде **Бақылау және есеп беру** → **Есептер** бөліміне өтіңіз.

2. Экспорттағыңыз келетін есептерді таңдаңыз.

   Оннан астам есеп таңдасаңыз, **Есепті экспорттау** түймесі өшірулі болады.

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, қолданба оны Басқару серверінде орнату қажет екендігі туралы хабарламаны көрсетеді. Құралды қолмен орнатып, келесі қадамға өтіңіз.

5. **Есепті экспорттау** түймесін басыңыз.

Есеп файлға көрсетілген пішімде сақталады.

Есепті жасау және қарау.

Есепті жасау және қарау үшін:

1. Қолданбаның негізгі терезесінде **Бақылау және есеп беру** → **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** қойындысында:
  - 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. Қолданбаның негізгі терезесінде **Бақылау және есеп беру** → **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>).
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, қолданба 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. Есептер қалтаға сақталады ма, сол қалтада бұрын сақталған есептер қайта жазыла ма және қалтаға қатынасу үшін бөлек есептік жазба қолданыла ма (ортақ қатынасы бар қалта үшін).
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 қолданба 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 ай күндері таңдалмаған. Әдепкі бойынша басталу уақыты – 18:00.

- **Вирустық шабуылды анықтағанда**

Тапсырманы *Вирустық шабуыл* оқиғасы туындағаннан кейін іске қосуға болады. Вирустық шабуылдарды қадағалайтын қолданба түрлерін таңдаңыз. Қолданбалардың 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, қолданбалардың барлық түрлері таңдалған.

Вирустық шабуыл туралы хабарлайтын қауіпсіздік қолданбасының түріне байланысты әртүрлі тапсырмаларды іске қосуға болады. Бұл жағдайда, сізге қажет емес қолданба 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.

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 "Лаборатория Касперского" қолданбасын 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.

8. Шебердің **Тапсырманы іске қосу үшін есептік жазбаны таңдау** қадамында тапсырманы іске қосу үшін пайдаланылатын есептік жазба деректерін көрсетіңіз.

9. Егер тапсырманың басқа параметрлерін ол жасалғаннан кейін өзгерту қажет болса, шебердің **Тапсырманы жасауды аяқтау** қадамында **Жасап болған соң, тапсырма туралы мәліметтерді ашу** параметрін қосыңыз.

Әдепкі бойынша, параметр қосулы.

10. Тапсырма жасау және шеберді жабу үшін **Аяқтау** түймесін басыңыз.

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. Қолданбаның негізгі терезесінде **Бақылау және есеп беру** → **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.

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, басқарылатын қолданбаларға орнатылған "Лаборатория Касперского" Басқару сервері мен қолданбаларының 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 "Лаборатория Касперского" басқарылатын қолданбаларында туындайды. Мысалы, Вирустық шабуыл жалпы оқиға. Жалпы оқиғалар қатаң белгіленген синтаксис пен семантикаға ие. Жалпы оқиғалар, мысалы, есептер мен мониторинг тақтасында қолданылады.
- "Лаборатория Касперского" басқарылатын қолданбаларының айрықша оқиғалары. "Лаборатория Касперского" әрбір басқарылатын қолданбасы өзіндік оқиғалар жиынтығына ие.

Дереккөз бойынша оқиғалар

Қолданба жасай алатын оқиғалардың толық тізімі қолданба саясаты сипаттарындағы **Оқиғаны конфигурациялау** қойыншасында келтірілген. Басқару сервері үшін, Басқару серверінің сипаттарындағы оқиғалар тізімін қосымша түрде қарап шығуға болады.

Оқиғалар келесі қолданбалар тарапынан жасалуы мүмкін:

- Kaspersky Security Center Linux қолданбасының құрамдастары:
  - Басқару сервері
  - Желілік агент
- "Лаборатория Касперского" басқарылатын қолданбалары

  "Лаборатория Касперского" басқарылатын қолданбалары жасайтын оқиғалар туралы толығырақ ақпарат тиісті қолданбаның 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 қолданбаның жұмысы деректерді немесе функционалдық мүмкіндіктерді жоғалтпай қалпына келтіріле алса, осы оқиғалар көбінесе Ескертулерге қатысты болып келеді.
- *Ақпараттық хабарлар* – операцияның сәтті орындалуы, қолданбаның 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 Kaspersky Security Center басқару серверінде және желілік агентте орын алатын оқиғалардың түрлері берілген. "Лаборатория Касперского" қолданбаларында орын алатын оқиғалар түрлері бұл бөлімде атап көрсетілмеген.

Қолданба жасай алатын әрбір оқиға үшін, қолданба саясаты сипаттарындағы **Оқиғаны 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.

  Оқиғаларды сақтау уақытын өзгертуге болады: Оқиғаны сақтау мерзімін конфигурациялау.

Басқару сервері оқиғалары

Бұл бөлімде Басқару сервері оқиғалары туралы ақпарат бар.

Басқару серверінің критикалық оқиғалары

Төмендегі кестеде маңыздылық деңгейі **Критикалық** Kaspersky Security Center басқару серверінің оқиғалары берілген.

Қолданба жасай алатын әрбір оқиға үшін, қолданба саясаты сипаттарындағы **Оқиғаны 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 критикалық оқиғалары

Оқиға түрінің көрсетілетін атауы	Оқиға түрі идентификаторы	Оқиға түрі	Сипаттамасы
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 "Лаборатория Касперского" қолданбаларының 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 белсенді кодын немесе кілт файлын қосыңыз).

			Kaspersky Security Center Linux бағдарламасы, лицензиялық шектеуден асып кеткен жағдайда оқиғаларды жасау ережесін айқындайды.
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.
Құрылғының күйі «Критикалық»	4113	KLSRV_HOST_STATUS_CRITICAL	Осы түрдегі оқиғалар, басқарылатын құрылғыға *Критикалық* күйі тағайындалса туындайды. Сіз шарттарды конфигурациялай аласыз, оларды орындау кезінде құрылғының күйі *Критикалық* болып өзгереді.
Кілт файлы қара тізімге қосылды	4124	KLSRV_LICENSE_BLACKLISTED	Осы түрдегі оқиғалар, "Лаборатория Касперского" бағдарламасы сіз қолданып жатқан белсендіру кодын немесе лицензиялық кілтті тыйым салынғандар тізіміне қосқан болса туындайды.

			Толығырақ ақпарат алу үшін Техникалық қолдау қызметіне жүгініңіз.
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 өшірулі болса, лицензия мерзімі аяқталатын көрсетілген күні, 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.	
Сертификаттың жарамдылық мерзімі бітті	4132	KLSRV_CERTIFICATE_EXPIRED	Осы түрдегі оқиғалар, Ұялы құрылғыларды басқару үшін Басқару сервері сертификатының жарамдылық мерзімі аяқталуға жақын болғанда туындайды. Сізге жарамдылық мерзімі бітейін деп жатқан сертификатты жаңарту керек.	
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.	

Басқару серверінің функционалдық ақауы оқиғалары

Төмендегі кестеде маңыздылық деңгейі **Функционалдық ақау** Kaspersky Security Center басқару серверінің оқиғалары берілген.

Қолданба жасай алатын әрбір оқиға үшін, қолданба саясаты сипаттарындағы **Оқиғаны 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 функционалдық ақауы оқиғалары

Оқиға түрінің көрсетілетін атауы	Оқиға түрі идентификаторы	Оқиға түрі	Сипаттамасы	Ә бо с м

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.	18(
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 қолданбасында 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 өндірушінің қолданбасын, ол қолданылмайтын құрылғылардан жойыңыз. • Үшінші тарап лицензиясын көптеген	18(

			құрылғыларға қолданыңыз. Лицензиялы қолданбалар тобының функционалдылығын қолдана отырып, лицензиялы қолданбалардың лицензиялық кілттерін басқара аласыз. Лицензиялы қолданбалар тобына, сіз белгілеген өлшемшарттарға сай келетін үшінші тарап өндірушілердің қолданбалары кіреді.	
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. • Қалтаға (қалталарға) арналған пайдаланушы аты және/немесе құпиясөз өзгертілгенін тексеріңіз. • Интернет қосылымын тексеріңіз, себебі бұл оқиғаның себебі	18(

			болуы мүмкін. Дерекқорлар мен қолданба модульдерін жаңарту жөніндегі нұсқауларды орындаңыз.	
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.	18(
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.	18(
Басқару серверінің дерекқоры қолжетімсіз	4109	KLSRV_DATABASE_UNAVAILABLE	Осы түрдегі оқиғалар Басқару сервері дерекқоры қолжетімсіз болған	18(

			жағдайда пайда болады. Сіз оқиғаға келесі тәсілдермен жауап бере аласыз: • SQL сервері орнатылған қашықтағы сервердің қолжетімді ме екенін тексеріңіз. • ДҚБЖ оқиғалар журналдарын қарап шығыңыз және Басқару сервері дерекқорының қолжетімсіздігінің себебін табыңыз. Мысалы, алдын алу жұмыстарына байланысты, SQL Server сервері орнатылған қашықтағы сервер қолжетімді болмауы мүмкін.	
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	18(

			сақталатын оқиғалар санын шектеңіз. • Басқару сервері дерекқорында қолданбаларды басқару құрамдасы жіберген оқиғалар өте көп. Басқару серверінің дерекқорында Қолданбаларды басқару құрамдасының оқиғаларын сақтауға қатысты Kaspersky Endpoint Security саясатының параметрлерін өзгертуге болады. ДҚБЖ таңдау туралы ақпаратты қарап шығыңыз.	

Басқару серверінің ескерту оқиғалары

Төмендегі кестеде **Ескерту** маңыздылық деңгейі бар Kaspersky Security Center Басқару серверінің оқиғалары келтірілген.

Қолданба жасай алатын әрбір оқиға үшін, қолданба саясаты сипаттарындағы **Оқиғаны 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
Жиі болатын оқиға 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.

Лицензиялық шектеу асырылды	4098	KLSRV_EV_LICENSE_CHECK_100_110	Күніне бір рет Kaspersky Security Center Linux бағдарламасы лицензиялық шектеулердің асып кетпегенін тексеріп тұрады. Осы түрдегі оқиғалар, Басқару сервері клие құрылғыларына орнатылған "Лаборатория Касперского" қолданбаларының лицензиялық шектеуінің асып кеткенін тіркесе және бір лицензияның қолданылатын лицензиялық бірліктерінің саны лицензия қамтитын бірліктердің жалпы саны 100%-дан 110%-ғ дейін құраса туындайды. Осы оқиға туындаса д 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 белсенді кодын немесе кілт файлы қосыңыз). Kaspersky Security Center Linux бағдарламасы, лицензиялық шектеуден асып кетке жағдайда оқиғаларды жасау ережесін айқындайды.

Құрылғы желіде ұзақ уақыт бойы белсенді емес болып қалды	4103	KLSRV_EVENT_HOSTS_NOT_VISIBLE	Осы түрдегі оқиғалар, басқарылатын құрылғ бірнеше уақыт бойы белсенді емес болған кезде туындайды. Көбінесе, басқарылатын құрылғ істен шыққан жағдайд 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 жасалаты уақыт аралығын көрсетіңіз. • Құрылғы Kaspersky Security Center Web Console веб-консолінің көмегімен автоматты түрде жойылатын уақыт аралығын көрсетіңіз.
Құрылғылар атауларының қайшылығы	4102	KLSRV_EVENT_HOSTS_CONFLICT	Осы түрдегі оқиғалар, егер Басқару сервері екі немесе одан да кө басқарылатын құрылғыны бір құрылғ ретінде қарастырған кезде туындайды.

			Көбінесе, клондалған қатты диск қолданбаларды 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 агент эталонды құрылғыда дискіні клондау режиміне ауыстырып қосыңыз.
Құрылғының күйі «Ескерту»	4114	KLSRV_HOST_STATUS_WARNING	Осы түрдегі оқиғалар, басқарылатын құрылғыға *Ескерту* күйі тағайындалса туындайды. Сіз шарттарды конфигурациялай аласыз, оларды орындау кезінде құрылғының күйі *Ескерту* болып өзгереді.
Лицензиялы бағдарламалар топтарының біреуі үшін орнатулар санының шектеуі жақын арада асырылады	4127	KLSRV_INVLICPROD_FILLED	Лицензиялық қолданбалар тобына қосылған үшінші тарап өндірушілердің қолданбаларын орнат саны лицензиялық кілттің сипаттарында көрсетілген ең жоғар рұқсат етілген мәннің 90%-на жетсе, осы типтегі оқиғалар туындайды. Сіз оқиғаға келесі тәсілдермен жауап бере аласыз: • Егер үшінші тарап өндірушінің қолданбасы басқарылатын құрылғыларда қолданылмаса, қолданбаны сол

			құрылғылардан жойыңыз. • Жақын арада үшінш тарап қолданбасына арналған орнату саны рұқсат етілге шектен асады деп күтсеңіз, көптеген құрылғыларға үшінші тарап қолданбасының лицензиясын алу мүмкіндігін алдын ала қарастырыңыз Лицензиялы қолданбалар тобының функционалдылығын қолдана отырып, лицензиялы қолданбалардың лицензиялық кілттерін басқара аласыз.
Сертификат сұралды	4133	KLSRV_CERTIFICATE_REQUESTED	Ұялы құрылғыларды басқару үшін сертификатты автоматты түрде қайт 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 өшірілге сертификат үшін басталды. Бұл жағдай, сертифика жасау кезінде пайд болған қатеге байланысты болуы мүмкін. Сертификатты қолмен қайта шығару қажет болу мүмкін. • Егер сіз жалпыға ортақ

			инфрақұрылымыме біріктіруді қолдансаңыз, оның себебі PKI-мен біріктіру және сертификат шығар үшін қолданылатын есептік жазбаның SAM-Account-Name атрибутының болмауына байланысты болуы мүмкін. Есептік жазба сипаттарын қарап шығыңыз.
Сертификат жойылды	4134	KLSRV_CERTIFICATE_REMOVED	Егер әкімші Ұялы құрылғыларды басқар үшін кез келген түрдег сертификатты (жалпы пошталық, VPN) жойс осы түрдегі оқиғалар туындайды. Сертификат жойылғаннан кейін, ос сертификатқа қосылға ұялы құрылғылар Басқару серверіне қосыла алмайды. Бұл оқиға Ұялы құрылғыларды басқаруға қатысты ақауларды зерттеуде пайдалы болуы мүмкін
APNs сертификатының жарамдылық мерзімі бітті	4135	KLSRV_APN_CERTIFICATE_EXPIRED	Осы түрдегі оқиғалар, APNs сертификатының жарамдылық мерзімі бітейін деп жатқан кезде туындайды. Сізге қолмен APNs сертификатын жаңарт және оны iOS MDM серверіне орнату қажет.
APNs сертификатының жарамдылық мерзімі бітейін деп жатыр	4136	KLSRV_APN_CERTIFICATE_EXPIRES_SOON	Егер APNs сертификатының жарамдылық мерзімін аяқталуына дейін 14 күннен аз уақыт қалса осы түрдегі оқиғалар орын алады.

			APNs сертификаты жарамдылық мерзімі аяқталғаннан кейін, қолмен APNs сертификатын жаңартып, оны iOS MDM серверіне орнат керек. APNs сертификатын жарамдылық мерзімі аяқталғанға дейін жаңартуды жоспарлау ұсынылады.
FCM хабарын ұялы құрылғыға 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 сервер Басқару серверінен алынған кейбір сұрауларды өңдей алмаса туындайды. Бұ 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 messag error response codes" тарауын қараңыз).
FCM хабарын FCM серверіне жіберу кезінде туындаған HTTP қатесі	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 Басқар 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 жауа беріңіз. FCM серверінен алынға 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 жауа беріңіз.
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, оларғ тиісінше ден қойыңыз Егер сіз мәселенің шешімін өзіңіз таба алмасаңыз, "Лаборатория Касперского" Техникалық қолдау қызметіне хабарласуд ұсынамыз.
Қатты дискіде бос орын аз	4105	KLSRV_NO_SPACE_ON_VOLUMES	Бұл түрдегі оқиғалар, Басқару сервері орнатылған құрылғыда диск кеңістігі таусылу жақын қалған жағдайд туындайды. Құрылғыдағы диск кеңістігін босатыңыз.
Басқару серверінің дерекқорында бос орын аз	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 істеме қалады. Төменде, қолданылатын ДҚБЖ жүйесіне тәуелді оқиғаның туындау себептері және оқиға 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.
Қосалқы	4116	KLSRV_EV_SLAVE_SRV_DISCONNECTED	Бұл түрдегі оқиғалар

Басқару серверімен байланыс үзілді			қосалқы Басқару серверімен байланыс үзілген кезде пайда болады. Қосалқы басқару сервері орнатылған құрылғыдағы операциялық жүйенің оқиғалар журналын оқып, соған сәйкес әрекет етіңіз.
Негізгі Басқару серверімен байланыс үзілді	4118	KLSRV_EV_MASTER_SRV_DISCONNECTED	Бұл түрдегі оқиғалар негізгі Басқару серверімен байланыс үзілген кезде пайда болады. Негізгі басқару серве орнатылған құрылғыдағы операциялық жүйенің оқиғалар журналын оқып, соған сәйкес әрекет етіңіз.
«Лаборатория Касперского» бағдарламалық жасақтама модульдерінің жаңа жаңартулары тіркелді	4141	KLSRV_SEAMLESS_UPDATE_REGISTERED	Бұл түрдегі оқиғалар, Басқару сервері, орнатуды мақұлдауды қажет ететін басқарылатын құрылғыларда орнатылған "Лаборатория Касперского" қолданбаларының жаңа жаңартуларын тіркеген жағдайда ор алады. Kaspersky Security Center Web Console арқылы жаңартулард растаңыз немесе қабылдамаңыз.
Дерекқордағы оқиғалар санының шектеуі асырылды, оқиғаларды жою басталған	4145	KLSRV_EVP_DB_TRUNCATING	Мұндай түрдегі оқиғалар, Басқару сервері дерекқорына 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.
Дерекқордағы оқиғалар санының шектеуі асырылды, оқиғалар жойылған	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.
Аудит: SIEM серверімен сынақ байланысын орнату сәтсіз аяқталды	5120	KLAUD_EV_SIEM_TEST_FAILED	Бұл түрдегі оқиғалар, SIEM серверіне қосылуды автоматты түрде тексеру сәтсіз аяқталғанда орын алады.

Басқару серверінің ақпараттық оқиғалары

Төмендегі кестеде **Ақпараттық** маңыздылық деңгейі бар Kaspersky Security Center Басқару серверінің оқиғалары келтірілген.

Қолданба жасай алатын әрбір оқиға үшін, қолданба саясаты сипаттарындағы **Оқиғаны 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	Әдепкі бойынша сақтау мерзімі	Пі
Лицензиялық кілттің 90%-дан көп бөлігі қолданылып қойған	4097	KLSRV_EV_LICENSE_CHECK_90	30 күн	
Жаңа құрылғы анықталды	4100	KLSRV_EVENT_HOSTS_NEW_DETECTED	30 күн	
Құрылғы топқа автоматты түрде қосылды	4101	KLSRV_EVENT_HOSTS_NEW_REDIRECTED	30 күн	
Құрылғы топтан жойылды: желіде ұзақ уақыт бойы белсенді емес	4104	KLSRV_INVISIBLE_HOSTS_REMOVED	30 күн	
Лицензиялы бағдарламалар топтарының біреуі үшін рұқсат етілген орнатулардың саны (95%-дан) асты	4128	KLSRV_INVLICPROD_EXPIRED_SOON	30 күн	
«Лаборатория Касперского» зертханасына талдауға жіберетін файлдар пайда болды	4131	KLSRV_APS_FILE_APPEARED	30 күн	
Осы ұялы құрылғыда FCM үлгісінің идентификаторы өзгертілді	4137	KLSRV_GCM_DEVICE_REGID_CHANGED	30 күн	
Жаңартулар белгіленген қалтаға сәтті көшірілді	4122	KLSRV_UPD_REPL_OK	30 күн	
Қосалқы Басқару серверімен	4115	KLSRV_EV_SLAVE_SRV_CONNECTED	30 күн	

байланыс орнатылды				
Негізгі Басқару серверімен байланыс орнатылды	4117	KLSRV_EV_MASTER_SRV_CONNECTED	30 күн	
Дерекқорлар жаңартылды	4144	KLSRV_UPD_BASES_UPDATED	30 күн	
Аудит: Басқару серверіне қосылым орнатылды	4147	KLAUD_EV_SERVERCONNECT	30 күн	
Аудит: нысан өзгертілді	4148	KLAUD_EV_OBJECTMODIFY	30 күн	Бұл оқиға нысандар, өзгерістер қадағалай • басқар • қауіпсіз топтар • пайдал • орнату • тапсыр • саясат • сервер • виртуа сервер
Аудит: нысан күйі өзгертілді	4150	KLAUD_EV_TASK_STATE_CHANGED	30 күн	Мысалы, т қатемен а бұл оқиға туындайды
Аудит: топ параметрлері өзгертілді	4149	KLAUD_EV_ADMGROUP_CHANGED	30 күн	
Аудит: Басқару серверіне қосылу тоқтатылды	4151	KLAUD_EV_SERVERDISCONNECT	30 күн	
Аудит: Нысанның сипаттары өзгертілді	4152	KLAUD_EV_OBJECTPROPMODIFIED	30 күн	Бұл оқиға параметр. өзгерістер қадағалай • пайдал • лицен

				• Серве • виртуа сервер
Аудит: Пайдаланушы рұқсаттары өзгертілді	4153	KLAUD_EV_OBJECTACLMODIFIED	30 күн	
Аудит: Басқару серверінен импортталған немесе экспортталған шифрлау кілттері	5100	KLAUD_EV_DPEKEYSEXPORT	30 күн	
Аудит: SIEM серверімен сынақ байланысын орнату сәтті аяқталды	5110	KLAUD_EV_SIEM_TEST_SUCCESS	30 күн	

Желілік агент оқиғалары

Бұл бөлімде Желілік агент оқиғалары туралы ақпарат бар.

Желілік агенттің ескертулері оқиғалары

Төмендегі кестеде **Ескерту** маңыздылық деңгейі бар желілік агент оқиғалары келтірілген.

Қолданба жасай алатын әрбір оқиға үшін, қолданба саясаты сипаттарындағы **Оқиғаны 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	Әдепкі бойынша сақтау мерзімі
Қауіпсіздік мәселесі пайда болды	549	GNRL_EV_APP_INCIDENT_OCCURED	30 күн
KSN Проксиі іске қосылды. KSN қолжетімділігін тексеру сәтсіз аяқталды	7718	KSNPROXY_STARTED_CON_CHK_FAILED	30 күн

Желілік агенттің ақпараттық оқиғалары

Төмендегі кестеде **Ақпараттық** маңыздылық деңгейі бар желілік агент оқиғалары көрсетілген.

Қолданба жасай алатын әрбір оқиға үшін, қолданба саясаты сипаттарындағы **Оқиғаны 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
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
Құрылғы жойылды	7709	KLNAG_EV_DEVICE_REMOVE	30 күн
Жаңа құрылғы анықталды	7710	KLNAG_EV_NAC_DEVICE_DISCOVERED	30 күн
Құрылғы авторизацияланды	7711	KLNAG_EV_NAC_HOST_AUTHORIZED	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

Оқиға таңдауларын пайдалану

Оқиғаларды таңдау, экранда Басқару серверінің дерекқорынан таңдалған аталған оқиғалар жиынтығын көруге арналған. Осы оқиға түрлері келесі санаттар бойынша топтастырылған:

- Маңыздылық деңгейі: **Критикалық оқиғалар**, **Функциялық 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 **Бақылау және есеп беру** → **Оқиғаларды таңдау** бөлімінде қолжетімді.

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 хабарлар.**
- **Пайдаланушылардың сұраулары** (басқарылатын қолданба 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, қолданба 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. Қолданбаның негізгі терезесінде **Бақылау және есеп беру** → **Оқиғаларды таңдау** бөліміне өтіңіз.
2. **Қосу** түймесін басыңыз.
3. Ашылған **Жаңа оқиғаны таңдау** терезесінде жаңа оқиғалар таңдауы параметрлерін көрсетіңіз. Параметрлерді осы терезенің бірнеше бөлімдерінде көрсетуге болады.
4. Өзгерістерді 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. Қолданбаның негізгі терезесінде **Бақылау және есеп беру** → **Оқиғаларды таңдау** бөліміне өтіңіз.

2. Өзгертуді қажет ететін оқиғалар таңдауына қарама-қарсы жалаушаны қойыңыз.

3. **Сипаттар** түймесін басыңыз.

   Оқиғалар таңдауы сипаттары терезесі ашылады.

4. Оқиғалар таңдауы сипаттарын өңдеңіз.

   > Стандартты оқиғалар таңдауы үшін сипаттарды тек келесі қойыншаларда өңдеуге болады: **Жалпы** (таңдау атауын қоспағанда), **Уақыт** және **Қатынасу құқықтары**.

   Пайдаланушы таңдаулары үшін барлық сипаттарды өзгертуге болады.

5. Өзгерістерді сақтау үшін **Сақтау** түймесін басыңыз.

Өзгертілген оқиғалар таңдауы тізімде көрсетіледі.

Оқиғалар таңдауы тізімін қарау

Оқиғалар таңдауын қарап шығу:

1. Қолданбаның негізгі терезесінде **Бақылау және есеп беру** → **Оқиғаларды таңдау** бөліміне өтіңіз.

2. Іске қосу қажет оқиғалар таңдауына қарама-қарсы жалаушаны қойыңыз.

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.

     c. Таңдаудың атауын басыңыз.

- Әйтпесе, оқиғалар тізімін Басқару серверінде сақталғандай етіп көргіңіз келсе, таңдаудың атауын басыңыз.

Оқиғалар таңдауы нәтижесі көрсетіледі.

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 **Бақылау және есеп беру → 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 **Бақылау және есеп беру → 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 импорттalса, 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.
3. Ашылған терезеде келесі әрекеттерді орындауға болады:
   - Таңдалған оқиғаның ақпаратын қарау.
   - Тізімдегі келесі немесе алдыңғы оқиғаға өту — оқиғаларды таңдаудың нәтижелері.
   - Оқиға туындаған құрылғыға өту.
   - Оқиға туындаған құрылғыны қамтитын басқару тобына өту.
   - Тапсырмамен байланысты оқиға үшін тапсырманың сипаттарына өтіңіз.

Оқиғаларды файлға экспорттау

Оқиғаларды файлға экспорттау үшін:

1. Оқиғалар таңдауын іске қосыңыз.
2. Қажетті оқиғаның жанындағы жалаушаны қойыңыз.
3. **Файлға экспорттау** түймесін басыңыз.

Таңдалған оқиғалар файлға экспортталды.

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

Бір немесе бірнеше оқиғаны жою үшін:

1. Оқиғалар таңдауын іске қосыңыз.
2. Қажетті оқиғалардың жанында жалаушаларды қойыңыз.
3. **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 жою мүмкін емес.

Оқиғалар таңдауын жою үшін:

1. Қолданбаның негізгі терезесінде **Бақылау және есеп беру** → **Оқиғаларды таңдау** бөліміне өтіңіз.
2. Жойғыңыз келетін оқиғалар таңдауына қарсы жалаушаларды қойыңыз.
3. **Жою** түймесін басыңыз.
4. Пайда болған терезеде **OK** түймесін басыңыз.

Оқиғалар таңдауы жойылады.

Оқиғаны сақтау мерзімін конфигурациялау

Kaspersky Security Center Linux, басқарылатын қолданбаларға орнатылған "Лаборатория Касперского" Басқару сервері мен қолданбаларының 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, "Лаборатория Касперского" қолданбасы 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 ұзақ уақыт аралығында қарауға мүмкіндік береді.

Басқару сервері дерекқорында оқиғаны сақтау мерзімін белгілеу үшін:

1. Қолданбаның негізгі терезесінде **Активтер (құрылғылар)** → **Саясат және профильдер** бөліміне өтіңіз.
2. Келесі әрекеттердің бірін орындаңыз:
   - Желілік агенттің немесе "Лаборатория Касперского" басқарылатын қолданбасы оқиғаларының жарамдылық мерзімін конфигурациялау үшін тиісті саясаттың атын басыңыз.

     Саясат сипаттары беті ашылады.
   - Басқару сервері оқиғаларын конфигурациялау үшін, басты мәзірде қажетті Басқару сервері атауының жанындағы параметрлер (⚙) белгішесін басыңыз.

     Егер сізде Басқару серверіне арналған саясат болса, сол саясаттың атын басуға болады.

     Басқару сервері сипаттары беті (немесе Басқару сервері саясаты сипаттары беті) ашылады.
3. **Оқиғаны конфигурациялау** қойындысын таңдаңыз.

   Байланысты оқиғалар тізімі бар **Критикалық** бөлімі көрсетіледі.
4. **Функционалдық ақау**, **Ескерту** немесе **Ақпараттық** бөлімін таңдаңыз.
5. Оң жақ тақтадағы оқиғалар түрлерінің тізімінде сақтау мерзімін өзгерткіңіз келетін оқиға атауының сілтемесіне өтіңіз.

   Оқиғаларды тіркеу бөлімінде ашылған терезеде **Басқару серверінің дерекқорында сақтау мерзімі (күндер)** параметрін қосыңыз.
6. Қосқыштың астындағы өңдеу өрісінде оқиғаны сақтау күндерінің санын көрсетіңіз.
7. 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 Kaspersky Security Center Басқару сервері саясатында бұғатталған болса, оқиғаны сақтау мерзімінің мәнін өзгерте алмайсыз.
8. **OK** 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 қолданба 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. Басты мәзірде қажетті Басқару сервері атауының жанындағы параметрлер (⚙) белгішесін 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. Басты мәзірде қажетті Басқару сервері атауының жанындағы параметрлер (⚙) белгішесін 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 құрылғылардың жұмысындағы оқиғалар туралы ақпарат Басқару серверінің дерекқорында сақталады. Әрбір оқиға белгілі бір түрге және маңыздылық деңгейіне қатысты болып келеді (*Критикалық оқиға*, *Функционалдық ақау*, *Ескерту*, *Ақпараттық хабарлар*). Оқиға болған жағдайларға байланысты, қолданба 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, қолданба 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.

Қолданба дерекқорды 10 минут сайын тексереді. Оқиғалар саны көрсетілген максималды мәннен 10 000 артық болса, қолданба 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.

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.

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:

- **Бақылау және есеп беру** → **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.
- **Бақылау және есеп беру** → **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. Қолданбаның негізгі терезесінде **Бақылау және есеп беру** → **Хабарландырулар** бөліміне өтіңіз.

   Сол жақ тақтада **Барлық хабарландырулар** санаты таңдалған, ал сол жақта барлық хабарландырулар көрсетіледі.

2. Сол жақ тақтадан келесі санаттардың бірін таңдаңыз:

   - **Орналастыру**
   - **Құрылғылар**
   - **Қорғаныс**
   - **Жаңартулар** (бұған жүктеуге болатын "Лаборатория Касперского" қолданбалары туралы хабарландырулар және жүктелген антивирустық дерекқор жаңартулары туралы хабарландырулар кіреді)
   - **Эксплойттан қорғаныс**
   - **Басқару сервері** (бұл хабарландыру тек Басқару серверіне қатысты оқиғаларды қамтиды)
   - **Пайдалы сілтемелер** (бұған "Лаборатория Касперского" ресурстарына сілтемелер, мысалы, "Лаборатория Касперского" Техникалық қолдау қызметіне, "Лаборатория Касперского" форумына, лицензияны ұзарту бетіне немесе Вирустық энциклопедияға сілтеме кіреді)
   - **«Лаборатория Касперского» корпоративтік жаңалықтары** (бұған "Лаборатория Касперского" қолданбалары шығарылымдары туралы мәліметтер 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: **Критикалық 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 қолданбасын 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** қойындысын таңдаңыз.

   Критикалық хабарландырулар () және *Ескерту хабарландырулары* () 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** қойындысын 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 **Веб-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. **Бақылау және есеп беру** 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 жағдайларда Kaspersky Security Center Linux құрылғысына күй тағайындау кезінде құрылғының желіде көрінуін ескереді (төмендегі кестені қараңыз). 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 қолданбасы 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 бағдарлама сканерлеуі ұзақ уақыт орындалмады	Құрылғы желіде көрінеді және құрылғыда қауіпсіздік қолданбасы 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 қолданбасы 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 іске қосу керек	Құрылғы желіде көрінеді, бірақ қолданба таңдалған себептердің біріне байланысты құрылғыны белгіленген уақыттан ұзағырақ қайта жүктеуді талап етеді.	0 минуттан көбірек.
Үйлесімді емес бағдарламалар орнатылды	Құрылғы желіде көрінеді, бірақ Желілік агент орындаған қолданбалық жасақтаманы түгендеу кезінде, құрылғыда үйлесімсіз қолданбалардың 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 қолданбаларда осалдықтар анықталды.	• Критикалық. • Жоғары. • Орташа. • Осалдықты жабу мүмкін болмаса, елемеу. • Жаңарту орнатуға белгіленген болса, елемеу.
Лицензия	Құрылғы желіде көрінеді, бірақ лицензияның жарамдылық	• Қосқыш өшірулі.

мерзімі өтті	мерзімі өтіп кеткен.	• 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.
Windows Update жаңартуларын іздеу ұзақ уақыт бойы орындалмады	*Windows Update жаңартуларын синхрондау* тапсырмасы көрсетілген уақыттан артық 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.
Ұялы 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 клиент құрылғысында орнатылған "Лаборатория Касперского" басқарылатын қолданбаларының көмегімен автоматты түрде де, әкімші тарапынан қолмен де жасалуы мүмкін.	• Қосқыш өшірулі. • Қосқыш қосулы.
Бағдарлама анықтаған құрылғы күйі	Құрылғының күйін басқарылатын қолданба анықтайды.	• 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 *OK* 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 қолданбасы көрсетілген уақыттан артық өшірулі. Бұл жағдайда қауіпсіздік қолданбасының 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 қолданбасы 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 *OK* 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 Дерекқорлар ескірген күйін тағайындау үшін *Databases are outdated* шартының мәні өзгермейді.

Kaspersky Security Center Linux қолданбасы құрылғыға күй тағайындаған кезде, кейбір шарттар үшін (жоғарыдағы кестеде "Шарттар сипаттамасы" бағанын қараңыз) құрылғылардың көзге көрінуі ескеріледі. Мысалы, басқарылатын құрылғыға *Критикалық* күйі берілген болса, Дерекқорлар ескірген шарты орындалғандықтан, құрылғы үшін көзге көрінетін болғандықтан, құрылғыға *OK* күйі беріледі.

Құрылғылардың күйлерін ауыстыруды конфигурациялау

Құрылғыға *Критикалық* немесе *Ескерту* күйлерін тағайындау шарттарын өзгерте аласыз.

Құрылғының күйін Критикалық деп өзгерту үшін:

1. Қолданбаның негізгі терезесінде **Активтер (құрылғылар)** → **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** қойындысын таңдаңыз.

4. **Критикалық** бөлімін таңдаңыз.
5. **Егер олар көрсетілген болса, Критикалыққа орнатыңыз** 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.

Белгіленген шарттарды орындамаған жағдайда, басқарылатын құрылғыға *Критикалық* күйі тағайындалады.

Құрылғының күйін Ескерту деп өзгерту үшін:

1. Қолданбаның негізгі терезесінде **Активтер (құрылғылар)** → **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** қойындысын таңдаңыз.
4. **Ескерту** бөлімін таңдаңыз.
5. **Егер олар көрсетілген болса, Ескертуге орнатыңыз** 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.

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 қолданбасы көрсетілген электрондық пошта мекенжайларына хабарландыру жібереді.
- SMS – оқиға болған кезде Kaspersky Security Center Linux қолданбасы 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. Басты мәзірде қажетті Басқару сервері атауының жанындағы параметрлер (⚙) белгішесін 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. Файлдарды жүктеу тәртібі маңызды емес. Екі файл да жүктелген кезде жеке кілттің шифрсыздау үшін құпиясөзді көрсету керек. Жеке кілт шифрланбаған болса, құпиясөздің мәні бос болуы мүмкін.

- PKCS#12 пішіміндегі сертификаты бар контейнер:

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: қолданба 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 қолданба 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, қолданба 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 қолданба 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: қолданба көрсетілген алушыларға мәтіндік хабарлар жібереді.

Хабарландырулар санының шегін конфигурациялау сілтемесінен өтіп, қолданба 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 қолданба 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, қолданба көрсетілген уақыт аралығында жібере алатын хабарландырулардың ең көп санын көрсетуге болады.

3. Қойыншада хабарландыру параметрлерін конфигурациялаңыз.

4. Басқару сервері сипаттары терезесін жабу үшін **ОК** түймесін басыңыз.

Сақталған хабарландыруларды жеткізу параметрлері Kaspersky Security Center Linux бағдарламасында болатын барлық оқиғаларға қолданылады.

Оқиғаны конфигурациялау бөлімінде, Басқару сервері параметрлерінде, саясат параметрлерінде немесе қолданба 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. Қолданбаның негізгі терезесінде **Бақылау және есеп беру** → **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 қолданбаларының 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 алмастырылатын параметрлері бар басқа орындалатын файл болуы керек.

Оқиғаны сипаттауға арналған алмастырылатын параметрлер

Алмастырылатын параметр	Алмастырылатын параметр сипаттамасы
%SEVERITY%	Оқиғаның маңыздылық деңгейі
%COMPUTER%	Оқиға болған құрылғының атауы
%DOMAIN%	Домен.
%EVENT%	Оқиға
%DESCR%	Оқиғаның сипаттамасы
%RISE_TIME%	Пайда болу уақыты
%KLCSAK_EVENT_TASK_DISPLAY_NAME%	Тапсырма атауы
%KL_PRODUCT%	Желілік агент
%KL_VERSION%	Желілік агент нұсқасының нөмірі
%HOST_IP%	IP мекенжайы
%HOST_CONN_IP%	Қосылым 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.

"Лаборатория Касперского" хабарландырулары

Бұл бөлімде "Лаборатория Касперского" хабарландыруларын қолдану, конфигурациялау және өшіру тәсілі сипатталған.

"Лаборатория Касперского" хабарландырулары туралы

"Лаборатория Касперского" хабарландырулары бөлімі (**Бақылау және есеп беру → "Лаборатория Касперского" хабарландырулары**) Kaspersky Security Center нұсқаңыз және басқарылатын құрылғыларға орнатылған басқарылатын қолданбалар 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 "Лаборатория Касперского" қолданбаларына қатысты "Лаборатория Касперского" хабарландыруларын ғана көрсетеді. Хабарландырулар Басқару серверінің кез келген түрі (негізгі, қосалқы немесе виртуалды) үшін жеке-жеке көрсетіледі.

"Лаборатория Касперского" хабарландыруларын алу үшін Басқару серверінде интернет қосылымы болуы тиіс.

Хабарландыруларға келесі түрдегі ақпарат кіреді:

- Қауіпсіздікке қатысты хабарландырулар.

  Қауіпсіздікке қатысты хабарландырулар сіздің желіңізде орнатылған "Лаборатория Касперского" қолданбалары өзекті күйде болуына және толығымен жұмыс істеуге жарамды болуына арналған. Хабарландыруларда "Лаборатория Касперского" қолданбаларына арналған критикалық жаңартулар, табылған осалдықтарға арналған түзетулер және "Лаборатория Касперского" қолданбаларындағы 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 қолданбасы деректерді "Лаборатория Касперского" бұлтты серверлеріне жібереді және сіздің желіңізде орнатылған "Лаборатория Касперского" қолданбаларына қатысты хабарландыруларды ғана алады. Серверлерге жіберілуі мүмкін деректер Kaspersky Security Center Басқару серверін орнату кезінде қабылдайтын Лицензиялық келісімде сипатталған.

- Жарнамалық хабарландырулар.

  Жарнамалық хабарландырулар "Лаборатория Касперского" қолданбаларыңыз үшін арнайы ұсыныстар туралы ақпаратты, "Лаборатория Касперского" 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 "Лаборатория Касперского" 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.

"Лаборатория Касперского" Хабарландырулар бөлімінде жаңа ақпарат пайда болған кезде, Kaspersky Security Center Web Console қолданбасы хабарландырулардың маңыздылық деңгейіне сәйкес келетін хабарландыру белгісін көрсетеді. Бұл хабарландыруды "Лаборатория Касперского" Хабарландырулар бөлімінде көру үшін белгіні түртуге болады.

"Лаборатория Касперского" хабарландырулар параметрлерін, соның ішінде көргіңіз келетін хабарландыру санаттарын және хабарландыру белгісін көрсету орнын көрсете аласыз. Хабарландыруларды алып тұрғыңыз келмесе, бұл функцияны өшіре аласыз.

"Лаборатория Касперского" хабарландыру параметрлерін конфигурациялау

"Лаборатория Касперского" хабарландырулары бөлімінде сіз көргіңіз келетін хабарландырулар санаттарын қоса алғанда, "Лаборатория Касперского" хабарландырулары параметрлерін және хабарландыру белгісін қайда көрсету керектігін көрсете аласыз.

"Лаборатория Касперского" хабарландыруларын конфигурациялау үшін:

1. Қолданбаның негізгі терезесінде **Бақылау және есеп беру → «Лаборатория Касперского» хабарландырулары** бөліміне өтіңіз.

2. **Параметрлер** сілтемесінен өтіңіз.

   "Лаборатория Касперского" 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 **Бақылау және есеп беру** бөлімінде және оның бөлікшелерінде көрсетілуі мүмкін.

4. **OK** түймесін басыңыз.

   "Лаборатория Касперского" хабарландырулары параметрлері конфигурацияланған.

"Лаборатория Касперского" хабарландыруларын өшіру

"Лаборатория Касперского" хабарландырулары бөлімі (**Бақылау және есеп беру → "Лаборатория Касперского" хабарландырулары**) Kaspersky Security Center нұсқаңыз және басқарылатын құрылғыларға орнатылған басқарылатын қолданбалар туралы ақпаратты ұсынады. "Лаборатория Касперского" хабарландыруларын алып тұрғыңыз келмесе, бұл функцияны өшіре аласыз.

"Лаборатория Касперского" хабарландырулары екі түрлі ақпаратты қамтиды: қауіпсіздікке қатысты хабарландырулар және жарнамалық хабарландырулар. Сіз әрбір түрдегі хабарландыруларды бөлек өшіре аласыз.

Қауіпсіздікпен байланысты хабарландыруларды өшіру үшін:

1. Басты мәзірде қажетті Басқару сервері атауының жанындағы параметрлер (⚙) белгішесін басыңыз.

Басқару серверінің сипаттары терезесі ашылады.

2. **Жалпы** қойыншасында **"Лаборатория Касперского" хабарландырулары** бөлімін таңдаңыз.

3. Қосқышты **Қауіпсіздікке қатысты хабарландырулар** өшірілген күйіне ауыстырыңыз.

4. **Сақтау** түймесін басыңыз.

   "Лаборатория Касперского" 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. Басты мәзірде қажетті Басқару сервері атауының жанындағы параметрлер (⚙) белгішесін басыңыз.

   Басқару серверінің сипаттары терезесі ашылады.

2. **Жалпы** қойындысында **KSN-прокси параметрлері** бөлімін таңдаңыз.

3. **Kaspersky Security Network пайдалану Қосулы** параметрін өшіріңіз.

4. **Сақтау** түймесін басыңыз.

   Хабарландырулар өшірулі.

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 Security Center Linux EDR Optimum немесе XDR Expert лицензиясы бойынша 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. Толық ақпаратты Kaspersky Next анықтамасынан қараңыз.

Бұлттық сервистерге 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 функционал: Негізгі функционалдылық** **Жазу** Write рұқсатыңыз болуы керек.

Cloud Discovery веб-виджеті көмегімен Cloud Discovery функциясын қосу үшін:

1. Kaspersky Security Center Linux ашыңыз.
2. Негізгі қолданба терезесінде **Бақылау және есеп беру** → **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 функционал: Негізгі функционалдылық**Жазу**Жазу** рұқсаты болуы керек.

Cloud Discovery веб-виджетін бақылау тақтасына қосу үшін:

1. Kaspersky Security Center Linux ашыңыз.
2. Негізгі қолданба терезесінде **Бақылау және есеп беру** → **Бақылау тақтасы** бөліміне өтіңіз.
3. **Веб-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 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 функционал: Негізгі функционалдылық**Оқу**Оқу** құқығыңыз бар.

Cloud Discovery веб-виджетін көру үшін:

1. Kaspersky Security Center Linux ашыңыз.
2. Негізгі қолданба терезесінде **Бақылау және есеп беру** → **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.

Веб-виджетте сұралған деректер көрсетіледі.

Көрсетілген веб-виджетте келесі әрекеттерді орындауға болады:

- Cloud Discovery есептерін көру үшін **Бақылау және есеп беру** → **Есептер** тармағына өтіңіз.
- Таңдалған бұлттық сервиске қол жеткізуді бұғаттаңыз немесе оған рұқсат беріңіз.

Бұғаттау мүмкіндігі Kaspersky Security Center Linux бағдарламасын Kaspersky Security Center Linux EDR Optimum немесе XDR Expert лицензиясы бойынша 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 сервиске қол жеткізуді бұғаттау туралы шешім қабылдағанда тәуекел деңгейін ескеруге болады.

Тәуекел деңгейі бағалау болып табылады және бұлттық сервис немесе өндіруші сапасы туралы ештеңе айтпайды. Тәуекел деңгейі – "Лаборатория Касперского" сарапшыларының ұсынысы.

Бұлттық сервистің тәуекел деңгейлері Cloud Discovery веб-виджетінде және барлық бақыланатын бұлттық сервистер 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 сервиске 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.

Сценарий: оқиғаларды SIEM жүйелеріне экспорттауды конфигурациялау

Kaspersky Security Center Linux жүйесі оқиғаларды SIEM жүйелеріне экспорттауды келесі жолдардың бірімен теңшеуге мүмкіндік береді: Syslog пішімін пайдаланып кез келген SIEM жүйесіне 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. "Лаборатория Касперского" басқарылатын барлық қолданбаларында туындайтын жалпы оқиғаларды белгілеңіз. Кейін белгілі бір басқарылатын қолданба үшін экспортталатын оқиғаларды белгілеуге болады.

- **Оқиғаларды SIEM жүйесіне экспорттауды конфигурациялау**

  Оқиғаларды келесі жолдармен экспорттауға болады:

  - TCP/IP, UDP немесе TLS over TCP протоколдарын көрсетіңіз.
  - Оқиғаларды тікелей Kaspersky Security Center дерекқорынан экспорттауды қолдану. Kaspersky Security Center дерекқорында көпшілікке арналған көріністер жиынтығы ұсынылған; сіз осы жалпыға қолжетімді көріністердің сипаттамасын klakdb.chm құжатында 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, басқарылатын қолданбаларға орнатылған "Лаборатория Касперского" Басқару сервері мен қолданбаларының 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. Конфигурациялаудың бірізділігі маңызды емес: Сіз алдымен оқиғаларды Kaspersky Security Center Linux-ге жіберуді конфигурациялай аласыз, содан соң оқиғаларды SIEM жүйесінде алуды немесе керісінше конфигурациялай аласыз.

Syslog пішіміндегі оқиғаларды экспорттау

Оқиғаларды Syslog пішімінде кез келген SIEM жүйесіне жіберуге болады. Syslog пішімін пайдаланып, Басқару серверде және басқарылатын құрылғыларға орнатылған "Лаборатория Касперского" қолданбаларында орын алған кез келген оқиғаны жіберуге болады. Оқиғаларды Syslog пішімінде экспорттау кезінде SIEM жүйесіне қандай оқиғалар берілетінін таңдауға 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**

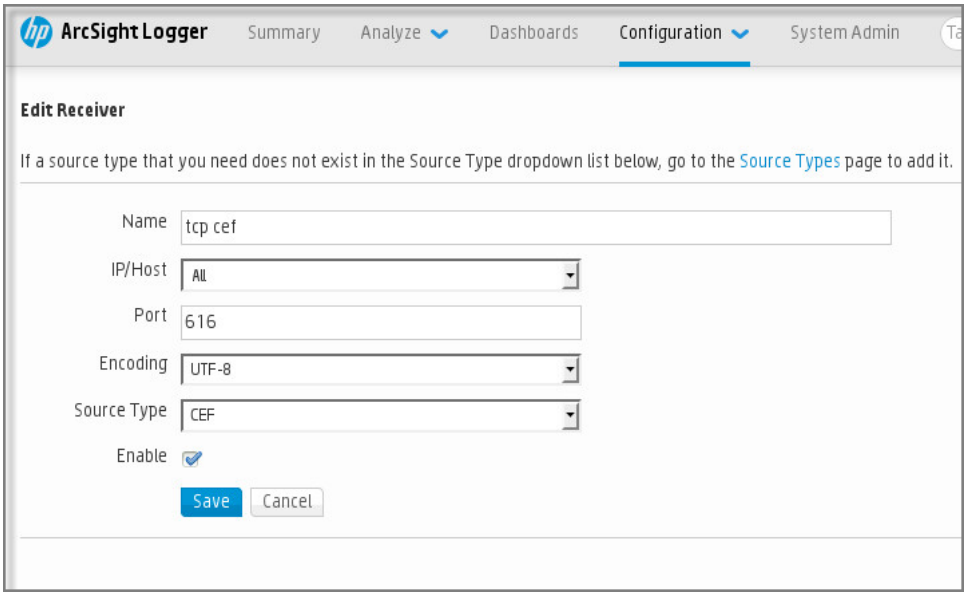
  Kaspersky Security Center Linux-ке қосылуға арналған порт нөмірін көрсетіңіз. Бұл порт оқиғаны SIEM жүйесіне экспорттауды конфигурациялау кезінде Kaspersky Security Center Linux жүйесінде көрсеткен портқа сәйкес келуі керек.

- **Күн пішімі**

  Syslog 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 және басқа да параметрлер сияқты өрістерге бөлу үшін қолданылады. Нәтижесінде, SIEM жүйесі Kaspersky Security Center Linux-ден алынған оқиғаларды SIEM жүйесінің дерекқорында сақталатындай етіп өңдеу мүмкіндігіне ие.

SIEM жүйелеріне Syslog пішімінде экспортталатын оқиғаларды таңдау

Бұл бөлімде Syslog пішімінде SIEM жүйелеріне одан әрі экспорттау үшін оқиғаларды қалай таңдау керектігі сипатталған.

SIEM жүйесіне Syslog пішімінде экспорттау үшін оқиғаларды таңдау туралы

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 қолданбаларда орын алған таңдалған оқиғалар SIEM жүйесіне жіберіледі. Егер экспортталатын оқиғалар саясатта таңдалған болса, сіз осы саясатпен басқарылатын жеке қолданба үшін оларды қайта анықтай алмайсыз.

- Басқарылатын қолданба үшін оқиғаларды таңдау. Егер сіз басқарылатын құрылғыларда орнатылған басқарылатын қолданба үшін экспортталатын оқиғаларды таңдасаңыз, онда SIEM жүйесіне тек осы қолданбада орын алған оқиғалар ғана жіберіледі.

"Лаборатория Касперского" қолданбалары оқиғаларын Syslog пішімінде экспорттау үшін таңдау

Егер сіз басқарылатын құрылғыларда орнатылған белгілі бір басқарылатын қолданбада болған оқиғаларды экспорттағыңыз келсе, қолданба саясатында экспортталатын оқиғаларды таңдаңыз. Бұл жағдайда, белгіленген оқиғалар саясаттың әрекет ету ауқымына кіретін барлық құрылғылардан экспортталады.

Белгілі бір басқарылатын қолданба үшін экспортталатын оқиғаларды белгілеу үшін:

1. Қолданбаның негізгі терезесінде **Активтер (құрылғылар)** → **Саясат және профильдер** бөліміне өтіңіз.

2. Оқиғаларды белгілеу қажет қолданба саясатын таңдаңыз.

   Саясат сипаттары терезесі ашылады.

3. **Оқиғаны 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 қолданбадан SIEM жүйесіне экспорттауға дайын.

Белгілі бір басқарылатын құрылғы үшін SIEM жүйесіне қандай оқиғаларды экспорттау керектігін атап өтуге болады. Егер экспортталатын оқиғалар бұған дейін қолданба саясатында таңдалған болса, сіз басқарылатын құрылғы үшін таңдалған оқиғаларды қайта анықтай алмайсыз.

Басқарылатын құрылғыға арналған оқиғаларды таңдау үшін:

1. Қолданбаның негізгі терезесінде **Активтер (құрылғылар)** → **Басқарылатын 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 өтіңіз.

4. Қолданбалар тізімінде қажетті қолданбаның атауы бар сілтемеге өтіңіз.

5. **Оқиғаны конфигурациялау** бөліміне өтіңіз.

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. Келесі әрекеттердің бірін орындаңыз:

   - Басты мәзірде қажетті Басқару сервері атауының жанындағы параметрлер (⚙) белгішесін басыңыз.
   - Қолданбаның негізгі терезесінде **Активтер (құрылғылар)** → **Саясат және профильдер** бөліміне өтіңіз, содан соң саясат сілтемесінен өтіңіз.

2. Ашылған терезеде **Оқиғаны конфигурациялау** қойындысына өтіңіз.

3. **Syslog көмегімен SIEM жүйесіне экспорттауды белгілеу** 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 теңшелген болса, Басқару сервері SIEM жүйесіне таңдалған оқиғаларды жібереді.

Syslog пішіміндегі оқиғаларды экспорттау туралы

Syslog пішімін қолдана отырып, басқарылатын құрылғыларда орнатылған "Лаборатория Касперского" Басқару сервері мен басқа да қолданбаларында 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-ден 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 экспорттолтанын 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.

Kaspersky Security Center Web Console веб-консолінен SIEM жүйелеріне экспорттауды конфигурациялау үшін:

1. Басты мәзірде қажетті Басқару сервері атауының жанындағы параметрлер (⚙) белгішесін басыңыз.

   Басқару серверінің сипаттары терезесі ашылады.

2. **Жалпы** қойындысында **SIEM** 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/IP, UPD немесе TLS over TCP протоколын таңдай аласыз.

TLS over TCP таңдасаңыз, келесі TLS параметрлерін көрсетіңіз:

- **Сервердің түпнұсқалық растамасы**

  Сервердің түпнұсқалық растамасы өрісінде **Сенімді сертификаттар** немесе **SHA сәйкестендіру белгілері** мәндерін таңдауға болады:

  - **Сенімді сертификаттар**. Сертификаттар тізімі бар файлды сенімді сертификаттау орталығынан (CA) ала аласыз және оны Kaspersky Security Center Linux бағдарламасына жүктей аласыз. Kaspersky Security Center Linux бағдарламасы SIEM жүйесінің сертификатына 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 SHA-1 бағдарламасында SIEM жүйесі сертификаттарының сәйкестендіру белгілерін көрсете аласыз. SHA-1 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**. Сертификат файлын **Сертификаты бар файл** өрісіне және жабық кілт файлын **Кілті бар файл** өрісіне жүктеп салыңыз. Екі файл да бір-біріне тәуелді емес. Файлдарды жүктеу тәртібі 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.

5. Мұрағатталған оқиғаларды Басқару серверінің дерекқорынан экспорттауға және мұрағатталған оқиғаларды экспорттауды бастағыңыз келетін басталу күнін орнатуға болады:

   a. **Экспорттың басталу күнін орнату** сілтемесіне өтіңіз.

   b. Ашылатын бөлімде экспорттың басталу күнін **Экспорттың басталу күні** өрісінде көрсетіңіз.

   c. **OK** түймесін басыңыз.

6. Параметрді **Оқиғаларды SIEM жүйесінің дерекқорына автоматты түрде экспорттау Қосулы** жайғасымына ауыстырып қосыңыз.

7. SIEM жүйесіне қосылым сәтті конфигурацияланғанына көз жеткізу үшін **Байланысты тексеру** түймесін басыңыз.

   Қосылым күйі көрсетіледі.

8. **Сақтау** түймесін басыңыз.

SIEM жүйесіне экспорттау теңшелді. SIEM жүйесінде оқиғаларды қабылдауды конфигурациялаған болсаңыз, Басқару сервері таңдалған оқиғаларды SIEM жүйесіне экспорттайды. Экспорттың басталу күнін орнатсаңыз, Басқару сервер өзінің дерекқорында сақталған белгіленген оқиғаларды да көрсетілген күннен бастап экспорттайды.

Оқиғаларды тікелей дерекқордан экспорттау

Kaspersky Security Center 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, қолданбаларға, пайдаланушыларға қатысты жария көріністер туралы ақпарат та бар. Сіз бұл ақпаратты сұраулар жасау кезінде пайдалана аласыз.

Бұл бөлімде klsql2 утилитасы арқылы SQL сұрауын жасау бойынша нұсқаулар, сондай-ақ осындай сұраудың мысалы келтірілген.

Сондай-ақ, SQL сұраулары мен дерекқор көріністерін жасау үшін дерекқорлармен жұмыс істеуге арналған кез келген басқа қолданбаларды 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 бөлімде klsql2 утилитасын пайдалану, сондай-ақ осы утилитаны пайдаланып SQL сұрауын жасау бойынша нұсқаулар берілген. Kaspersky Security Center Linux жүйесінің орнатылған нұсқасына кіретін klsql2 утилитасының нұсқасын пайдаланыңыз.

klsql2 утилитасын пайдалану үшін:

1. Kaspersky Security Center басқару сервері орнатылған құрылғыдағы /opt/kaspersky/ksc64/sbin/klsql2 каталогіне өтіңіз.

2. Бұл директорияда бос src.sql файлын жасаңыз.

3. src.sql файлын кез келген мәтіндік редактордың көмегімен ашыңыз.

4. src.sql файлында қажетті SQL сұрауын енгізіп, файлды сақтаңыз.

5. Kaspersky Security Center Басқару сервері орнатылған құрылғыда, src.sql файлынан SQL сұрауын іске қосу және нәтижелерді result.xml файлына сақтау үшін келесі пәрменді енгізіңіз:
   ```
   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. Жасалған result.xml файлын ашып, сұраудың орындалу нәтижелерін қараңыз.

Сіз src.sql файлын өңдей аласыз және онда көпшілікке ұсынуға кез келген сұраулар 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 келтірілген.

Келесі мысал, пайдаланушылардың құрылғыларында соңғы 7 күнде болған оқиғалардың тізімін қалай алуға болатындығын және оны оқиғалардың пайда болу уақыты бойынша сұрыптауға болатындығын көрсетеді, алдымен ең соңғы оқиғалар көрсетіледі.

Мысалы:

```
SELECT
e.nId,                                          /* оқиға идентификаторы */
e.tmRiseTime,                                   /* оқиғаның пайда болу
уақыты */
e.strEventType,                                 /* оқиға түрінің ішкі атауы
*/
e.wstrEventTypeDisplayName,                     /* көрсетілген оқиға атауы
*/
e.wstrDescription,                              /* көрсетілген оқиға
сипаттамасы */
e.wstrGroupName,                                /* құрылғылар тобының атауы
*/
```

```
h.wstrDisplayName,                                    /* оқиға болған құрылғының
көрсетілетін атауы */
CAST(((h.nIp / 16777216) & 255) AS varchar(4)) + '.' +
CAST(((h.nIp / 65536) & 255) AS varchar(4)) + '.' +
CAST(((h.nIp / 256) & 255) AS varchar(4)) + '.' +
CAST(((h.nIp) & 255) AS varchar(4)) as strIp          /* оқиға болған құрылғының
IP мекенжайы */
FROM v_akpub_ev_event e
INNER JOIN v_akpub_host h ON h.nId=e.nHostId
WHERE e.tmRiseTime>=DATEADD(Day, -7, GETUTCDATE())
ORDER BY e.tmRiseTime DESC
```

Kaspersky Security Center Linux дерекқорының атауын қарау

Kaspersky Security Center Linux дерекқорына SQL Server, 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. Басты мәзірде қажетті Басқару сервері атауының жанындағы параметрлер (⚙) белгішесін 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.

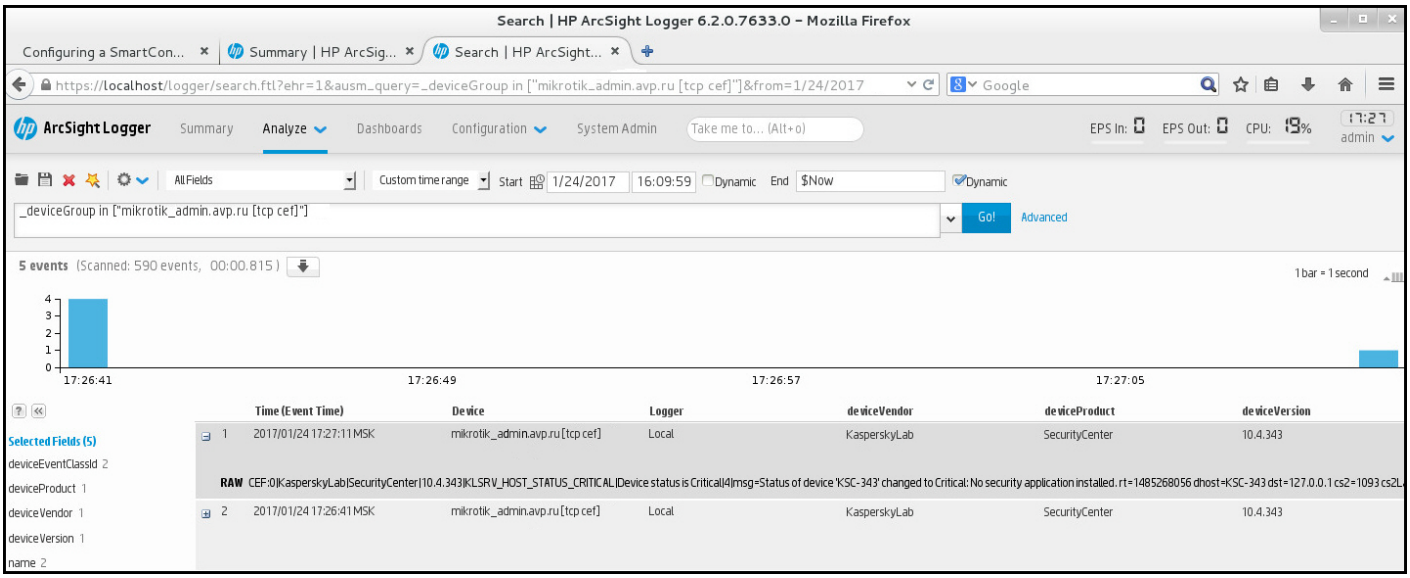
Экспорт нәтижелерін қарау

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 сипаттары;
- 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.
- **Веб-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 **Активтер (құрылғылар)** → **Саясат және профильдер** 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.

Саясаттың тексерісін JSON файлына сақтау үшін,

Саясат тексерістері тізімінде сақтағыңыз келетін тексерісті таңдап, **Файлға сақталуда** түймесін басыңыз.

Тексеріс JSON файлында сақталады.

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** қойындысына 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.

Нысандарды жою

Бұл бөлімде нысандарды жою және олар жойылғаннан кейін, нысандардың ақпаратын қарау әдісі сипатталған.

Сіз келесі нысандарды жоя аласыз:

- саясаттар;
- тапсырмалар;
- орнату пакеттері;
- виртуалды Басқару серверлері;
- пайдаланушылар;
- қауіпсіздік топтары;
- басқару топтары.

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, қолданба құрылғыны Тағайындалмаған құрылғылар тобына жылжытады. Құрылғы жойылғаннан кейін, "Лаборатория Касперского" орнатылған қолданбалары – Желілік агент және Kaspersky Endpoint Security сияқты қауіпсіздік қолданбасы 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. 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 Windows жүйесіне арналған Kaspersky Endpoint Security сияқты дискіні шифрлау үшін пайдаланылған қауіпсіздік қолданбасы орнатылған.

Егер диск Kaspersky Disk Encryption технологиясы арқылы шифрланған болса, FDERT Restore утилитасын пайдаланып деректерді қалпына келтіруге де болады.

Құрылғыны Тағайындалмаған құрылғылар тобынан қолмен жойған кезде, қолданба құрылғыны тізімнен жояды. Құрылғы жойылғаннан кейін, "Лаборатория Касперского" орнатылған қолданбалары (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 Сақтық көшірмелеуге жүктеу және одан жою

Бұл бөлімде, файлдарды Карантин мен Сақтық көшірмелеуден Kaspersky Security Center Web Console веб-консоліне жүктеу және одан жою тәсілі туралы ақпарат келтірілген.

Файлдарды Карантинге және Сақтық көшірмелеуге жүктеу

Келесі екі шарттың бірі орындалса ғана, файлдарды Карантин мен Сақтық көшірмелеуден 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 резервтік сақтау орнынан 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** → **Сақтық көшірмелеу** 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 немесе Белсенді қауіптерден жою туралы

Клиент құрылғыларына орнатылған "Лаборатория Касперского" қауіпсіздік қолданбалары нысандарды Карантин, Сақтық көшірмелеу немесе Белсенді қауіптерге салған кезде, олар қосылған нысандар туралы ақпаратты, **Карантин**, **Сақтық көшірмелеу** немесе **Белсенді қауіптер** бөлімдеріне қосылған нысандар туралы ақпаратты Kaspersky Security Center Linux бағдарламасына береді. Осы бөлімдердің бірін ашқан кезде тізімдегі нысанды таңдаңыз және **Жою** түймесін басыңыз, Kaspersky Security Center Linux бағдарламасы келесі әрекеттердің бірін немесе екі әрекетті де орындайды:

- Таңдалған нысанды тізімнен жояды.
- Таңдалған нысанды қоймадан жояды.

Орындалуы тиісті әрекет, таңдалған нысанды қоймаға салынған "Лаборатория Касперского" қолданбасы тарапынан анықталады. "Лаборатория Касперского" қолданбасы **Жазба қосылды** өрісінде көрсетілген. Қандай әрекетті орындау керектігі туралы толық ақпаратты "Лаборатория Касперского" қолданбасына арналған құжаттамадан қараңыз.

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 қолданба параметрлерін жүктеу;
- оқиғалар журналдарын жүктеу;
- қолданбадан алынған қоқыс файлын жасау;
- диагностиканы іске қосу және диагностика нәтижелерін жүктеу;
- қолданбаларды іске қосу, тоқтату және қайта іске қосу.

Ақауларды жою үшін клиент құрылғысынан жүктелген оқиғалар журналы мен диагностикалық есептерді пайдалануыңызға болады. Сондай-ақ, "Лаборатория Касперского" Техникалық қолдау қызметіне хабарласатын болсаңыз, онда "Лаборатория Касперского" техникалық қолдау маманы сізден трассалау файлдарын, қоқыс файлдарын, оқиғалар журналын және диагностикалық есептерді "Лаборатория Касперского" зертханасында 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 **Активтер (құрылғылар)** → **Басқарылатын құрылғылар** бөліміне өтіңіз.
   - Құрылғы тағайындалмаған құрылғылар тобына жататын болса, басты мәзірде **Табу және орналастыру** → **Тағайындалмаған құрылғылар** бөліміне өтіңіз.
2. Қажетті құрылғының атауын басыңыз.
3. Ашылған құрылғының сипаттар терезесінде **Кеңейтілген** бөлімін таңдаңыз.
4. Пайда болған терезеде **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.

Қолданбалар үшін трассалауды қосу және өшіру

xperf трассалауын қоса, қолданбалар 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 **«Лаборатория Касперского» бағдарламалары** бөлімін таңдаңыз.

   Бағдарламаларды басқару бөлімінде құрылғыға орнатылған "Лаборатория Касперского" бағдарламаларының тізімі ашылады.
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

     Трассирлеу деңгейі, трассирлеу файлындағы ақпарат құрамын анықтайды.

   - Айналдыру негізіндегі трассирлеу

     Қолданба 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 қолданба үшін қосулы. Кейбір жағдайларда, қауіпсіздік қолданбасын трассалауды қосу үшін осы қолданбаны 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 қолданба 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 **«Лаборатория Касперского» бағдарламалары** бөлімін таңдаңыз.

   Бағдарламаларды басқару бөлімінде құрылғыға орнатылған "Лаборатория Касперского" бағдарламаларының тізімі ашылады.

3. Қолданбалар 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 трассирлеу файлы *Жеңіл деңгей* типті файлдан да егжей-тегжейлі ақпаратты қамтиды және *жеңіл деңгейлі* трассирлеу 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 қолданбалардың тізімін, өнімділікті бағалау үшін пайдаланылатын оқиғаларды және Windows жүйесін бағалау құралының оқиғаларын қамтиды.

   b. Xperf трассалау деңгейлерінің бірін таңдаңыз:

   - **Негізгі түрі**

     Қолданба трассалау деректерін Kaspersky Endpoint Security қолданбасы жұмыс істеп тұрған кезде алады.

     Әдепкі бойынша, осы нұсқа таңдалған.

- **Қайта бастау түрі**

  Қолданба, 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.

Қолданбаны трассалау файлын жүктеу

Қолданбаны трассирлеу файлын жүктеп алу үшін:

1. Клиент құрылғысын қашықтан диагностикалау утилитасын ашыңыз.

2. Қашықтан диагностикалау терезесінде **«Лаборатория Касперского» бағдарламалары** бөлімін таңдаңыз.

   Бағдарламаларды басқару бөлімінде құрылғыға орнатылған "Лаборатория Касперского" бағдарламаларының тізімі ашылады.

3. Қолданбалар тізімінен трассирлеу файлын іске қосқыңыз келетін қолданбаны таңдаңыз.

4. **Трассирлеу** бөлімінде **Файлдарды трассирлеу** 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 **Файлдарды трассирлеу** 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.

Қолданбалар параметрлерін жүктеу

Клиент құрылғысынан қолданба параметрлерін жүктеп алу үшін:

1. Клиент құрылғысын қашықтан диагностикалау утилитасын ашыңыз.
2. Қашықтан диагностикалау терезесінде **«Лаборатория Касперского» 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.

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.

Қолданбаларды іске қосу, тоқтату және қайта іске қосу

Сіз клиент құрылғысында қолданбаларды іске қоса, тоқтата және қайта іске қоса аласыз.

Қолданбаны іске қосу, тоқтату және қайта қосу үшін:

1. Клиент құрылғысын қашықтан диагностикалау утилитасын ашыңыз.
2. Қашықтан диагностикалау терезесінде **«Лаборатория Касперского» бағдарламалары** бөлімін таңдаңыз.

   Бағдарламаларды басқару бөлімінде құрылғыға орнатылған "Лаборатория Касперского" бағдарламаларының тізімі ашылады.
3. Қолданбалар тізімінен іске қосқыңыз, тоқтатқыңыз немесе қайта іске қосқыңыз келетін қолданбаны таңдаңыз.
4. Келесі түймелердің бірін басып, әрекетті таңдаңыз:

- **Бағдарламаны тоқтату**

  Бұл түйме, қолданба қазіргі сәтте іске қосылған болса ғана қолжетімді.

- **Бағдарламаны қайта іске қосу**

  Бұл түйме, қолданба қазіргі сәтте іске қосылған болса ғана қолжетімді.

- **Бағдарламаны іске қосу**

  Бұл түйме, қолданба қазіргі сәтте іске қосылмаған болса ғана қолжетімді.

Өзіңіз таңдаған әрекетке байланысты, қажетті қолданба 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 **«Лаборатория Касперского» бағдарламалары** бөлімін таңдаңыз.

   Бағдарламаларды басқару бөлімінде құрылғыға орнатылған "Лаборатория Касперского" бағдарламаларының тізімі ашылады.
3. Қолданбалар тізімінде **Kaspersky Security Center for Linux Желілік агентін** таңдаңыз.

   Қашықтан диагностикалау параметрлері тізімі ашады.
4. **Диагностикалық есеп** бөлімінде **Диагностиканы іске қосу** түймесін басыңыз.

   Қашықтан диагностикалау процесі іске қосылып, диагностика туралы есеп құрастырылады. Диагностика процесі аяқталғаннан кейін, **Диагностикалық есепті жүктеп алу** түймесі қолжетімді болмайды.
5. Есепті жүктеп алу үшін **Диагностикалық есепті жүктеп алу** түймесін басыңыз.

Есеп көрсетілген орынға жүктеледі.

Қолданбаны клиент құрылғысында іске қосу

Сізден "Лаборатория Касперского" техникалық қолдау қызметінің маманы сұраса, сізге клиент құрылғысында қолданбаны іске қосу қажет болуы мүмкін. Сізге қолданбаны осы құрылғыға өз бетіңізше орнатудың қажеті жоқ.

Қолданбаны 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. **Бағдарлама файлдары** бөлімінде клиенттік құрылғыда іске қосқыңыз келетін бағдарламамен ZIP мұрағатын таңдау үшін **Шолу** түймесін басыңыз.

   ZIP мұрағатында утилита қалтасы болуы керек. Бұл қалта қашықтағы құрылғыда іске қосу үшін орындалатын файлды қамтиды.

   Қажет болса, орындалатын файлдың атауын және пәрмен жолы аргументтерін көрсетуге болады. Ол үшін **Қашықтағы құрылғыда жұмыс істейтін мұрағаттағы орындалатын файл** және **Пәрмен жолының аргументтері** өрістерін толтырыңыз.

4. Клиенттік құрылғыда көрсетілген қолданбаны іске қосу үшін **Жүктеп салу және іске қосу** түймесін басыңыз.

5. "Лаборатория Касперского" қолдау көрсету қызметі өкілінің нұсқауларын орындаңыз.

Қолданбадан алынған қоқыс файлын жасау

Қолданбадан алынған қоқыс файлы белгілі бір уақытта клиент құрылғысында жұмыс істейтін қолданбаның параметрлерін көруге мүмкіндік береді. Бұл файлда қолданба үшін жүктелген модульдер туралы ақпарат та бар.

Қоқыс файлын жасау Windows негізіндегі клиент құрылғыларында жұмыс істейтін 32 разрядтық процестер үшін ғана қолжетімді. Бұл функцияға Linux арқылы басқарылатын клиенттік құрылғылар мен 64 биттік процестерде қолдау көрсетілмейді.

Қолданбаға арналған қоқыс файлын жасау үшін:

1. Клиент құрылғысын қашықтан диагностикалау утилитасын ашыңыз.

2. Қашықтан диагностикалау терезесінде **Қашықтан жұмыс істейтін бағдарламаны іске қосу** бөлімін таңдаңыз.

3. **Процестің дамп файлын жасау** бөлімінде қоқыс жасағыңыз келетін қолданбаның орындалатын файлын көрсетіңіз.

4. Көрсетілген қолданбаның қоқыс файлын сақтау үшін **Жүктеп алу** түймесін басыңыз.

   Көрсетілген қолданба клиент құрылғысында іске қосылмаса, қате туралы хабар көрсетіледі.

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 "Лаборатория Касперского" бағдарламасының collect.sh скриптісін пайдаланып, Linux операциялық жүйесімен жұмыс істейтін құрылғы туралы диагностикалық ақпаратты алуға болады. Бұл скрипт Linux операциялық жүйесі бар диагностикалануы қажет клиенттік құрылғыда іске қосылады. Содан кейін, диагностикалық ақпарат, сол құрылғы туралы жүйелік ақпарат, қолданбаны трассалау файлдары, құрылғының оқиғалар туралы журналдары және қате жағдайларға, үзілген қолданбаларға арналған қоқыс файлы бар файл жасалады.

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 "Лаборатория Касперского" 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 үшінші тарап қолданбаларын басқару

Бұл бөлімде клиент құрылғыларындағы үшінші тарап қолданбаларын басқарумен байланысты Kaspersky Security Center Linux мүмкіндіктері сипатталған.

Үшінші тарап қолданбалары туралы

Kaspersky Security Center Linux сізге клиент құрылғыларында орнатылған үшінші тарап қолданбаларын жаңартуға және үшінші тарап қолданбаларының осалдықтарын түзетуге көмектеседі. Kaspersky Security Center Linux үшінші тарап қолданбаларын тек ағымдағы нұсқадан соңғы нұсқаға дейін жаңарта алады. Келесі тізімде Kaspersky Security Center Linux көмегімен жаңартуға болатын үшінші тарап қолданбалары бар:

Үшінші тарап қолданбаларының тізімі жаңа қолданбалар арқылы жаңартылуы және ұлғаюы мүмкін. Сіз Kaspersky Security Center Web Console веб-консолінде қолжетімді жаңартулар тізімін қарап шығып, үшінші тарап қолданбасын (пайдаланушылардың құрылғыларында орнатылған) Kaspersky Security Center Linux көмегімен жаңарта алатыныңызды тексере аласыз.

- 7-Zip Developers: 7-Zip.
- Adobe Systems:
  - Adobe Acrobat DC;
  - Adobe Acrobat Reader DC;
  - Adobe Acrobat;
  - Adobe Reader;
  - Adobe Shockwave Player.
- AIMPDevTeam: AIMP.
- ALTAP: Altap Salamander.
- Apache Software Foundation: Apache Tomcat.
- Apple:
  - Apple iTunes;
  - Apple QuickTime.
- Armory Technologies, Inc.: Armory.
- Cerulean Studios: Trillian Basic.
- Ciphrex Corporation: mSIGNA
- Cisco: Cisco Jabber.
- Code Sector:

- Codec Guide:
  - K-Lite Codec Pack Basic;
  - K-Lite Codec Pack Full;
  - K-Lite Codec Pack Mega;
  - K-Lite Codec Pack Standard.
- DbVis Software AB:
- Decho Corp.:
  - Mozy Enterprise;
  - Mozy Home;
  - Mozy Pro.
- Dominik Reichl: KeePass Password Safe.
- Don HO don.h@free.fr: Notepad++.
- DoubleGIS: 2GIS.
- Dropbox, Inc.: Dropbox.
- EaseUs: EaseUS Todo Backup Free.
- Electrum Technologies GmbH:
- Enter Srl: Iperius Backup.
- Eric Lawrence:
- EverNote: EverNote.
- Exodus Movement Inc: Exodus.
- EZB Systems:
- Famatech:
  - Radmin;
  - Remote Administrator.
- Far Manager: FAR Manager.
- FastStone Soft: FastStone Image Viewer.
- FileZilla Project:
- Firebird Developers:

- Foxit Corporation:
  - Foxit Reader;
  - Foxit Reader Enterprise.
- Free Download Manager.ORG: Free Download Manager.
- GIMP project:
- GlavSoft LLC.: TightVNC.
- GNU Project: Gpg4win.
- Google:
  - Google Earth;
  - Google Chrome;
  - Google Chrome Enterprise;
  - Google Earth Pro.
- Inkscape Project:
- IrfanView: IrfanView.
- iterate GmbH:
- Logitech: SetPoint.
- LogMeIn, Inc.:
  - LogMeIn;
  - Hamachi;
  - LogMeIn Rescue Technician Console.
- Martin Prikryl:
- Mozilla Foundation:
  - Mozilla Firefox;
  - Mozilla Firefox ESR;
  - Mozilla SeaMonkey;
  - Mozilla Thunderbird.
- New Cloud Technologies Ltd: Home Edition.
- OpenOffice.org: OpenOffice.

- Opera Software: Opera.
- Oracle Corporation:
  - Oracle Java JRE;
  - Oracle VirtualBox.
- PDF44: PDF24 MSI/EXE.
- Piriform:
  - CCleaner;
  - Defraggler;
  - Recuva;
  - Speccy.
- Postgresql: PostgreSQL.
- RealPlayer Cloud.
- RealVNC:
  - RealVNC Server;
  - RealVNC Viewer.
- Right Hemisphere Inc.: SAP Visual Enterprise Viewer (Complete/Minimum).
- Simon Tatham:
- Skype Technologies: Skype for Windows.
- Sober Lemur S.a.s.:
  - PDFsam Basic;
  - PDFsam Visual.
- Softland: FBackup.
- Splashtop Inc.: Splashtop Streamer.
- Stefan Haglund, Fredrik Haglund, Florian Schmitz: CDBurnerXP.
- Sublime HQ Pty Ltd: Sublime Text.
- TeamViewer GmbH:
  - TeamViewer Host;
  - TeamViewer.

- Telegram Messenger LLP: Telegram Desktop.
- The Document Foundation:
  - LibreOffice;
  - LibreOffice HelpPack.
- The Git Development Community:
  - Git for Windows;
  - Git LFS.
- The Pidgin developer community:
- TortoiseSVN Developers:
- VLC media player.
- VMware:
  - VMware Player;
  - VMware Workstation.
- WinRAR Developers: WinRAR.
- WinZip: WinZip.
- Wireshark Foundation: Wireshark.
- Wrike: Wrike.
- Zimbra: Zimbra Desktop.

Сценарий: қолданбаларды басқару

Сіз пайдаланушы құрылғыларында қолданбаларды іске қосуды басқара аласыз. Сіз басқарылатын құрылғыларда қолданбаларды іске қосуға рұқсат бере аласыз немесе тыйым сала аласыз. Бұл функционалдылық Қолданбаны басқару құрамдасы арқылы іске асырылады. Сіз Windows немесе Linux басқаратын құрылғыларға орнатылған қолданбаларды басқара аласыз.

Linux операциялық жүйелері үшін Қолданбаны 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.

Кезеңдер

Қолданбаны басқару құрамдасын қолдану сценарийі келесі кезеңдерден тұрады:

1. **Клиент құрылғыларында қолданбалар тізімін құрастыру және қарау**

   Бұл кезең сізге басқарылатын құрылғыларға қандай қолданбалардың орнатылғанын анықтауға көмектеседі. Сіз қолданбалар тізімін қарап, ұйымыңыздың қауіпсіздік саясаттарына сәйкес қолданбалардың қайсысына рұқсат бергіңіз келетінін, қайсысына тыйым салғыңыз келетінін шеше аласыз. Шектеулер ұйымдағы ақпараттық қауіпсіздік саясаттарымен байланысты болуы мүмкін. Басқарылатын құрылғыларда қандай қолданбалардың орнатылғанын нақты білсеңіз, бұл кезеңді өткізіп жіберсеңіз болады.

   Нұсқаулар: Клиент құрылғыларында орнатылған қолданбалар тізімін алу және қарау.

2. **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. Басқарылатын құрылғыларда қандай орындалатын файлдардың орнатылғанын нақты білсеңіз, бұл кезеңді өткізіп жіберсеңіз болады.

   Нұсқаулар: Клиент құрылғыларында сақталған орындалатын файлдардың тізімін алу және қарау.

3. **Ұйымыңызда қолданылатын қолданбалар үшін қолданба санаттарын құру**

   Басқарылатын құрылғыларда сақталған қолданбалар мен орындалатын файлдардың тізімдерін талдаңыз. Талдау негізінде қолданба санаттарын жасаңыз. Ұйымыңызда қолданылатын қолданбалардың стандартты жиынтығын қамтитын "Жұмыс қолданбалары" санатын құру ұсынылады. Егер әртүрлі қауіпсіздік топтары өз жұмысында әртүрлі қолданбалар жиынтығын қолданса, әр қауіпсіздік тобы үшін әртүрлі қолданбалар санатын құруға болады.

   Қолданба санатын құру критерийлерінің жиынтығына байланысты сіз екі типті қолданба санаттарын жасай аласыз.

   Нұсқаулар: қолмен толықтырылатын қолданбалар санатын жасау, Таңдалған құрылғылардан орындалатын файлдарды қамтитын қолданбалар санатын жасау.

4. **Kaspersky Endpoint Security саясатындағы Қолданбаларды басқару құрамдасын конфигурациялау**

   Алдыңғы кезеңде жасаған қолданбалардың санаттарын қолдана отырып, Kaspersky Endpoint Security for Linux саясатындағы Қолданбаларды басқару құрамдасын конфигурациялаңыз.

   Нұсқаулар: Kaspersky Endpoint Security for Windows саясатындағы Қолданбаларды басқару құрамдасын конфигурациялау

5. **Тест режимінде Қолданбаларды басқару құрамдасын қосу**

   Қолданбаларды басқару ережелері пайдаланушылардың жұмысына қажетті қолданбаларды бұғаттамауы үшін, Қолданбаларды бақылау ережелерін тестілеуді қосып, ережелер жасалғаннан кейін олардың жұмысын талдау ұсынылады. Тестілеу қосылған кезде, Kaspersky Endpoint Security for Windows Қолданбаларды басқару ережелерімен іске қосуға тыйым салынған қолданбаларды бұғаттамайды, оның орнына оларды іске қосу туралы хабарландыруларды Басқару серверіне жібереді.

   Қолданбаларды бақылау ережелерін тестілеу кезінде келесі әрекеттерді орындау ұсынылады:

   - Тестілеу кезеңін анықтаңыз. Тестілеу кезеңі бірнеше күннен екі айға дейін өзгеруі мүмкін.
   - Қолданбаны басқару құрамдасының жұмысын тексеру нәтижесінде пайда болатын оқиғаларды зерттеңіз.

Kaspersky Security Center Web Console үшін нұсқаулар: Kaspersky Endpoint Security for Windows саясатында Қолданбаны басқару құрамдасын конфигурациялау. Осы нұсқаулықты орындаңыз және орнату процесінде **Сынақ режимі** опциясын қосыңыз.

6. **Қолданбаны басқару құрамдасының қолданбалар санаты параметрлерін өзгерту**

   Қажет болса, Қолданбаларды басқару құрамдасының параметрлерін өзгертіңіз. Тестілеу нәтижелеріне сүйене отырып, Қолданбаларды басқару құрамдасының оқиғаларына байланысты орындалатын файлдарды қолмен толықтырылатын қолданбалар санатына қосуға болады.

   Нұсқаулар: Kaspersky Security Center Web Console: Қолданба санатына оқиғамен байланысты орындалатын файлдарды қосу.

7. **Жұмыс режимінде Қолданбаларды бақылау ережелерін қолдану**

   Қолданбаларды бақылау ережелерін тексергеннен кейін және қолданба санаттарын конфигурациялауды аяқтағаннан кейін, сіз жұмыс режимінде Қолданбаларды басқару ережелерін қолдана аласыз.

   Kaspersky Security Center Web Console үшін нұсқаулар: Kaspersky Endpoint Security for Windows саясатында Қолданбаны басқару құрамдасын конфигурациялау. Осы нұсқаулықты орындап, конфигурациялау барысында **Сынақ режимі** параметрін өшіріңіз.

8. **Қолданбаны басқару конфигурациясын тексеру**

   Келесіні орындағаныңызға көз жеткізіңіз:

   - Қолданба санаттарын жасадыңыз.
   - Қолданбалар санаттарын қолдана отырып, Қолданба санаттарын конфигурацияладыңыз.
   - Жұмыс режимінде Қолданбаларды бақылау ережелерін қолдандыңыз.

Нәтижелер

Сценарий аяқталғаннан кейін, басқарылатын құрылғыларда қолданбалардың іске қосылуы бақыланады. Пайдаланушылар сіздің ұйымыңызда рұқсат етілген қолданбаларды ғана басқара алады және сіздің ұйымыңызда тыйым салынған қолданбаларды іске қоса алмайды.

Қолданбаларды бақылау құрамдас бөлігінің толық сипаттамасын Kaspersky Endpoint Security for Linux және Kaspersky Endpoint Security for Windows қолданбасының анықтамасынан қараңыз.

Қолданбаларды бақылау туралы

Қолданбаны басқару құрамдасы пайдаланушылардың қолданбаларды іске қосу әрекеттерін бақылайды және Қолданбаны басқару ережелері арқылы қолданбалардың іске қосылуын реттейді.

Қолданбаларды бақылау құрамдас бөлігі Linux және одан жоғары нұсқаларға арналған Kaspersky Endpoint Security 11.2 қолданбасының нұсқасы үшін қолжетімді.

Қолданбаны басқару ережесінің ешқайсысына сәйкес келмейтін параметрлері бар қолданбаларды іске қосу, келесі құрамдастың таңдалған жұмыс режимі тарапынан реттеледі:

- *Тыйым салу тізімі.* Егер сіз тыйым салу ережелерінде көрсетілген қолданбалардан басқа барлық қолданбалардың іске қосылуына рұқсат бергіңіз келсе, режим қолданылады. Әдепкі бойынша осы режим таңдалған.

- *Рұқсат ету тізімі*. Егер сіз рұқсат ету ережелерінде көрсетілген қолданбалардан басқа барлық қолданбалардың іске қосылуын бұғаттағыңыз келсе, режим қолданылады.

Қолданбаны басқару ережесі қолданбалардың санаттары арқылы жүзеге асырылады. Сіз белгілі бір өлшемшарттары бар қолданба санаттарын жасайсыз. Kaspersky Security Center Linux қолданбасында қолданба 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.

Қолданбаларды бақылау құрамдас бөлігінің толық сипаттамасын Kaspersky Endpoint Security for Linux және Kaspersky Endpoint Security for Windows қолданбасының анықтамасынан қараңыз.

Клиент құрылғыларында орнатылған қолданбалар 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 қолданбалар тізімін құрастырып, тізімді Басқару серверіне жібереді. Желілік агентке қолданбалар тізімін жаңарту үшін шамамен 10-15 минут кетеді.

Windows операциялық жүйесі бар клиент құрылғылары үшін Желілік агент орнатылған қолданбалар туралы ақпараттың көп бөлігін Windows тізімдемесінен алады. Linux операциялық жүйесі бар клиент құрылғылары үшін орнатылған қолданбалар туралы ақпаратты Желілік агент пакет диспетчерлерінен алады.

Басқарылатын құрылғыларда орнатылған қолданбалар тізімін көру үшін,

1. Қолданбаның негізгі терезесінде **Операциялар** → **Үшінші тарап бағдарламалары** → **Бағдарламалар тізімдемесі** бөліміне өтіңіз.

   Бетте басқарылатын құрылғыларда орнатылған қолданбалары бар кесте көрсетіледі. Сол қолданбаның қасиеттерін көру үшін қолданбаны таңдаңыз, мысалы: өндірушінің аты, нұсқа нөмірі, орындалатын файлдар тізімі, қолданба орнатылған құрылғылардың тізімі.

2. Орнатылған қолданбалары бар кесте деректерін келесідей топтастыруға және сүзуге болады:

   - Кестенің жоғарғы оң жақ бұрышындағы ( ) параметрлері белгішесін нұқыңыз.

     Ашылған **Бағандар параметрлері** мәзірінен кестеде көрсетілетін бағандарды таңдаңыз. Қолданба орнатылған клиент құрылғыларының операциялық жүйесінің түрін көру үшін **Операциялық жүйенің түрі** бағанын таңдаңыз.

   - Кестенің жоғарғы оң жақ бұрышындағы ( ) сүзу белгішесін нұқыңыз, ашылған мәзірде сүзу критерийін көрсетіңіз және қолданыңыз.

     Орнатылған қолданбалардың сүзілген кестесі көрсетіледі.

Таңдалған басқарылатын құрылғыда орнатылған қолданбалар тізімін көру үшін,

Қолданбаның негізгі терезесінде **Құрылғылар → Басқарылатын құрылғылар → <құрылғы атауы> → Кеңейтілген → Бағдарламалар тізімдемесі** бөліміне өтіңіз. Бұл мәзірде қолданбалар тізімін CSV немесе TXT пішіміндегі файлдарға экспорттауға болады.

Қолданбаларды бақылау құрамдас бөлігінің толық сипаттамасын Kaspersky Endpoint Security for Linux және Kaspersky Endpoint Security for Windows қолданбасының анықтамасынан қараңыз.

Клиент құрылғыларында сақталған орындалатын файлдардың тізімін алу және қарау

Басқарылатын құрылғыларда сақталған орындалатын файлдардың тізімін алуға болады. Орындалатын файлдарды түгендеу үшін түгендеу тапсырмасын жасау қажет.

Орындалатын файлдарды түгендеу функциясы Kaspersky Endpoint Security for Linux 11.2 және одан да жоғары нұсқасы қолданбасы үшін қолжетімді.

Клиент құрылғыларында орындалатын файлдарды түгендеу тапсырмасын жасау үшін:

1. Негізгі қолданба терезесінде **Активтер (құрылғылар) → 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 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, қолданба MZ, COM, PE, NE, SYS, CMD, BAT, PS1, JS, VBS, REG, MSI, CPL, DLL, JAR пішіміндегі орындалатын файлдарды және HTML файлдарын анықтайды.

Клиент құрылғыларында сақталатын орындалатын файлдар тізімін көру үшін,

Қолданбаның негізгі терезесінде **Операциялар → Үшінші тарап бағдарламалары → Орындалатын файлдар** бөліміне өтіңіз.

Бетте клиент құрылғыларында сақталған орындалатын файлдардың тізімі көрсетіледі.

Қолмен толықтырылатын қолданбалар санатын жасау

Сіз өзіңіздің ұйымыңызда іске қосуға рұқсат бергіңіз немесе тыйым салғыңыз келетін орындалатын файлдарға арналған үлгі ретінде критерийлер жиынтығын көрсете аласыз. Өлшемшарттарға сәйкес орындалатын файлдардың негізінде, сіз қолданбалар санатын құра аласыз және оны Қолданбаны басқару құрамдасының конфигурациясында қолдана аласыз.

Қолмен толықтырылатын қолданбалар санатын жасау үшін:

1. Қолданбаның негізгі терезесінде **Операциялар** → **Үшінші тарап бағдарламалары** → **Бағдарлама санаттары** бөліміне өтіңіз.

   Қолданба 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 тізімдегі санатты жасау үшін ереже түрін таңдаңыз:

   - KL санатынан

     Осы нұсқа таңдалған болса, қолданбаларды пайдаланушы санатына қосу шарты ретінде "Лаборатория Касперского" қолданбалары санатын қосуға болады. Көрсетілген KL санатына кіретін қолданбалар қолданбалардың пайдаланушы санатына қосылатын болады.

   - Репозиторийден сертификатты таңдау

     Осы нұсқа таңдалған болса, қоймадағы сертификаттарды көрсетуге болады. Көрсетілген сертификаттарға сай қол қойылған орындалатын файлдар пайдаланушы санатына қосылады.

   - Қолданба жолын көрсету (қолдау көрсетілетін маскалар)

     Осы нұсқа таңдалған болса, орындалатын файлдары қолданбалардың пайдаланушы санаттарына қосылатын клиент құрылғысындағы қалтаны көрсетуге болады.

   - Алынбалы жетек

     Осы нұсқа таңдалған болса, қолданба іске қосылатын тасушының түрін (кез келген немесе алынбалы диск) көрсетуге болады. Таңдалған типтегі тасушыда іске қосылатын қолданбалар қолданбалардың пайдаланушы санатына қосылады.

- **Хэш, метадеректер немесе сертификат**:
  - **Орындалатын файлдар тізімінен таңдау**

    Осы нұсқа таңдалған болса, санатқа қосылатын қолданбаларды клиент құрылғысындағы орындалатын файлдар тізімінен таңдауға болады.

  - **Бағдарламалар тізімдемесінен таңдау**

    Егер бұл параметр таңдалса, қолданбалар тізімдемесі көрсетіледі. Қолданбаларды тізімдемеден таңдап, келесі файл метадеректерін көрсетуге болады:

    - Файл атауы.
    - Файл нұсқасы. Сіз нұсқаның нақты мәнін көрсете аласыз немесе "5.0-ден артық" сияқты шарт жаза аласыз.
    - Қолданба атауы.
    - Қолданба нұсқасы. Сіз нұсқаның нақты мәнін көрсете аласыз немесе "5.0-ден артық" сияқты шарт жаза аласыз.
    - Өндіруші.

  - **Қолмен көрсету**

    Егер бұл нұсқа таңдалса, қолданбаларды пайдаланушы санатына қосу шарты ретінде файл хэшін, метадеректерді немесе сертификатты көрсету қажет.

    Файл хэші

    Желіңіздегі құрылғыларға орнатылған қауіпсіздік қолданбасы нұсқасына байланысты, санат файлдары үшін хеш функциясын Kaspersky Security Center Linux қолданбасы тарапынан есептеп шығару алгоритмін таңдау керек. Есептеп шығарылған хеш функциялары туралы ақпарат Басқару серверінің дерекқорында сақталады. Хеш функцияларын сақтау арқасында дерекқордың өлшемі шамалы ұлғаяды.

    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 қолданбасы тарапынан хеш функциясын есептеп шығару нұсқаларының бірін таңдаңыз:

    - Егер желіңізде орнатылған қауіпсіздік қолданбаларының барлық үлгілері Linux үшін Kaspersky Endpoint Security 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. Метадеректер Басқару серверіне жіберілетін болады. Осындай метадеректері бар орындалатын файлдар қолданбалар санатына қосылады.

    Сертификат

    Осы нұсқа таңдалған болса, қоймадағы сертификаттарды көрсетуге болады. Көрсетілген сертификаттарға сай қол қойылған орындалатын файлдар пайдаланушы санатына қосылады.

- **Мұрағат қалтасынан**

  Бұл параметр таңдалған болса, мұрағат қалтасында файлды көрсетуге және пайдаланушы санатына қолданбаларды 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 қолданбалар қолданбалардың 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 қолданбалардың 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.

Бұл параметр таңдалған болса, мұрағат қалтасында файлды көрсетуге және пайдаланушы санатына қолданбаларды 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 қолданбалар қолданбалардың 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 қолданбалардың 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.

Таңдалған критерий шарттар тізіміне қосылды.

Қолданба санатын жасау үшін қанша критерий қосуға болады.

6. **Ерекшеліктер** қадамында, ерекшеліктер аймағына критерий қосу және файлдарды жасалып жатқан санаттан шығару үшін **Қосу** түймесін басыңыз.

7. **Жағдай шарттары** қадамында, санатты жасау үшін ереже түрін таңдағаныңыздай, тізімнен ереже түрін таңдаңыз.

Шебер аяқталғаннан кейін, қолданбалар санаты құрылады. Ол қолданба санаттарының тізімінде пайда болады. Қолданбаны басқару құрамдасын конфигурациялау кезінде қолданбалар санатын жасауға болады.

Қолданбаларды бақылау құрамдас бөлігінің толық сипаттамасын Kaspersky Endpoint Security for Linux және Kaspersky Endpoint Security for Windows қолданбасының анықтамасынан қараңыз.

Таңдалған құрылғылардан орындалатын файлдарды қамтитын қолданбалар 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 қолданбалар санатын құра аласыз және оны Қолданбаны басқару құрамдасын конфигурациялау үшін пайдалана аласыз.

Таңдалған құрылғылардан орындалатын файлдарды қамтитын қолданбалар санатын құру үшін:

1. Қолданбаның негізгі терезесінде **Операциялар** → **Үшінші тарап бағдарламалары** → **Бағдарлама санаттары** бөліміне өтіңіз.

   Қолданба 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 көрсетіп, **Таңдалған құрылғылардағы орындалатын файлдарды қамтитын санат. Осы орындалатын файлдар автоматты түрде өңделеді және метрикалары санатқа қосылады**.

4. **Қосу** түймесін басыңыз.

5. Ашылған терезеде қолданбалар санатын құру үшін орындалатын файлдары пайдаланылатын құрылғыны немесе құрылғыларды таңдаңыз.

6. Келесі параметрлерді белгілеңіз:

   - **Хеш функциясын есептеп шығару алгоритмі**

Желіңіздегі құрылғыларға орнатылған қауіпсіздік қолданбасы нұсқасына байланысты, санат файлдары үшін хеш функциясын Kaspersky Security Center Linux қолданбасы тарапынан есептеп шығару алгоритмін таңдау керек. Есептеп шығарылған хеш функциялары туралы ақпарат Басқару серверінің дерекқорында сақталады. Хеш функцияларын сақтау арқасында дерекқордың өлшемі шамалы ұлғаяды.

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 қолданбасы тарапынан хеш функциясын есептеп шығару нұсқаларының бірін таңдаңыз:

- Егер желіңізде орнатылған қауіпсіздік қолданбаларының барлық үлгілері Linux үшін Kaspersky Endpoint Security 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 қолданбалар 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 қолданба санаттарынан тыс файлдар ескеріледі.

- **Қалталар**

  Бұл бөлімде қолданбалар 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 қажет.

Шебер аяқталғаннан кейін, қолданбалар санаты құрылады. Ол қолданба санаттарының тізімінде пайда болады. Қолданбаны басқару құрамдасын конфигурациялау кезінде қолданбалар санатын жасауға болады.

Таңдалған қалталардан орындалатын файлдарды қамтитын қолданбалар 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 қолданбалар санатын құра аласыз және оны Қолданбаны басқару құрамдасын конфигурациялау үшін пайдалана аласыз.

Таңдалған қалталардан орындалатын файлдарды қамтитын қолданбалар санатын құру үшін:

1. Қолданбаның негізгі терезесінде **Операциялар → Үшінші тарап бағдарламалары → Бағдарлама санаттары** бөліміне өтіңіз.

   Қолданба 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 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 қолданбалар санатын құру үшін пайдаланылатын қалтаны көрсетіңіз.

5. Келесі параметрлерді конфигурациялаңыз:

   - Санатқа динамикалық түрде қосылатын кітапханаларды (DLL) қосу

     Қолданбалар санатына динамикалық түрде қосылатын кітапханалар (DLL пішіміндегі файлдар) қосылады және Қолданбаны басқару құрамдасы жүйеде іске қосылған осындай кітапханалардың әрекеттерін тіркейді. DLL пішіміндегі файлдарды санатқа қосу кезінде Kaspersky Security Center жұмысының өнімділігі төмендеуі мүмкін.

     Әдепкі бойынша, жалауша алынып тасталған.

   - Санатқа скрипт туралы деректерді қосу

     Қолданба санатына скрипт туралы деректер қосылады және скрипттер Веб-қауіптен қорғаныс құрамдасы тарапынан бұғатталмайды. Скрипт туралы деректерді санатқа қосу кезінде Kaspersky Security Center 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 қолданбасы нұсқасына байланысты, санат файлдары үшін хеш функциясын Kaspersky Security Center Linux қолданбасы тарапынан есептеп шығару алгоритмін таңдау керек. Есептеп шығарылған хеш функциялары туралы ақпарат Басқару серверінің дерекқорында сақталады. Хеш функцияларын сақтау арқасында дерекқордың өлшемі шамалы ұлғаяды.

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 қолданбасы тарапынан хеш функциясын есептеп шығару нұсқаларының бірін таңдаңыз:

- Егер желіңізде орнатылған қауіпсіздік қолданбаларының барлық үлгілері Linux үшін Kaspersky Endpoint Security 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, қолданба 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.

Шебер аяқталғаннан кейін, қолданбалар санаты құрылады. Ол қолданба санаттарының тізімінде пайда болады. Қолданбаны басқару құрамдасын конфигурациялау үшін қолданбалар санатын пайдалануға болады.

Қолданбаларды бақылау құрамдас бөлігінің толық сипаттамасын Kaspersky Endpoint Security for Linux және Kaspersky Endpoint Security for Windows қолданбасының анықтамасынан қараңыз.

Қолданба санаттары тізімін қарап шығу

Сіз конфигурацияланған қолданба санаттарының тізімін және әр қолданба санатының параметрлерін көре аласыз.

Қолданба санаттары тізімін көру үшін,

Қолданбаның негізгі терезесінде **Операциялар → Үшінші тарап бағдарламалары → Бағдарлама санаттары** бөліміне өтіңіз.

Қолданба санаттары тізімі бар бет ашылады.

Қолданба санаты сипаттарын көру үшін,

қолданба санатының атауын басыңыз.

Таңдалған қолданбалар санатының сипаттар терезесі ашылады. Параметрлер бірнеше қойындыда топтастырылған.

Kaspersky Endpoint Security for Windows саясатындағы Қолданбаларды бақылау құрамдасын конфигурациялау

Қолданбаны басқаруға арналған санаттарды жасағаннан кейін, оларды Kaspersky Endpoint Security for Windows саясатындағы Қолданбаны басқаруды конфигурациялау үшін пайдалануға болады.

Kaspersky Endpoint Security for Windows саясатындағы Қолданбаны басқару құрамдасын конфигурациялау үшін:

1. Қолданбаның негізгі терезесінде **Активтер (құрылғылар)** → **Саясат және профильдер** бөліміне өтіңіз.

   Саясаттар тізімі бар бет көрсетіледі.

2. **Kaspersky Endpoint Security for Windows** саясатын басыңыз.

   Саясат сипаттары терезесі ашылады.

3. **Бағдарлама параметрлері** → **Қауіпсіздікті бақылау** → **Қолданбаны басқару** бөліміне өтіңіз.

   Қолданбаны басқару құрамдасының параметрлері бар **Қолданбаны басқару** терезесі ашылады.

4. **Қолданбаны басқару** параметрі әдепкі бойынша қосулы. Параметрді өшіру үшін **Қолданбаны басқару [Өшірулі]** қосқышын өшіріңіз.

5. **Қолданбаны басқару параметрлері** блогында Қолданбаны басқару ережелерін қолдана отырып жұмыс режимін қосыңыз және Kaspersky Endpoint Security for Windows қолданбасына қолданбаларын іске қосуды бұғаттауға мүмкіндік беріңіз.

   Қолданбаны басқару ережесін сынап көргіңіз келсе, **Қолданбаны басқару параметрлері** бөлімінде сынақ режимін қосыңыз. Сынақ режимінде Kaspersky Endpoint Security for Windows қолданбасы қолданбалардың іске қосылуын бұғаттамайды, бірақ есепте іске қосылған ережелер туралы ақпаратты жазып алады. Осы ақпаратты қарау үшін **Есепті қарап шығу** сілтемесінен өтіңіз.

6. Пайдаланушылар қолданбаларды іске қосқан кезде Kaspersky Endpoint Security for Windows қолданбасы DLL модульдерін жүктеуді бақылағанын қаласаңыз, **DLL модульдерін жүктеуді басқару** параметрін қосыңыз.

   Модуль туралы ақпарат және модульді жүктеген қолданба 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 қолданбасы барлық DLL модульдері мен драйверлерін, соның ішінде Kaspersky Endpoint Security for Windows іске қосылғанға дейін жүктелгендерді басқарғанын қаласаңыз, **DLL модульдерін жүктеуді басқару** параметрін таңдағаннан кейін құрылғыны қайта іске қосыңыз.

7. (Қажет болса.) **Хабар үлгілері** блогында, қолданба іске қосу үшін бұғатталған кезде көрсетілетін хабар үлгісін және сізге жіберілетін электрондық пошта хабары үлгісін өзгертіңіз.

8. **Қолданбаны 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.

   Қолданба 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.

    Қолданбаны басқару ережесі терезесі ашылады.

11. **Өтініш, санатты таңдаңыз** сілтемесінен өтіңіз.

    Қолданба санаттары терезесі ашылады.

12. Бұрын жасаған қолданбалар 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. Қолданба санаттарының тізімін жасау аяқталғаннан кейін **OK** түймесін басыңыз.

    Қолданба санаттары терезесі жабылады.

14. **Қолданбаны басқару** ережесі терезесінде, **Субъектілер және олардың құқықтары** бөлімінде Қолданбаны басқару ережелерін қолдану үшін пайдаланушылар мен пайдаланушылар топтарының тізімін жасаңыз.

15. Параметрлерді сақтау және **Қолданбаны 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 **Қолданбаны басқару** ережесі терезесін жабу үшін **OK** түймесін басыңыз.

18. Kaspersky Endpoint Security for Windows саясаты параметрлері терезесін жабыңыз.

Қолданбаны басқару құрамдасы конфигурацияланған. Саясатты клиент құрылғыларына таратқаннан кейін, орындалатын файлдардың іске қосылуы бақыланады.

Қолданбаларды бақылау құрамдас бөлігінің толық сипаттамасын Kaspersky Endpoint Security for Linux және Kaspersky Endpoint Security for Windows қолданбасының анықтамасынан қараңыз.

Қолданба санатына оқиғамен байланысты орындалатын файлдарды қосу

Қолданбаны басқару құрамдасы конфигурацияланғаннан кейін, Kaspersky Endpoint Security саясаттарында, оқиғалар тізімінде келесі оқиғалар көрсетілуі мүмкін:

- **Қолданбаны іске қосуға тыйым салынған** (*Критикалық* оқиға). Егер сіз ережелерді қолдану үшін Қолданбаны басқаруды конфигурациялаған болсаңыз, бұл оқиға көрсетіледі.
- **Қолданбаны іске қосуға сынақ режиміне тыйым салынған** (*Ақпараттық* оқиға). Егер сіз сынақ режимінде ережелерді қолдану үшін Қолданбаны басқаруды конфигурациялаған болсаңыз, бұл оқиға көрсетіледі.

- **Әкімшіге қолданбаның іске қосылуына тыйым салынғаны туралы хабар** (*Ескерту* маңыздылық деңгейі бар хабар). Егер сіз ережелерді қолдану үшін Қолданбаны басқаруды конфигурациялаған болсаңыз, ал пайдаланушы іске қосу үшін бұғатталған қолданбаға қатынасуды сұраса, бұл оқиға көрсетіледі.

Қолданбаны басқару құрамдасына қатысты оқиғаларды көру үшін оқиғалар таңдауын жасау ұсынылады.

Қолданбаны басқару оқиғаларына қатысты орындалатын файлдарды қолданыстағы қолданбалар санатына немесе жаңа қолданбалар санатына қосуға болады. Орындалатын файлдарды тек қолмен толтырылатын қолданбалар санатына қосуға болады.

Қолданбаны басқару құрамдасының оқиғаларымен байланысты орындалатын файлдарды қолданбалар санатына қосу үшін:

1. Қолданбаның негізгі терезесінде **Бақылау және есеп беру** → **Оқиғаларды таңдау** бөліміне өтіңіз.

   Оқиғалар таңдауы тізімі көрсетіледі.

2. Қолданбаны басқаруға қатысты оқиғаларды көру үшін оқиғалар таңдауын таңдап, сол оқиғалар таңдауын құруды іске қосыңыз.

   Қолданбаны басқарумен байланысты оқиғалар таңдауын жасамаған болсаңыз, **Соңғы оқиғалар** сияқты алдын ала анықталған таңдауды таңдап, іске қосуға болады.

   Оқиғалар тізімі көрсетіледі.

3. Қолданбалар 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 қолданбалар 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 қолданбалар 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 қолданбалар санатын таңдаңыз.

   - **Ереже түрі** бөлімінде келесі параметрлерді 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 қолданбаның әртүрлі нұсқаларына бір сертификатпен қол қоюға болады немесе бір өндірушінің бірнеше түрлі қолданбаларына бір сертификатпен қол қоюға болады. Сертификатты таңдаған кезде санатқа қолданбаның бірнеше нұсқасы немесе бір өндірушінің бірнеше қолданбасы кіруі мүмкін.

  Әрбір файлдың өзіндік бірегей SHA256 хэш функциясы бар. SHA256 хэш функциясын таңдағанда, санатқа қолданбаның 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 қолданбаның әртүрлі нұсқаларына бір сертификатпен қол қоюға болады немесе бір өндірушінің бірнеше түрлі қолданбаларына бір сертификатпен қол қоюға болады. Сертификатты таңдаған кезде санатқа қолданбаның бірнеше нұсқасы немесе бір өндірушінің бірнеше қолданбасы 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 қолданбаның 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 қолданбаның белгіленген нұсқасы сияқты бір ғана тиісті файл кіреді.

5. **ОК** түймесін басыңыз.

Шебердің жұмысы аяқталғаннан кейін, Қолданбаны басқару оқиғаларымен байланысты орындалатын файлдар қолданыстағы қолданбалар санатына немесе жаңа қолданбалар санатына қосылады. Сіз өзгерткен немесе жасаған қолданбалар санатының параметрлерін көре аласыз.

Қолданбаларды бақылау құрамдас бөлігінің толық сипаттамасын Kaspersky Endpoint Security for Linux және Kaspersky Endpoint Security for Windows қолданбасының анықтамасынан қараңыз.

Үшінші тарап қолданбаларының жаңартуларын орнату

Бұл бөлімде клиент құрылғыларында орнатылған үшінші тарап қолданбаларына жаңартуларды орнатуға қатысты Kaspersky Security Center Linux мүмкіндіктері сипатталған.

Үшінші тарап қолданбаларының жаңартулары туралы

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 қолданбаларын жаңарту кезінде немесе басқарылатын құрылғыдағы үшінші тарап қолданбаларында осалдықтарды түзету кезінде қажет болуы мүмкін. Мысалы, пайдаланушыдан үшінші тарап қолданбасын жабу сұралуы мүмкін.

Қауіпсіздік мақсатында, Осалдықтар мен патчтарды басқару арқылы орнатқан кез келген үшінші тарап қолданбасы жаңартулары "Лаборатория Касперского" 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.

"Лаборатория Касперского" мамандары Осалдықтар мен патчтарды басқару арқылы орнатуға болатын үшінші тарап қолданбасы жаңартуларын қолмен талдамайды. Сонымен қатар "Лаборатория Касперского" 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 өндірушілердің қолданбаларын 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 қажетті үшінші тарап қолданбасының 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 18:00:00-де қолмен іске қосылады.

Қажетті жаңартуларды орнату және осалдықтарды түзету тапсырмасын жасаған болсаңыз, оны *Осалдықтарды және қажетті жаңартуларды іздеу* тапсырмасымен бірдей жиілікте немесе жиірек жұмыс істейтіндей етіп орнатуға болады.

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 Осалдықтар мен патчтарды басқару лицензиясы болса ғана жасауға болады. Бұл тапсырманы үшінші тарап қолданбалары үшін жаңартуларды орнату үшін пайдалануға болады.

Пайдаланушының араласуы үшінші тарап қолданбаларын жаңарту кезінде немесе басқарылатын құрылғыдағы үшінші тарап қолданбаларында осалдықтарды түзету кезінде қажет болуы мүмкін. Мысалы, пайдаланушыдан үшінші тарап қолданбасын 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 қолданбаларының жаңартуларын орнату

Үшінші тарап қолданбаларының жаңартуларын орнату үшін:

1. Жаңартулар тізімін келесі тәсілдердің бірімен ашыңыз:

   - **Операциялар → Патчтарды басқару → Бағдарламалық жасақтама жаңартулары**.
   - **Активтер (құрылғылар) → Басқарылатын құрылғылар →** <device name> **→ Кеңейтілген → Қолжетімді жаңартулар**.
   - **Операциялар → 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 басқару лицензиясы болса, *Қажетті жаңартуларды орнату және осалдықтарды түзету* тапсырма түрі әдепкі бойынша таңдалады. Тапсырма жасауды аяқтау үшін шебердің алдағы нұсқауларын орындаңыз.

   - **Жаңартуды орнату (көрсетілген тапсырмаға ереже қосу)**

     Таңдалған жаңартуларды қосқыңыз келетін тапсырманы таңдаңыз. Жүйе әкімшілігі лицензиясы 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. Өзгерістерді сақтау үшін **Сақтау** түймесін басыңыз.

Тапсырма жасауды таңдаған болсаңыз, ол тапсырмалар тізімінде, **Активтер (құрылғылар)** → **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 қолданбаларының жаңартуларын орнату

Осалдықтар мен патчтарды басқару үшін лицензия болған кезде, жаңартуды орнату шебері қолжетімді болады.

Жаңартуды орнату шеберін пайдаланып, үшінші тарап қолданбалары жаңартуларын орнату тапсырмасын жасау үшін:

1. Қолданбаның негізгі терезесінде **Операциялар** → **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 "Лаборатория Касперского" 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 (Microsoft 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 қолданбаларын жаңарту үшін қолжетімді. Kaspersky Security Center Linux тек таңдалған жаңартумен бірдей өндірушінің қолданбаларына қатысты жаңартуларды орнатады. Басқа өндірушілердің қабылданбаған жаңартулары мен қолданба 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, қолданбалардың аралық нұсқаларын орнатуға келіссеңіз, осы параметрді қосыңыз.

  Егер бұл параметр өшірулі болса, қолданбалардың тек таңдалған нұсқалары орнатылады. Қолданбалардың нұсқаларын дәйекті түрде орнатуға тырыспай, қолданбаларды тікелей жаңартқыңыз келсе, бұл параметрді өшіріңіз. Егер таңдалған жаңартуларды қолданбаның алдыңғы нұсқаларын орнатпай-ақ орнату мүмкін болмаса, қолданбаны жаңарту қатемен аяқталады.

  Мысалы, сізде құрылғыда қолданбаның 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. Өзгерістерді 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 "Лаборатория Касперского" 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 (Microsoft 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 қолданбаларын жаңарту үшін қолжетімді. Kaspersky Security Center Linux тек таңдалған жаңартумен бірдей өндірушінің қолданбаларына қатысты жаңартуларды орнатады. Басқа өндірушілердің қабылданбаған жаңартулары мен қолданба 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, қолданбалардың аралық нұсқаларын орнатуға келіссеңіз, осы параметрді қосыңыз.

  Егер бұл параметр өшірулі болса, қолданбалардың тек таңдалған нұсқалары орнатылады. Қолданбалардың нұсқаларын дәйекті түрде орнатуға тырыспай, қолданбаларды тікелей жаңартқыңыз келсе, бұл параметрді өшіріңіз. Егер таңдалған жаңартуларды қолданбаның алдыңғы нұсқаларын орнатпай-ақ орнату мүмкін болмаса, қолданбаны жаңарту қатемен аяқталады.

  Мысалы, сізде құрылғыда қолданбаның 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* 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 қолданбалардың жаңартулары үшін әртүрлі параметрлері бар әртүрлі тапсырмалар болса, осы параметрді өшіруге болады.

  Әдепкі бойынша, параметр қосулы.

- **Деректерді жаңарту үшін жаңарту серверіне қосылу**

  Басқарылатын құрылғыдағы Windows Update агенті Microsoft жаңарту көзіне қосылады. Келесі қызметтер Microsoft жаңарту көздері бола алады:

  - Kaspersky Security Center Linux Басқару сервері (Желілік агент саясатының параметрлерін қараңыз).
  - 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 және құрылғы кэшінде сақталатын 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 жаңартулар алу үшін Microsoft жаңарту серверіне тек **Деректерді жаңарту үшін жаңарту серверіне қосылу** параметрлер тобындағы **Белсенді** параметрі мен **Windows Update жаңартуларын іздеу режимі** параметрі қосулы болса ғана қосылады.
  - Басқарылатын құрылғыдағы Windows Update агенті, **Деректерді жаңарту үшін жаңарту серверіне қосылу** параметрлер тобында **Пассив** және **Windows Update жаңартуларын іздеу режимі** қосулы болса немесе **Деректерді жаңарту үшін жаңарту серверіне қосылу** параметрі өшірулі болып, **Windows Update жаңартуларын іздеу режимі** параметрлер тобында **Белсенді** параметрі таңдалған болса, бұған дейін Microsoft жаңартулар көзінен алынған және құрылғының кэшінде сақталған Microsoft Windows қолжетімді жаңартулары туралы ақпаратты қолданады.
  - **Деректерді жаңарту үшін жаңарту серверіне қосылу** параметріне қарамастан (қосулы немесе өшірулі), **Өшірулі** параметрлер тобында **Windows Update жаңартуларын іздеу режимі** параметрі таңдалса, онда Kaspersky Security Center Linux бағдарламасы жаңартулар туралы ақпаратты сұрамайды.

- **«Лаборатория Касперского» 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 ("Лаборатория Касперского" және Microsoft-тан басқа өндірушілер шығарған қолданбалар) үшін осалдықтар мен қажетті жаңартуларды іздейді. Қолдау көрсетілетін үшінші тарап қолданбаларының толық тізімін "Лаборатория Касперского" 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 қолданбалардың 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.

  Қолданбалар орнатылған қалталарды көрсетіңіз. Әдепкі бойынша, тізімде көптеген қолданбалар орнатылған жүйелік қалталар бар.

- **Кеңейтілген диагностикалау параметрін қосу**

  Егер бұл параметр қосулы болса, Желілік агент Kaspersky Security Center Linux қашықтан диагностикалау утилитасындағы Желілік агент үшін трассалау өшірулі болса да, трассалауды жазып алады. 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. "Лаборатория Касперского" 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 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 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. Қолданбаның негізгі терезесінде **Активтер (құрылғылар)** → **Тапсырмалар** бөліміне өтіңіз.
2. **Қосу** түймесін басыңыз.

   Жаңа тапсырма жасау шебері іске қосылады. Шебердің жұмысын жалғастыру үшін **Келесі** түймесін басыңыз.
3. Kaspersky Security Center қолданбасы 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 қолданбалардың жаңартулары үшін әртүрлі параметрлері бар әртүрлі тапсырмалар болса, осы параметрді өшіруге болады.
     >
     > Әдепкі бойынша, параметр қосулы.

   - Деректерді жаңарту үшін жаңарту серверіне қосылу

Басқарылатын құрылғыдағы Windows Update агенті Microsoft жаңарту көзіне қосылады. Келесі қызметтер Microsoft жаңарту көздері бола алады:

- Kaspersky Security Center Linux Басқару сервері (Желілік агент саясатының параметрлерін қараңыз).
- 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 және құрылғы кэшінде сақталатын 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 жаңартулар алу үшін Microsoft жаңарту серверіне тек **Деректерді жаңарту үшін жаңарту серверіне қосылу** параметрлер тобындағы **Белсенді** параметрі мен **Windows Update жаңартуларын іздеу режимі** параметрі қосулы болса ғана қосылады.
- Басқарылатын құрылғыдағы Windows Update агенті, **Деректерді жаңарту үшін жаңарту серверіне қосылу** параметрлер тобында **Пассив** және **Windows Update жаңартуларын іздеу режимі** қосулы болса немесе **Деректерді жаңарту үшін жаңарту серверіне қосылу** параметрі өшірулі болып, **Windows Update жаңартуларын іздеу режимі** параметрлер тобында **Белсенді** параметрі таңдалған болса, бұған дейін Microsoft жаңартулар көзінен алынған және құрылғының кэшінде сақталған Microsoft Windows қолжетімді жаңартулары туралы ақпаратты қолданады.
- **Деректерді жаңарту үшін жаңарту серверіне қосылу** параметріне қарамастан (қосулы немесе өшірулі), **Өшірулі** параметрлер тобында **Windows Update жаңартуларын іздеу режимі** параметрі таңдалса, онда Kaspersky Security Center Linux бағдарламасы жаңартулар туралы ақпаратты сұрамайды.

- «Лаборатория Касперского» 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 ("Лаборатория Касперского" және Microsoft-тан басқа өндірушілер шығарған қолданбалар) үшін осалдықтар мен қажетті жаңартуларды іздейді. Қолдау көрсетілетін үшінші тарап қолданбаларының толық тізімін "Лаборатория Касперского" 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 қолданбалардың 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.

Қолданбалар орнатылған қалталарды көрсетіңіз. Әдепкі бойынша, тізімде көптеген қолданбалар орнатылған жүйелік қалталар бар.

Тапсырма сипаттары терезесіндегі **Бағдарлама параметрлері** қойындысында тапсырманы жасағаннан кейін көрсетілген жолдарды өзгертуге болады.

8. **Кеңейтілген диагностикалау параметрін қосу** керек болса

Егер бұл параметр қосулы болса, Желілік агент Kaspersky Security Center Linux қашықтан диагностикалау утилитасындағы Желілік агент үшін трассалау өшірулі болса да, трассалауды жазып алады. 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. "Лаборатория Касперского" 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 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 **Күн сайын (жазғы уақытқа өтуге қолдау көрсетілмейді)** қойындысындағы **Тапсырманы бастау** ашылмалы тізімінен **Кесте** 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 қолданбаларының қолжетімді жаңартулары туралы ақпаратты қарау

Клиент құрылғыларында орнатылған Microsoft қолданбалық жасақтамасын қоса, үшінші тарап қолданбалары үшін қолжетімді жаңартулар тізімін көруге болады.

Клиент құрылғыларында орнатылған үшінші тарап қолданбалары үшін қолжетімді жаңартулар тізімін көру үшін,

Қолданбаның негізгі терезесінде **Операциялар → Патчтарды басқару → Бағдарламалық жасақтама жаңартулары** бөліміне өтіңіз.

Қолжетімді жаңартулар тізімі көрсетіледі.

Қолданба 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 қолданбалар отбасы.
  - Жаңарту қолданылатын қолданба.
  - 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 қолданба 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 қолданбалары, соның ішінде таңдалған Windows басқарылатын құрылғысында орнатылған Microsoft қолданбалық жасақтамасы үшін қолжетімді жаңартулар туралы ақпаратты көре аласыз.

Таңдалған басқарылатын құрылғы орнатылған үшінші тарап қолданбалары үшін қолжетімді жаңартулар тізімін көру үшін:

1. Қолданбаның негізгі терезесінде **Активтер (құрылғылар)** → **Басқарылатын құрылғылар** бөліміне өтіңіз.

   Басқарылатын құрылғылардың тізімі көрсетіледі.

2. Басқарылатын құрылғылар тізімінде үшінші тарап қолданбаларының 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 қолданбалық 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 қолданбалары үшін қолжетімді жаңартулар тізімін барлық басқарылатын құрылғыларда орнатылған мәтіндік файлға экспорттау үшін:

1. Қолданбаның 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 қолданбалары үшін қолжетімді жаңартулар тізімін таңдалған басқарылатын құрылғыда орнатылған мәтіндік файлға экспорттау үшін:

1. Таңдалған басқарылатын құрылғыда қолжетімді үшінші тарап қолданбалары 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 қолданбаларының 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. Қолданбаның негізгі терезесінде **Операциялар** → **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. Қолданбаның негізгі терезесінде **Операциялар → 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. Өзгерістерді сақтау үшін **Сақтау** түймесін басыңыз.

Таңдалған жаңарту сіз көрсеткен күйге ие.

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 лицензиясымен 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.
- Жаңартуды орнатуға арналған ережені бұрыннан бар *Қажетті жаңартуларды орнату және осалдықтарды түзету* тапсырмасына қосыңыз.

Қажетті жаңартуларды орнату және осалдықтарды түзету тапсырмасын жасау үшін:

1. Қолданбаның негізгі терезесінде **Активтер (құрылғылар) → 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 таңдаңыз.

4. **Тапсырма түрі** тізімінде **Қажетті жаңартуларды орнату және осалдықтарды түзету** тапсырма түрін таңдаңыз.

   Егер тапсырма көрсетілмесе, Жүйені басқару: **Осалдықтар мен патчтарды басқару** функционалдық аймағында сіздің есептік жазбаңызда **Оқу**, **Жазу** және **Орындау құқықтары** бар ма 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 жаңарту 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 орнату кезінде 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, қолданба 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**

Егер бұл параметр қосулы болса, жаңартуларды қолданбаның жаңа нұсқасын орнатылатын болса ғана орнатуға болады.

Бұл параметр өшірулі болса, қолданба жаңартылмайды. Қолданбалардың жаңа нұсқаларын кейінірек қолмен немесе басқа тапсырманы қолдана отырып, орнатуға болады. Мысалы, егер сіздің компанияңыздың инфрақұрылымы қолданбаның жаңа нұсқасын қолдамаса немесе сынақ инфрақұрылымындағы жаңартуды тексеру қажет болса, бұл параметрді пайдалануға болады.

Әдепкі бойынша, параметр қосулы.

Қолданбаның жаңа нұсқасын орнатқаннан кейін, клиент құрылғыларында орнатылған және жаңартылатын қолданбаның жұмысына байланысты басқа қолданбалардың жұмысы бұзылуы мүмкін.

- **Жаңартуларды құрылғыға орнатпастан жүктеп алу**

  Егер жалауша қойылса, қолданба жаңартуларды құрылғыға жүктейді, бірақ оларды автоматты түрде орнатпайды. Содан кейін, жүктелген жаңартуларды қолмен орнатуға болады.

  Microsoft жаңартулары Windows қызметтік қалтасына жүктеледі. Үшінші тарап қолданбаларының жаңартулары ("Лаборатория Касперского" мен Microsoft корпорациясынан басқа өндірушілер шығарған қолданбалар) **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 қолданбаларының ("Лаборатория Касперского" мен Microsoft корпорациясынан басқа өндірушілер шығарған қолданбалар) жаңартуларын жүктеу үшін қолданылады.

- **Кеңейтілген диагностикалау параметрін қосу**

  Егер бұл параметр қосулы болса, Желілік агент Kaspersky Security Center Linux қашықтан диагностикалау утилитасындағы Желілік агент үшін трассалау өшірулі болса да, трассалауды жазып алады. 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. "Лаборатория Касперского" 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 қолданба 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, қолданба 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 сессияларда бағдар. келесі уақыттан кейін мәжбүрлеп жабу (мин)**

Пайдаланушының құрылғысы бұғатталған кезде қолданбаларды мәжбүрлеп аяқтау (белсенді емес кезеңнен кейін автоматты түрде немесе қолмен).

Егер параметр қосулы болса, бұғатталған құрылғыдағы қолданбалардың жұмысы енгізу өрісінде көрсетілген уақыт өткеннен кейін тоқтатылады.

Егер параметр өшірулі болса, бұғатталған құрылғыдағы қолданбалардың 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.

Жаңартуларды орнату үшін ережелер қосу

Бұл функционалдық, Осалдықтар мен патчтарды басқаруға арналған лицензия болған кезде қолжетімді.

Қажетті жаңартуларды орнату және осалдықтарды түзету тапсырмасы арқылы бағдарламалық жасақтама жаңартуларын орнатқанда немесе қолданбаның осалдықтарын түзету кезінде жаңартуды орнату ережелерін көрсету керек. 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 "Лаборатория Касперского" 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* тапсырмасын жасау 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 "Лаборатория Касперского" 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 қолданбаларды жаңарту үшін немесе тек қажетті қолданбаларды 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, қолданбалардың аралық нұсқаларын орнатуға келіссеңіз, осы параметрді қосыңыз.

    Егер бұл параметр өшірулі болса, қолданбалардың тек таңдалған нұсқалары орнатылады. Қолданбалардың нұсқаларын дәйекті түрде орнатуға тырыспай, қолданбаларды тікелей жаңартқыңыз келсе, бұл параметрді өшіріңіз. Егер таңдалған жаңартуларды қолданбаның алдыңғы нұсқаларын орнатпай-ақ орнату мүмкін болмаса, қолданбаны жаңарту қатемен аяқталады.

    Мысалы, сізде құрылғыда қолданбаның 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 қолданбалардағы осалдықтарды түзету немесе тек қажетті қолданбалардағы осалдықтарды түзету үшін.

   Шебердің келесі қадамына өтіңіз.

6. Қосып жатқан ереженің атауын енгізіңіз. Ереже атауын кейінірек, **Бағдарлама параметрлері** бөлімінде, жасалған тапсырманың сипаттары терезесінде 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 "Лаборатория Касперского" 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. **Қолданбалар** терезесінде жаңартуларды орнатқыңыз келетін қолданбалар мен қолданба нұсқаларын таңдаңыз. Әдепкі бойынша барлық қолданбалар 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 қолданбаларын 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 "Лаборатория Касперского" 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 қолданбалар таңдалған.

   Шебердің келесі қадамына өтіңіз.

5. Қосып жатқан ереженің атауын енгізіңіз. Ереже атауын кейінірек, **Бағдарлама параметрлері** бөлімінде, жасалған тапсырманың сипаттары терезесінде 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 қолданбаларын автоматты түрде жаңарту

Кейбір үшінші тарап қолданбалары автоматты түрде жаңартылуы мүмкін. Қолданба өндірушісі қолданбаның автоматты түрде жаңарту функциясын қолдайтынын анықтайды. Егер басқарылатын құрылғыда орнатылған үшінші тарап қолданбасы автоматты түрде жаңартуды қолдаса, қолданба сипаттарында автоматты түрде жаңарту параметрін көрсетуге болады. Автоматты жаңарту параметрін өзгерткеннен кейін, Желілік агенттер қолданба 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 қолданбасына арналған автоматты жаңарту параметрін конфигурациялау үшін:

1. Қолданбаның негізгі терезесінде **Операциялар → Үшінші тарап бағдарламалары → Бағдарламалар тізімдемесі** бөліміне өтіңіз.

2. Автоматты жаңарту параметрін өзгерткіңіз келетін қолданбаның атын басыңыз.

   Іздеуді жеңілдету үшін тізімді **Автоматты жаңартулар күйі** және **Автоматты жаңартуларды басқару** бағандары арқылы сүзуге болады.

   Қолданба 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 Linux Center келесі тапсырмалар арқылы үшінші тарап қолданбалары үшін жаңартуларды орнатады: *Қажетті жаңартуларды орнату және осалдықтарды түзету* және *Осалдықтарды түзету*.

   - **Рұқсат етілген**

     Өндіруші қолданба үшін жаңартуды шығарғаннан кейін, бұл жаңарту автоматты түрде басқарылатын құрылғыларға орнатылады. Қосымша әрекеттер керек емес.

   - **Бұғатталған**

     Қолданба жаңартулары автоматты түрде орнатылмайды. Kaspersky Security Linux Center келесі тапсырмалар арқылы үшінші тарап қолданбалары үшін жаңартуларды орнатады: *Қажетті жаңартуларды орнату және осалдықтарды түзету* және *Осалдықтарды түзету*.

4. Өзгерістерді сақтау үшін **Сақтау** түймесін басыңыз.

Автоматты жаңарту конфигурациясы таңдалған қолданбаға қолданылады.

Үшінші тарап қолданбаларында осалдықтарды түзету

Бұл бөлімде, басқарылатын құрылғыларда орнатылған қолданбаларда осалдықтарды түзетумен байланысты Kaspersky Security Center Linux мүмкіндіктері сипатталған.

Қолданбалардың 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 қолданбалық жасақтамасын қоса, үшінші тарап қолданбаларында кездеседі.

Қолданбалардың осалдықтарын анықтау

Осалдықтарды анықтау үшін Kaspersky Security Center Linux қолданбасы белгілі осалдықтар туралы дерекқордағы белгілерге негізделген қолданбаның белгілі осалдықтарын іздейді. Дерекқорды "Лаборатория Касперского" мамандары жасап, өзекті күйде ұстайды. Онда осалдықтардың сипаттамасы, осалдықтарды анықтау күні және осалдықтардың қауіптілік деңгейі сияқты осалдықтар туралы ақпарат бар. Қолданбаның осалдықтары туралы ақпаратты "Лаборатория Касперского" сайтында алуға болады.

Kaspersky Security Center Linux жүйесінде қолданбалардағы осалдықтарды іздеу үшін *Осалдықтарды және қажетті жаңартуларды іздеу* тапсырмасы пайдаланылады.

Қолданбаларда 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 "Лаборатория Касперского" 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 да жасай аласыз.

Осалдықтарды түзетуге арналған бағдарламалық жасақтаманың жаңартулары толық дистрибутивтер немесе патчтар түрінде ұсынылуы мүмкін. Қолданбалардың осалдықтарын түзететін бағдарламалық жасақтама жаңартулары *түзетулер* деп аталады. *Ұсынылған түзетулер* – бұл "Лаборатория Касперского" 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 қолданбасы жаңартулары "Лаборатория Касперского" 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.

"Лаборатория Касперского" мамандары Осалдықтар мен патчтарды басқару арқылы орнатуға болатын үшінші тарап қолданбасы жаңартуларын қолмен талдамайды. Сонымен қатар "Лаборатория Касперского" мамандары мұндай жаңартулардағы осалдықтарды (белгілі немесе белгісіз) немесе құжатталмаған мүмкіндіктерді іздеумен айналыспайды және жоғарыда аталған талдаудың басқа түрлерін жүргізбейді.

> Пайдаланушының араласуы үшінші тарап қолданбаларын жаңарту кезінде немесе басқарылатын құрылғыдағы үшінші тарап қолданбаларында осалдықтарды түзету кезінде қажет болуы мүмкін. Мысалы, пайдаланушыдан үшінші тарап қолданбасын жабу сұралуы мүмкін.

Қолданбаның кейбір осалдықтарын түзету үшін қажет болса, қолданбаны орнату лицензиялық келісімін қабылдау қажет. Егер сіз Лицензиялық келісімнен бас тартсаңыз, қолданбаның осалдығы түзетілмейді.

Үшінші тарап қолданбаларындағы осалдықтарды анықтау және түзету.

Бұл бөлімде, Windows басқаруымен жұмыс істейтін құрылғылардағы осалдықтарды анықтау және түзету сценарийі келтірілген. Операциялық жүйелердегі, үшінші тарап қолданбаларындағы, соның ішінде Microsoft қолданбаларындағы 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 қолданбалық жасақтама осалдықтарының ұсынылған түзетулер тізімін жасау. Тізімді "Лаборатория Касперского" 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. Қолданбаның осалдықтарын түзету үшін *Қажетті жаңартуларды орнату және осалдықтарды түзету* тапсырмасы ұсынылған қолданба жаңартуларын пайдаланады.

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 *Осалдықтарды және қажетті жаңартуларды іздеу* тапсырмасымен бірдей жиілікте немесе жиірек жұмыс істейтіндей етіп орнатуға болады. *Осалдықтарды түзету* тапсырмасының кестесін белгілеген кезде, тапсырманы іске қоспас бұрын Microsoft қолданбаларының түзетулерін таңдау немесе үшінші тарап қолданбалары үшін арнайы түзетулерді көрсету керек.

Тапсырмалар кестесін белгілеу кезінде, осалдықтарды түзету тапсырмасы *Осалдықтарды және қажетті жаңартуларды іздеу* аяқталғаннан кейін іске қосылатынына көз жеткізіңіз.

5 Қолданбалардың осалдықтарын елемеу (қажет болса)

Барлық басқарылатын құрылғылардағы немесе тек таңдалған басқарылатын құрылғылардағы қолданбалардағы осалдықты елемеуге болады.

6 Осалдықтарды түзету тапсырмасын іске қосу

Қажетті жаңартуларды орнату және осалдықтарды түзету немесе *Осалдықтарды түзету* тапсырмасын іске қосыңыз. 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 қолданбаларында 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 қолданбаларын жаңарту кезінде немесе басқарылатын құрылғыдағы үшінші тарап қолданбаларында осалдықтарды түзету кезінде қажет болуы мүмкін. Мысалы, пайдаланушыдан үшінші тарап қолданбасын жабу сұралуы мүмкін.

Сондай-ақ, қолданбалардағы осалдықтарды түзету үшін тапсырманы келесі жолдармен жасауға болады:

- Осалдықтар тізімін ашып, қандай осалдықтарды түзету керектігін көрсетіңіз.

  Нәтижесінде, қолданбалардағы 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.

Қолданбалардағы осалдықтарды осалдықтар тізімімен түзету

Қолданбаның осалдықтарын осалдықтар тізімін пайдаланып түзету үшін:

1. Төмендегі әрекеттердің бірін орындау арқылы өзгерту үшін осалдықтар тізімін ашыңыз:

- Қолданбаның негізгі терезесінде **Операциялар** → **Патчтарды басқару** → **Бағдарламалық жасақтама осалдықтары** бөліміне өтіңіз.
- Қолданбаның негізгі терезесінде **Активтер (құрылғылар)** → **Басқарылатын құрылғылар** → <құрылғының атауы> → **Кеңейтілген** → **Бағдарламалық жасақтама осалдықтары** бөліміне өтіңіз.
- Қолданбаның негізгі терезесінде **Операциялар** → **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.

   Қолданбаның кейбір осалдықтарын түзету үшін қажет болса, қолданбаны орнату лицензиялық келісімін қабылдау қажет. Егер сіз Лицензиялық келісімнен бас тартсаңыз, қолданбаның 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. Өзгерістерді сақтау үшін **Сақтау** түймесін басыңыз.

Тапсырма жасауды таңдаған болсаңыз, ол тапсырмалар тізімінде, **Активтер (құрылғылар)** → **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 қолданбалардағы осалдықтарды түзету

Осалдықтар мен патчтарды басқару үшін лицензия болған кезде, осалдықтарды түзету шебері қолжетімді болады.

Осалдықтарды түзету шебері арқылы қолданбалардағы осалдықтарды түзету үшін:

1. Қолданбаның негізгі терезесінде **Операциялар → 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 күрделілік 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 "Лаборатория Касперского" 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. Өзгерістерді сақтау үшін **Сақтау** түймесін басыңыз.

- Тапсырма жасау үшін:

a. **Жаңа тапсырма** түймесін басыңыз.

b. Ашылған бетте жаңа ережені орнатыңыз:

- Осы күрделілік 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 "Лаборатория Касперского" 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 қолданбаларын қоса алғанда, үшінші тарап қолданбалары 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 ғана *Осалдықтарды түзету* тапсырмасын жасай аласыз.

Осалдықтар мен патчтарды басқаруға арналған лицензияңыз болса, сіз *Осалдықтарды түзету* түріндегі тапсырмаларды жасай аласыз. 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 қолданбаларын жаңарту кезінде немесе басқарылатын құрылғыдағы үшінші тарап қолданбаларында осалдықтарды түзету кезінде қажет болуы мүмкін. Мысалы, пайдаланушыдан үшінші тарап қолданбасын жабу сұралуы мүмкін.

Осалдықтарды түзету тапсырмасын жасау үшін мына қадамдарды орындаңыз:

1. Қолданбаның негізгі терезесінде **Активтер (құрылғылар)** → **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 қолданбаларының осалдықтары үшін әдетте ұсынылған түзетулер бар. Олар үшін қосымша әрекеттер қажет емес.

   Үшінші тарап қолданбалары 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 қолданба 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, қолданба 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, қолданба құрылғыны қайта жүктеуге мүмкіндік бермейді.

  Егер бұл параметр қосулы болса, құрылғыны қайта іске қоспас бұрын бұғатталған құрылғылардағы мұндай қолданбалар 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 қолданбаларды 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 қолданба 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 жасаған кезде көрсетілген параметрлерді өзгертуге болады.

    Тапсырмалар тізіміндегі жасалған тапсырма атауын басу арқылы тапсырма сипаттарының терезесін ашуға да болады.

    Тапсырма жасалады, теңшеледі және тапсырмалар тізімінде, **Активтер (құрылғылар)** → **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 қолданбаларындағы 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 қолданбаларындағы осалдықтарға арналған пайдаланушылық түзетулерді таңдау үшін:

1. Қолданбаның негізгі терезесінде **Операциялар → Патчтарды басқару → Бағдарламалық жасақтама осалдықтары** бөліміне өтіңіз.

   Басқарылатын құрылғыларда орнатылған үшінші тарап қолданбаларындағы осалдықтар тізімі бар бет ашылады.

2. Қолданбалардың 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.

   Қолданбаларда таңдалған осалдықтар үшін пайдаланушылық түзетулердің тізімі көрсетіледі.

4. **Қосу** түймесін басыңыз.

   Қолжетімді орнату пакеттері тізімі көрсетіледі. Көрсетілген орнату пакеттері тізімі **Операциялар → Қоймалар → 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.

Қолданбалардың 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 қолданбалардағы осалдықтар туралы ақпаратты қарау

Басқарылатын құрылғылардағы бағдарламалық жасақтаманы осалдықтарға сканерлегеннен кейін, қолданбаларда анықталған осалдықтар тізімін көруге болады. Сондай-ақ, осалдықтар туралы есепті жасауға және көруге болады.

Барлық басқарылатын құрылғыларда анықталған қолданбалардағы осалдықтар тізімін қарау үшін,

Қолданбаның 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,

қолданбалардың осалдықтары тізімінде осалдықтың атауы көрсетілген сілтемеден өтіңіз.

Қолданбалардың осалдықтары сипаттары терезесі ашылады.

Таңдалған басқарылатын құрылғыларда анықталған қолданбалардағы осалдықтар туралы ақпаратты қарау

Сіз осалдықтар туралы ақпаратты таңдалған Windows басқарылатын құрылғысында табылған қолданбалардан көре аласыз.

Таңдалған басқарылатын құрылғыда анықталған қолданбалардағы осалдықтар тізімін экспорттау үшін:

1. Қолданбаның негізгі терезесінде **Активтер (құрылғылар) → Басқарылатын құрылғылар** бөліміне өтіңіз.

   Басқарылатын құрылғылардың тізімі көрсетіледі.

2. Басқарылатын құрылғылар тізімінде, қолданбаларда 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 қолданбалық жасақтама осалдықтары тізімі көрсетіледі.

Таңдалған қолданбалардың осалдықтары сипаттарын көру үшін,

қолданбалардағы осалдықтар тізіміндегі осалдық атауы бар сілтемеге өтіңіз.

Таңдалған қолданбалардың осалдықтары сипаттары терезесі ашылады.

Басқарылатын құрылғылардағы осалдықтардың статистикасын қарау.

Басқарылатын құрылғылардағы қолданбалардағы 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. Қолданбаның 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.

Қолданбалардағы 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 қолданбалардағы осалдықтар тізімін мәтіндік файлға экспорттау үшін:

1. Қолданбаның 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 қолданбалардағы осалдықтар тізімін экспорттау үшін:

1. Қолданбаның негізгі терезесінде **Активтер (құрылғылар)** → **Басқарылатын құрылғылар** бөліміне өтіңіз.

   Басқарылатын құрылғылардың тізімі көрсетіледі.

2. Басқарылатын құрылғылар тізімінде, қолданбаларда 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 қолданбалық жасақтама осалдықтары тізімі көрсетіледі.

   Әдепкі бойынша, ағымдағы бетте көрсетілетін осалдықтар ғана экспортталады.

   Белгілі бір осалдықтарды ғана экспорттағыңыз келсе, сол осалдықтардың жанындағы құсбелгілерді қойыңыз.

5. 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.

Қолданбалардағы осалдықтарды елемеу

Қолданбалардың осалдықтарын елемеуіңіз және оларды түзетпеуіңіз мүмкін. Қолданбалардағы осалдықтарды елемеу себептері, мысалы, келесідей болуы мүмкін:

- Сіз қолданбадағы осалдықты ұйымыңыз үшін критикалық деп санамайсыз.
- Қолданбалардың осалдықтарын түзету, осалдықты түзетуді қажет ететін қолданбаның деректерін зақымдауы мүмкін екенін түсінесіз.
- Қолданбалардың осалдықтары сіздің ұйымыңыздың желісіне қауіп төндірмейтініне сенімдісіз, өйткені сіз басқарылатын құрылғыларды қорғау үшін басқа шараларды қолданасыз.

Барлық басқарылатын құрылғылардағы немесе тек таңдалған басқарылатын құрылғылардағы қолданбалардағы осалдықты елемеуге болады.

Барлық басқарылатын құрылғылардағы қолданбалардың осалдықтарын өткізіп жіберу үшін:

1. Қолданбаның негізгі терезесінде **Операциялар** → **Патчтарды басқару** → **Бағдарламалық жасақтама осалдықтары** бөліміне өтіңіз.

   Басқарылатын құрылғыларда табылған қолданбалардың осалдықтары тізімі көрсетіледі.

2. Қолданбалардың осалдықтары тізімінде өткізіп жібергіңіз келетін қолданбалардың осалдықтары атауын басыңыз.

   Қолданбалардың осалдықтары сипаттары терезесі ашылады.

3. **Жалпы** қойындысында **Осалдықты елемеу** параметрін қосыңыз.

4. **Сақтау** түймесін басыңыз.

   Қолданбалардың осалдықтары сипаттары терезесі жабылады.

Қолданбалардың осалдықтары барлық басқарылатын құрылғыларда өткізіп жіберіледі.

Барлық басқарылатын құрылғылардағы қолданбалардың осалдықтарын өткізіп жіберу үшін:

1. Қолданбаның негізгі терезесінде **Активтер (құрылғылар)** → **Басқарылатын құрылғылар** бөліміне өтіңіз.

   Басқарылатын құрылғылардың тізімі көрсетіледі.

2. Басқарылатын құрылғылар тізімінде қолданбалардың 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 қолданбалардың осалдықтары тізімі көрсетіледі.

5. Қолданбалардың осалдықтары тізімінен таңдалған құрылғыда өткізіп жібергіңіз келетін осалдықты таңдаңыз.

   Қолданбалардың осалдықтары сипаттары терезесі ашылады.

6. Қолданбалардың осалдықтары сипаттары терезесінде, **Жалпы** қойындысында **Осалдықты елемеу** параметрін қосыңыз.

7. **Сақтау** түймесін басыңыз.

   Қолданбалардың осалдықтары сипаттары терезесі жабылады.

8. Құрылғының сипаттар терезесін жабыңыз.

Қолданбалардың осалдықтары таңдалған құрылғыда өткізіп жіберіледі.

Қолданбалардағы жіберіп алған осалдықтар *Осалдықтарды түзету* тапсырмасы және *Қажетті жаңартуларды орнату және осалдықтарды түзету* тапсырмалары аяқталғаннан кейін түзетілмейді. Қолданбалардағы жетіспейтін осалдықтарды осалдықтар тізімінен сүзгі арқылы алып тастауға болады.

"Лаборатория Касперского" дерекқорынан үшінші тарап қолданбасы үшін орнату пакетін жасау

Kaspersky Security Center Web Console сервері орнату пакеттері көмегімен үшінші тарап қолданбаларын қашықтан орнатуды орындауға мүмкіндік береді. Осындай үшінші тарап қолданбалары тиісті "Лаборатория Касперского" 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 "Лаборатория Касперского" дерекқорынан үшінші тарап қолданбасы үшін орнату пакетін жасауға болады.

"Лаборатория Касперского" дерекқорынан үшінші тарап қолданбасына арналған орнату пакетін жасау үшін:

1. Қолданбаның негізгі терезесінде **Табу және орналастыру → Орналастыру және тағайындау → 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 «Лаборатория Касперского» 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, қолданба 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 Түпкі пайдаланушының лицензиялық келісімінің ережелері мен шарттарын толық оқып шыққанымды, түсінгенімді және қабылдайтынымды растаймын** 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 "Лаборатория Касперского" дерекқорындағы үшінші тарап қолданбаларын орнату пакетін пайдаланып, *Бағдарламаны қашықтан орнату* тапсырмасын жасауға және қайта конфигурациялауға болады.

"Лаборатория Касперского" дерекқорынан үшінші тарап қолданбасына арналған орнату пакетінің параметрлерін қарау және өзгерту

Егер сіз бұрын "Лаборатория Касперского" дерекқорында атап көрсетілген үшінші тарап қолданбаларының қандай да бір орнату пакеттерін жасаған болсаңыз, онда сіз осы пакеттердің параметрлерін қарап, өзгерте аласыз.

"Лаборатория Касперского" дерекқорынан үшінші тарап қолданбасының орнату пакетінің параметрлерін өзгерту жүйелік Осалдықтар мен патчтарды басқаруға арналған лицензия болған жағдайда ғана қолжетімді.

"Лаборатория Касперского" дерекқорынан үшінші тарап қолданбасына арналған орнату пакетінің параметрлерін қарау және өзгерту үшін:

1. Қолданбаның негізгі терезесінде **Табу және орналастыру** → **Орналастыру және тағайындау** → **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.

"Лаборатория Касперского" дерекқорынан үшінші тарап қолданбасына 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** қойындысы:
  - Қолмен өзгертуге болатын орнату пакетінің атауын қамтитын енгізу өрісі.
  - **Бағдарлама**

    Орнату пакеті жасалған үшінші тарап қолданбасының атауы.
  - **Нұсқа**

    Орнату пакеті жасалған үшінші тарап қолданбасының нұсқа нөмірі.

- **Өлшемі**

  Үшінші тарап қолданбасына арналған орнату пакетінің өлшемі (килобайт түрінде).

- **Жасалған күні**

  Үшінші тарап қолданбасы үшін орнату пакетін жасау күні мен уақыты.

- **Жолы**

  Үшінші тарап қолданбасына арналған орнату пакеті орналасқан желілік қалтаға апаратын толық жол.

- **Орнату реті** қойындысы:

  - **Қажетті жалпы жүйелік құрамдастарды орнату**

    Егер жалауша қойылса, жаңартуды орнатпас бұрын, қолданба 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 қолданбаға 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**

  "Лаборатория Касперского" анықтаған жаңартудың маңыздылық деңгейі.

- **Патчтың маңыздылық деңгейі**

  "Лаборатория Касперского" қолданбаларына 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**

  Қолданба 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 қолданбалар тобының аты көрсетіледі.

- **Бағдарлама**

  Жаңарту қатысты болып табылатын қолданбаның 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.

  - **Веб-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 қолданбаларындағы осалдықтарды түзету үшін қолдануға болатын әрекеттер сипатталған.

Оқшауланған желідегі үшінші тарап қолданбаларының осалдықтарын түзету

Жаңартуларды орнатуға және оқшауланған желідегі басқарылатын құрылғыларда орнатылған үшінші тарап қолданбаларының 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 қолданбалық жасақтама өндірушілері шығарған үшінші тарап қолданбалық жасақтамасының жаңартуларын жүктей аласыз, бірақ Microsoft қолданбалық 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**

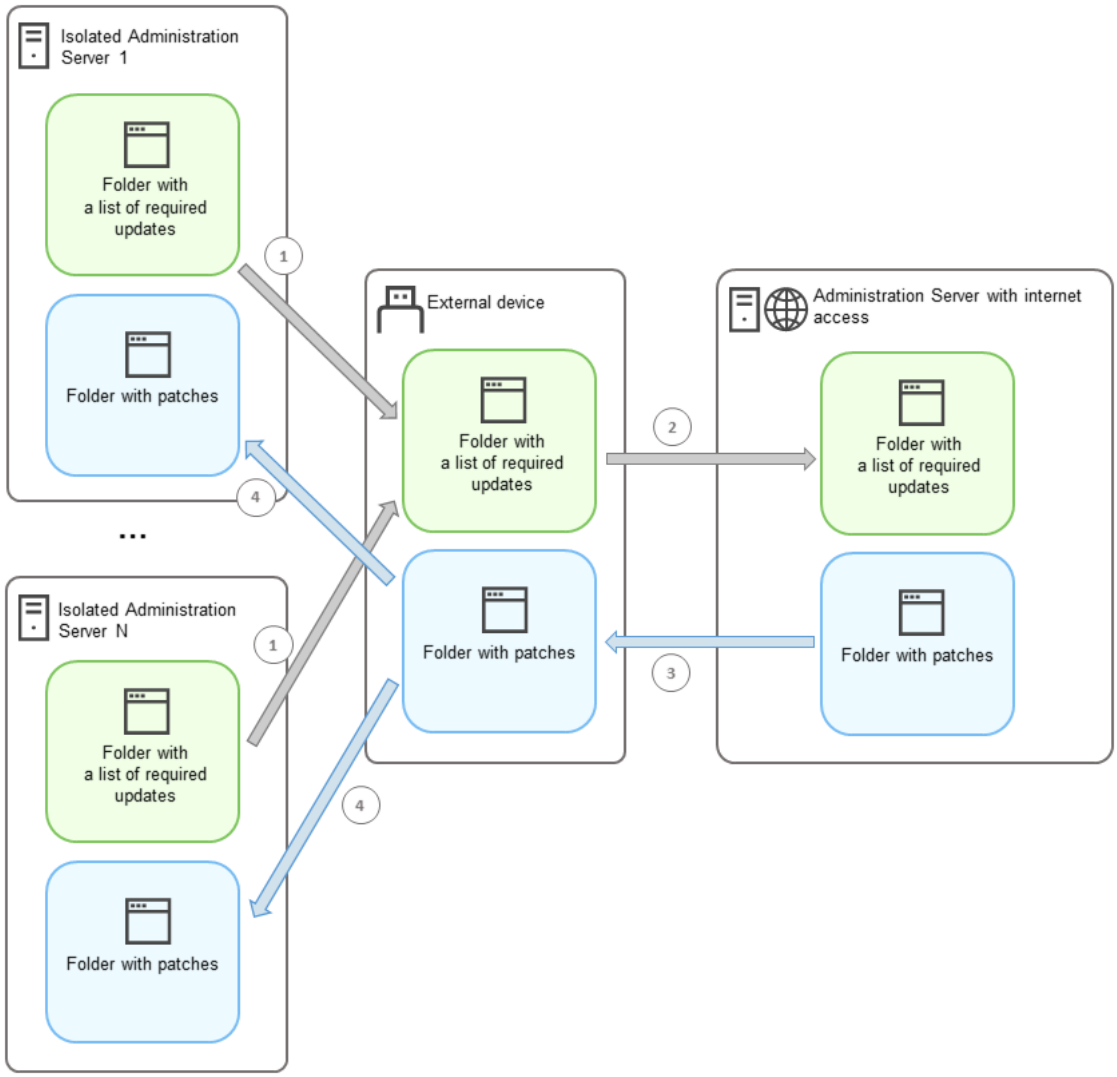
Басқару серверлерінің конфигурациясы аяқталғанда, жаңартулар мен патчтардың тізімдерін Интернетке кіру мүмкіндігі бар Басқару серверінен оқшауланған Басқару серверлеріне тасымалдауға болады. Әрі қарай, түзетулердің жаңартулары басқарылатын құрылғыларға *Қажетті жаңартуларды орнату және осалдықтарды түзету* тапсырмасы арқылы 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 қолданбаларының 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 каталогті 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 "<path to the folder>"
     ```
   - Қажетті жаңартулар тізімі үшін қалта жолын белгілеу үшін:
     ```
     klscflag -fset -pv klserver -n VAPM_REQ_IMPORT_PATH -t s -v "<path to the folder>"
     ```

   Мысалы: `klscflag -fset -pv klserver -n VAPM_DATA_EXPORT_PATH -t s -v "/FolderForPatches"`

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 <value in seconds>`

   Әдепкі бойынша, 120 секунд мәні көрсетілген.

   Мысалы: `klscflag -fset -pv klserver -n VAPM_DATA_EXPORT_PERIOD_SEC -t d -v 120`

6. 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 каталогті 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 <value in seconds>
   ```
   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. *Осалдықтарды және қажетті жаңартуларды іздеу* тапсырмасын жасап, тапсырманы іске қосу кестесін конфигурациялаңыз. Тапсырма кестесінде көрсетілгеннен ертерек орындалуын қаласаңыз, тапсырманы қолмен іске қосыңыз.

9. Басқару сервері қызметін қайта іске қосыңыз.

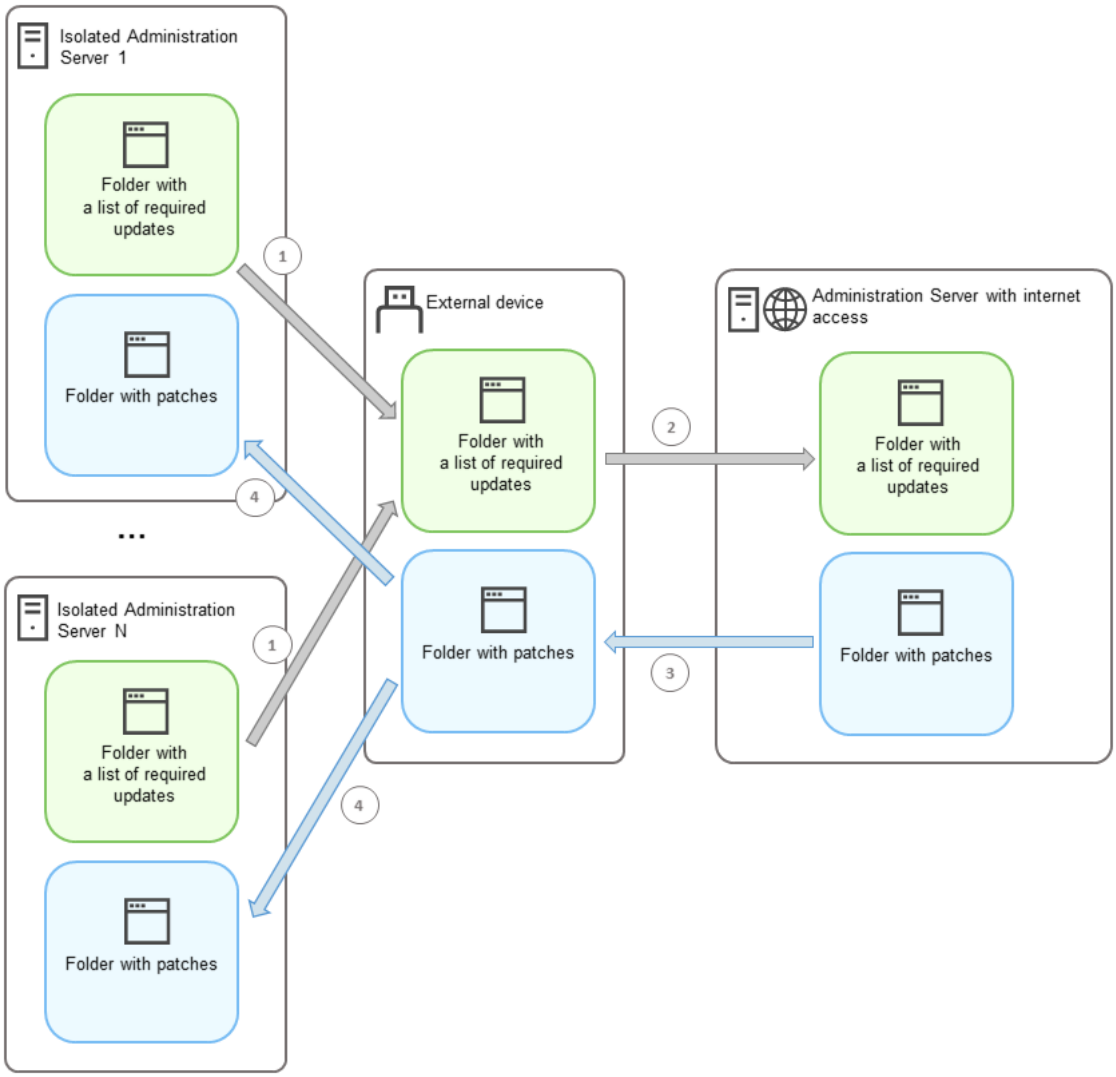
Барлық Басқару серверлерін орнатқаннан кейін, сіз түзетулер мен қажетті жаңартулар тізімдерін жылжыта аласыз және оқшауланған желідегі басқарылатын құрылғылардағы үшінші тарап қолданбаларының осалдықтарын түзете аласыз.

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 қосылмаған болса, 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. Бұл патчтар оқшауланған Басқару серверлерінде пайда болғанда , *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 резервтік қоймасы* тапсырмасын іске қоспаңыз (бұл да артық жүктелуге себеп болады). Нәтижесінде, *Қажетті жаңартуларды орнату және осалдықтарды түзету* тапсырмасы үзіліп, 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 каталогті 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 қолданбаны 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 сценарийлерді іске қосу үшін:

1. KlAkOAPI.tar.gz мұрағатын жүктеп алыңыз. Бұл мұрағатта KlAkOAPI пакеті және мысалдар бар (оларды мұрағаттан немесе OpenAPI анықтамалық нұсқаулығынан көшіріп алуға болады). KlAkOAPI.tar.gz мұрағаты Kaspersky Security Center Linux орнату қалтасында да болады.

2. Басқару сервері орнатылған құрылғыда KlAkOAPI.tar.gz мұрағатынан KlAkOAPI пакетін орнатыңыз.

   OpenAPI әдістерін шақыру, мысалдар мен сценарийлеріңізді іске қосу тек Басқару сервері мен KlAkOAPI пакеті орнатылған құрылғыларда ғана жүзеге асырылуы мүмкін.

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	Сіз өзіңіздің құрылғыңыздағы Желілік агентке қосылым шлюзі арқылы қосыла аласыз, содан кейін желілер тізімі	Тарату нүктелері мен қосылым

көрсетілген құрылғыға қосылым шлюзі арқылы жүктеңіз	бар файлды компьютерге жүктей аласыз.	шлюздерін конфигурациялау
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 қолданбаларды 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).	"Лаборатория Касперского" дерекқорлары мен қолданбаларын 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.	Тапсырманы жасау

	• 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.	
Лицензиялық кілттерді атап көрсету	Басқару серверінің басқарылатын құрылғыларында орнатылған "Лаборатория Касперского" қолданбаларына 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 қолданбалар санатын жасай аласыз.	Қолмен толықтырылатын қолданбалар 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

OpenAPI арқылы Kaspersky Security Center Linux қолданбасымен өзара әрекеттесетін қолданбалар

Кейбір қолданбалар OpenAPI арқылы Kaspersky Security Center Linux қолданбасымен өзара әрекеттеседі. Мұндай қолданбаларға, мысалы, Kaspersky Anti Targeted Attack Platform немесе Kaspersky Security for Virtualization кіреді. Сондай-ақ, бұл OpenAPI негізінде жасалған пайдаланушы клиенттік қолданбасы болуы мүмкін.

OpenAPI арқылы Kaspersky Security Center Linux қолданбасымен өзара әрекеттесетін қолданбалар Басқару серверіне қосылады. Басқару серверіне қосылу үшін рұқсат етілген IP мекенжайларының тізімін конфигурациялаған болсаңыз, Kaspersky Security Center Linux OpenAPI пайдаланатын қолданбалар орнатылған құрылғылардың IP мекенжайларын қосыңыз. Сіз қолданатын қолданба OpenAPI-мен жұмыс істейтінін білу үшін осы қолданбаның анықтамасын қараңыз.

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 "Лаборатория Касперского" 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;
- 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.

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.

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

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	24 ГБ

Диск кеңістігі	250 ГБ, 150 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	8 ядро, 2500 МГц
ЖЖҚ	18 ГБ
Диск кеңістігі	200 ГБ, 150 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.
- "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 қолданбалар туралы хабардар етуді қосуды жоспарласаңыз, онда іске қосылатын қолданбалар 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 ("SQL Server" ДҚБЖ қолданған жағдайда, әдепкі бойынша KAV.MDF файлы) көбінесе дерекқордағы бос емес орыннан шамамен екі есе көп болады.

Транзакциялар журналының өлшемін нақты шектеу ұсынылмайды (егер сіз SQL Server серверін ДҚБЖ ретінде қолдансаңыз, әдепкі бойынша KAV_log.LDF файлы). MAXSIZE параметрінің әдепкі бойынша мәнін қалдыру ұсынылады. Егер сізге осы файлдың өлшемін шектеу қажет болса, KAV_log.LDF үшін MAXSIZE параметрінің қажетті мәні 20480 МБ құрайтынын ескеру қажет.

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.
- "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;
- Қолданбаларды 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 қолданба модульдеріне жаңартуларды тікелей "Лаборатория Касперского" жаңарту серверлерінен алатын схеманы пайдалансаңыз, тарату нүктелері интернетке қосылған болуы керек.

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-ден 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-ден 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-ден 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-ден 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.

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 деректерін сақтық көшірмелеу;
- дерекқорларға 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.

"Лаборатория Касперского" 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.

Бағдарламалық жасақтаманы түгендеу тапсырмасы

Орнатылған қолданбалар туралы ақпаратты алу арқылы дерекқорға түсетін жүктемені азайтуға болады. Ол үшін түгендеу тапсырмасын стандартты қолданбалар 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	113 МБ	1,8 МБ

дерекқорларды бастапқы жаңарту (Kaspersky Security Network-ке қатысу өшірілсе)		
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
Қолданбалар тізімдемесі кестесін қосқаннан кейінгі бір реттік трафик	10 КБ-қа дейін	12 КБ-қа дейін
Қолданбалар 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.

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 қолданба туралы басқа ақпарат көздерінде өз сұрағыңыздың шешімін таппаған болсаңыз, "Лаборатория Касперского" Техникалық қолдау қызметіне хабарласыңыз. Техникалық қолдау қызметінің қызметкерлері Kaspersky Security Center Linux орнату және пайдалану туралы сұрақтарыңызға жауап береді.

"Лаборатория Касперского" ұйымы Kaspersky Security Center қолданбасы оның өмірлік циклі бойы қолдау көрсетеді (қолданбалардың 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 portal порталынан "Лаборатория Касперского" Техникалық қолдау қызметіне сұрау жіберу.

Kaspersky CompanyAccount арқылы техникалық қолдау

Kaspersky CompanyAccount – бұл "Лаборатория Касперского" қолданбаларын қолданатын ұйымдарға арналған портал. Kaspersky CompanyAccount порталы пайдаланушылардың "Лаборатория Касперского" мамандарымен электрондық сұрау салу арқылы өзара іс-қимыл жасауына арналған. Kaspersky CompanyAccount порталында электрондық сұрауларды "Лаборатория Касперского" 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 "Лаборатория Касперского" 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 "Лаборатория Касперского" зертханасына автоматты түрде жіберілмейді.

Басқару серверінде ақаулық болса, "Лаборатория Касперского" техникалық қолдау қызметіне хабарласуға болады. Техникалық қолдау қызметінің маманы "Лаборатория Касперского" зертханасына әрі қарай талдау үшін Басқару серверінің қоқыс файлдарын жіберуді сұрауы мүмкін.

Қоқыс файлдарында жеке деректер болуы мүмкін. Оны "Лаборатория Касперского" зертханасына жібермес бұрын ақпаратты рұқсатсыз кіруден қорғау ұсынылады.

Қолданба мәліметтері көздері

"Лаборатория Касперского" веб-сайтындағы Kaspersky Security Center Linux беті

Kaspersky Security Center Linux бетінде қолданба, оның мүмкіндіктері мен жұмыс ерекшеліктері туралы мәлімет ала аласыз.

Білім базасындағы Kaspersky Security Center Linux беті

Білім базасы – "Лаборатория Касперского" Техникалық қолдау қызметі веб-сайтындағы бөлім.

Білім базасындағы Kaspersky Security Center Linux бетінде қолданбаны 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 "Лаборатория Касперского" басқа да қолданбаларымен байланысты сұрақтарға жауап бере алады. Сонымен қатар, Білім базасының мақалаларында Техникалық қолдау қызметі жаңалықтары болуы мүмкін.

"Лаборатория Касперского" қолданбаларын пайдаланушылар қауымдастығында талқылау

Сіздің сұрағыңызға тез арада жауап беру қажет болмаса, сіз оны "Лаборатория Касперского" 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.

Анықтаманы көрсету үшін интернет қосылымы керек.

Мәселеңіздің шешімін таба алмасаңыз, Техникалық қолдау қызметіне хабарласыңыз.

Шектеулер тізімі

Kaspersky Security Center Linux қолданбаның жұмыс істеуі үшін критикалық емес бірқатар шектеулерге ие:

- *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 адұрыс импортталмайды.

- Желіңізде бірнеше мың нысаннан (басқарылатын құрылғылар, қауіпсіздік топтары және пайдаланушылардың есептік жазбалары) тұратын Microsoft Active Directory домені болса, ал жауап бетінің өлшемі (`MaxPageSize` параметрі) 5000-нан аз болса, домен контроллерінің сауалнамасы қолжетімді болмайды және домен нысандары туралы ақпарат келмейді. Домен контроллеріне сауалнама жүргізуге әрекет жасалса, *Өлшемнің критикалық мәнінен асып кетті* қатесі көрсетіледі. Бет өлшемін арттыру арқылы қате түзелуі мүмкін. `MaxPageSize` параметрінің мәнін `5000` немесе қажет болса, `10000` мәніне дейін арттыру үшін Ntdsutil.exe утилитасын пайдалана аласыз.

- Басқару серверінің сипаттарында KPSN мүмкіндігін қоссаңыз және 17111 HTTPS портын пайдалансаңыз, ds.kaspersky.com қосылымы үзілмейді.

- Kaspersky Endpoint Security for Windows бағдарламасы KSN прокси сервері қызметіне қолдау көрсетпейді, егер әкімші сервері сипаттарының KSN прокси серверінің параметрлерінде **HTTPS пайдалану** опциясы қосылған болса және Әкімшілік серверінің мекенжайында латын емес таңбалар болса.

- Kaspersky Security Center Linux негізгі Басқару серверінің интерфейсінен қосалқы Серверге ауысқанда, "Лаборатория Касперского" жаңарту қызметі арқылы жаңарту функционалдылығы (Seamless Update – SMU) қолжетімді емес.

- Mac жүйесіне арналған Kaspersky Endpoint Security 11.3 үшін *Кілт қосу* тапсырмасын жасаған кезде шебер лицензия кілттерінің кестесін көрсетеді, онда бос жолдар болуы мүмкін.

- Windows жүйесіне арналған Kaspersky Endpoint Security саясатында көрсетілген қорғаныс деңгейі Windows жүйесіне арналған Kaspersky Endpoint Security интерфейсіндегі қорғаныс деңгейіне сәйкес келмейді.

- Басқарылатын құрылғыдан Kaspersky Endpoint Security for Linux қолданбасын жою үшін *Бағдарламаны қашықтан жою* тапсырмасын іске қосқанда, тапсырма сәтті аяқталады, бірақ Kaspersky Endpoint Security for Linux жойылмайды. Бұл мәселе Kaspersky Endpoint Security for Linux, Kaspersky Embedded Systems Security for Linux және Kaspersky Industrial CyberSecurity for Linux Nodes түйіндеріне қатысты.

- Басқару сервер сипаттары терезесі мобильдік құрылғыларға арналған параметрлерді қамтиды, бірақ Kaspersky Security Center Linux мобильдік құрылғыларды басқаруға қолдау көрсетпейді.

- **Бағдарламалар тізімдемесі** бөлімдегі қолданба Linux операциялық жүйесі бар құрылғыда табылса, қолданба сипаттарында онымен байланысты орындалатын файлдар туралы ақпарат жоқ.

- Қашықтан орнату тапсырмасын пайдаланып, ALT Linux операциялық жүйесімен жұмыс істейтін құрылғыға Желілік агентті орнатсаңыз және бұл тапсырманы root-тан басқа құқықтары бар есептік жазба астында іске қоссаңыз, тапсырма орындалмайды. Қашықтан орнату тапсырмасын root есептік жазбасының астында іске қосыңыз немесе қолданбаны жергілікті орнату үшін Желілік агенттің автономды орнату пакетін жасаңыз және пайдаланыңыз.

- Әріптік пішімімен есептерде бет үзілімі мәтін жолын көлденеңінен кесіп алуы мүмкін.

- Болашақ қосалқы Серверде, **Қосалқы Басқару серверін қосу** шеберінде түпнұсқалық растама үшін екі қадамдық тексеруы қосылған есептік жазбаны көрсетсеңіз, шебер өз жұмысын қатемен аяқтайды. Бұл

мәселені шешу үшін, екі қадамдық тексеруі өшірілген есептік жазбаны көрсетіңіз немесе болашақ қосалқы Серверден иерархия жасаңыз.

- 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.

- Бірнеше желілік адаптері бар басқарылатын құрылғы Басқару серверіне қосылу үшін пайдаланылатын желілік адаптерден ерекшеленетін желілік адаптердің MAC мекенжайы туралы ақпаратты Басқару серверіне жібереді.

- Astra Linux жүйесінің 64 разрядты нұсқасында klnagent-astra пакетін klnagent64_14 пакетімен жаңарту мүмкін емес: ескі klnagent64-astra пакеті жойылады, ал жаңартудың орнына жаңа klnagent64 жаңа пакеті орнатылады, сондықтан klnagent64_14 пакеті бар құрылғы үшін жаңа белгіше қосылатын болады. Бұл құрылғының ескі белгішесін жоюға болады.

- *Сценарийлерді қашықтан іске қосу* 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.

- Пайдаланушы құрылғысында *SELinux* қосылған болса, Есептік жазба құпиясөзін өзгерту тапсырмасы дұрыс жұмыс істемеуі мүмкін. SELinux өшіру туралы қосымша ақпарат алу үшін операциялық жүйеңізге арналған пайдаланушы нұсқаулығын қараңыз.

Глоссарий

"Лаборатория Касперского" жаңарту серверлері

"Лаборатория Касперского" қолданбаларына дерекқорлар мен модульдердің жаңартуларын жіберетін "Лаборатория Касперского" HTTP серверлері мен HTTPS серверлері.

Cloud Discovery

Cloud Discovery — ұйымның бұлттық инфрақұрылымын қорғайтын Cloud Access Security Broker (CASB) шешімінің құрамдасы. Cloud Discovery пайдаланушылардың бұлттық сервистерге қол жеткізуін басқарады. Бұлттық сервистерге, мысалы, Microsoft Teams, Salesforce, Microsoft Office 365 кіреді. Бұлттық сервистер санаттарға топтастырылған, мысалы, *Деректер алмасу*, *Мессенджерлер*, *Электрондық пошта*.

HTTPS

Шифрлауды қолдана отырып шолғыш пен веб-сервер арасында деректерді жіберудің қауіпсіз протоколы. HTTPS корпоративтік немесе қаржылық деректер сияқты жабық ақпаратқа қатынасу үшін пайдаланылады.

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 "Лаборатория Касперского" қолданбалары орнатылған құрылғыларды пайдаланушыларға өз құрылғыларынан Kaspersky Security Network қолданбасына 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 қолданбаның жұмысын басқаратын адам.

Kaspersky Security Center System Health Validator (SHV)

Microsoft NAP-пен Kaspersky Security Center Linux қолданбасының бірлескен жұмысы кезінде операциялық жүйенің жұмысқа қабілетін тексеруге арналған Kaspersky Security Center Linux қолданбасының құрамдасы.

Kaspersky Security Center операторы

Kaspersky Security Center көмегімен басқарылатын қорғаныс жүйесінің күйі мен жұмысын бақылайтын пайдаланушы.

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 "Лаборатория Касперского" белгілі компьютерлік қауіпсіздік қауіптері туралы ақпаратты қамтитын дерекқорлар. Антивирустық дерекқорлардағы жазбалар тексерілетін нысандарда зиянды кодты анықтауға көмектеседі. Антивирустық дерекқорларды "Лаборатория Касперского" мамандары қалыптастырады және сағат сайын жаңартылады.

Антивирустық қорғаныс провайдері

"Лаборатория Касперского" 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 "Лаборатория Касперского" қолданбаларының деректқорында қалыптастырылған ұйымның желісін орталықтандырылған қорғанысының жүйесін құрады.

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 "Лаборатория Касперского" қолданбалары туралы ақпаратты орталықтандырылған сақтау функцияларын жүзеге асыратын Kaspersky Security Center Linux қолданбасының құрамдасы. Басқару сервері осы қолданбаларды 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 деректқоры (оқиғаның Басқару серверінде сақталған саясаттар, тапсырмалар, қолданба параметрлері);
- басқару топтарының құрылымы және клиент құрылғылары туралы конфигурациялық ақпарат;
- қашықтан орнатуға арналған қолданбалар 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, қолданба параметрлері);
- басқару топтарының құрылымы және клиент құрылғылары туралы конфигурациялық ақпарат;
- қашықтан орнатуға арналған қолданбалар дистрибутивтерінің қоймасы (Packages, Uninstall, Updates қалталарының мазмұны);
- Басқару сервері сертификаты.

Басқару серверінің клиенті (Клиент құрылғысы)

Желілік агент және "Лаборатория Касперского" басқарылатын қолданбалары орнатылған құрылғы, сервер немесе жұмыс станциясы.

Басқару тобы

Орындалатын функцияларға және оларға орнатылатын "Лаборатория Касперского" қолданбалар жиынтығына сәйкес біріктірілген арнайы құрылғылар. Құрылғылар оларды біртұтас құрылғы ретінде басқару ыңғайлылығы үшін топтастырылады. Топтың құрамына басқа топтар кіруі мүмкін. Топқа орнатылған әрбір қолданба үшін топтық саясаттар жасалуы және топтық тапсырмалар қалыптастырылуы мүмкін.

Басқарылатын құрылғылар

Басқару топтарының біріне қосылатын ұйым желісінің құрылғылары.

Белсенді кілт

Қолданбаның жұмысы үшін ағымдағы сәтте қолданылатын кілт.

Виртуалды Басқару сервері

Ұйым-клиенттің желісін қорғау жүйесін басқаруға арналған Kaspersky Security Center Linux қолданбасының 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.

Жалпы сертификат

Пайдаланушының ұялы құрылғысын сәйкестендіруге арналған сертификат.

Жаңарту

"Лаборатория Касперского" жаңартулар серверінен алынатын жаңа файлдарды ауыстыру немесе қосу рәсімі (дерекқор немесе қолданба модульдері).

Желілік агент

Нақты желілік түйінге орнатылған (жұмыс станциясы немесе сервер) Басқару сервері және "Лаборатория Касперского" қолданбалары арасында өзара әрекеттесуді жүргізетін Kaspersky Security Center Linux қолданбасының құрамдасы. Бұл құрамдас Microsoft Windows жүйелері үшін әзірленген барлық қолданбалар үшін бірыңғай болып табылады. UNIX операциялық жүйелері мен оларға ұқсас және macOS арналған "Лаборатория Касперского" қолданбалары 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 қауіпсіздігі қауіпсіздік қолданбалары 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 қолданбаларының болуы, лицензиялық кілттерді пайдалану, анықталған қауіптердің саны мен түрлері сияқты факторларды қамтиды.

Жергілікті тапсырма

Бөлек клиент компьютерінде анықталған және орындалатын тапсырма.

Жергілікті түрде орнату

Қауіпсіздік қолданбасының дистрибутивінен орнатуды қолмен іске қосуды немесе құрылғыға алдын ала жүктелген жарияланған орнату пакетін қолмен іске қосуды көздейтін ұйым желісінің құрылғысына қауіпсіздік қолданбасын орнату.

Ішкі пайдаланушылар

Ішкі пайдаланушы есептік жазбалары виртуалды Басқару серверлерімен жұмыс істеу үшін пайдаланылады. Kaspersky Security Center Linux қолданбасында 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 "Лаборатория Касперского" қолданбасын 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 қолданбасы ұсынатын құралдар көмегімен "Лаборатория Касперского" қолданбаларын орнату.

Қолданба параметрлері

Оның тапсырмаларының барлық түрлері үшін ортақ және жалпы қолданбаның жұмысы үшін жауапты қолданба жұмысының параметрлері: мысалы, қолданба өнімділігінің параметрлері, есептерді жүргізу параметрлері, сақтық қойманың параметрлері.

Қолданбалар дүкені

Kaspersky Security Center Linux қолданбасының құрамдасы. Қолданбалар дүкені пайдаланушылардың Android құрылғысына қолданбаларды орнату үшін пайдаланылады. Қолданбалар дүкенінде қолданбалардың apk-файлдарын және Google Play-де қолданбаларға сілтемелерді жариялауға болады.

Қолданбаны орталықтандырылған басқару

Kaspersky Security Center ұсынатын басқару қызметтері көмегімен қолданбаны қашықтан басқару.

Қолданбаны тікелей басқару

Жергілікті интерфейс арқылы қолданбаны басқару

Қолжетімді жаңарту

Құрамына белгілі кезеңде жиналған жедел жаңартулар жиынтығы және қолданба архитектурасындағы өзгерістер қосылған "Лаборатория Касперского" қолданбалар модульдерінің жаңарту бумасы.

Қолмен орнату

Қауіпсіздік қолданбасының дистрибутивінен ұйым желісінің құрылғысына қауіпсіздік қолданбасын 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 лицензиялық кілт

Қолданбаны 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 қолданба функцияларын және қосымша қызметтерді пайдалана алатын кезең. Қолжетімді функциялар мен қосымша қызметтер көлемі лицензияның түріне байланысты.

Лицензиялы қолданбалар тобы

Клиент құрылғыларында олар үшін орнатудың есебі жүргізілетін әкімші белгілеген өлшемшарттар (мысалы, өндіруші бойынша) негізінде жасалған қолданбалар тобы.

Оқиғалар қоймасы

Kaspersky Security Center Linux-те туындайтын оқиғалар туралы ақпаратты сақтауға арналған Басқару серверінің дерекқорының бөлігі.

Оқиғаның маңыздылық деңгейі

"Лаборатория Касперского" қолданбасының 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 "Лаборатория Касперского" қолданбасын қашықтан орнату үшін қалыптастырылатын файлдар жиынтығы. Орнату пакеті қолданбаны орнатуға және бірден орнатқаннан кейін оның жұмысқа қабілетін қамтамасыз етуге қажетті параметрлер жиынтығын қамтиды. Параметрлердің мәндері әдепкі бойынша қолданба параметрлерінің мәндеріне сәйкес келеді. Орнату пакеті қолданба дистрибутивінің құрамына кіретін kpd және kud кеңейтімдері бар файлдардың негізінде жасалады.

Осалдық

Зиянды қолданбалық жасақтама өндірушілері операциялық жүйеге немесе қолданбаға ену және оның тұтастығын бұзу үшін қолдана алатын операциялық жүйенің немесе қолданбаның кемшілігі. Операциялық жүйедегі көптеген осалдықтар, оның жұмысын сенімсіз етеді, өйткені операциялық жүйеге енгізілген вирустар операциялық жүйенің өзінде де, орнатылған қолданбаларда 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. "Лаборатория Касперского" 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 қолданба жұмысының параметрлерін және басқару тобының құрылғыларында орнатылған қолданбаны конфигурациялауға қатынасты анықтайды. Әр қолданба үшін өз саясатын жасау қажет. Сіз әр басқару тобындағы құрылғыларға орнатылған қолданбалар үшін көптеген саясаттар жасай аласыз, бірақ басқару тобының шегінде тек бір саясат бір уақытта әр қолданбаға пайдаланылуы мүмкін.

Тапсырма

"Лаборатория Касперского" қолданбасы орындайтын функциялар тапсырмалар түрінде іске асырылған, мысалы: Файлдарды нақты уақыт режимінде қорғау, Құрылғыны толықтай тексеру, дерекқорды жаңарту.

Тапсырма параметрлері

Әр тапсырма түрі үшін ерекше қолданба жұмысының параметрлері.

Тарату нүктесі

Жаңартуларды тарату, қолданбаларды 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 қолданба

Үшінші тараптың антивирустық қолданбасы немесе Kaspersky Security Center Linux арқылы басқаруға қолдау көрсетпейтін "Лаборатория Касперского" қолданбасы.

Үшінші тарап коды туралы ақпарат

Үшінші тарап коды туралы ақпарат қолданбаны 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, Shockwave, PostScript – бұл 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 — Apache Software Foundation компаниясының тіркелген сауда белгісі немесе сауда 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 – АҚШ пен басқа елдердің патенттік кеңсесінде тіркелген Citrix Systems, Inc және/немесе еншілес компаниялардың тауар 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 – Америка Құрама Штаттарында және басқа елдерде тіркелген Intel корпорациясының тауар 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.

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.

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.

VMware, VMware vSphere, VMware Workstation – тауар белгілері немесе АҚШ-та немесе басқа юрисдикцияларда тіркелген VMware, Inc. сауда белгілері.