MaxPatrol VM версия 2.0

Настройка источников

Дата редакции документа: 22.09.2023

Содержание

1. Об этом документе

Руководство по настройке источников содержит рекомендации по интеграции элементов IT-инфраструктуры организации с Positive Technologies MaxPatrol VM (далее также — MaxPatrol VM) для аудита активов.

Руководство адресовано специалистам, выполняющим установку и интеграцию MaxPatrol VM в организации.

Комплект документации MaxPatrol VM включает в себя следующие документы:

- Этот документ.
- Руководство по внедрению — содержит информацию для внедрения продукта в инфраструктуре организации: от типовых схем развертывания до инструкций по установке, первоначальной настройке, обновлению и удалению продукта.
- Руководство администратора — содержит справочную информацию и инструкции по настройке и администрированию продукта.
- Руководство оператора — содержит сценарии использования продукта для управления информационными активами организации.
- Синтаксис языка запроса PDQL — содержит справочную информацию и примеры синтаксиса, основных функций и операторов языка PDQL, используемых при работе с MaxPatrol VM.
- PDQL-запросы для анализа активов — содержит информацию о стандартных запросах на языке PDQL, предназначенных для проверки конфигураций активов при работе в MaxPatrol VM.
- Руководство разработчика — содержит информацию о доступных в MaxPatrol VM функциях сервиса REST API.

2. Межсетевые экраны

Раздел содержит инструкции для настройки аудита поддерживаемых в MaxPatrol VM межсетевых экранов.

В этом разделе

2.1. Cisco ASA 8, 9: настройка актива

Настройку актива нужно выполнять от имени учетной записи с правом перехода в режим глобальной конфигурации.

> **Внимание!** При использовании в IT-инфраструктуре организации межсетевого экрана или других средств для контроля сетевого трафика требуется настроить в них правила, разрешающие трафик в обоих направлениях между узлом актива и узлом MP 10 Collector. Для проведения аудита актива по протоколу SSH используется порт TCP 22.

Для проведения аудита на активе нужно создать учетную запись для доступа MP 10 Collector по протоколу SSH.

> **Внимание!** Эта инструкция разработана для аутентификации пользователей на сетевом устройстве методом Local. В этом случае данные учетных записей хранятся на самом устройстве.

Для аутентификации пользователей методом Local в файле конфигурации сетевого устройства должны присутствовать строки:

```
aaa authentication ssh console LOCAL
aaa authorization exec LOCAL auto-enable
```

> **Примечание.** Вы можете просмотреть файл конфигурации сетевого устройства, выполнив команду `show running-config`.

Для проведения аудита требуется учетная запись с уровнем привилегий 15. Для повышения привилегий до уровня 15 на сетевом устройстве должен быть разрешен переход в привилегированный режим EXEC (выполнение команды enable) после ввода пароля. Для этого в файле конфигурации сетевого устройства должна присутствовать строка:

```
aaa authorization exec LOCAL auto-enable
```

► Чтобы создать учетную запись для доступа к активу:

1. На узле, с которого производится настройка актива, запустите терминальный клиент, поддерживающий сетевые протоколы SSH и Telnet.
2. Авторизуйтесь на активе.
3. Перейдите в режим конфигурирования:
   `configure terminal`
4. Создайте учетную запись для доступа к активу:
   `username <Логин> password <Пароль> privilege 15`

   Примечание. Если для ограничения доступа к активу по протоколу SSH используется список доступа, добавьте IP-адрес узла MP 10 Collector в этот список.
5. Выйдите из режима конфигурирования:
   `end`
6. Сохраните изменения:
   `write memory`

Учетная запись создана.

2.2. Cisco ASA 8, 9: настройка MaxPatrol VM

Для проведения аудита актива по протоколу SSH в MaxPatrol VM нужно добавить учетную запись для доступа к активу, пароль для повышения привилегий (перехода в привилегированный режим EXEC) и создать задачу на проведение аудита.

В этом разделе

2.2.1. Добавление учетной записи для доступа по SSH

► Чтобы добавить в MaxPatrol VM учетную запись для доступа к активу:

1. В главном меню в разделе **Сбор данных** выберите пункт **Учетные записи**.

   Откроется страница **Учетные записи**.
2. В панели инструментов нажмите кнопку **Добавить учетную запись** и в раскрывшемся меню выберите пункт **Логин — пароль**.

   Откроется страница **Добавление учетной записи**.
3. В поле **Название** введите название учетной записи.

Примечание. В поле **Описание** вы можете ввести любой текстовый комментарий.

4. В раскрывающемся списке **Метки** установите флажок **Terminal**.
5. В поле **Логин** введите логин учетной записи.
6. В поле **Пароль** введите пароль и подтвердите его в поле **Подтверждение пароля**.
7. Нажмите кнопку **Сохранить**.

Учетная запись добавлена.

2.2.2. Добавление пароля для повышения привилегий для аудита по SSH

► Чтобы добавить в MaxPatrol VM пароль для повышения привилегий:

1. В главном меню в разделе **Сбор данных** выберите пункт **Учетные записи**.

   Откроется страница **Учетные записи**.

2. В панели инструментов нажмите кнопку **Добавить учетную запись** и в раскрывшемся меню выберите пункт **Пароль**.

   Откроется страница **Добавление учетной записи**.

3. В поле **Название** введите название учетной записи.

   Примечание. В поле **Описание** вы можете ввести любой текстовый комментарий.

4. В раскрывающемся списке **Метки** установите флажок **Terminal**.
5. В поле **Пароль** введите пароль и подтвердите его в поле **Подтверждение пароля**.
6. Нажмите кнопку **Сохранить**.

Пароль добавлен.

2.2.3. Создание задачи на аудит актива по SSH

► Чтобы создать задачу на проведение аудита актива:

1. В главном меню в разделе **Сбор данных** выберите пункт **Задачи**.

   Откроется страница **Задачи по сбору данных**.

2. В панели инструментов нажмите кнопку **Создать задачу** и в раскрывшемся меню выберите пункт **Сбор данных**.

   Откроется страница **Создание задачи на сбор данных**.

3. В поле **Название** введите название задачи.
4. Если требуется, добавьте подробное описание задачи по ссылке **Добавить описание**.

5. В раскрывающемся списке **Профиль** выберите **SSH Cisco Audit in Enable Mode**.

   Внимание! Если для доступа к активу по протоколу SSH вы используете учетную запись с уровнем привилегий 15 (не требуется повышение привилегий), для проведения аудита нужно использовать профиль SSH Network Device Audit.

6. В иерархическом списке выберите пункт **Сканирование систем** → **Через терминал: SSH и Telnet**.

7. В раскрывающемся списке **Учетная запись** выберите учетную запись для доступа к активу.

8. В раскрывающемся списке **Учетная запись для повышения привилегий** выберите учетную запись для повышения привилегий на активе.

9. Если требуется, в раскрывающемся списке **Коллекторы** выберите коллекторы для сбора данных.

10. В панели **Цели сбора данных** на вкладке **Включить** в поле **Активы** введите IP-адрес или доменное имя (в формате FQDN) узла актива.

    Примечание. В панели **Расписание** вы можете включить и настроить автоматический запуск задачи по расписанию.

11. Нажмите кнопку **Сохранить**.

Задача на проведение аудита актива создана.

2.3. FortiNet FortiGate 5.4.2, 6.0.1: настройка актива

Внимание! Эта инструкция разработана для устройств с отключенной технологией виртуальных доменов VDOM.

Настройку актива нужно выполнять от имени учетной записи администратора устройства.

Внимание! При использовании в IT-инфраструктуре организации межсетевого экрана или других средств для контроля сетевого трафика требуется настроить в них правила, разрешающие трафик в обоих направлениях между узлом актива и узлом MP 10 Collector. Для проведения аудита актива по протоколу SSH используется порт TCP 22.

Для проведения аудита на активе нужно создать учетную запись для доступа MP 10 Collector по протоколу SSH.

► Чтобы создать учетную запись для доступа к активу:

1. На узле, с которого производится настройка актива, запустите терминальный клиент, поддерживающий сетевые протоколы SSH и Telnet.

2. Авторизуйтесь на активе.

3. Перейдите в режим конфигурирования:

   ```
   config system admin
   ```

4. Создайте учетную запись для доступа к активу:

```
edit "<Логин>"
set accprofile "super_admin"
set vdom "root"
set password "<Пароль>"
```

5. Выйдите из режима конфигурирования:

```
end
```

Учетная запись создана.

2.4. FortiNet FortiGate 5.4.2, 6.0.1: настройка MaxPatrol VM

Для проведения аудита актива по протоколу SSH в MaxPatrol VM нужно добавить учетную запись для доступа к активу, создать и запустить задачу на проведение аудита.

В этом разделе

2.4.1. Добавление учетной записи для доступа по SSH

► Чтобы добавить в MaxPatrol VM учетную запись для доступа к активу:

1. В главном меню в разделе **Сбор данных** выберите пункт **Учетные записи**.

   Откроется страница **Учетные записи**.

2. В панели инструментов нажмите кнопку **Добавить учетную запись** и в раскрывшемся меню выберите пункт **Логин — пароль**.

   Откроется страница **Добавление учетной записи**.

3. В поле **Название** введите название учетной записи.

   Примечание. В поле **Описание** вы можете ввести любой текстовый комментарий.

4. В раскрывающемся списке **Метки** установите флажок **Terminal**.
5. В поле **Логин** введите логин учетной записи.
6. В поле **Пароль** введите пароль и подтвердите его в поле **Подтверждение пароля**.
7. Нажмите кнопку **Сохранить**.

Учетная запись добавлена.

2.4.2. Создание задачи на аудит актива по SSH

► Чтобы создать задачу на проведение аудита актива:

1. В главном меню в разделе **Сбор данных** выберите пункт **Задачи**.

   Откроется страница **Задачи по сбору данных**.

2. В панели инструментов нажмите кнопку **Создать задачу** и в раскрывшемся меню выберите пункт **Сбор данных**.

   Откроется страница **Создание задачи на сбор данных**.

3. В поле **Название** введите название задачи.
4. Если требуется, добавьте подробное описание задачи по ссылке **Добавить описание**.
5. В раскрывающемся списке **Профиль** выберите **SSH Network Device Audit**.
6. В иерархическом списке выберите пункт **Сканирование систем** → **Через терминал: SSH и Telnet**.
7. В раскрывающемся списке **Учетная запись** выберите учетную запись для доступа к активу.
8. Если требуется, в раскрывающемся списке **Коллекторы** выберите коллекторы для сбора данных.
9. В панели **Цели сбора данных** на вкладке **Включить** в поле **Активы** введите IP-адрес или доменное имя (в формате FQDN) узла актива.

   Примечание. В панели **Расписание** вы можете включить и настроить автоматический запуск задачи по расписанию.

10. Нажмите кнопку **Сохранить**.

Задача на проведение аудита актива создана.

3. Операционные системы

Раздел содержит инструкции для настройки аудита поддерживаемых в MaxPatrol VM операционных систем.

В этом разделе

3.1. «Базальт СПО». «Альт 8 СП», «Альт Рабочая станция» 9, 10: настройка актива

Настройку актива нужно выполнять от имени учетной записи root.

Внимание! При использовании в IT-инфраструктуре организации межсетевого экрана или других средств для контроля сетевого трафика требуется настроить в них правила, разрешающие трафик в обоих направлениях между узлом актива и узлом MP 10 Collector. Для проведения аудита актива по протоколу SSH используется порт TCP 22.

Внимание! На узле актива должна быть установлена программа sudo.

Для проведения аудита на активе нужно:

1. Создать учетную запись пользователя ОС для доступа MP 10 Collector к активу. В домашнем каталоге учетной записи создать каталог `bin` для файлов сценариев.

   Примечание. Данные этой учетной записи нужно указать при добавлении учетной записи в MaxPatrol VM.

2. Поместить в каталог `bin` файлы сценариев для проведения аудита. В домашний каталог созданной учетной записи поместить файл `.bash_profile` с параметрами переменной окружения `$PATH`.

   Примечание. В комплект поставки MaxPatrol VM входит архив `audit_sudo_wrappers.tar`. В этом архиве, в папках с названиями операционных систем, находятся файлы сценариев (в архиве `bin.tar`) и файлы `.bash_profile`.

3. Настроить программу sudo и предоставить созданной учетной записи права на выполнение команд для запуска сценариев.

В этом разделе

3.1.1. Создание учетной записи ОС

► Чтобы создать и настроить учетную запись:

1. Создайте учетную запись и укажите для нее пароль:
   ```
   useradd -m -g users -s /bin/bash <Логин>
   passwd <Логин>
   <Пароль>
   ```
2. Настройте права доступа к домашнему каталогу:
   ```
   chmod 700 /home/<Логин>
   ```
3. Авторизуйтесь под именем созданной учетной записи:
   ```
   su - <Логин>
   <Пароль>
   ```

Учетная запись создана.

3.1.2. Подготовка сценариев для аудита

► Чтобы подготовить сценарии для проведения аудита:

1. Перенесите архив `bin.tar`, входящий в комплект поставки MaxPatrol VM, в домашний каталог созданной учетной записи.
2. Перейдите в домашний каталог:
   ```
   cd /home/<Логин>
   ```
3. Создайте каталог `/home/<Логин>/bin`:
   ```
   mkdir ~/bin
   ```
4. Распакуйте архив:
   ```
   tar -xf bin.tar
   ```
5. Настройте права доступа к каталогу:
   ```
   chmod 700 -R ~/bin
   ```
6. Удалите архив:
   ```
   rm bin.tar
   ```
7. Перенесите файл `.bash_profile` в домашний каталог.

   Примечание. Вы можете просмотреть список каталогов в переменной окружения `$PATH`, выполнив команду `echo $PATH`. Название каталога `/home/<Логин>/bin` должно располагаться первым в списке на экране.

Сценарии для аудита подготовлены.

3.1.3. Настройка программы sudo

► Чтобы настроить программу sudo:

1. Откройте для изменения файл `/etc/sudoers`:
   ```
   visudo
   ```
2. Добавьте в файл строки с псевдонимами для сценариев:
   ```
   Cmnd_Alias MPROOTCMD = /usr/bin/at -l, /usr/bin/crontab * -l, /sbin/fdisk -l, /sbin/iptables-save, /bin/netstat, /usr/sbin/ss, /usr/sbin/dmidecode, /sbin/vgdisplay, /sbin/lvdisplay, /sbin/auditctl -[lv]
   Cmnd_Alias MPFILECMD = /bin/cat, /usr/bin/find *, /bin/ls, /usr/bin/getfacl, /usr/bin/test
   Cmnd_Alias MPEXCPTNSCMD = !/usr/bin/find *-exec*, !/usr/bin/find *-fprint*, !/usr/bin/find *-ok*, !/usr/bin/find *-delete*, !/usr/bin/find *-fls*, !/usr/sbin/ss *--diag*, !/usr/sbin/ss *-D*, !/usr/sbin/dmidecode *--dump*
   ```
3. Добавьте в файл строки, предоставляющие учетной записи права на выполнение команд для запуска сценариев:
   ```
   mpuser ALL = (ALL) NOPASSWD: MPROOTCMD
   mpuser ALL = (ALL) NOPASSWD: MPFILECMD
   mpuser ALL = (ALL) NOPASSWD: MPEXCPTNSCMD
   ```
4. Если в файле отсутствует строка с директивой `Defaults env_reset`, добавьте ее:
   ```
   Defaults env_reset
   ```
5. Если в файле есть строка с директивой `Defaults env_keep` и она содержит переменную окружения `PATH`, удалите эту переменную из строки (или всю строку, если переменная единственная).
6. Сохраните изменения и закройте файл.

Программа sudo настроена.

3.2. «Базальт СПО». «Альт 8 СП», «Альт Рабочая станция» 9, 10: настройка MaxPatrol VM

Для аудита актива в MaxPatrol VM нужно добавить учетную запись для доступа к активу, создать и запустить задачу на проведение аудита с профилем Unix Audit.

В этом разделе

3.2.1. Добавление учетной записи

► Чтобы добавить в MaxPatrol VM учетную запись для доступа к активу:

1. В главном меню в разделе **Сбор данных** выберите пункт **Учетные записи**.

Откроется страница **Учетные записи**.

2. В панели инструментов нажмите кнопку **Добавить учетную запись** и в раскрывшемся меню выберите пункт **Логин — пароль**.

   Откроется страница **Добавление учетной записи**.

3. В поле **Название** введите название учетной записи.

   Примечание. В поле **Описание** вы можете ввести любой текстовый комментарий.

4. В поле **Логин** введите логин учетной записи.
5. В поле **Пароль** введите пароль и подтвердите его в поле **Подтверждение пароля**.
6. Нажмите кнопку **Сохранить**.

Учетная запись добавлена.

3.2.2. Создание и запуск задачи на аудит актива

► Чтобы создать и запустить задачу на проведение аудита актива:

1. В главном меню в разделе **Сбор данных** выберите пункт **Задачи**.

   Откроется страница **Задачи по сбору данных**.

2. В панели инструментов нажмите кнопку **Создать задачу** и в раскрывшемся меню выберите пункт **Сбор данных**.

   Откроется страница **Создание задачи на сбор данных**.

3. В поле **Название** введите название задачи.
4. Если требуется, добавьте подробное описание задачи по ссылке **Добавить описание**.
5. В раскрывающемся списке **Профиль** выберите **Unix Audit**.
6. В иерархическом списке выберите пункт **Сканирование систем** → **Через терминал: SSH**.
7. В раскрывающемся списке **Учетная запись** выберите учетную запись для доступа к активу.
8. Если требуется, в раскрывающемся списке **Коллекторы** выберите коллекторы для сбора данных.
9. В панели **Цели сбора данных** на вкладке **Включить** в поле **Активы** введите IP-адрес или доменное имя (в формате FQDN) узла актива.

   Примечание. В панели **Расписание** вы можете включить и настроить автоматический запуск задачи по расписанию.

10. Нажмите кнопку **Сохранить и запустить**.

Задача на проведение аудита актива создана и запущена.

3.3. «РЕД СОФТ». «РЕД ОС» 7.1—7.3: настройка актива

Настройку актива нужно выполнять от имени учетной записи root.

Внимание! При использовании в IT-инфраструктуре организации межсетевого экрана или других средств для контроля сетевого трафика требуется настроить в них правила, разрешающие трафик в обоих направлениях между узлом актива и узлом MP 10 Collector. Для проведения аудита актива по протоколу SSH используется порт TCP 22.

Внимание! На узле актива должна быть установлена программа sudo.

Для проведения аудита на активе нужно:

1. Создать учетную запись пользователя ОС для доступа MP 10 Collector к активу. В домашнем каталоге учетной записи создать каталог `bin` для файлов сценариев.

   Примечание. Данные этой учетной записи нужно указать при добавлении учетной записи в MaxPatrol VM.

2. Поместить в каталог `bin` файлы сценариев для проведения аудита. В домашний каталог созданной учетной записи поместить файл `.bash_profile` с параметрами переменной окружения `$PATH`.

   Примечание. В комплект поставки MaxPatrol VM входит архив `audit_sudo_wrappers.tar`. В этом архиве, в папках с названиями операционных систем, находятся файлы сценариев (в архиве `bin.tar`) и файлы `.bash_profile`.

3. Настроить программу sudo и предоставить созданной учетной записи права на выполнение команд для запуска сценариев.

В этом разделе

3.3.1. Создание учетной записи ОС

► Чтобы создать и настроить учетную запись:

1. Создайте учетную запись и укажите для нее пароль:
   ```
   useradd -m -g users -s /bin/bash <Логин>
   passwd <Логин>
   <Пароль>
   ```
2. Настройте права доступа к домашнему каталогу:
   ```
   chmod 700 /home/<Логин>
   ```
3. Авторизуйтесь под именем созданной учетной записи:
   ```
   su - <Логин>
   <Пароль>
   ```

Учетная запись создана.

3.3.2. Подготовка сценариев для аудита

► Чтобы подготовить сценарии для проведения аудита:

1. Перенесите архив `bin.tar`, входящий в комплект поставки MaxPatrol VM, в домашний каталог созданной учетной записи.
2. Перейдите в домашний каталог:
   ```
   cd /home/<Логин>
   ```
3. Создайте каталог `/home/<Логин>/bin`:
   ```
   mkdir ~/bin
   ```
4. Распакуйте архив:
   ```
   tar -xf bin.tar
   ```
5. Настройте права доступа к каталогу:
   ```
   chmod 700 -R ~/bin
   ```
6. Удалите архив:
   ```
   rm bin.tar
   ```
7. Перенесите файл `.bash_profile` в домашний каталог.

   Примечание. Вы можете просмотреть список каталогов в переменной окружения `$PATH`, выполнив команду `echo $PATH`. Название каталога `/home/<Логин>/bin` должно располагаться первым в списке на экране.

Сценарии для аудита подготовлены.

3.3.3. Настройка программы sudo

► Чтобы настроить программу sudo:

1. Откройте для изменения файл `/etc/sudoers`:
   ```
   visudo
   ```
2. Добавьте в файл строки с псевдонимами для сценариев:
   ```
   Cmnd_Alias MPROOTCMD = /usr/bin/at -l, /usr/bin/crontab * -l, /usr/sbin/fdisk -l, /usr/sbin/iptables-save, /usr/bin/netstat, /usr/sbin/ss, /usr/sbin/dmidecode, /usr/sbin/vgdisplay, /usr/sbin/lvdisplay, /usr/sbin/auditctl -[vl], /usr/sbin/grubby --info ALL
   Cmnd_Alias MPFILECMD = /usr/bin/egrep, /usr/bin/cat, /usr/bin/find *, /usr/bin/ls, /usr/bin/getfacl, /usr/bin/test
   Cmnd_Alias MPEXCPTNSCMD = !/usr/bin/find *-exec*, !/usr/bin/find *-fprint*, !/usr/bin/find *-ok*, !/usr/bin/find *-delete*, !/usr/bin/find *-fls*, !/usr/sbin/ss *--diag*, !/usr/sbin/ss *-D*, !/usr/sbin/dmidecode *--dump*
   ```
3. Добавьте в файл строки, предоставляющие учетной записи права на выполнение команд для запуска сценариев:
   ```
   mpuser ALL = (ALL) NOPASSWD: MPROOTCMD
   mpuser ALL = (ALL) NOPASSWD: MPFILECMD
   mpuser ALL = (ALL) NOPASSWD: MPEXCPTNSCMD
   ```
4. Если в файле отсутствует строка с директивой `Defaults env_reset`, добавьте ее:
   ```
   Defaults env_reset
   ```
5. Если в файле есть строка с директивой `Defaults env_keep` и она содержит переменную окружения `PATH`, удалите эту переменную из строки (или всю строку, если переменная единственная).
6. Сохраните изменения и закройте файл.

Программа sudo настроена.

3.4. «РЕД СОФТ». «РЕД ОС» 7.1—7.3: настройка MaxPatrol VM

Для аудита актива в MaxPatrol VM нужно добавить учетную запись для доступа к активу, создать и запустить задачу на проведение аудита с профилем Unix Audit.

В этом разделе

3.4.1. Добавление учетной записи

► Чтобы добавить в MaxPatrol VM учетную запись для доступа к активу:

1. В главном меню в разделе **Сбор данных** выберите пункт **Учетные записи**.

   Откроется страница **Учетные записи**.

2. В панели инструментов нажмите кнопку **Добавить учетную запись** и в раскрывшемся меню выберите пункт **Логин — пароль**.

   Откроется страница **Добавление учетной записи**.

3. В поле **Название** введите название учетной записи.

   Примечание. В поле **Описание** вы можете ввести любой текстовый комментарий.

4. В поле **Логин** введите логин учетной записи.
5. В поле **Пароль** введите пароль и подтвердите его в поле **Подтверждение пароля**.
6. Нажмите кнопку **Сохранить**.

Учетная запись добавлена.

3.4.2. Создание и запуск задачи на аудит актива

► Чтобы создать и запустить задачу на проведение аудита актива:

1. В главном меню в разделе **Сбор данных** выберите пункт **Задачи**.

   Откроется страница **Задачи по сбору данных**.

2. В панели инструментов нажмите кнопку **Создать задачу** и в раскрывшемся меню выберите пункт **Сбор данных**.

   Откроется страница **Создание задачи на сбор данных**.

3. В поле **Название** введите название задачи.
4. Если требуется, добавьте подробное описание задачи по ссылке **Добавить описание**.
5. В раскрывающемся списке **Профиль** выберите **Unix Audit**.
6. В иерархическом списке выберите пункт **Сканирование систем** → **Через терминал: SSH**.
7. В раскрывающемся списке **Учетная запись** выберите учетную запись для доступа к активу.
8. Если требуется, в раскрывающемся списке **Коллекторы** выберите коллекторы для сбора данных.
9. В панели **Цели сбора данных** на вкладке **Включить** в поле **Активы** введите IP-адрес или доменное имя (в формате FQDN) узла актива.

Примечание. В панели **Расписание** вы можете включить и настроить автоматический запуск задачи по расписанию.

10. Нажмите кнопку **Сохранить и запустить**.

Задача на проведение аудита актива создана и запущена.

3.5. Canonical Ubuntu 16.04, 18.04, 20.04, 22.04: настройка актива

Настройку актива нужно выполнять от имени учетной записи root.

Внимание! При использовании в IT-инфраструктуре организации межсетевого экрана или других средств для контроля сетевого трафика требуется настроить в них правила, разрешающие трафик в обоих направлениях между узлом актива и узлом MP 10 Collector. Для проведения аудита актива по протоколу SSH используется порт TCP 22.

Внимание! На узле актива должна быть установлена программа sudo.

Для проведения аудита на активе нужно:

1. Создать учетную запись пользователя ОС для доступа MP 10 Collector к активу. В домашнем каталоге учетной записи создать каталог `bin` для файлов сценариев.

   Примечание. Данные этой учетной записи нужно указать при добавлении учетной записи в MaxPatrol VM.

2. Поместить в каталог `bin` файлы сценариев для проведения аудита. В домашний каталог созданной учетной записи поместить файл `.bash_profile` с параметрами переменной окружения `$PATH`.

   Примечание. В комплект поставки MaxPatrol VM входит архив `audit_sudo_wrappers.tar`. В этом архиве, в папках с названиями операционных систем, находятся файлы сценариев (в архиве `bin.tar`) и файлы `.bash_profile`.

3. Настроить программу sudo и предоставить созданной учетной записи права на выполнение команд для запуска сценариев.

В этом разделе

3.5.1. Создание учетной записи ОС

► Чтобы создать и настроить учетную запись:

1. Создайте учетную запись и укажите для нее пароль:
   ```
   useradd -m -g users -s /bin/bash <Логин>
   passwd <Логин>
   <Пароль>
   ```
2. Настройте права доступа к домашнему каталогу:
   ```
   chmod 700 /home/<Логин>
   ```
3. Авторизуйтесь под именем созданной учетной записи:
   ```
   su - <Логин>
   <Пароль>
   ```

Учетная запись создана.

3.5.2. Подготовка сценариев для аудита

► Чтобы подготовить сценарии для проведения аудита:

1. Перенесите архив `bin.tar`, входящий в комплект поставки MaxPatrol VM, в домашний каталог созданной учетной записи.
2. Перейдите в домашний каталог:
   ```
   cd /home/<Логин>
   ```
3. Создайте каталог `/home/<Логин>/bin`:
   ```
   mkdir ~/bin
   ```
4. Распакуйте архив:
   ```
   tar -xf bin.tar
   ```
5. Настройте права доступа к каталогу:
   ```
   chmod 700 -R ~/bin
   ```
6. Удалите архив:
   ```
   rm bin.tar
   ```
7. Перенесите файл `.bash_profile` в домашний каталог.

   Примечание. Вы можете просмотреть список каталогов в переменной окружения `$PATH`, выполнив команду `echo $PATH`. Название каталога `/home/<Логин>/bin` должно располагаться первым в списке на экране.

Сценарии для аудита подготовлены.

3.5.3. Настройка программы sudo

► Чтобы настроить программу sudo:

1. Откройте для изменения файл `/etc/sudoers`:
   ```
   visudo
   ```
2. Добавьте в файл строки с псевдонимами для сценариев:
   ```
   Cmnd_Alias MPROOTCMD = /usr/bin/at -l, /usr/bin/crontab * -l, /sbin/fdisk -l, /sbin/iptables-save, /bin/netstat, /bin/ss, /usr/sbin/dmidecode, /sbin/vgdisplay, /sbin/lvdisplay, /sbin/auditctl -[vl]
   Cmnd_Alias MPFILECMD = /bin/cat, /usr/bin/find *, /bin/ls, /usr/bin/getfacl, /usr/bin/test
   Cmnd_Alias MPEXCPTNSCMD = !/usr/bin/find *-exec*, !/usr/bin/find *-fprint*, !/usr/bin/find *-ok*, !/usr/bin/find *-delete*, !/usr/bin/find *-fls*, !/bin/ss *--diag*, !/bin/ss *-D*, !/usr/sbin/dmidecode *--dump*
   ```
3. Добавьте в файл строки, предоставляющие учетной записи права на выполнение команд для запуска сценариев:
   ```
   <Логин> ALL = (ALL) NOPASSWD: MPROOTCMD
   <Логин> ALL = (ALL) NOPASSWD: MPFILECMD
   <Логин> ALL = (ALL) NOPASSWD: MPEXCPTNSCMD
   ```
4. Если в файле отсутствует строка с директивой `Defaults env_reset`, добавьте ее:
   ```
   Defaults env_reset
   ```
5. Если в файле есть строка с директивой `Defaults env_keep` и она содержит переменную окружения `PATH`, удалите эту переменную из строки (или всю строку, если переменная единственная).
6. Сохраните изменения и закройте файл.

Программа sudo настроена.

3.6. Canonical Ubuntu 16.04, 18.04, 20.04, 22.04: настройка MaxPatrol VM

Для аудита актива в MaxPatrol VM нужно добавить учетную запись для доступа к активу, создать и запустить задачу на проведение аудита с профилем Unix Audit.

В этом разделе

3.6.1. Добавление учетной записи

► Чтобы добавить в MaxPatrol VM учетную запись для доступа к активу:

1. В главном меню в разделе **Сбор данных** выберите пункт **Учетные записи**.

Откроется страница **Учетные записи**.

2. В панели инструментов нажмите кнопку **Добавить учетную запись** и в раскрывшемся меню выберите пункт **Логин — пароль**.

   Откроется страница **Добавление учетной записи**.

3. В поле **Название** введите название учетной записи.

   Примечание. В поле **Описание** вы можете ввести любой текстовый комментарий.

4. В поле **Логин** введите логин учетной записи.
5. В поле **Пароль** введите пароль и подтвердите его в поле **Подтверждение пароля**.
6. Нажмите кнопку **Сохранить**.

Учетная запись добавлена.

3.6.2. Создание и запуск задачи на аудит актива

► Чтобы создать и запустить задачу на проведение аудита актива:

1. В главном меню в разделе **Сбор данных** выберите пункт **Задачи**.

   Откроется страница **Задачи по сбору данных**.

2. В панели инструментов нажмите кнопку **Создать задачу** и в раскрывшемся меню выберите пункт **Сбор данных**.

   Откроется страница **Создание задачи на сбор данных**.

3. В поле **Название** введите название задачи.
4. Если требуется, добавьте подробное описание задачи по ссылке **Добавить описание**.
5. В раскрывающемся списке **Профиль** выберите **Unix Audit**.
6. В иерархическом списке выберите пункт **Сканирование систем** → **Через терминал: SSH**.
7. В раскрывающемся списке **Учетная запись** выберите учетную запись для доступа к активу.
8. Если требуется, в раскрывающемся списке **Коллекторы** выберите коллекторы для сбора данных.
9. В панели **Цели сбора данных** на вкладке **Включить** в поле **Активы** введите IP-адрес или доменное имя (в формате FQDN) узла актива.

   Примечание. В панели **Расписание** вы можете включить и настроить автоматический запуск задачи по расписанию.

10. Нажмите кнопку **Сохранить и запустить**.

Задача на проведение аудита актива создана и запущена.

3.7. CentOS 6, 7: настройка актива

Настройку актива нужно выполнять от имени учетной записи root.

Внимание! При использовании в IT-инфраструктуре организации межсетевого экрана или других средств для контроля сетевого трафика требуется настроить в них правила, разрешающие трафик в обоих направлениях между узлом актива и узлом MP 10 Collector. Для проведения аудита актива по протоколу SSH используется порт TCP 22.

Внимание! На узле актива должна быть установлена программа sudo.

Для проведения аудита на активе нужно:

1. Создать учетную запись пользователя ОС для доступа MP 10 Collector к активу. В домашнем каталоге учетной записи создать каталог `bin` для файлов сценариев.

   Примечание. Данные этой учетной записи нужно указать при добавлении учетной записи в MaxPatrol VM.

2. Поместить в каталог `bin` файлы сценариев для проведения аудита. В домашний каталог созданной учетной записи поместить файл `.bash_profile` с параметрами переменной окружения `$PATH`.

   Примечание. В комплект поставки MaxPatrol VM входит архив `audit_sudo_wrappers.tar`. В этом архиве, в папках с названиями операционных систем, находятся файлы сценариев (в архиве `bin.tar`) и файлы `.bash_profile`.

3. Настроить программу sudo и предоставить созданной учетной записи права на выполнение команд для запуска сценариев.

В этом разделе

3.7.1. Создание учетной записи ОС

► Чтобы создать и настроить учетную запись:

1. Создайте учетную запись и укажите для нее пароль:
   ```
   useradd -m -g users -s /bin/bash <Логин>
   passwd <Логин>
   <Пароль>
   ```
2. Настройте права доступа к домашнему каталогу:
   ```
   chmod 700 /home/<Логин>
   ```
3. Авторизуйтесь под именем созданной учетной записи:
   ```
   su - <Логин>
   <Пароль>
   ```

Учетная запись создана.

3.7.2. Подготовка сценариев для аудита

► Чтобы подготовить сценарии для проведения аудита:

1. Перенесите архив `bin.tar`, входящий в комплект поставки MaxPatrol VM, в домашний каталог созданной учетной записи.
2. Перейдите в домашний каталог:
   ```
   cd /home/<Логин>
   ```
3. Создайте каталог `/home/<Логин>/bin`:
   ```
   mkdir ~/bin
   ```
4. Распакуйте архив:
   ```
   tar -xf bin.tar
   ```
5. Настройте права доступа к каталогу:
   ```
   chmod 700 -R ~/bin
   ```
6. Удалите архив:
   ```
   rm bin.tar
   ```
7. Перенесите файл `.bash_profile` в домашний каталог.

   Примечание. Вы можете просмотреть список каталогов в переменной окружения `$PATH`, выполнив команду `echo $PATH`. Название каталога `/home/<Логин>/bin` должно располагаться первым в списке на экране.

Сценарии для аудита подготовлены.

3.7.3. Настройка программы sudo

► Чтобы настроить программу sudo:

1. Откройте для изменения файл `/etc/sudoers`:
   ```
   visudo
   ```
2. Добавьте в файл строки с псевдонимами для сценариев:
   ```
   Cmnd_Alias MPROOTCMD = /usr/bin/at -l, /usr/bin/crontab * -l, /sbin/fdisk -l, /sbin/iptables-save, /bin/netstat, /usr/sbin/ss, /usr/sbin/dmidecode, /sbin/vgdisplay, /sbin/lvdisplay, /sbin/auditctl -[lv], /sbin/grubby --info ALL
   Cmnd_Alias MPFILECMD = /bin/egrep, /bin/cat, /usr/bin/find *, /bin/ls, /usr/bin/getfacl, /usr/bin/test
   Cmnd_Alias MPEXCPTNSCMD = !/usr/bin/find *-exec*, !/usr/bin/find *-fprint*, !/usr/bin/find *-ok*, !/usr/bin/find *-delete*, !/usr/bin/find *-fls*, !/usr/sbin/ss *--diag*, !/usr/sbin/ss *-D*, !/usr/sbin/dmidecode *--dump*
   ```
3. Добавьте в файл строки, предоставляющие учетной записи права на выполнение команд для запуска сценариев:
   ```
   <Логин> ALL = (ALL) NOPASSWD: MPROOTCMD
   <Логин> ALL = (ALL) NOPASSWD: MPFILECMD
   <Логин> ALL = (ALL) NOPASSWD: MPEXCPTNSCMD
   ```
4. Если в файле отсутствует строка с директивой `Defaults env_reset`, добавьте ее:
   ```
   Defaults env_reset
   ```
5. Если в файле есть строка с директивой `Defaults env_keep` и она содержит переменную окружения `PATH`, удалите эту переменную из строки (или всю строку, если переменная единственная).
6. Сохраните изменения и закройте файл.

Программа sudo настроена.

3.8. CentOS 6, 7: настройка MaxPatrol VM

Для аудита актива в MaxPatrol VM нужно добавить учетную запись для доступа к активу, создать и запустить задачу на проведение аудита с профилем Unix Audit.

В этом разделе

3.8.1. Добавление учетной записи

► Чтобы добавить в MaxPatrol VM учетную запись для доступа к активу:

1. В главном меню в разделе **Сбор данных** выберите пункт **Учетные записи**.

Откроется страница **Учетные записи**.

2. В панели инструментов нажмите кнопку **Добавить учетную запись** и в раскрывшемся меню выберите пункт **Логин — пароль**.

   Откроется страница **Добавление учетной записи**.

3. В поле **Название** введите название учетной записи.

   Примечание. В поле **Описание** вы можете ввести любой текстовый комментарий.

4. В поле **Логин** введите логин учетной записи.
5. В поле **Пароль** введите пароль и подтвердите его в поле **Подтверждение пароля**.
6. Нажмите кнопку **Сохранить**.

Учетная запись добавлена.

3.8.2. Создание и запуск задачи на аудит актива

► Чтобы создать и запустить задачу на проведение аудита актива:

1. В главном меню в разделе **Сбор данных** выберите пункт **Задачи**.

   Откроется страница **Задачи по сбору данных**.

2. В панели инструментов нажмите кнопку **Создать задачу** и в раскрывшемся меню выберите пункт **Сбор данных**.

   Откроется страница **Создание задачи на сбор данных**.

3. В поле **Название** введите название задачи.
4. Если требуется, добавьте подробное описание задачи по ссылке **Добавить описание**.
5. В раскрывающемся списке **Профиль** выберите **Unix Audit**.
6. В иерархическом списке выберите пункт **Сканирование систем** → **Через терминал: SSH**.
7. В раскрывающемся списке **Учетная запись** выберите учетную запись для доступа к активу.
8. Если требуется, в раскрывающемся списке **Коллекторы** выберите коллекторы для сбора данных.
9. В панели **Цели сбора данных** на вкладке **Включить** в поле **Активы** введите IP-адрес или доменное имя (в формате FQDN) узла актива.

   Примечание. В панели **Расписание** вы можете включить и настроить автоматический запуск задачи по расписанию.

10. Нажмите кнопку **Сохранить и запустить**.

Задача на проведение аудита актива создана и запущена.

3.9. Debian 9, 10: настройка актива

Настройку актива нужно выполнять от имени учетной записи root.

Внимание! При использовании в IT-инфраструктуре организации межсетевого экрана или других средств для контроля сетевого трафика требуется настроить в них правила, разрешающие трафик в обоих направлениях между узлом актива и узлом MP 10 Collector. Для проведения аудита актива по протоколу SSH используется порт TCP 22.

Внимание! На узле актива должна быть установлена программа sudo.

Для проведения аудита на активе нужно:

1. Создать учетную запись пользователя ОС для доступа MP 10 Collector к активу. В домашнем каталоге учетной записи создать каталог `bin` для файлов сценариев.

   Примечание. Данные этой учетной записи нужно указать при добавлении учетной записи в MaxPatrol VM.

2. Поместить в каталог `bin` файлы сценариев для проведения аудита. В домашний каталог созданной учетной записи поместить файл `.bash_profile` с параметрами переменной окружения `$PATH`.

   Примечание. В комплект поставки MaxPatrol VM входит архив `audit_sudo_wrappers.tar`. В этом архиве, в папках с названиями операционных систем, находятся файлы сценариев (в архиве `bin.tar`) и файлы `.bash_profile`.

3. Настроить программу sudo и предоставить созданной учетной записи права на выполнение команд для запуска сценариев.

В этом разделе

3.9.1. Создание учетной записи ОС

► Чтобы создать и настроить учетную запись:

1. Создайте учетную запись и укажите для нее пароль:
   ```
   useradd -m -g users -s /bin/bash <Логин>
   passwd <Логин>
   <Пароль>
   ```
2. Настройте права доступа к домашнему каталогу:
   ```
   chmod 700 /home/<Логин>
   ```
3. Авторизуйтесь под именем созданной учетной записи:
   ```
   su - <Логин>
   <Пароль>
   ```

Учетная запись создана.

3.9.2. Подготовка сценариев для аудита

► Чтобы подготовить сценарии для проведения аудита:

1. Перенесите архив `bin.tar`, входящий в комплект поставки MaxPatrol VM, в домашний каталог созданной учетной записи.
2. Перейдите в домашний каталог:
   ```
   cd /home/<Логин>
   ```
3. Создайте каталог `/home/<Логин>/bin`:
   ```
   mkdir ~/bin
   ```
4. Распакуйте архив:
   ```
   tar -xf bin.tar
   ```
5. Настройте права доступа к каталогу:
   ```
   chmod 700 -R ~/bin
   ```
6. Удалите архив:
   ```
   rm bin.tar
   ```
7. Перенесите файл `.bash_profile` в домашний каталог.

   Примечание. Вы можете просмотреть список каталогов в переменной окружения `$PATH`, выполнив команду `echo $PATH`. Название каталога `/home/<Логин>/bin` должно располагаться первым в списке на экране.

Сценарии для аудита подготовлены.

3.9.3. Настройка программы sudo

► Чтобы настроить программу sudo:

1. Откройте для изменения файл `/etc/sudoers`:
   ```
   visudo
   ```
2. Добавьте в файл строки с псевдонимами для сценариев:
   ```
   Cmnd_Alias MPROOTCMD = /usr/bin/at -l, /usr/bin/crontab * -l, /sbin/fdisk -l, /sbin/iptables-save, /bin/netstat, /bin/ss, /usr/sbin/dmidecode, /sbin/vgdisplay, /sbin/lvdisplay, /sbin/auditctl -[lv]
   Cmnd_Alias MPFILECMD = /bin/cat, /usr/bin/find *, /bin/ls, /usr/bin/getfacl, /usr/bin/test
   Cmnd_Alias MPEXCPTNSCMD = !/usr/bin/find *-exec*, !/usr/bin/find *-fprint*, !/usr/bin/find *-ok*, !/usr/bin/find *-delete*, !/usr/bin/find *-fls*, !/bin/ss *--diag*, !/bin/ss *-D*, !/usr/sbin/dmidecode *-dump*
   ```
3. Добавьте в файл строки, предоставляющие учетной записи права на выполнение команд для запуска сценариев:
   ```
   <Логин> ALL = (ALL) NOPASSWD: MPROOTCMD
   <Логин> ALL = (ALL) NOPASSWD: MPFILECMD
   <Логин> ALL = (ALL) NOPASSWD: MPEXCPTNSCMD
   ```
4. Если в файле отсутствует строка с директивой `Defaults env_reset`, добавьте ее:
   ```
   Defaults env_reset
   ```
5. Если в файле есть строка с директивой `Defaults env_keep` и она содержит переменную окружения `PATH`, удалите эту переменную из строки (или всю строку, если переменная единственная).
6. Сохраните изменения и закройте файл.

Программа sudo настроена.

3.10. Debian 9, 10: настройка MaxPatrol VM

Для аудита актива в MaxPatrol VM нужно добавить учетную запись для доступа к активу, создать и запустить задачу на проведение аудита с профилем Unix Audit.

В этом разделе

3.10.1. Добавление учетной записи

► Чтобы добавить в MaxPatrol VM учетную запись для доступа к активу:

1. В главном меню в разделе **Сбор данных** выберите пункт **Учетные записи**.

Откроется страница **Учетные записи**.

2. В панели инструментов нажмите кнопку **Добавить учетную запись** и в раскрывшемся меню выберите пункт **Логин — пароль**.

   Откроется страница **Добавление учетной записи**.

3. В поле **Название** введите название учетной записи.

   Примечание. В поле **Описание** вы можете ввести любой текстовый комментарий.

4. В поле **Логин** введите логин учетной записи.
5. В поле **Пароль** введите пароль и подтвердите его в поле **Подтверждение пароля**.
6. Нажмите кнопку **Сохранить**.

Учетная запись добавлена.

3.10.2. Создание и запуск задачи на аудит актива

► Чтобы создать и запустить задачу на проведение аудита актива:

1. В главном меню в разделе **Сбор данных** выберите пункт **Задачи**.

   Откроется страница **Задачи по сбору данных**.

2. В панели инструментов нажмите кнопку **Создать задачу** и в раскрывшемся меню выберите пункт **Сбор данных**.

   Откроется страница **Создание задачи на сбор данных**.

3. В поле **Название** введите название задачи.
4. Если требуется, добавьте подробное описание задачи по ссылке **Добавить описание**.
5. В раскрывающемся списке **Профиль** выберите **Unix Audit**.
6. В иерархическом списке выберите пункт **Сканирование систем** → **Через терминал: SSH**.
7. В раскрывающемся списке **Учетная запись** выберите учетную запись для доступа к активу.
8. Если требуется, в раскрывающемся списке **Коллекторы** выберите коллекторы для сбора данных.
9. В панели **Цели сбора данных** на вкладке **Включить** в поле **Активы** введите IP-адрес или доменное имя (в формате FQDN) узла актива.

   Примечание. В панели **Расписание** вы можете включить и настроить автоматический запуск задачи по расписанию.

10. Нажмите кнопку **Сохранить и запустить**.

Задача на проведение аудита актива создана и запущена.

3.11. FreeBSD 11, 12: настройка актива

Настройку актива нужно выполнять от имени учетной записи root.

Внимание! При использовании в IT-инфраструктуре организации межсетевого экрана или других средств для контроля сетевого трафика требуется настроить в них правила, разрешающие трафик в обоих направлениях между узлом актива и узлом MP 10 Collector. Для проведения аудита актива по протоколу SSH используется порт TCP 22.

Внимание! На узле актива должна быть установлена программа sudo.

Для проведения аудита на активе нужно:

1. Создать учетную запись пользователя ОС для доступа MP 10 Collector к активу. В домашнем каталоге учетной записи создать каталог `bin` для файлов сценариев.

   Примечание. Данные этой учетной записи нужно указать при добавлении учетной записи в MaxPatrol VM.

2. Поместить в каталог `bin` файлы сценариев для проведения аудита. В домашний каталог созданной учетной записи поместить файл `.bash_profile` (или `.profile`) с параметрами переменной окружения `$PATH`.

   Примечание. В комплект поставки MaxPatrol VM входит архив `audit_sudo_wrappers.tar`. В этом архиве, в папках с названиями операционных систем, находятся файлы сценариев (в архиве `bin.tar`) и файлы `.bash_profile` (`.profile`).

3. Настроить программу sudo и предоставить созданной учетной записи права на выполнение команд для запуска сценариев.

В этом разделе

3.11.1. Создание учетной записи ОС

► Чтобы создать и настроить учетную запись:

1. Создайте учетную запись и укажите для нее пароль:

```
adduser
Login: <Логин>
Shell: sh
Home directory: /home/<Логин>
```

```
Password: empty - no, random - no
<Пароль>
```

2. Настройте права доступа к домашнему каталогу:
   ```
   chmod 700 /home/<Логин>
   ```
3. Авторизуйтесь под именем созданной учетной записи:
   ```
   su - <Логин>
   <Пароль>
   ```

Учетная запись создана.

3.11.2. Подготовка сценариев для аудита

► Чтобы подготовить сценарии для проведения аудита:

1. Перенесите архив `bin.tar`, входящий в комплект поставки MaxPatrol VM, в домашний каталог созданной учетной записи.
2. Перейдите в домашний каталог:
   ```
   cd /home/<Логин>
   ```
3. Создайте каталог `/home/<Логин>/bin`:
   ```
   mkdir ~/bin
   ```
4. Распакуйте архив:
   ```
   tar -xf bin.tar
   ```
5. Настройте права доступа к каталогу:
   ```
   chmod 700 -R ~/bin
   ```
6. Удалите архив:
   ```
   rm bin.tar
   ```
7. Перенесите в домашний каталог учетной записи файл:
   - Если используется командная оболочка Bash, — `.bash_profile`.
   - Если командная оболочка Bourne shell (sh), — `.profile`.

   Примечание. Вы можете просмотреть список каталогов в переменной окружения `$PATH`, выполнив команду `echo $PATH`. Название каталога `/home/<Логин>/bin` должно располагаться первым в списке на экране.

Сценарии для аудита подготовлены.

3.11.3. Настройка программы sudo

► Чтобы настроить программу sudo:

1. Откройте для изменения файл `/etc/sudoers`:
   ```
   visudo
   ```
2. Добавьте в файл строки с псевдонимами для сценариев:
   ```
   Cmnd_Alias MPROOTCMD = /usr/bin/crontab * -l, /usr/bin/netstat, /usr/local/sbin/dmidecode
   Cmnd_Alias MPFILECMD = /bin/cat, /usr/bin/find *, /bin/ls, /usr/bin/test
   Cmnd_Alias MPEXCPTNSCMD = !/usr/bin/find *-exec*, !/usr/bin/find *-fprint*, !/usr/bin/find *-ok*, !/usr/bin/find *-delete*, !/usr/bin/find *-fls*, !/usr/local/sbin/dmidecode *--dump*
   ```
3. Добавьте в файл строки, предоставляющие учетной записи права на выполнение команд для запуска сценариев:
   ```
   <Логин> ALL = (ALL) NOPASSWD: MPROOTCMD
   <Логин> ALL = (ALL) NOPASSWD: MPFILECMD
   <Логин> ALL = (ALL) NOPASSWD: MPEXCPTNSCMD
   ```
4. Если в файле отсутствует строка с директивой `Defaults env_reset`, добавьте ее:
   ```
   Defaults env_reset
   ```
5. Если в файле есть строка с директивой `Defaults env_keep` и она содержит переменную окружения `PATH`, удалите эту переменную из строки (или всю строку, если переменная единственная).
6. Сохраните изменения и закройте файл.

Программа sudo настроена.

3.12. FreeBSD 11, 12: настройка MaxPatrol VM

Для аудита актива в MaxPatrol VM нужно добавить учетную запись для доступа к активу, создать и запустить задачу на проведение аудита с профилем Unix Audit.

В этом разделе

3.12.1. Добавление учетной записи

► Чтобы добавить в MaxPatrol VM учетную запись для доступа к активу:

1. В главном меню в разделе **Сбор данных** выберите пункт **Учетные записи**.

Откроется страница **Учетные записи**.

2. В панели инструментов нажмите кнопку **Добавить учетную запись** и в раскрывшемся меню выберите пункт **Логин — пароль**.

   Откроется страница **Добавление учетной записи**.

3. В поле **Название** введите название учетной записи.

   Примечание. В поле **Описание** вы можете ввести любой текстовый комментарий.

4. В поле **Логин** введите логин учетной записи.
5. В поле **Пароль** введите пароль и подтвердите его в поле **Подтверждение пароля**.
6. Нажмите кнопку **Сохранить**.

Учетная запись добавлена.

3.12.2. Создание и запуск задачи на аудит актива

► Чтобы создать и запустить задачу на проведение аудита актива:

1. В главном меню в разделе **Сбор данных** выберите пункт **Задачи**.

   Откроется страница **Задачи по сбору данных**.

2. В панели инструментов нажмите кнопку **Создать задачу** и в раскрывшемся меню выберите пункт **Сбор данных**.

   Откроется страница **Создание задачи на сбор данных**.

3. В поле **Название** введите название задачи.
4. Если требуется, добавьте подробное описание задачи по ссылке **Добавить описание**.
5. В раскрывающемся списке **Профиль** выберите **Unix Audit**.
6. В иерархическом списке выберите пункт **Сканирование систем** → **Через терминал: SSH**.
7. В раскрывающемся списке **Учетная запись** выберите учетную запись для доступа к активу.
8. Если требуется, в раскрывающемся списке **Коллекторы** выберите коллекторы для сбора данных.
9. В панели **Цели сбора данных** на вкладке **Включить** в поле **Активы** введите IP-адрес или доменное имя (в формате FQDN) узла актива.

   Примечание. В панели **Расписание** вы можете включить и настроить автоматический запуск задачи по расписанию.

10. Нажмите кнопку **Сохранить и запустить**.

Задача на проведение аудита актива создана и запущена.

3.13. HPE HP-UX 11.31: настройка актива

Настройку актива нужно выполнять от имени учетной записи root.

Внимание! При использовании в IT-инфраструктуре организации межсетевого экрана или других средств для контроля сетевого трафика требуется настроить в них правила, разрешающие трафик в обоих направлениях между узлом актива и узлом MP 10 Collector. Для проведения аудита актива по протоколу SSH используется порт TCP 22.

Внимание! На узле актива должна быть установлена программа sudo.

Для проведения аудита на активе нужно:

1. Создать учетную запись пользователя ОС для доступа MP 10 Collector к активу. В домашнем каталоге учетной записи создать каталог `bin` для файлов сценариев.

   Примечание. Данные этой учетной записи нужно указать при добавлении учетной записи в MaxPatrol VM.

2. Поместить в каталог `bin` файлы сценариев для проведения аудита. В домашний каталог созданной учетной записи поместить файл `.bash_profile` с параметрами переменной окружения `$PATH`.

   Примечание. В комплект поставки MaxPatrol VM входит архив `audit_sudo_wrappers.tar`. В этом архиве, в папках с названиями операционных систем, находятся файлы сценариев (в архиве `bin.tar`) и файлы `.bash_profile`.

3. Настроить программу sudo и предоставить созданной учетной записи права на выполнение команд для запуска сценариев.

В этом разделе

3.13.1. Создание учетной записи ОС

► Чтобы создать и настроить учетную запись:

1. Создайте учетную запись и укажите для нее пароль:
   ```
   useradd -m -g users -s /bin/bash <Логин>
   passwd <Логин>
   <Пароль>
   ```
2. Настройте права доступа к домашнему каталогу:
   ```
   chmod 700 /home/<Логин>
   ```
3. Авторизуйтесь под именем созданной учетной записи:
   ```
   su - <Логин>
   <Пароль>
   ```

Учетная запись создана.

3.13.2. Подготовка сценариев для аудита

► Чтобы подготовить сценарии для проведения аудита:

1. Перенесите архив `bin.tar`, входящий в комплект поставки MaxPatrol VM, в домашний каталог созданной учетной записи.
2. Перейдите в домашний каталог:
   ```
   cd /home/<Логин>
   ```
3. Создайте каталог `/home/<Логин>/bin`:
   ```
   mkdir ~/bin
   ```
4. Распакуйте архив:
   ```
   tar -xf bin.tar
   ```
5. Настройте права доступа к каталогу:
   ```
   chmod 700 -R ~/bin
   ```
6. Удалите архив:
   ```
   rm bin.tar
   ```
7. Перенесите в домашний каталог учетной записи файл:
   - Если используется командная оболочка Bash, — `.bash_profile`.
   - Если командная оболочка Bourne shell (sh), — `.profile`.

   Примечание. Вы можете просмотреть список каталогов в переменной окружения `$PATH`, выполнив команду `echo $PATH`. Название каталога `/home/<Логин>/bin` должно располагаться первым в списке на экране.

Сценарии для аудита подготовлены.

3.13.3. Настройка программы sudo

► Чтобы настроить программу sudo:

1. Откройте для изменения файл `/etc/sudoers`:
   ```
   visudo
   ```
2. Добавьте в файл строки с псевдонимами для сценариев:
   ```
   Cmnd_Alias MPROOTCMD = /usr/bin/crontab -l *, /bin/netstat, /opt/ipf/bin/ipfstat -io, /usr/sbin/diskinfo, /usr/sbin/nwmgr
   Cmnd_Alias MPFILECMD = /bin/cat, /usr/bin/find, /bin/ls, /usr/bin/test
   Cmnd_Alias MPEXCPTNCMD = !/usr/sbin/nwmgr *-*
   ```
3. Добавьте в файл строки, предоставляющие учетной записи права на выполнение команд для запуска сценариев:
   ```
   <Логин> ALL = (ALL) NOPASSWD: MPROOTCMD
   <Логин> ALL = (ALL) NOPASSWD: MPFILECMD
   <Логин> ALL = (ALL) NOPASSWD: MPEXCPTNSCMD
   ```
4. Если в файле отсутствует строка с директивой `Defaults env_reset`, добавьте ее:
   ```
   Defaults env_reset
   ```
5. Если в файле есть строка с директивой `Defaults env_keep` и она содержит переменную окружения `PATH`, удалите эту переменную из строки (или всю строку, если переменная единственная).
6. Сохраните изменения и закройте файл.

Программа sudo настроена.

3.14. HPE HP-UX 11.31: настройка MaxPatrol VM

Для аудита актива в MaxPatrol VM нужно добавить учетную запись для доступа к активу, создать и запустить задачу на проведение аудита с профилем Unix Audit.

В этом разделе

3.14.1. Добавление учетной записи

► Чтобы добавить в MaxPatrol VM учетную запись для доступа к активу:

1. В главном меню в разделе **Сбор данных** выберите пункт **Учетные записи**.

   Откроется страница **Учетные записи**.
2. В панели инструментов нажмите кнопку **Добавить учетную запись** и в раскрывшемся меню выберите пункт **Логин — пароль**.

Откроется страница **Добавление учетной записи**.

3. В поле **Название** введите название учетной записи.

   Примечание. В поле **Описание** вы можете ввести любой текстовый комментарий.

4. В поле **Логин** введите логин учетной записи.
5. В поле **Пароль** введите пароль и подтвердите его в поле **Подтверждение пароля**.
6. Нажмите кнопку **Сохранить**.

Учетная запись добавлена.

3.14.2. Создание и запуск задачи на аудит актива

► Чтобы создать и запустить задачу на проведение аудита актива:

1. В главном меню в разделе **Сбор данных** выберите пункт **Задачи**.

   Откроется страница **Задачи по сбору данных**.

2. В панели инструментов нажмите кнопку **Создать задачу** и в раскрывшемся меню выберите пункт **Сбор данных**.

   Откроется страница **Создание задачи на сбор данных**.

3. В поле **Название** введите название задачи.
4. Если требуется, добавьте подробное описание задачи по ссылке **Добавить описание**.
5. В раскрывающемся списке **Профиль** выберите **Unix Audit**.
6. В иерархическом списке выберите пункт **Сканирование систем** → **Через терминал: SSH**.
7. В раскрывающемся списке **Учетная запись** выберите учетную запись для доступа к активу.
8. Если требуется, в раскрывающемся списке **Коллекторы** выберите коллекторы для сбора данных.
9. В панели **Цели сбора данных** на вкладке **Включить** в поле **Активы** введите IP-адрес или доменное имя (в формате FQDN) узла актива.

   Примечание. В панели **Расписание** вы можете включить и настроить автоматический запуск задачи по расписанию.

10. Нажмите кнопку **Сохранить и запустить**.

Задача на проведение аудита актива создана и запущена.

3.15. IBM AIX 7.1, 7.2: настройка актива

Настройку актива нужно выполнять от имени учетной записи root.

Внимание! При использовании в IT-инфраструктуре организации межсетевого экрана или других средств для контроля сетевого трафика требуется настроить в них правила, разрешающие трафик в обоих направлениях между узлом актива и узлом MP 10 Collector. Для проведения аудита актива по протоколу SSH используется порт TCP 22.

Внимание! На узле актива должна быть установлена программа sudo.

Для проведения аудита на активе нужно:

1. Создать учетную запись пользователя ОС для доступа MP 10 Collector к активу. В домашнем каталоге учетной записи создать каталог `bin` для файлов сценариев.

   Примечание. Данные этой учетной записи нужно указать при добавлении учетной записи в MaxPatrol VM.

2. Поместить в каталог `bin` файлы сценариев для проведения аудита. В домашний каталог созданной учетной записи поместить файл `.bash_profile` с параметрами переменной окружения `$PATH`.

   Примечание. В комплект поставки MaxPatrol VM входит архив `audit_sudo_wrappers.tar`. В этом архиве, в папках с названиями операционных систем, находятся файлы сценариев (в архиве `bin.tar`) и файлы `.bash_profile`.

3. Настроить программу sudo и предоставить созданной учетной записи права на выполнение команд для запуска сценариев.

В этом разделе

3.15.1. Создание учетной записи ОС

► Чтобы создать и настроить учетную запись:

1. Создайте учетную запись и укажите для нее пароль:

   ```
   useradd -m -d /home/<Логин> <Логин>
   passwd <Логин>
   <Пароль>
   ```

2. Настройте права доступа к домашнему каталогу:

   ```
   chmod 700 /home/<Логин>
   ```

3. Авторизуйтесь под именем созданной учетной записи:

   ```
   su - <Логин>
   <Пароль>
   ```

Учетная запись создана.

3.15.2. Подготовка сценариев для аудита

► Чтобы подготовить сценарии для проведения аудита:

1. Перенесите архив `bin.tar`, входящий в комплект поставки MaxPatrol VM, в домашний каталог созданной учетной записи.
2. Перейдите в домашний каталог:
   ```
   cd /home/<Логин>
   ```
3. Создайте каталог `/home/<Логин>/bin`:
   ```
   mkdir ~/bin
   ```
4. Распакуйте архив:
   ```
   tar -xf bin.tar
   ```
5. Настройте права доступа к каталогу:
   ```
   chmod 700 -R ~/bin
   ```
6. Удалите архив:
   ```
   rm bin.tar
   ```
7. Перенесите в домашний каталог учетной записи файл:
   - Если используется командная оболочка Bash, — `.bash_profile`.
   - Если командная оболочка Bourne shell (sh), — `.profile`.

   Примечание. Вы можете просмотреть список каталогов в переменной окружения `$PATH`, выполнив команду `echo $PATH`. Название каталога `/home/<Логин>/bin` должно располагаться первым в списке на экране.

Сценарии для аудита подготовлены.

3.15.3. Настройка программы sudo

► Чтобы настроить программу sudo:

1. Откройте для изменения файл `/etc/sudoers`:
   ```
   visudo
   ```
2. Добавьте в файл строки с псевдонимами для сценариев:
   ```
   Cmnd_Alias MPROOTCMD = /usr/bin/crontab -l *, /bin/netstat, /usr/sbin/lsfilt
   Cmnd_Alias MPFILECMD = /bin/cat, /usr/bin/find, /bin/ls, /usr/bin/test
   ```
3. Добавьте в файл строки, предоставляющие учетной записи права на выполнение команд для запуска сценариев:
   ```
   <Логин> ALL = (ALL) NOPASSWD: MPROOTCMD
   <Логин> ALL = (ALL) NOPASSWD: MPFILECMD
   ```
4. Если в файле отсутствует строка с директивой `Defaults env_reset`, добавьте ее:
   ```
   Defaults env_reset
   ```

5. Если в файле есть строка с директивой `Defaults env_keep` и она содержит переменную окружения `PATH`, удалите эту переменную из строки (или всю строку, если переменная единственная).
6. Сохраните изменения и закройте файл.

Программа sudo настроена.

3.16. IBM AIX 7.1, 7.2: настройка MaxPatrol VM

Для аудита актива в MaxPatrol VM нужно добавить учетную запись для доступа к активу, создать и запустить задачу на проведение аудита с профилем Unix Audit.

В этом разделе

3.16.1. Добавление учетной записи

► Чтобы добавить в MaxPatrol VM учетную запись для доступа к активу:

1. В главном меню в разделе **Сбор данных** выберите пункт **Учетные записи**.

   Откроется страница **Учетные записи**.
2. В панели инструментов нажмите кнопку **Добавить учетную запись** и в раскрывшемся меню выберите пункт **Логин — пароль**.

   Откроется страница **Добавление учетной записи**.
3. В поле **Название** введите название учетной записи.

   Примечание. В поле **Описание** вы можете ввести любой текстовый комментарий.
4. В поле **Логин** введите логин учетной записи.
5. В поле **Пароль** введите пароль и подтвердите его в поле **Подтверждение пароля**.
6. Нажмите кнопку **Сохранить**.

Учетная запись добавлена.

3.16.2. Создание и запуск задачи на аудит актива

► Чтобы создать и запустить задачу на проведение аудита актива:

1. В главном меню в разделе **Сбор данных** выберите пункт **Задачи**.

Откроется страница **Задачи по сбору данных**.

2. В панели инструментов нажмите кнопку **Создать задачу** и в раскрывшемся меню выберите пункт **Сбор данных**.

   Откроется страница **Создание задачи на сбор данных**.

3. В поле **Название** введите название задачи.
4. Если требуется, добавьте подробное описание задачи по ссылке **Добавить описание**.
5. В раскрывающемся списке **Профиль** выберите **Unix Audit**.
6. В иерархическом списке выберите пункт **Сканирование систем** → **Через терминал: SSH**.
7. В раскрывающемся списке **Учетная запись** выберите учетную запись для доступа к активу.
8. Если требуется, в раскрывающемся списке **Коллекторы** выберите коллекторы для сбора данных.
9. В панели **Цели сбора данных** на вкладке **Включить** в поле **Активы** введите IP-адрес или доменное имя (в формате FQDN) узла актива.

   Примечание. В панели **Расписание** вы можете включить и настроить автоматический запуск задачи по расписанию.

10. Нажмите кнопку **Сохранить и запустить**.

Задача на проведение аудита актива создана и запущена.

3.17. Microsoft Windows XP—10; Windows Server 2003—2019: настройка актива

Настройку актива нужно выполнять от имени учетной записи администратора.

Внимание! При использовании в IT-инфраструктуре организации межсетевого экрана или других средств для контроля сетевого трафика требуется настроить в них правила, разрешающие трафик в обоих направлениях между узлом источника и узлом MP 10 Collector. В Windows XP и Windows Server 2003, 2003 R2 используются динамические TCP-порты 1025—5000[1]. В Windows версии от Vista до 10 и Windows Server версии от 2008 до 2019 используются TCP-порты 135, 139, 445, динамические TCP-порты 49152—65535[1] и UDP-порты 135, 137, 138, 445.

Для проведения аудита на активе нужно создать учетную запись администратора ОС для доступа MP 10 Collector к активу. Данные этой учетной записи нужно указать при добавлении учетной записи в MaxPatrol VM.

1 Диапазон динамических портов может быть изменен в ОС.

Примечание. Вы можете детально настроить учетную запись, предоставив ей права на выполнение команд для проведения аудита (см. приложение).

3.18. Microsoft Windows XP—10; Windows Server 2003—2019: настройка MaxPatrol VM

Для аудита актива в MaxPatrol VM нужно добавить учетную запись для доступа к активу, создать и запустить задачу на проведение аудита с профилем Windows Audit.

В этом разделе

3.18.1. Добавление учетной записи ОС

► Чтобы добавить в MaxPatrol VM учетную запись для доступа к источнику:

1. В главном меню в разделе **Сбор данных** выберите пункт **Учетные записи**.

   Откроется страница **Учетные записи**.

2. В панели инструментов нажмите кнопку **Добавить учетную запись** и в раскрывшемся меню выберите пункт **Логин — пароль**.

   Откроется страница **Добавление учетной записи**.

3. В поле **Название** введите название учетной записи.

   Примечание. В поле **Описание** вы можете ввести любой текстовый комментарий.

4. В раскрывающемся списке Метки установите флажок **WindowsAudit**.
5. В поле **Логин** введите логин учетной записи.
6. Если требуется, в поле **Пароль** введите пароль и подтвердите его в поле **Подтверждение пароля**.
7. Если для доступа к источнику используется доменная учетная запись, в поле **Домен** введите имя домена.
8. Нажмите кнопку **Сохранить**.

Учетная запись добавлена.

3.18.2. Создание и запуск задачи на аудит актива

► Чтобы создать и запустить задачу на проведение аудита актива:

1. В главном меню в разделе **Сбор данных** выберите пункт **Задачи**.

Откроется страница **Задачи по сбору данных**.

2. В панели инструментов нажмите кнопку **Создать задачу** и в раскрывшемся меню выберите пункт **Сбор данных**.

   Откроется страница **Создание задачи на сбор данных**.

3. В поле **Название** введите название задачи.
4. Если требуется, добавьте подробное описание задачи по ссылке **Добавить описание**.
5. В раскрывающемся списке **Профиль** выберите **Windows Audit**.
6. В иерархическом списке выберите пункт **Сканирование систем** → **Windows**.
7. В раскрывающемся списке **Учетная запись** выберите учетную запись пользователя ОС.
8. Если требуется, в раскрывающемся списке **Коллекторы** выберите коллекторы для сбора данных.
9. В панели **Цели сбора данных** на вкладке **Включить** в поле **Активы** введите IP-адрес или доменное имя (в формате FQDN) узла актива.

   Примечание. В панели **Расписание** вы можете включить и настроить автоматический запуск задачи по расписанию.

10. Нажмите кнопку **Сохранить и запустить**.

Задача на проведение аудита актива создана и запущена.

3.19. Oracle Linux 6, 7, 8: настройка актива

Настройку актива нужно выполнять от имени учетной записи root.

Внимание! При использовании в IT-инфраструктуре организации межсетевого экрана или других средств для контроля сетевого трафика требуется настроить в них правила, разрешающие трафик в обоих направлениях между узлом актива и узлом MP 10 Collector. Для проведения аудита актива по протоколу SSH используется порт TCP 22.

Внимание! На узле актива должна быть установлена программа sudo.

Для проведения аудита на активе нужно:

1. Создать учетную запись пользователя ОС для доступа MP 10 Collector к активу. В домашнем каталоге учетной записи создать каталог `bin` для файлов сценариев.

   Примечание. Данные этой учетной записи нужно указать при добавлении учетной записи в MaxPatrol VM.

2. Поместить в каталог `bin` файлы сценариев для проведения аудита. В домашний каталог созданной учетной записи поместить файл `.bash_profile` с параметрами переменной окружения `$PATH`.

Примечание. В комплект поставки MaxPatrol VM входит архив `audit_sudo_wrappers.tar`. В этом архиве, в папках с названиями операционных систем, находятся файлы сценариев (в архиве `bin.tar`) и файлы `.bash_profile`.

3. Настроить программу sudo и предоставить созданной учетной записи права на выполнение команд для запуска сценариев.

В этом разделе

3.19.1. Создание учетной записи ОС

► Чтобы создать и настроить учетную запись:

1. Создайте учетную запись и укажите для нее пароль:
```
useradd -m -g users -s /bin/bash <Логин>
passwd <Логин>
<Пароль>
```
2. Настройте права доступа к домашнему каталогу:
```
chmod 700 /home/<Логин>
```
3. Авторизуйтесь под именем созданной учетной записи:
```
su - <Логин>
<Пароль>
```

Учетная запись создана.

3.19.2. Подготовка сценариев для аудита

► Чтобы подготовить сценарии для проведения аудита:

1. Перенесите архив `bin.tar`, входящий в комплект поставки MaxPatrol VM, в домашний каталог созданной учетной записи.
2. Перейдите в домашний каталог:
```
cd /home/<Логин>
```
3. Создайте каталог `/home/<Логин>/bin`:
```
mkdir ~/bin
```
4. Распакуйте архив:
```
tar -xf bin.tar
```
5. Настройте права доступа к каталогу:
```
chmod 700 -R ~/bin
```

6. Удалите архив:
   ```
   rm bin.tar
   ```
7. Перенесите файл `.bash_profile` в домашний каталог.

   Примечание. Вы можете просмотреть список каталогов в переменной окружения `$PATH`, выполнив команду `echo $PATH`. Название каталога `/home/<Логин>/bin` должно располагаться первым в списке на экране.

Сценарии для аудита подготовлены.

3.19.3. Настройка программы sudo

► Чтобы настроить программу sudo:

1. Откройте для изменения файл `/etc/sudoers`:
   ```
   visudo
   ```
2. Добавьте в файл строки с псевдонимами для сценариев:
   ```
   Cmnd_Alias MPROOTCMD = /usr/bin/at -l, /usr/bin/crontab * -l, /sbin/fdisk -l, /sbin/iptables-save, /bin/netstat, /usr/sbin/ss, /usr/sbin/dmidecode, /sbin/vgdisplay, /sbin/lvdisplay, /sbin/auditctl -[lv], /sbin/grubby --info ALL
   Cmnd_Alias MPFILECMD = /bin/egrep, /bin/cat, /usr/bin/find *, /bin/ls, /usr/bin/getfacl, /usr/bin/test
   Cmnd_Alias MPEXCPTNSCMD = !/usr/bin/find *-exec*, !/usr/bin/find *-fprint*, !/usr/bin/find *-ok*, !/usr/bin/find *-delete*, !/usr/bin/find *-fls*, !/usr/sbin/ss *--diag*, !/usr/sbin/ss *-D*, !/usr/sbin/dmidecode *--dump*
   ```
3. Добавьте в файл строки, предоставляющие учетной записи права на выполнение команд для запуска сценариев:
   ```
   <Логин> ALL = (ALL) NOPASSWD: MPROOTCMD
   <Логин> ALL = (ALL) NOPASSWD: MPFILECMD
   <Логин> ALL = (ALL) NOPASSWD: MPEXCPTNSCMD
   ```
4. Если в файле отсутствует строка с директивой `Defaults env_reset`, добавьте ее:
   ```
   Defaults env_reset
   ```
5. Если в файле есть строка с директивой `Defaults env_keep` и она содержит переменную окружения `PATH`, удалите эту переменную из строки (или всю строку, если переменная единственная).
6. Сохраните изменения и закройте файл.

Программа sudo настроена.

3.20. Oracle Linux 6, 7, 8: настройка MaxPatrol VM

Для аудита актива в MaxPatrol VM нужно добавить учетную запись для доступа к активу, создать и запустить задачу на проведение аудита с профилем Unix Audit.

В этом разделе

3.20.1. Добавление учетной записи

► Чтобы добавить в MaxPatrol VM учетную запись для доступа к активу:

1. В главном меню в разделе **Сбор данных** выберите пункт **Учетные записи**.

   Откроется страница **Учетные записи**.

2. В панели инструментов нажмите кнопку **Добавить учетную запись** и в раскрывшемся меню выберите пункт **Логин — пароль**.

   Откроется страница **Добавление учетной записи**.

3. В поле **Название** введите название учетной записи.

   Примечание. В поле **Описание** вы можете ввести любой текстовый комментарий.

4. В поле **Логин** введите логин учетной записи.
5. В поле **Пароль** введите пароль и подтвердите его в поле **Подтверждение пароля**.
6. Нажмите кнопку **Сохранить**.

Учетная запись добавлена.

3.20.2. Создание и запуск задачи на аудит актива

► Чтобы создать и запустить задачу на проведение аудита актива:

1. В главном меню в разделе **Сбор данных** выберите пункт **Задачи**.

   Откроется страница **Задачи по сбору данных**.

2. В панели инструментов нажмите кнопку **Создать задачу** и в раскрывшемся меню выберите пункт **Сбор данных**.

   Откроется страница **Создание задачи на сбор данных**.

3. В поле **Название** введите название задачи.
4. Если требуется, добавьте подробное описание задачи по ссылке **Добавить описание**.
5. В раскрывающемся списке **Профиль** выберите **Unix Audit**.
6. В иерархическом списке выберите пункт **Сканирование систем** → **Через терминал: SSH**.
7. В раскрывающемся списке **Учетная запись** выберите учетную запись для доступа к активу.

8. Если требуется, в раскрывающемся списке **Коллекторы** выберите коллекторы для сбора данных.
9. В панели **Цели сбора данных** на вкладке **Включить** в поле **Активы** введите IP-адрес или доменное имя (в формате FQDN) узла актива.

   Примечание. В панели **Расписание** вы можете включить и настроить автоматический запуск задачи по расписанию.

10. Нажмите кнопку **Сохранить и запустить**.

Задача на проведение аудита актива создана и запущена.

3.21. Oracle Solaris 11.0—11.4: настройка актива

Настройку актива нужно выполнять от имени учетной записи root.

Внимание! При использовании в IT-инфраструктуре организации межсетевого экрана или других средств для контроля сетевого трафика требуется настроить в них правила, разрешающие трафик в обоих направлениях между узлом актива и узлом MP 10 Collector. Для проведения аудита актива по протоколу SSH используется порт TCP 22.

Внимание! На узле актива должна быть установлена программа sudo.

Для проведения аудита на активе нужно:

1. Создать учетную запись пользователя ОС для доступа MP 10 Collector к активу. В домашнем каталоге учетной записи создать каталог `bin` для файлов сценариев.

   Примечание. Данные этой учетной записи нужно указать при добавлении учетной записи в MaxPatrol VM.

2. Поместить в каталог `bin` файлы сценариев для проведения аудита. В домашний каталог созданной учетной записи поместить файл `.bash_profile` с параметрами переменной окружения `$PATH`.

   Примечание. В комплект поставки MaxPatrol VM входит архив `audit_sudo_wrappers.tar`. В этом архиве, в папках с названиями операционных систем, находятся файлы сценариев (в архиве `bin.tar`) и файлы `.bash_profile`.

3. Настроить программу sudo и предоставить созданной учетной записи права на выполнение команд для запуска сценариев.

В этом разделе

3.21.1. Создание учетной записи ОС

► Чтобы создать и настроить учетную запись:

1. Создайте учетную запись и укажите для нее пароль:
   ```
   useradd -m -d /export/home/<Логин> <Логин>
   passwd <Логин>
   <Пароль>
   ```
2. Настройте права доступа к домашнему каталогу:
   ```
   chmod 700 /export/home/<Логин>
   ```
3. Авторизуйтесь под именем созданной учетной записи:
   ```
   su - <Логин>
   <Пароль>
   ```

Учетная запись создана.

3.21.2. Подготовка сценариев для аудита

► Чтобы подготовить сценарии для проведения аудита:

1. Перенесите архив `bin.tar`, входящий в комплект поставки MaxPatrol VM, в домашний каталог созданной учетной записи.
2. Перейдите в домашний каталог:
   ```
   cd /export/home/<Логин>
   ```
3. Создайте каталог `/export/home/<Логин>/bin`:
   ```
   mkdir ~/bin
   ```
4. Распакуйте архив:
   ```
   tar -xf bin.tar
   ```
5. Настройте права доступа к каталогу:
   ```
   chmod 700 -R ~/bin
   ```
6. Удалите архив:
   ```
   rm bin.tar
   ```
7. Перенесите файл `.bash_profile` в домашний каталог.

   Примечание. Вы можете просмотреть список каталогов в переменной окружения `$PATH`, выполнив команду `echo $PATH`. Название каталога `/export/home/<Логин>/bin` должно располагаться первым в списке на экране.

Сценарии для аудита подготовлены.

3.21.3. Настройка программы sudo

► Чтобы настроить программу sudo:

1. Откройте для изменения файл `/etc/sudoers`:
   ```
   visudo
   ```
2. Добавьте в файл строки с псевдонимами для сценариев:
   ```
   Cmnd_Alias MPROOTCMD = /usr/bin/crontab -l *, /bin/netstat, /usr/bin/scanpci, /usr/sbin/bootadm list-menu, /usr/sbin/bootadm set-menu-password -l, /usr/sbin/bootadm show-entry -i *
   Cmnd_Alias MPFILECMD = /bin/cat, /usr/bin/find, /bin/ls, /usr/bin/test
   ```
3. Добавьте в файл строки, предоставляющие учетной записи права на выполнение команд для запуска сценариев:
   ```
   <Логин> ALL = (ALL) NOPASSWD: MPROOTCMD
   <Логин> ALL = (ALL) NOPASSWD: MPFILECMD
   ```
4. Если в файле отсутствует строка с директивой `Defaults env_reset`, добавьте ее:
   ```
   Defaults env_reset
   ```
5. Если в файле есть строка с директивой `Defaults env_keep` и она содержит переменную окружения `PATH`, удалите эту переменную из строки (или всю строку, если переменная единственная).
6. Сохраните изменения и закройте файл.

Программа sudo настроена.

3.22. Oracle Solaris 11.0—11.4: настройка MaxPatrol VM

Для аудита актива в MaxPatrol VM нужно добавить учетную запись для доступа к активу, создать и запустить задачу на проведение аудита с профилем Unix Audit.

В этом разделе

3.22.1. Добавление учетной записи

► Чтобы добавить в MaxPatrol VM учетную запись для доступа к активу:

1. В главном меню в разделе **Сбор данных** выберите пункт **Учетные записи**.

   Откроется страница **Учетные записи**.
2. В панели инструментов нажмите кнопку **Добавить учетную запись** и в раскрывшемся меню выберите пункт **Логин — пароль**.

Откроется страница **Добавление учетной записи**.

3. В поле **Название** введите название учетной записи.

   Примечание. В поле **Описание** вы можете ввести любой текстовый комментарий.

4. В поле **Логин** введите логин учетной записи.
5. В поле **Пароль** введите пароль и подтвердите его в поле **Подтверждение пароля**.
6. Нажмите кнопку **Сохранить**.

Учетная запись добавлена.

3.22.2. Создание и запуск задачи на аудит актива

► Чтобы создать и запустить задачу на проведение аудита актива:

1. В главном меню в разделе **Сбор данных** выберите пункт **Задачи**.

   Откроется страница **Задачи по сбору данных**.

2. В панели инструментов нажмите кнопку **Создать задачу** и в раскрывшемся меню выберите пункт **Сбор данных**.

   Откроется страница **Создание задачи на сбор данных**.

3. В поле **Название** введите название задачи.
4. Если требуется, добавьте подробное описание задачи по ссылке **Добавить описание**.
5. В раскрывающемся списке **Профиль** выберите **Unix Audit**.
6. В иерархическом списке выберите пункт **Сканирование систем** → **Через терминал: SSH**.
7. В раскрывающемся списке **Учетная запись** выберите учетную запись для доступа к активу.
8. Если требуется, в раскрывающемся списке **Коллекторы** выберите коллекторы для сбора данных.
9. В панели **Цели сбора данных** на вкладке **Включить** в поле **Активы** введите IP-адрес или доменное имя (в формате FQDN) узла актива.

   Примечание. В панели **Расписание** вы можете включить и настроить автоматический запуск задачи по расписанию.

10. Нажмите кнопку **Сохранить и запустить**.

Задача на проведение аудита актива создана и запущена.

3.23. Red Hat Enterprise Linux 6—9: настройка актива

Настройку актива нужно выполнять от имени учетной записи root.

Внимание! При использовании в IT-инфраструктуре организации межсетевого экрана или других средств для контроля сетевого трафика требуется настроить в них правила, разрешающие трафик в обоих направлениях между узлом актива и узлом MP 10 Collector. Для проведения аудита актива по протоколу SSH используется порт TCP 22.

Внимание! На узле актива должна быть установлена программа sudo.

Для проведения аудита на активе нужно:

1. Создать учетную запись пользователя ОС для доступа MP 10 Collector к активу. В домашнем каталоге учетной записи создать каталог `bin` для файлов сценариев.

   Примечание. Данные этой учетной записи нужно указать при добавлении учетной записи в MaxPatrol VM.

2. Поместить в каталог `bin` файлы сценариев для проведения аудита. В домашний каталог созданной учетной записи поместить файл `.bash_profile` с параметрами переменной окружения `$PATH`.

   Примечание. В комплект поставки MaxPatrol VM входит архив `audit_sudo_wrappers.tar`. В этом архиве, в папках с названиями операционных систем, находятся файлы сценариев (в архиве `bin.tar`) и файлы `.bash_profile`.

3. Настроить программу sudo и предоставить созданной учетной записи права на выполнение команд для запуска сценариев.

В этом разделе

3.23.1. Создание учетной записи ОС

► Чтобы создать и настроить учетную запись:

1. Создайте учетную запись и укажите для нее пароль:
   ```
   useradd -m -g users -s /bin/bash <Логин>
   passwd <Логин>
   <Пароль>
   ```
2. Настройте права доступа к домашнему каталогу:
   ```
   chmod 700 /home/<Логин>
   ```
3. Авторизуйтесь под именем созданной учетной записи:
   ```
   su - <Логин>
   <Пароль>
   ```

Учетная запись создана.

3.23.2. Подготовка сценариев для аудита

► Чтобы подготовить сценарии для проведения аудита:

1. Перенесите архив `bin.tar`, входящий в комплект поставки MaxPatrol VM, в домашний каталог созданной учетной записи.
2. Перейдите в домашний каталог:
   ```
   cd /home/<Логин>
   ```
3. Создайте каталог `/home/<Логин>/bin`:
   ```
   mkdir ~/bin
   ```
4. Распакуйте архив:
   ```
   tar -xf bin.tar
   ```
5. Настройте права доступа к каталогу:
   ```
   chmod 700 -R ~/bin
   ```
6. Удалите архив:
   ```
   rm bin.tar
   ```
7. Перенесите файл `.bash_profile` в домашний каталог.

   Примечание. Вы можете просмотреть список каталогов в переменной окружения `$PATH`, выполнив команду `echo $PATH`. Название каталога `/home/<Логин>/bin` должно располагаться первым в списке на экране.

Сценарии для аудита подготовлены.

3.23.3. Настройка программы sudo

► Чтобы настроить программу sudo:

1. Откройте для изменения файл `/etc/sudoers`:
   ```
   visudo
   ```
2. Добавьте в файл строки с псевдонимами для сценариев:
   ```
   Cmnd_Alias MPROOTCMD = /usr/bin/at -l, /usr/bin/crontab * -l, /sbin/fdisk -l, /sbin/iptables-save, /bin/netstat, /usr/sbin/ss, /usr/sbin/dmidecode, /sbin/vgdisplay, /sbin/lvdisplay, /sbin/auditctl -[lv]
   Cmnd_Alias MPFILECMD = /bin/egrep, /bin/cat, /usr/bin/find *, /bin/ls, /usr/bin/getfacl, /usr/bin/test
   Cmnd_Alias MPEXCPTNSCMD = !/usr/bin/find *-exec*, !/usr/bin/find *-fprint*, !/usr/bin/find *-ok*, !/usr/bin/find *-delete*, !/usr/bin/find *-fls*, !/usr/sbin/ss *--diag*, !/usr/sbin/ss *-D*, !/usr/sbin/dmidecode *--dump*
   ```
3. Добавьте в файл строки, предоставляющие учетной записи права на выполнение команд для запуска сценариев:
   ```
   <Логин> ALL = (ALL) NOPASSWD: MPROOTCMD
   <Логин> ALL = (ALL) NOPASSWD: MPFILECMD
   <Логин> ALL = (ALL) NOPASSWD: MPEXCPTNSCMD
   ```

4. Если в файле отсутствует строка с директивой `Defaults env_reset`, добавьте ее:
   `Defaults env_reset`
5. Если в файле есть строка с директивой `Defaults env_keep` и она содержит переменную окружения `PATH`, удалите эту переменную из строки (или всю строку, если переменная единственная).
6. Сохраните изменения и закройте файл.

Программа sudo настроена.

3.24. Red Hat Enterprise Linux 6—9: настройка MaxPatrol VM

Для аудита актива в MaxPatrol VM нужно добавить учетную запись для доступа к активу, создать и запустить задачу на проведение аудита с профилем Unix Audit.

В этом разделе

3.24.1. Добавление учетной записи

► Чтобы добавить в MaxPatrol VM учетную запись для доступа к активу:

1. В главном меню в разделе **Сбор данных** выберите пункт **Учетные записи**.

   Откроется страница **Учетные записи**.
2. В панели инструментов нажмите кнопку **Добавить учетную запись** и в раскрывшемся меню выберите пункт **Логин — пароль**.

   Откроется страница **Добавление учетной записи**.
3. В поле **Название** введите название учетной записи.

   Примечание. В поле **Описание** вы можете ввести любой текстовый комментарий.
4. В поле **Логин** введите логин учетной записи.
5. В поле **Пароль** введите пароль и подтвердите его в поле **Подтверждение пароля**.
6. Нажмите кнопку **Сохранить**.

Учетная запись добавлена.

3.24.2. Создание и запуск задачи на аудит актива

► Чтобы создать и запустить задачу на проведение аудита актива:

1. В главном меню в разделе **Сбор данных** выберите пункт **Задачи**.

   Откроется страница **Задачи по сбору данных**.

2. В панели инструментов нажмите кнопку **Создать задачу** и в раскрывшемся меню выберите пункт **Сбор данных**.

   Откроется страница **Создание задачи на сбор данных**.

3. В поле **Название** введите название задачи.
4. Если требуется, добавьте подробное описание задачи по ссылке **Добавить описание**.
5. В раскрывающемся списке **Профиль** выберите **Unix Audit**.
6. В иерархическом списке выберите пункт **Сканирование систем** → **Через терминал: SSH**.
7. В раскрывающемся списке **Учетная запись** выберите учетную запись для доступа к активу.
8. Если требуется, в раскрывающемся списке **Коллекторы** выберите коллекторы для сбора данных.
9. В панели **Цели сбора данных** на вкладке **Включить** в поле **Активы** введите IP-адрес или доменное имя (в формате FQDN) узла актива.

   Примечание. В панели **Расписание** вы можете включить и настроить автоматический запуск задачи по расписанию.

10. Нажмите кнопку **Сохранить и запустить**.

Задача на проведение аудита актива создана и запущена.

3.25. SUSE Linux Enterprise Server 15: настройка актива

Настройку актива нужно выполнять от имени учетной записи root.

Внимание! При использовании в IT-инфраструктуре организации межсетевого экрана или других средств для контроля сетевого трафика требуется настроить в них правила, разрешающие трафик в обоих направлениях между узлом актива и узлом MP 10 Collector. Для проведения аудита актива по протоколу SSH используется порт TCP 22.

Внимание! На узле актива должна быть установлена программа sudo.

Для проведения аудита на активе нужно:

1. Создать учетную запись пользователя ОС для доступа MP 10 Collector к активу. В домашнем каталоге учетной записи создать каталог `bin` для файлов сценариев.

   Примечание. Данные этой учетной записи нужно указать при добавлении учетной записи в MaxPatrol VM.

2. Поместить в каталог `bin` файлы сценариев для проведения аудита. В домашний каталог созданной учетной записи поместить файл `.bash_profile` с параметрами переменной окружения `$PATH`.

   Примечание. В комплект поставки MaxPatrol VM входит архив `audit_sudo_wrappers.tar`. В этом архиве, в папках с названиями операционных систем, находятся файлы сценариев (в архиве `bin.tar`) и файлы `.bash_profile`.

3. Настроить программу sudo и предоставить созданной учетной записи права на выполнение команд для запуска сценариев.

В этом разделе

3.25.1. Создание учетной записи ОС

► Чтобы создать и настроить учетную запись:

1. Создайте учетную запись и укажите для нее пароль:
   ```
   useradd -m -g users -s /bin/bash <Логин>
   passwd <Логин>
   <Пароль>
   ```
2. Настройте права доступа к домашнему каталогу:
   ```
   chmod 700 /home/<Логин>
   ```
3. Авторизуйтесь под именем созданной учетной записи:
   ```
   su - <Логин>
   <Пароль>
   ```

Учетная запись создана.

3.25.2. Подготовка сценариев для аудита

► Чтобы подготовить сценарии для проведения аудита:

1. Перенесите архив `bin.tar`, входящий в комплект поставки MaxPatrol VM, в домашний каталог созданной учетной записи.
2. Перейдите в домашний каталог:
   ```
   cd /home/<Логин>
   ```
3. Создайте каталог `/home/<Логин>/bin`:
   ```
   mkdir ~/bin
   ```
4. Распакуйте архив:
   ```
   tar -xf bin.tar
   ```
5. Настройте права доступа к каталогу:
   ```
   chmod 700 -R ~/bin
   ```
6. Удалите архив:
   ```
   rm bin.tar
   ```
7. Перенесите файл `.bash_profile` в домашний каталог.

   Примечание. Вы можете просмотреть список каталогов в переменной окружения `$PATH`, выполнив команду `echo $PATH`. Название каталога `/home/<Логин>/bin` должно располагаться первым в списке на экране.

Сценарии для аудита подготовлены.

3.25.3. Настройка программы sudo

► Чтобы настроить программу sudo:

1. Откройте для изменения файл `/etc/sudoers`:
   ```
   visudo
   ```
2. Добавьте в файл строки с псевдонимами для сценариев:
   ```
   Cmnd_Alias MPROOTCMD = /usr/bin/at -l, /usr/bin/crontab * -l, /sbin/fdisk -l, /sbin/iptables-save, /bin/netstat, /usr/sbin/ss, /usr/sbin/dmidecode, /sbin/vgdisplay, /sbin/lvdisplay, /sbin/auditctl -[lv]
   Cmnd_Alias MPFILECMD = /bin/cat, /usr/bin/find *, /bin/ls, /usr/bin/getfacl, /usr/bin/test
   Cmnd_Alias MPEXCPTNSCMD = !/usr/bin/find *-exec*, !/usr/bin/find *-fprint*, !/usr/bin/find *-ok*, !/usr/bin/find *-delete*, !/usr/bin/find *-fls*, !/usr/sbin/ss *--diag*, !/usr/sbin/ss *-D*, !/usr/sbin/dmidecode *--dump*
   ```
3. Добавьте в файл строки, предоставляющие учетной записи права на выполнение команд для запуска сценариев:
   ```
   <Логин> ALL = (ALL) NOPASSWD: MPROOTCMD
   <Логин> ALL = (ALL) NOPASSWD: MPFILECMD
   <Логин> ALL = (ALL) NOPASSWD: MPEXCPTNSCMD
   ```

4. Если в файле отсутствует строка с директивой `Defaults env_reset`, добавьте ее:
   `Defaults env_reset`
5. Если в файле есть строка с директивой `Defaults env_keep` и она содержит переменную окружения `PATH`, удалите эту переменную из строки (или всю строку, если переменная единственная).
6. Сохраните изменения и закройте файл.

Программа sudo настроена.

3.26. SUSE Linux Enterprise Server 15: настройка MaxPatrol VM

Для аудита актива в MaxPatrol VM нужно добавить учетную запись для доступа к активу, создать и запустить задачу на проведение аудита с профилем Unix Audit.

В этом разделе

3.26.1. Добавление учетной записи

► Чтобы добавить в MaxPatrol VM учетную запись для доступа к активу:

1. В главном меню в разделе **Сбор данных** выберите пункт **Учетные записи**.

   Откроется страница **Учетные записи**.
2. В панели инструментов нажмите кнопку **Добавить учетную запись** и в раскрывшемся меню выберите пункт **Логин — пароль**.

   Откроется страница **Добавление учетной записи**.
3. В поле **Название** введите название учетной записи.

   Примечание. В поле **Описание** вы можете ввести любой текстовый комментарий.
4. В поле **Логин** введите логин учетной записи.
5. В поле **Пароль** введите пароль и подтвердите его в поле **Подтверждение пароля**.
6. Нажмите кнопку **Сохранить**.

Учетная запись добавлена.

3.26.2. Создание и запуск задачи на аудит актива

► Чтобы создать и запустить задачу на проведение аудита актива:

1. В главном меню в разделе **Сбор данных** выберите пункт **Задачи**.

   Откроется страница **Задачи по сбору данных**.

2. В панели инструментов нажмите кнопку **Создать задачу** и в раскрывшемся меню выберите пункт **Сбор данных**.

   Откроется страница **Создание задачи на сбор данных**.

3. В поле **Название** введите название задачи.
4. Если требуется, добавьте подробное описание задачи по ссылке **Добавить описание**.
5. В раскрывающемся списке **Профиль** выберите **Unix Audit**.
6. В иерархическом списке выберите пункт **Сканирование систем** → **Через терминал: SSH**.
7. В раскрывающемся списке **Учетная запись** выберите учетную запись для доступа к активу.
8. Если требуется, в раскрывающемся списке **Коллекторы** выберите коллекторы для сбора данных.
9. В панели **Цели сбора данных** на вкладке **Включить** в поле **Активы** введите IP-адрес или доменное имя (в формате FQDN) узла актива.

   Примечание. В панели **Расписание** вы можете включить и настроить автоматический запуск задачи по расписанию.

10. Нажмите кнопку **Сохранить и запустить**.

Задача на проведение аудита актива создана и запущена.

4. Прокси-серверы

Раздел содержит инструкции для настройки аудита поддерживаемых в MaxPatrol VM прокси-серверов.

В этом разделе

4.1. HAProxy Technologies HAProxy 2: настройка актива

Настройку актива нужно выполнять от имени учетной записи администратора устройства.

Внимание! Для проведения аудита актива по протоколу SSH используется порт TCP 22.

Для проведения аудита на активе нужно настроить ОС для аудита (см. раздел 3).

4.2. HAProxy Technologies HAProxy 2: настройка MaxPatrol VM

Для проведения аудита актива по протоколу SSH в MaxPatrol VM нужно настроить MaxPatrol VM для аудита ОС (см. раздел 3).

5. Сетевые устройства

Раздел содержит инструкции для настройки аудита поддерживаемых в MaxPatrol VM сетевых устройств.

В этом разделе

5.1. Alcatel OmniSwitch 6.6.4: настройка актива

Настройку актива нужно выполнять от имени учетной записи администратора устройства.

> **Внимание!** При использовании в IT-инфраструктуре организации межсетевого экрана или других средств для контроля сетевого трафика требуется настроить в них правила, разрешающие трафик в обоих направлениях между узлом актива и узлом MP 10 Collector. Для проведения аудита актива по протоколу SSH используется порт TCP 22, по протоколу SNMP — порт UDP 162.

Для проведения аудита на активе нужно создать учетную запись для доступа MP 10 Collector по протоколу SSH и пароль для доступа по протоколу SNMP.

В этом разделе

5.1.1. Создание учетной записи для доступа к активу по SSH

► Чтобы создать учетную запись для доступа к активу:

1. На узле, с которого производится настройка актива, запустите терминальный клиент, поддерживающий сетевые протоколы SSH и Telnet.
2. Авторизуйтесь на активе.
3. Создайте учетную запись для доступа к активу:
   ```
   user <Логин> password <Пароль>
   ```
4. Сохраните изменения:
   ```
   configuration snapshot all
   ```

Учетная запись создана.

5.1.2. Создание учетной записи для доступа к активу по SNMP

► Чтобы создать учетную запись для доступа к активу:

1. На узле, с которого производится настройка актива, запустите терминальный клиент, поддерживающий сетевые протоколы SSH и Telnet.
2. Авторизуйтесь на активе.
3. Создайте учетную запись для доступа к активу:
   ```
   user <Логин> password <Пароль> read-write all no auth
   ```
4. Настройте сервис SNMP:
   ```
   security no security
   snmp community map "<Название группы>" user "<Логин>" on
   ```
5. Разрешите доступ по протоколу SNMP с IP-адрес узла MP 10 Collector:
   ```
   snmp station <IP-адрес MP 10 Collector> 162 enable v2 "<Логин>"
   ```
6. Сохраните изменения:
   ```
   configuration snapshot all
   ```

Учетная запись создана.

5.2. Alcatel OmniSwitch 6.6.4: настройка MaxPatrol VM

Для проведения аудита актива по протоколу SSH в MaxPatrol VM нужно добавить учетную запись для доступа к активу, пароль для повышения привилегий (перехода в привилегированный режим EXEC) и создать задачу на проведение аудита.

Для проведения аудита по протоколу SNMP в MaxPatrol VM нужно добавить пароль для доступа к активу и создать задачу на проведение аудита.

В этом разделе

5.2.1. Добавление учетной записи для доступа по SSH

► Чтобы добавить в MaxPatrol VM учетную запись для доступа к активу:

1. В главном меню в разделе **Сбор данных** выберите пункт **Учетные записи**.

Откроется страница **Учетные записи**.

2. В панели инструментов нажмите кнопку **Добавить учетную запись** и в раскрывшемся меню выберите пункт **Логин — пароль**.

   Откроется страница **Добавление учетной записи**.

3. В поле **Название** введите название учетной записи.

   Примечание. В поле **Описание** вы можете ввести любой текстовый комментарий.

4. В раскрывающемся списке **Метки** установите флажок **Terminal**.
5. В поле **Логин** введите логин учетной записи.
6. В поле **Пароль** введите пароль и подтвердите его в поле **Подтверждение пароля**.
7. Нажмите кнопку **Сохранить**.

Учетная запись добавлена.

5.2.2. Создание задачи на аудит актива по SSH

► Чтобы создать задачу на проведение аудита актива:

1. В главном меню в разделе **Сбор данных** выберите пункт **Задачи**.

   Откроется страница **Задачи по сбору данных**.

2. В панели инструментов нажмите кнопку **Создать задачу** и в раскрывшемся меню выберите пункт **Сбор данных**.

   Откроется страница **Создание задачи на сбор данных**.

3. В поле **Название** введите название задачи.
4. Если требуется, добавьте подробное описание задачи по ссылке **Добавить описание**.
5. В раскрывающемся списке **Профиль** выберите **SSH Network Device Audit**.
6. В иерархическом списке выберите пункт **Сканирование систем** → **Через терминал: SSH и Telnet**.
7. В раскрывающемся списке **Учетная запись** выберите учетную запись для доступа к активу.
8. Если требуется, в раскрывающемся списке **Коллекторы** выберите коллекторы для сбора данных.
9. В панели **Цели сбора данных** на вкладке **Включить** в поле **Активы** введите IP-адрес или доменное имя (в формате FQDN) узла актива.

Примечание. В панели **Расписание** вы можете включить и настроить автоматический запуск задачи по расписанию.

10. Нажмите кнопку **Сохранить**.

Задача на проведение аудита актива создана.

5.2.3. Добавление пароля для доступа по SNMP

► Чтобы добавить в MaxPatrol VM пароль для доступа к активу:

1. В главном меню в разделе **Сбор данных** выберите пункт **Учетные записи**.

   Откроется страница **Учетные записи**.

2. В панели инструментов нажмите кнопку **Добавить учетную запись** и в раскрывшемся меню выберите пункт **Пароль**.

   Откроется страница **Добавление учетной записи**.

3. В поле **Название** введите название учетной записи.

   Примечание. В поле **Описание** вы можете ввести любой текстовый комментарий.

4. В раскрывающемся списке **Метки** установите флажок **SNMP**.
5. В поле **Пароль** введите пароль и подтвердите его в поле **Подтверждение пароля**.
6. Нажмите кнопку **Сохранить**.

Пароль добавлен.

5.2.4. Создание задачи на аудит актива по SNMP

► Чтобы создать задачу на проведение аудита актива:

1. В главном меню в разделе **Сбор данных** выберите пункт **Задачи**.

   Откроется страница **Задачи по сбору данных**.

2. В панели инструментов нажмите кнопку **Создать задачу** и в раскрывшемся меню выберите пункт **Сбор данных**.

   Откроется страница **Создание задачи на сбор данных**.

3. В поле **Название** введите название задачи.
4. Если требуется, добавьте подробное описание задачи по ссылке **Добавить описание**.
5. В раскрывающемся списке **Профиль** выберите **SNMP Network Device Audit**.
6. В иерархическом списке выберите пункт **Сканирование систем** → **По протоколу SNMP**.
7. Если требуется, в раскрывающемся списке выберите другую версию протокола SNMP.

8. В раскрывающемся списке **Учетная запись** выберите учетную запись для доступа к активу.

   Внимание! При использовании протокола SNMP версии 3 пароль учетной записи должен содержать не менее 8 символов.

9. Если требуется, в раскрывающемся списке **Коллекторы** выберите коллекторы для сбора данных.

10. В панели **Цели сбора данных** на вкладке **Включить** в поле **Активы** введите IP-адрес или доменное имя (в формате FQDN) узла актива.

    Примечание. В панели **Расписание** вы можете включить и настроить автоматический запуск задачи по расписанию.

11. Нажмите кнопку **Сохранить**.

Задача на проведение аудита актива создана.

5.3. Avaya (Nortel) NOS, серия ERS: настройка актива

Проверка аудита производилась на ПО версии 5.1.0.015. Корректная работа аудита на других версиях не гарантируется.

Внимание! При использовании в IT-инфраструктуре организации межсетевого экрана или других средств для контроля сетевого трафика требуется настроить в них правила, разрешающие трафик в обоих направлениях между узлом актива и узлом MP 10 Collector. Для проведения аудита актива по протоколу SSH используется порт TCP 22, по протоколу SNMP — порт UDP 162.

На устройстве нельзя создавать учетные записи. Для доступа MP 10 Collector на актив и проведения аудита по протоколу SSH нужно использовать данные учетной записи RO или RW, для доступа по протоколу SNMP — пароль одной из этих учетных записей.

5.4. Avaya (Nortel) NOS, серия ERS: настройка MaxPatrol VM

Для проведения аудита актива по протоколу SSH в MaxPatrol VM нужно добавить учетную запись для доступа к активу, пароль для повышения привилегий (перехода в привилегированный режим EXEC) и создать задачу на проведение аудита.

Для проведения аудита по протоколу SNMP в MaxPatrol VM нужно добавить пароль для доступа к активу и создать задачу на проведение аудита.

В этом разделе

Добавление пароля для доступа по SNMP (см. раздел 5.4.3)

Создание задачи на аудит актива по SNMP (см. раздел 5.4.4)

5.4.1. Добавление учетной записи для доступа по SSH

► Чтобы добавить в MaxPatrol VM учетную запись для доступа к активу:

1. В главном меню в разделе **Сбор данных** выберите пункт **Учетные записи**.

   Откроется страница **Учетные записи**.

2. В панели инструментов нажмите кнопку **Добавить учетную запись** и в раскрывшемся меню выберите пункт **Логин — пароль**.

   Откроется страница **Добавление учетной записи**.

3. В поле **Название** введите название учетной записи.

   Примечание. В поле **Описание** вы можете ввести любой текстовый комментарий.

4. В раскрывающемся списке **Метки** установите флажок **Terminal**.
5. В поле **Логин** введите логин учетной записи.
6. В поле **Пароль** введите пароль и подтвердите его в поле **Подтверждение пароля**.
7. Нажмите кнопку **Сохранить**.

Учетная запись добавлена.

5.4.2. Создание задачи на аудит актива по SSH

► Чтобы создать задачу на проведение аудита актива:

1. В главном меню в разделе **Сбор данных** выберите пункт **Задачи**.

   Откроется страница **Задачи по сбору данных**.

2. В панели инструментов нажмите кнопку **Создать задачу** и в раскрывшемся меню выберите пункт **Сбор данных**.

   Откроется страница **Создание задачи на сбор данных**.

3. В поле **Название** введите название задачи.
4. Если требуется, добавьте подробное описание задачи по ссылке **Добавить описание**.
5. В раскрывающемся списке **Профиль** выберите **SSH Network Device Audit**.
6. В иерархическом списке выберите пункт **Сканирование систем** → **Через терминал: SSH и Telnet**.
7. В раскрывающемся списке **Учетная запись** выберите учетную запись для доступа к активу.

8. Если требуется, в раскрывающемся списке **Коллекторы** выберите коллекторы для сбора данных.
9. В панели **Цели сбора данных** на вкладке **Включить** в поле **Активы** введите IP-адрес или доменное имя (в формате FQDN) узла актива.

   Примечание. В панели **Расписание** вы можете включить и настроить автоматический запуск задачи по расписанию.
10. Нажмите кнопку **Сохранить**.

Задача на проведение аудита актива создана.

5.4.3. Добавление пароля для доступа по SNMP

► Чтобы добавить в MaxPatrol VM пароль для доступа к активу:

1. В главном меню в разделе **Сбор данных** выберите пункт **Учетные записи**.

   Откроется страница **Учетные записи**.
2. В панели инструментов нажмите кнопку **Добавить учетную запись** и в раскрывшемся меню выберите пункт **Пароль**.

   Откроется страница **Добавление учетной записи**.
3. В поле **Название** введите название учетной записи.

   Примечание. В поле **Описание** вы можете ввести любой текстовый комментарий.
4. В раскрывающемся списке **Метки** установите флажок **SNMP**.
5. В поле **Пароль** введите пароль и подтвердите его в поле **Подтверждение пароля**.
6. Нажмите кнопку **Сохранить**.

Пароль добавлен.

5.4.4. Создание задачи на аудит актива по SNMP

► Чтобы создать задачу на проведение аудита актива:

1. В главном меню в разделе **Сбор данных** выберите пункт **Задачи**.

   Откроется страница **Задачи по сбору данных**.
2. В панели инструментов нажмите кнопку **Создать задачу** и в раскрывшемся меню выберите пункт **Сбор данных**.

   Откроется страница **Создание задачи на сбор данных**.
3. В поле **Название** введите название задачи.
4. Если требуется, добавьте подробное описание задачи по ссылке **Добавить описание**.

5. В раскрывающемся списке **Профиль** выберите **SNMP Network Device Audit**.
6. В иерархическом списке выберите пункт **Сканирование систем** → **По протоколу SNMP**.
7. Если требуется, в раскрывающемся списке выберите другую версию протокола SNMP.
8. В раскрывающемся списке **Учетная запись** выберите учетную запись для доступа к активу.

   Внимание! При использовании протокола SNMP версии 3 пароль учетной записи должен содержать не менее 8 символов.
9. Если требуется, в раскрывающемся списке **Коллекторы** выберите коллекторы для сбора данных.
10. В панели **Цели сбора данных** на вкладке **Включить** в поле **Активы** введите IP-адрес или доменное имя (в формате FQDN) узла актива.

    Примечание. В панели **Расписание** вы можете включить и настроить автоматический запуск задачи по расписанию.
11. Нажмите кнопку **Сохранить**.

Задача на проведение аудита актива создана.

5.5. Check Point GAiA OS 76, 77.10, 77.20, 77.30: настройка актива

Настройку актива нужно выполнять от имени учетной записи администратора устройства.

Внимание! При использовании в IT-инфраструктуре организации межсетевого экрана или других средств для контроля сетевого трафика требуется настроить в них правила, разрешающие трафик в обоих направлениях между узлом актива и узлом MP 10 Collector. Для проведения аудита актива используются TCP-порт 18190. Для проведения аудита по протоколу SSH используется порт TCP 22.

Для проведения аудита для доступа MP 10 Collector на активе требуется создать учетную запись администратора и получить сертификат сервера управления. Для проведения аудита по протоколу SSH требуется создать учетную запись.

В этом разделе

5.5.1. Создание учетной записи

► Чтобы создать учетную запись администратора сервера управления:

1. Запустите SmartConsole.
2. В открывшемся окне введите данные учетной записи и IP-адрес для подключения к серверу управления. Нажмите кнопку **Login**.
3. Выберите вкладку **Users and Administrators**.
4. В контекстном меню узла **Administrators** выберите **New Administrator**.
5. В открывшемся окне **Administrator Properties** в поле **User Name** введите имя учетной записи.

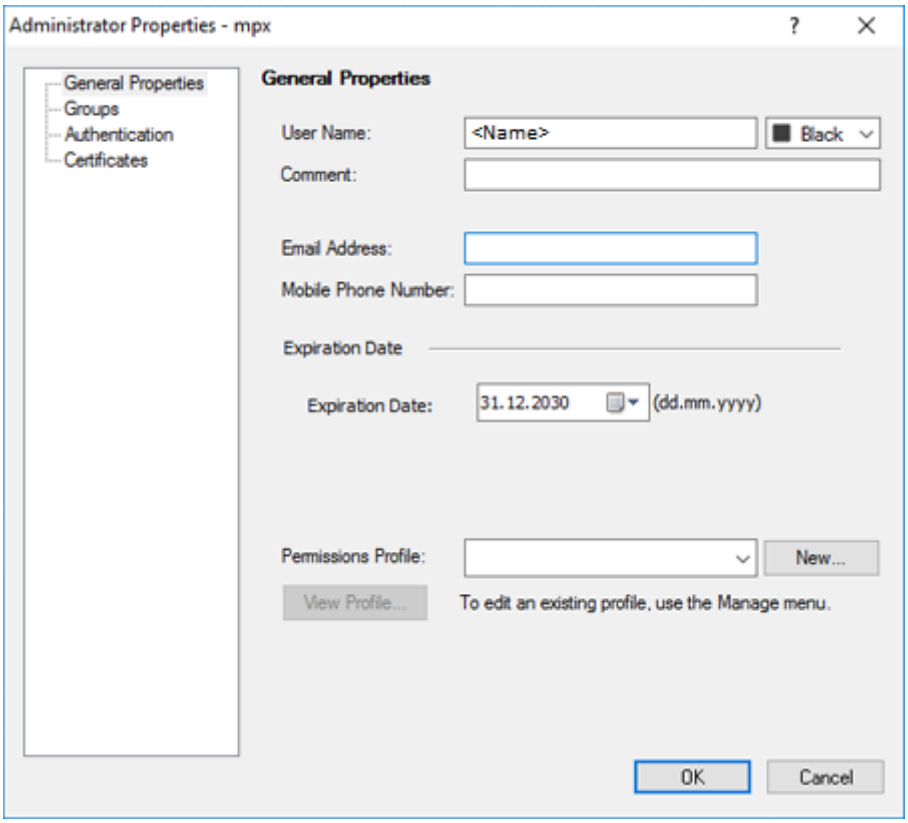

Рисунок 1. Настройка учетной записи

6. Справа от поля **Permission Profile** нажмите кнопку **New**.
7. В открывшемся окне **Permission Profile Properties** укажите параметры профиля.

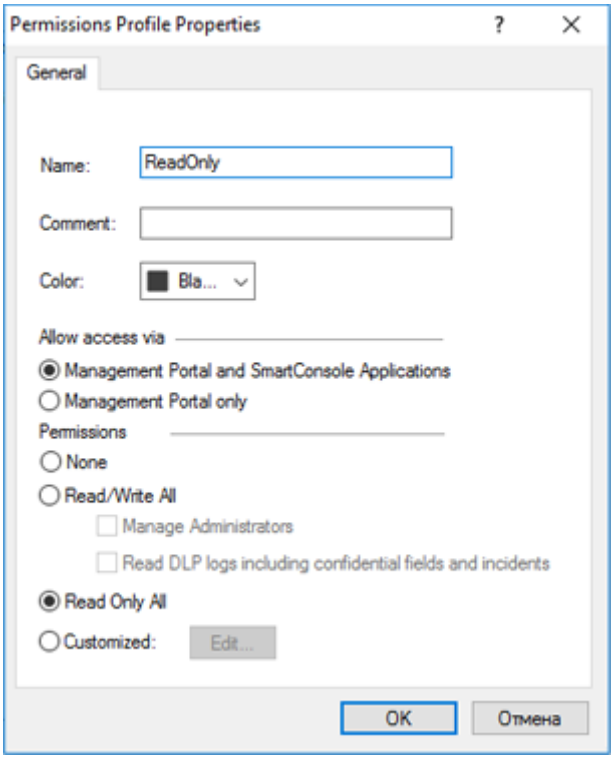

Рисунок 2. Настройка профиля учетной записи

8. В левой части окна **Administrator Properties** выберите узел **Authentication**.
9. В раскрывающемся списке **Authentication Scheme** выберите способ проверки **Check Point Password**.
10. В поле **Password** введите пароль для входа, в поле **Confirm Password** подтвердите его.

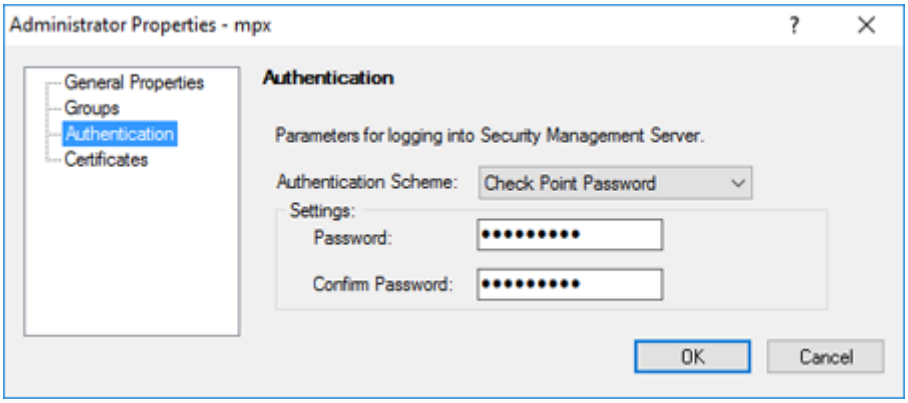

Рисунок 3. Настройка способа проверки учетной записи

11. Нажмите кнопку **OK**.

Учетная запись администратора создана.

5.5.2. Создание приложения OPSEC в GAiA R76, R77

► Чтобы создать приложение OPSEC:

1. Запустите SmartConsole.
2. В открывшемся окне введите данные учетной записи и IP-адрес для подключения к серверу управления. Нажмите кнопку **Login**.
3. Выберите вкладку **Servers and OPSEC**.
4. В контекстном меню узла **OPSEC Application** выберите **New OPSEC Application**.

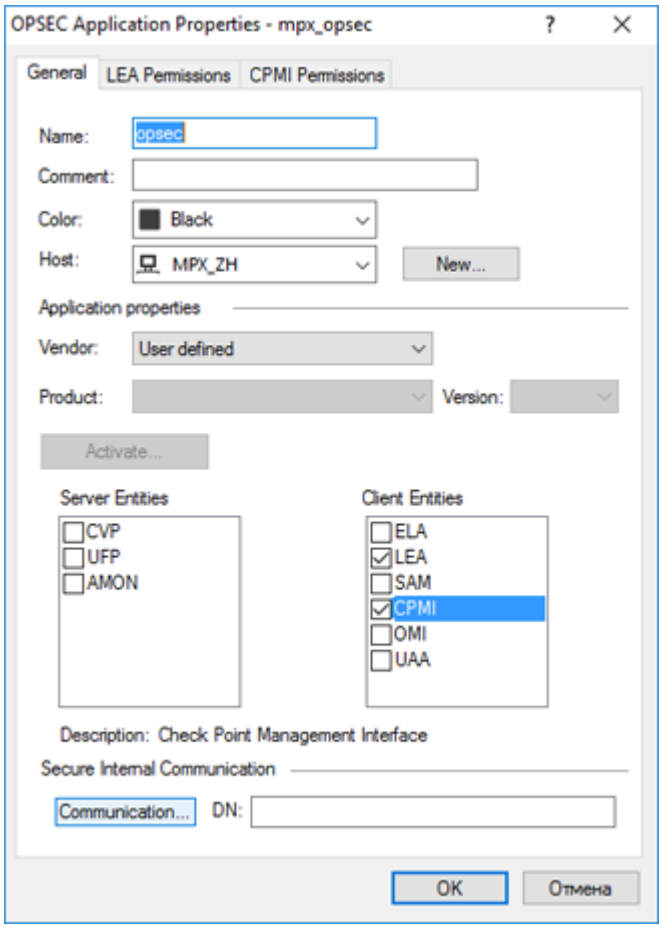

Рисунок 4. Настройка параметров приложения

5. В открывшемся окне в поле **Name** введите название приложения.

   Примечание. Название приложения OPSEC вам понадобится при экспорте сертификата.

6. Нажмите кнопку **New**.
7. В открывшемся окне введите IP-адрес узла MP 10 Collector и нажмите кнопку **OK**.
8. В списке **Client Entitles** установите флажки **CPMI** и **LEA**.

9. Выберите вкладку **CPMI Permissions**.

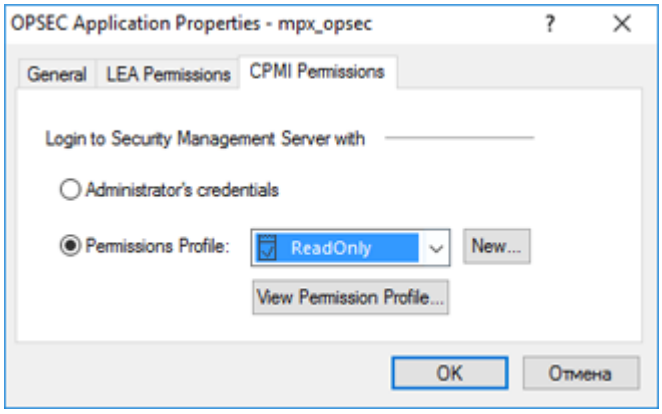

Рисунок 5. Настройка прав доступа приложения

10. Выберите вариант **Permissions Profile**, в раскрывающемся списке выберите **ReadOnly**.
11. Выберите вкладку **General**.
12. В нижней части вкладки нажмите кнопку **Communication**.

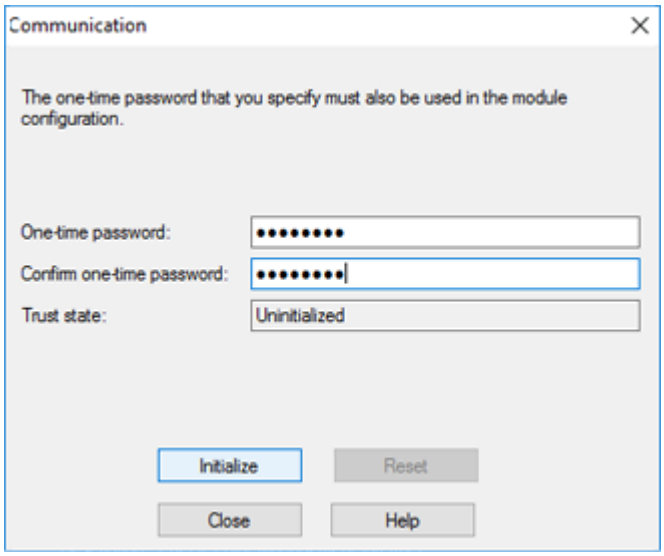

Рисунок 6. Создание пароля доступа

13. В открывшемся окне в поле **One-time password** введите пароль и повторите его в поле **Confirm one-time password**.

    Примечание. Созданный пароль вам понадобится при экспорте сертификата.

14. Нажмите кнопку **Initialize**.
15. Нажмите кнопку **Close**.
16. В окне **OPSEC Application Properties** нажмите кнопку **OK**.
17. В контекстном меню созданного приложения OPSEC выберите **Edit**.

Откроется окно **OPSEC Application Properties — <Название приложения>**. В поле **DN** будет указано SIC-имя приложения OPSEC.

Примечание. SIC-имя приложения OPSEC вам понадобится при добавлении сертификата в MaxPatrol VM.

18. Нажмите кнопку **OK**.
19. В панели инструментов нажмите кнопку , чтобы сохранить политику безопасности.
20. В панели инструментов нажмите кнопку . В открывшемся меню выберите **Policy** → **Install**, чтобы загрузить политику безопасности в устройства.

Приложение создано.

5.5.3. Экспорт сертификата

Для экспорта сертификата требуется утилита `opsec_pull_cert.exe`. Она входит в комплект разработчика OPSEC SDK, который вы можете скачать с сайта checkpoint.com.

► Чтобы экспортировать сертификат,

запустите утилиту со следующими параметрами:

```
opsec_pull_cert.exe -h <IP-адрес сервера управления> -n <Название приложения OPSEC> -p
<Пароль для входа в приложение OPSEC> -o <Имя файла сертификата>
```

Файл сертификата экспортирован.

5.5.4. Создание учетной записи для доступа к активу по SSH

► Чтобы создать учетную запись для доступа к активу:

1. На узле, с которого производится настройка актива, запустите терминальный клиент, поддерживающий сетевые протоколы SSH и Telnet.
2. Авторизуйтесь на активе.
3. Создайте учетную запись для доступа к активу:
4. `add user <Логин> uid 0 homedir /home/<Логин>`
5. Установите пароль учетной записи:
   `set user <Логин> password`
6. Введите пароль.

7. Назначьте учетной записи роль администратора:
   ```
   add rba user <Логин> roles adminRole
   ```
8. Сохраните изменения:
   ```
   save config
   ```

Учетная запись создана.

5.6. Check Point GAiA OS 76, 77.10, 77.20, 77.30: настройка MaxPatrol VM

Для аудита актива в MaxPatrol VM нужно добавить учетную запись и сертификат сервера управления и создать задачу на проведение аудита.

В этом разделе

5.6.1. Добавление учетной записи

► Чтобы добавить в MaxPatrol VM учетную запись для доступа к активу:

1. В главном меню в разделе **Сбор данных** выберите пункт **Учетные записи**.

   Откроется страница **Учетные записи**.
2. В панели инструментов нажмите кнопку **Добавить учетную запись** и в раскрывшемся меню выберите пункт **Логин — пароль**.

   Откроется страница **Добавление учетной записи**.
3. В поле **Название** введите название учетной записи.

   Примечание. В поле **Описание** вы можете ввести любой текстовый комментарий.
4. В раскрывающемся списке **Метки** установите флажки **OPSEC_Audit** и **OPSEC_Logs**.
5. В поле **Логин** введите логин учетной записи администратора сервера управления.
6. Если требуется, в поле **Пароль** введите пароль и подтвердите его в поле **Подтверждение пароля**.
7. Нажмите кнопку **Сохранить**.

Учетная запись добавлена.

5.6.2. Добавление сертификата

► Чтобы добавить в MaxPatrol VM сертификат для доступа к активу:

1. В главном меню в разделе **Сбор данных** выберите пункт **Учетные записи**.

   Откроется страница **Учетные записи**.

2. В панели инструментов нажмите кнопку **Добавить учетную запись** и в раскрывшемся меню выберите пункт **Сертификат**.

   Откроется страница **Добавление учетной записи**.

3. В поле **Название** введите название сертификата.

   Примечание. В поле **Описание** вы можете ввести любой текстовый комментарий.

4. В раскрывающемся списке **Метки** установите флажки **OPSEC_Audit** и **OPSEC_Logs**.

5. По ссылке **Выбрать** в блоке параметров **Сертификат** укажите расположение файла сертификата.

6. В поле **Логин** введите SIC-имя приложения OPSEC.

   `CN=<Название приложения OPSEC>, O=<SIC-имя приложения>`

7. Нажмите кнопку **Сохранить**.

Сертификат добавлен.

5.6.3. Создание задачи на аудит актива

► Чтобы создать задачу на проведение аудита актива:

1. В главном меню в разделе **Сбор данных** выберите пункт **Задачи**.

   Откроется страница **Задачи по сбору данных**.

2. В панели инструментов нажмите кнопку **Создать задачу** и в раскрывшемся меню выберите пункт **Сбор данных**.

   Откроется страница **Создание задачи на сбор данных**.

3. В поле **Название** введите название задачи.

4. Если требуется, добавьте подробное описание задачи по ссылке **Добавить описание**.

5. В раскрывающемся списке **Профиль** выберите **Checkpoint OPSEC Audit**.

6. В иерархическом списке выберите пункт **Сканирование систем** → **Check Point через OPSEC**.

7. В раскрывающемся списке **Учетная запись** выберите сертификат для доступа к активу.

8. В раскрывающемся списке **Учетная запись CPMI** выберите учетную запись для доступа к активу.

9. Если требуется, в раскрывающемся списке **Коллекторы** выберите коллекторы для сбора данных.
10. В панели **Цели сбора данных** на вкладке **Включить** в поле **Активы** введите IP-адрес или доменное имя (в формате FQDN) сервера управления.

    Примечание. В панели **Расписание** вы можете включить и настроить автоматический запуск задачи по расписанию.
11. Нажмите кнопку **Сохранить**.

Задача на проведение аудита актива создана.

5.6.4. Добавление учетной записи для доступа по SSH

► Чтобы добавить в MaxPatrol VM учетную запись для доступа к активу:

1. В главном меню в разделе **Сбор данных** выберите пункт **Учетные записи**.

   Откроется страница **Учетные записи**.
2. В панели инструментов нажмите кнопку **Добавить учетную запись** и в раскрывшемся меню выберите пункт **Логин — пароль**.

   Откроется страница **Добавление учетной записи**.
3. В поле **Название** введите название учетной записи.

   Примечание. В поле **Описание** вы можете ввести любой текстовый комментарий.
4. В раскрывающемся списке **Метки** установите флажок **Terminal**.
5. В поле **Логин** введите логин учетной записи.
6. В поле **Пароль** введите пароль и подтвердите его в поле **Подтверждение пароля**.
7. Нажмите кнопку **Сохранить**.

Учетная запись добавлена.

5.6.5. Создание задачи на аудит актива по SSH

► Чтобы создать задачу на проведение аудита актива:

1. В главном меню в разделе **Сбор данных** выберите пункт **Задачи**.

   Откроется страница **Задачи по сбору данных**.
2. В панели инструментов нажмите кнопку **Создать задачу** и в раскрывшемся меню выберите пункт **Сбор данных**.

   Откроется страница **Создание задачи на сбор данных**.
3. В поле **Название** введите название задачи.

4. Если требуется, добавьте подробное описание задачи по ссылке **Добавить описание**.
5. В раскрывающемся списке **Профиль** выберите **SSH Network Device Audit**.
6. В иерархическом списке выберите пункт **Сканирование систем** → **Через терминал: SSH и Telnet**.
7. В раскрывающемся списке **Учетная запись** выберите учетную запись для доступа к активу.
8. Если требуется, в раскрывающемся списке **Коллекторы** выберите коллекторы для сбора данных.
9. В панели **Цели сбора данных** на вкладке **Включить** в поле **Активы** введите IP-адрес или доменное имя (в формате FQDN) узла актива.

   Примечание. В панели **Расписание** вы можете включить и настроить автоматический запуск задачи по расписанию.
10. Нажмите кнопку **Сохранить**.

Задача на проведение аудита актива создана.

5.7. Check Point GAiA OS 80.10—81.10: настройка актива

Настройку актива нужно выполнять от имени учетной записи администратора с правом перехода в режим конфигурации.

Внимание! При использовании в IT-инфраструктуре организации межсетевого экрана или других средств для контроля сетевого трафика требуется настроить в них правила, разрешающие трафик в обоих направлениях между узлом актива и узлом MP 10 Collector. Для проведения аудита актива по протоколу SSH используется порт TCP 22.

Для проведения аудита требуется:

1. Запустить Management API на сервере управления Check Point GAiA.
2. Создать учетную запись для доступа MP 10 Collector на актив по протоколу SSH.

   Примечание. Данные этой учетной записи нужно указать при добавлении учетной записи и пароля в MaxPatrol VM.
3. На базе этой же учетной записи создать учетную запись администратора сервера управления Check Point GAiA.

В этом разделе

5.7.1. Запуск Management API

Для проведения аудита требуется компонент Management API, который входит в состав сервера управления Check Point GAiA.

► Чтобы запустить компонент Management API на сервере управления:

1. На узле, с которого производится настройка актива, запустите терминальный клиент, поддерживающий сетевые протоколы SSH и Telnet.
2. Авторизуйтесь на активе.
3. Проверьте статус Management API:
   `api status`
4. Если ответ на экране содержит `Overall API Status: The API Server Is Not Running!`, запустите Management API:
   `api start`

Management API запущен.

5.7.2. Создание учетной записи для доступа к активу по SSH

► Чтобы создать учетную запись для доступа к активу:

1. На узле, с которого производится настройка актива, запустите терминальный клиент, поддерживающий сетевые протоколы SSH и Telnet.
2. Авторизуйтесь на активе.
3. Создайте учетную запись для доступа к активу:
4. `add user <Логин> uid 0 homedir /home/<Логин>`
5. Установите пароль учетной записи:
   `set user <Логин> password`
6. Введите пароль.
7. Назначьте учетной записи роль администратора:
   `add rba user <Логин> roles adminRole`
8. Сохраните изменения:
   `save config`

Учетная запись создана.

5.7.3. Создание учетной записи администратора сервера управления

► Чтобы создать учетную запись администратора сервера управления:

1. Запустите SmartConsole.
2. В открывшемся окне введите данные учетной записи и IP-адрес для подключения к серверу управления. Нажмите кнопку **Login**.
3. В левой части страницы нажмите кнопку **MANAGE & SETTINGS**.
4. В боковой панели выберите **Permissions & Administrators** → **Permission Profile**.
5. Нажмите ✳.

   Откроется окно **Profile**.
6. В верхней части окна введите название профиля.
7. В левой части окна выберите пункт **Management**.
8. Установите флажок **Management API Login**.
9. Нажмите кнопку **Close**.
10. В боковой панели выберите **Permissions & Administrators** → **Administrators**.
11. Нажмите ✳.

    Откроется окно **Administrator**.
12. В верхней части окна введите логин созданной ранее учетной записи для доступа к активу по SSH.
13. В раскрывающемся списке **Authentication Method** выберите **OS Password**.
14. В раскрывающемся списке **Permission Profile** выберите созданный профиль.
15. Нажмите кнопку **OK**.
16. В верхней части окна нажмите кнопку **Publish** и подтвердите публикацию.
17. В верхней части окна нажмите кнопку **Install Policy** и подтвердите установку политики.

Учетная запись создана.

5.8. Check Point GAiA OS 80.10—81.10: настройка MaxPatrol VM

Для аудита актива в MaxPatrol VM нужно добавить учетную запись для доступа по протоколу SSH, пароль для повышения привилегий, создать и запустить задачу на проведение аудита.

В этом разделе

5.8.1. Добавление учетной записи для доступа по SSH

► Чтобы добавить в MaxPatrol VM учетную запись для доступа к активу:

1. В главном меню в разделе **Сбор данных** выберите пункт **Учетные записи**.

   Откроется страница **Учетные записи**.

2. В панели инструментов нажмите кнопку **Добавить учетную запись** и в раскрывшемся меню выберите пункт **Логин — пароль**.

   Откроется страница **Добавление учетной записи**.

3. В поле **Название** введите название учетной записи.

   Примечание. В поле **Описание** вы можете ввести любой текстовый комментарий.

4. В раскрывающемся списке **Метки** установите флажок **Terminal**.
5. В поле **Логин** введите логин учетной записи.
6. В поле **Пароль** введите пароль и подтвердите его в поле **Подтверждение пароля**.
7. Нажмите кнопку **Сохранить**.

Учетная запись добавлена.

5.8.2. Добавление пароля для повышения привилегий для аудита по SSH

► Чтобы добавить в MaxPatrol VM пароль для повышения привилегий:

1. В главном меню в разделе **Сбор данных** выберите пункт **Учетные записи**.

   Откроется страница **Учетные записи**.

2. В панели инструментов нажмите кнопку **Добавить учетную запись** и в раскрывшемся меню выберите пункт **Пароль**.

   Откроется страница **Добавление учетной записи**.

3. В поле **Название** введите название учетной записи.

   Примечание. В поле **Описание** вы можете ввести любой текстовый комментарий.

4. В раскрывающемся списке **Метки** установите флажок **Terminal**.

5. В поле **Пароль** введите пароль и подтвердите его в поле **Подтверждение пароля**.
6. Нажмите кнопку **Сохранить**.

Пароль добавлен.

5.8.3. Создание задачи на аудит актива по SSH

► Чтобы создать задачу на проведение аудита актива:

1. В главном меню в разделе **Сбор данных** выберите пункт **Задачи**.

   Откроется страница **Задачи по сбору данных**.
2. В панели инструментов нажмите кнопку **Создать задачу** и в раскрывшемся меню выберите пункт **Сбор данных**.

   Откроется страница **Создание задачи на сбор данных**.
3. В поле **Название** введите название задачи.
4. Если требуется, добавьте подробное описание задачи по ссылке **Добавить описание**.
5. В раскрывающемся списке **Профиль** выберите **Checkpoint Management Server SSH Audit**.
6. В иерархическом списке выберите пункт **Сканирование систем** → **Через терминал: SSH**.
7. В раскрывающемся списке **Учетная запись** выберите учетную запись для доступа к активу.
8. В раскрывающемся списке **Учетная запись для повышения привилегий** выберите пароль для повышения привилегий на активе.
9. Если требуется, в раскрывающемся списке **Коллекторы** выберите коллекторы для сбора данных.
10. В панели **Цели сбора данных** на вкладке **Включить** в поле **Активы** введите IP-адрес или доменное имя (в формате FQDN) узла актива.

    Примечание. В панели **Расписание** вы можете включить и настроить автоматический запуск задачи по расписанию.
11. Нажмите кнопку **Сохранить**.

Задача на проведение аудита актива создана.

5.9. Cisco IOS 12, 15, 16: настройка актива

Настройку актива нужно выполнять от имени учетной записи с правом перехода в режим глобальной конфигурации.

Внимание! При использовании в IT-инфраструктуре организации межсетевого экрана или других средств для контроля сетевого трафика требуется настроить в них правила, разрешающие трафик в обоих направлениях между узлом актива и узлом MP 10 Collector. Для проведения аудита актива по протоколу SSH используется порт TCP 22, по протоколу SNMP — порт UDP 162.

Для проведения аудита на активе нужно создать учетную запись для доступа MP 10 Collector по протоколу SSH и пароль для доступа по протоколу SNMP.

В этом разделе

5.9.1. Создание учетной записи для доступа к активу по SSH

Внимание! Эта инструкция разработана для аутентификации пользователей на сетевом устройстве методом Local. В этом случае данные учетных записей хранятся на самом устройстве.

Для аутентификации пользователей методом Local в файле конфигурации сетевого устройства должны присутствовать строки:

```
aaa new-model
aaa authentication login default local
aaa authorization exec default local
```

Примечание. Вы можете просмотреть файл конфигурации сетевого устройства, выполнив команду `show running-config`.

Для проведения аудита требуется учетная запись с уровнем привилегий 15 или с возможностью повышения до уровня 15 с помощью команды `enable`. Уровень 15 является максимальным и позволяет пользователю с такой учетной записью выполнять на сетевом устройстве все команды. Для повышения привилегий до уровня 15 на сетевом устройстве должен быть разрешен переход в привилегированный режим EXEC (выполнение команды `enable`) после ввода пароля. Для этого в файле конфигурации сетевого устройства должна присутствовать строка:

```
aaa authentication enable default enable
```

► Чтобы создать учетную запись для доступа к активу:

1. На узле, с которого производится настройка актива, запустите терминальный клиент, поддерживающий сетевые протоколы SSH и Telnet.
2. Авторизуйтесь на активе.
3. Перейдите в режим конфигурирования:
   `configure terminal`

4. Создайте учетную запись для доступа к активу:
   `username <Логин> secret <Пароль>`

   Примечание. Если для ограничения доступа к активу по протоколу SSH используется список доступа, добавьте IP-адрес узла MP 10 Collector в этот список.

5. Выйдите из режима конфигурирования:
   `end`

6. Сохраните изменения:
   `write memory`

Учетная запись создана.

5.9.2. Создание пароля для доступа к активу по SNMP

► Чтобы создать пароль для доступа к активу:

1. На узле, с которого производится настройка актива, запустите терминальный клиент, поддерживающий сетевые протоколы SSH и Telnet.
2. Авторизуйтесь на активе.
3. Перейдите в режим конфигурирования:
   `configure terminal`
4. Если для ограничения доступа по протоколу SNMP используется список доступа, добавьте IP-адрес узла MP 10 Collector в этот список:
   `access-list <Имя (номер) списка доступа> permit host <IP-адрес MP 10 Collector>`
5. Создайте пароль для доступа к активу и добавьте его в используемый список доступа:
   `snmp-server community <Пароль> ro <Имя (номер) списка доступа>`
6. Выйдите из режима конфигурирования:
   `end`
7. Сохраните изменения:
   `write memory`

Пароль создан.

5.10. Cisco IOS 12, 15, 16 : настройка MaxPatrol VM

Для проведения аудита актива по протоколу SSH в MaxPatrol VM нужно добавить учетную запись для доступа к активу, пароль для повышения привилегий (перехода в привилегированный режим EXEC) и создать задачу на проведение аудита.

Для проведения аудита по протоколу SNMP в MaxPatrol VM нужно добавить пароль для доступа к активу и создать задачу на проведение аудита.

В этом разделе

5.10.1. Добавление учетной записи для доступа по SSH

► Чтобы добавить в MaxPatrol VM учетную запись для доступа к активу:

1. В главном меню в разделе **Сбор данных** выберите пункт **Учетные записи**.

   Откроется страница **Учетные записи**.

2. В панели инструментов нажмите кнопку **Добавить учетную запись** и в раскрывшемся меню выберите пункт **Логин — пароль**.

   Откроется страница **Добавление учетной записи**.

3. В поле **Название** введите название учетной записи.

   Примечание. В поле **Описание** вы можете ввести любой текстовый комментарий.

4. В раскрывающемся списке **Метки** установите флажок **Terminal**.
5. В поле **Логин** введите логин учетной записи.
6. В поле **Пароль** введите пароль и подтвердите его в поле **Подтверждение пароля**.
7. Нажмите кнопку **Сохранить**.

Учетная запись добавлена.

5.10.2. Добавление пароля для повышения привилегий для аудита по SSH

► Чтобы добавить в MaxPatrol VM пароль для повышения привилегий:

1. В главном меню в разделе **Сбор данных** выберите пункт **Учетные записи**.

   Откроется страница **Учетные записи**.

2. В панели инструментов нажмите кнопку **Добавить учетную запись** и в раскрывшемся меню выберите пункт **Пароль**.

   Откроется страница **Добавление учетной записи**.

3. В поле **Название** введите название учетной записи.

Примечание. В поле **Описание** вы можете ввести любой текстовый комментарий.

4. В раскрывающемся списке **Метки** установите флажок **Terminal**.
5. В поле **Пароль** введите пароль и подтвердите его в поле **Подтверждение пароля**.
6. Нажмите кнопку **Сохранить**.

Пароль добавлен.

5.10.3. Создание задачи на аудит актива по SSH

► Чтобы создать задачу на проведение аудита актива:

1. В главном меню в разделе **Сбор данных** выберите пункт **Задачи**.

   Откроется страница **Задачи по сбору данных**.

2. В панели инструментов нажмите кнопку **Создать задачу** и в раскрывшемся меню выберите пункт **Сбор данных**.

   Откроется страница **Создание задачи на сбор данных**.

3. В поле **Название** введите название задачи.
4. Если требуется, добавьте подробное описание задачи по ссылке **Добавить описание**.
5. В раскрывающемся списке **Профиль** выберите **SSH Cisco Audit in Enable Mode**.

   Внимание! Если для доступа к активу по протоколу SSH вы используете учетную запись с уровнем привилегий 15 (не требуется повышение привилегий), для проведения аудита нужно использовать профиль SSH Network Device Audit.

6. В иерархическом списке выберите пункт **Сканирование систем** → **Через терминал: SSH и Telnet**.
7. В раскрывающемся списке **Учетная запись** выберите учетную запись для доступа к активу.
8. В раскрывающемся списке **Учетная запись для повышения привилегий** выберите учетную запись для повышения привилегий на активе.

   Примечание. Если в IT-инфраструктуре организации используется BGP-маршрутизация с полной таблицей маршрутов (Full View), включите отображение дополнительных параметров и добавьте разрешенную команду `^(?!show ip route vrf *).*$`.

9. Если требуется, в раскрывающемся списке **Коллекторы** выберите коллекторы для сбора данных.
10. В панели **Цели сбора данных** на вкладке **Включить** в поле **Активы** введите IP-адрес или доменное имя (в формате FQDN) узла актива.

Примечание. В панели **Расписание** вы можете включить и настроить автоматический запуск задачи по расписанию.

11. Нажмите кнопку **Сохранить**.

Задача на проведение аудита актива создана.

5.10.4. Добавление пароля для доступа по SNMP

► Чтобы добавить в MaxPatrol VM пароль для доступа к активу:

1. В главном меню в разделе **Сбор данных** выберите пункт **Учетные записи**.

   Откроется страница **Учетные записи**.

2. В панели инструментов нажмите кнопку **Добавить учетную запись** и в раскрывшемся меню выберите пункт **Пароль**.

   Откроется страница **Добавление учетной записи**.

3. В поле **Название** введите название учетной записи.

   Примечание. В поле **Описание** вы можете ввести любой текстовый комментарий.

4. В раскрывающемся списке **Метки** установите флажок **SNMP**.
5. В поле **Пароль** введите пароль и подтвердите его в поле **Подтверждение пароля**.
6. Нажмите кнопку **Сохранить**.

Пароль добавлен.

5.10.5. Создание задачи на аудит актива по SNMP

► Чтобы создать задачу на проведение аудита актива:

1. В главном меню в разделе **Сбор данных** выберите пункт **Задачи**.

   Откроется страница **Задачи по сбору данных**.

2. В панели инструментов нажмите кнопку **Создать задачу** и в раскрывшемся меню выберите пункт **Сбор данных**.

   Откроется страница **Создание задачи на сбор данных**.

3. В поле **Название** введите название задачи.
4. Если требуется, добавьте подробное описание задачи по ссылке **Добавить описание**.
5. В раскрывающемся списке **Профиль** выберите **SNMP Network Device Audit**.
6. В иерархическом списке выберите пункт **Сканирование систем** → **По протоколу SNMP**.
7. Если требуется, в раскрывающемся списке выберите другую версию протокола SNMP.

8. В раскрывающемся списке **Учетная запись** выберите учетную запись для доступа к активу.

   Внимание! При использовании протокола SNMP версии 3 пароль учетной записи должен содержать не менее 8 символов.

9. Если требуется, в раскрывающемся списке **Коллекторы** выберите коллекторы для сбора данных.

10. В панели **Цели сбора данных** на вкладке **Включить** в поле **Активы** введите IP-адрес или доменное имя (в формате FQDN) узла актива.

    Примечание. В панели **Расписание** вы можете включить и настроить автоматический запуск задачи по расписанию.

11. Нажмите кнопку **Сохранить**.

Задача на проведение аудита актива создана.

5.11. Cisco IOS XE 12, 15, 16: настройка актива

Настройка актива для проведения аудита выполняется аналогично Cisco IOS 12, 15, 16 (см. раздел 5.9).

5.12. Cisco IOS XE 12, 15, 16: настройка MaxPatrol VM

Настройка MaxPatrol VM для проведения аудита актива выполняется аналогично Cisco IOS 12, 15, 16 (см. раздел 5.10).

5.13. Cisco IOS XR, серия ASR9000: настройка актива

Проверка аудита производилась на ПО версий 4.3.4, 6.1.1, 6.4.2. Корректная работа аудита на других версиях не гарантируется.

Внимание! Эта инструкция разработана для случая локальной авторизации пользователей на активе и неприменима при использовании централизованной системы аутентификации.

Настройку актива нужно выполнять от имени учетной записи с правом перехода в режим глобальной конфигурации.

Внимание! При использовании в IT-инфраструктуре организации межсетевого экрана или других средств для контроля сетевого трафика требуется настроить в них правила, разрешающие трафик в обоих направлениях между узлом актива и узлом MP 10 Collector. Для проведения аудита актива по протоколу SSH используется порт TCP 22.

Для проведения аудита на активе нужно создать учетную запись для доступа MP 10 Collector по протоколу SSH.

► Чтобы создать учетную запись для доступа к активу:

1. На узле, с которого производится настройка актива, запустите терминальный клиент, поддерживающий сетевые протоколы SSH и Telnet.
2. Авторизуйтесь на активе.
3. Перейдите в режим конфигурирования:
   ```
   admin configure terminal
   ```
4. Создайте учетную запись для доступа к активу:
   ```
   username <Логин>
   secret <Пароль>
   group root-system
   ```
5. Примените внесенные изменения:
   ```
   commit
   ```
6. Выйдите из режима конфигурирования:
   ```
   exit
   ```

Учетная запись создана.

5.14. Cisco IOS XR, серия ASR9000: настройка MaxPatrol VM

Для проведения аудита актива по протоколу SSH в MaxPatrol VM нужно добавить учетную запись для доступа к активу, создать и запустить задачу на проведение аудита.

В этом разделе

5.14.1. Добавление учетной записи для доступа по SSH

► Чтобы добавить в MaxPatrol VM учетную запись для доступа к активу:

1. В главном меню в разделе **Сбор данных** выберите пункт **Учетные записи**.

   Откроется страница **Учетные записи**.
2. В панели инструментов нажмите кнопку **Добавить учетную запись** и в раскрывшемся меню выберите пункт **Логин — пароль**.

   Откроется страница **Добавление учетной записи**.
3. В поле **Название** введите название учетной записи.

   Примечание. В поле **Описание** вы можете ввести любой текстовый комментарий.

4. В раскрывающемся списке **Метки** установите флажок **Terminal**.
5. В поле **Логин** введите логин учетной записи.
6. В поле **Пароль** введите пароль и подтвердите его в поле **Подтверждение пароля**.
7. Нажмите кнопку **Сохранить**.

Учетная запись добавлена.

5.14.2. Создание задачи на аудит актива по SSH

► Чтобы создать задачу на проведение аудита актива:

1. В главном меню в разделе **Сбор данных** выберите пункт **Задачи**.

   Откроется страница **Задачи по сбору данных**.
2. В панели инструментов нажмите кнопку **Создать задачу** и в раскрывшемся меню выберите пункт **Сбор данных**.

   Откроется страница **Создание задачи на сбор данных**.
3. В поле **Название** введите название задачи.
4. Если требуется, добавьте подробное описание задачи по ссылке **Добавить описание**.
5. В раскрывающемся списке **Профиль** выберите **SSH Network Device Audit**.
6. В иерархическом списке выберите пункт **Сканирование систем** → **Через терминал: SSH и Telnet**.
7. В раскрывающемся списке **Учетная запись** выберите учетную запись для доступа к активу.
8. Если требуется, в раскрывающемся списке **Коллекторы** выберите коллекторы для сбора данных.
9. В панели **Цели сбора данных** на вкладке **Включить** в поле **Активы** введите IP-адрес или доменное имя (в формате FQDN) узла актива.

   Примечание. В панели **Расписание** вы можете включить и настроить автоматический запуск задачи по расписанию.
10. Нажмите кнопку **Сохранить**.

Задача на проведение аудита актива создана.

5.15. Cisco NX-OS 4—7: настройка актива

Настройку актива нужно выполнять от имени учетной записи с правом перехода в режим глобальной конфигурации.

Внимание! При использовании в IT-инфраструктуре организации межсетевого экрана или других средств для контроля сетевого трафика требуется настроить в них правила, разрешающие трафик в обоих направлениях между узлом актива и узлом MP 10 Collector. Для проведения аудита актива по протоколу SSH используется порт TCP 22, по протоколу SNMP — порт UDP 162.

Для проведения аудита на активе нужно создать учетную запись для доступа MP 10 Collector по протоколу SSH и пароль для доступа по протоколу SNMP.

В этом разделе

Создание учетной записи для доступа к активу по SSH (см. раздел 5.15.1)

Создание пароля для доступа к активу по SNMP (см. раздел 5.15.2)

5.15.1. Создание учетной записи для доступа к активу по SSH

Внимание! Эта инструкция разработана для аутентификации пользователей на сетевом устройстве методом Local. В этом случае данные учетных записей хранятся на самом устройстве.

Для аутентификации пользователей методом Local в файле конфигурации сетевого устройства должны присутствовать строки:

```
aaa authentication ssh console LOCAL
aaa authorization exec LOCAL auto-enable
```

Примечание. Вы можете просмотреть файл конфигурации сетевого устройства, выполнив команду `show running-config`.

► Чтобы создать учетную запись для доступа к активу:

1. На узле, с которого производится настройка актива, запустите терминальный клиент, поддерживающий сетевые протоколы SSH и Telnet.
2. Авторизуйтесь на активе.
3. Перейдите в режим конфигурирования:
   ```
   configure terminal
   ```
4. Создайте учетную запись для доступа к активу:
   ```
   username <Логин> password <Пароль> role network-admin
   ```

   Примечание. Если для ограничения доступа к активу по протоколу SSH используется список доступа, добавьте IP-адрес узла MP 10 Collector в этот список.

5. Выйдите из режима конфигурирования:
   ```
   end
   ```
6. Сохраните изменения:
   ```
   write memory
   ```

Учетная запись создана.

5.15.2. Создание пароля для доступа к активу по SNMP

► Чтобы создать пароль для доступа к активу:

1. На узле, с которого производится настройка актива, запустите терминальный клиент, поддерживающий сетевые протоколы SSH и Telnet.
2. Авторизуйтесь на активе.
3. Перейдите в режим конфигурирования:
   ```
   configure terminal
   ```
4. Если для ограничения доступа по протоколу SNMP используется список доступа, добавьте IP-адрес узла MP 10 Collector в этот список:
   ```
   ip access-list <Имя (номер) списка доступа>
   permit host <IP-адрес MP 10 Collector> any
   ```
5. Создайте пароль для доступа к активу:
   ```
   snmp-server community <Пароль> ro
   ```
6. Если для ограничения доступа по протоколу SNMP используется список доступа, добавьте пароль в этот список:
   ```
   snmp-server community <Пароль> use-acl <Имя (номер) списка доступа>
   ```
7. Выйдите из режима конфигурирования:
   ```
   end
   ```
8. Сохраните изменения:
   ```
   write memory
   ```

Пароль создан.

5.16. Cisco NX-OS 4—7: настройка MaxPatrol VM

Для проведения аудита актива по протоколу SSH в MaxPatrol VM нужно добавить учетную запись для доступа к активу, создать и запустить задачу на проведение аудита.

Для проведения аудита по протоколу SNMP в MaxPatrol VM нужно добавить пароль для доступа к активу и создать задачу на проведение аудита.

В этом разделе

5.16.1. Добавление учетной записи для доступа по SSH

► Чтобы добавить в MaxPatrol VM учетную запись для доступа к активу:

1. В главном меню в разделе **Сбор данных** выберите пункт **Учетные записи**.

   Откроется страница **Учетные записи**.

2. В панели инструментов нажмите кнопку **Добавить учетную запись** и в раскрывшемся меню выберите пункт **Логин — пароль**.

   Откроется страница **Добавление учетной записи**.

3. В поле **Название** введите название учетной записи.

   Примечание. В поле **Описание** вы можете ввести любой текстовый комментарий.

4. В раскрывающемся списке **Метки** установите флажок **Terminal**.
5. В поле **Логин** введите логин учетной записи.
6. В поле **Пароль** введите пароль и подтвердите его в поле **Подтверждение пароля**.
7. Нажмите кнопку **Сохранить**.

Учетная запись добавлена.

5.16.2. Создание задачи на аудит актива по SSH

► Чтобы создать задачу на проведение аудита актива:

1. В главном меню в разделе **Сбор данных** выберите пункт **Задачи**.

   Откроется страница **Задачи по сбору данных**.

2. В панели инструментов нажмите кнопку **Создать задачу** и в раскрывшемся меню выберите пункт **Сбор данных**.

   Откроется страница **Создание задачи на сбор данных**.

3. В поле **Название** введите название задачи.
4. Если требуется, добавьте подробное описание задачи по ссылке **Добавить описание**.
5. В раскрывающемся списке **Профиль** выберите **SSH Network Device Audit**.

6. В иерархическом списке выберите пункт **Сканирование систем** → **Через терминал: SSH и Telnet**.
7. В раскрывающемся списке **Учетная запись** выберите учетную запись для доступа к активу.
8. Если требуется, в раскрывающемся списке **Коллекторы** выберите коллекторы для сбора данных.
9. В панели **Цели сбора данных** на вкладке **Включить** в поле **Активы** введите IP-адрес или доменное имя (в формате FQDN) узла актива.

   Примечание. В панели **Расписание** вы можете включить и настроить автоматический запуск задачи по расписанию.
10. Нажмите кнопку **Сохранить**.

Задача на проведение аудита актива создана.

5.16.3. Добавление пароля для доступа по SNMP

► Чтобы добавить в MaxPatrol VM пароль для доступа к активу:

1. В главном меню в разделе **Сбор данных** выберите пункт **Учетные записи**.

   Откроется страница **Учетные записи**.
2. В панели инструментов нажмите кнопку **Добавить учетную запись** и в раскрывшемся меню выберите пункт **Пароль**.

   Откроется страница **Добавление учетной записи**.
3. В поле **Название** введите название учетной записи.

   Примечание. В поле **Описание** вы можете ввести любой текстовый комментарий.
4. В раскрывающемся списке **Метки** установите флажок **SNMP**.
5. В поле **Пароль** введите пароль и подтвердите его в поле **Подтверждение пароля**.
6. Нажмите кнопку **Сохранить**.

Пароль добавлен.

5.16.4. Создание задачи на аудит актива по SNMP

► Чтобы создать задачу на проведение аудита актива:

1. В главном меню в разделе **Сбор данных** выберите пункт **Задачи**.

   Откроется страница **Задачи по сбору данных**.
2. В панели инструментов нажмите кнопку **Создать задачу** и в раскрывшемся меню выберите пункт **Сбор данных**.

Откроется страница **Создание задачи на сбор данных**.

3. В поле **Название** введите название задачи.
4. Если требуется, добавьте подробное описание задачи по ссылке **Добавить описание**.
5. В раскрывающемся списке **Профиль** выберите **SNMP Network Device Audit**.
6. В иерархическом списке выберите пункт **Сканирование систем** → **По протоколу SNMP**.
7. Если требуется, в раскрывающемся списке выберите другую версию протокола SNMP.
8. В раскрывающемся списке **Учетная запись** выберите учетную запись для доступа к активу.

   Внимание! При использовании протокола SNMP версии 3 пароль учетной записи должен содержать не менее 8 символов.

9. Если требуется, в раскрывающемся списке **Коллекторы** выберите коллекторы для сбора данных.
10. В панели **Цели сбора данных** на вкладке **Включить** в поле **Активы** введите IP-адрес или доменное имя (в формате FQDN) узла актива.

    Примечание. В панели **Расписание** вы можете включить и настроить автоматический запуск задачи по расписанию.

11. Нажмите кнопку **Сохранить**.

Задача на проведение аудита актива создана.

5.17. Eltex, серия ESR: настройка актива

Проверка аудита производилась на ПО версии 1.4.4. Корректная работа аудита на других версиях не гарантируется.

Внимание! Эта инструкция разработана для случая локальной авторизации пользователей на активе и неприменима при использовании централизованной системы аутентификации.

Настройку актива нужно выполнять от имени учетной записи с правом перехода в режим глобальной конфигурации.

Внимание! При использовании в IT-инфраструктуре организации межсетевого экрана или других средств для контроля сетевого трафика требуется настроить в них правила, разрешающие трафик в обоих направлениях между узлом актива и узлом MP 10 Collector. Для проведения аудита актива по протоколу SSH используется порт TCP 22.

Для проведения аудита на активе нужно создать учетную запись для доступа MP 10 Collector по протоколу SSH.

► Чтобы создать учетную запись для доступа к активу:

1. На узле, с которого производится настройка актива, запустите терминальный клиент, поддерживающий сетевые протоколы SSH и Telnet.
2. Авторизуйтесь на активе.
3. Перейдите в режим конфигурирования:
   ```
   configure terminal
   ```
4. Создайте учетную запись для доступа к активу:
   ```
   username <Логин>
   password <Пароль>
   privilege 15
   ```
5. Выйдите из режима конфигурирования:
   ```
   exit
   ```
6. Примените внесенные изменения:
   ```
   commit
   confirm
   ```

Учетная запись создана.

5.18. Eltex, серия ESR: настройка MaxPatrol VM

Для проведения аудита актива по протоколу SSH в MaxPatrol VM нужно добавить учетную запись для доступа к активу, создать и запустить задачу на проведение аудита.

В этом разделе

5.18.1. Добавление учетной записи для доступа по SSH

► Чтобы добавить в MaxPatrol VM учетную запись для доступа к активу:

1. В главном меню в разделе **Сбор данных** выберите пункт **Учетные записи**.

   Откроется страница **Учетные записи**.
2. В панели инструментов нажмите кнопку **Добавить учетную запись** и в раскрывшемся меню выберите пункт **Логин — пароль**.

   Откроется страница **Добавление учетной записи**.
3. В поле **Название** введите название учетной записи.

   Примечание. В поле **Описание** вы можете ввести любой текстовый комментарий.
4. В раскрывающемся списке **Метки** установите флажок **Terminal**.

5. В поле **Логин** введите логин учетной записи.
6. В поле **Пароль** введите пароль и подтвердите его в поле **Подтверждение пароля**.
7. Нажмите кнопку **Сохранить**.

Учетная запись добавлена.

5.18.2. Создание задачи на аудит актива по SSH

► Чтобы создать задачу на проведение аудита актива:

1. В главном меню в разделе **Сбор данных** выберите пункт **Задачи**.

   Откроется страница **Задачи по сбору данных**.
2. В панели инструментов нажмите кнопку **Создать задачу** и в раскрывшемся меню выберите пункт **Сбор данных**.

   Откроется страница **Создание задачи на сбор данных**.
3. В поле **Название** введите название задачи.
4. Если требуется, добавьте подробное описание задачи по ссылке **Добавить описание**.
5. В раскрывающемся списке **Профиль** выберите **SSH Network Device Audit**.
6. В иерархическом списке выберите пункт **Сканирование систем** → **Через терминал: SSH и Telnet**.
7. В раскрывающемся списке **Учетная запись** выберите учетную запись для доступа к активу.
8. Если требуется, в раскрывающемся списке **Коллекторы** выберите коллекторы для сбора данных.
9. В панели **Цели сбора данных** на вкладке **Включить** в поле **Активы** введите IP-адрес или доменное имя (в формате FQDN) узла актива.

   Примечание. В панели **Расписание** вы можете включить и настроить автоматический запуск задачи по расписанию.
10. Нажмите кнопку **Сохранить**.

Задача на проведение аудита актива создана.

5.19. Eltex ROS, серии MES 1xxx, 2xxx, 3xxx, 51xx, 52xx: настройка актива

Проверка аудита производилась на ПО версий 1.1.44, 4.0.9.3. Корректная работа аудита на других версиях не гарантируется.

Внимание! Эта инструкция разработана для случая локальной авторизации пользователей на активе и неприменима при использовании централизованной системы аутентификации.

Настройку актива нужно выполнять от имени учетной записи с правом перехода в режим глобальной конфигурации.

Внимание! При использовании в IT-инфраструктуре организации межсетевого экрана или других средств для контроля сетевого трафика требуется настроить в них правила, разрешающие трафик в обоих направлениях между узлом актива и узлом MP 10 Collector. Для проведения аудита актива по протоколу SSH используется порт TCP 22.

Для проведения аудита на активе нужно создать учетную запись для доступа MP 10 Collector по протоколу SSH.

► Чтобы создать учетную запись для доступа к активу:

1. На узле, с которого производится настройка актива, запустите терминальный клиент, поддерживающий сетевые протоколы SSH и Telnet.
2. Авторизуйтесь на активе.
3. Перейдите в режим конфигурирования:
   `configure terminal`
4. Создайте учетную запись для доступа к активу:
   `username <Логин> password <Пароль> privilege 15`
5. Выйдите из режима конфигурирования:
   `exit`
6. Сохраните изменения:
   `write memory`

Учетная запись создана.

5.20. Eltex ROS, серии MES 1xxx, 2xxx, 3xxx, 51xx, 52xx: настройка MaxPatrol VM

Для проведения аудита актива по протоколу SSH в MaxPatrol VM нужно добавить учетную запись для доступа к активу, создать и запустить задачу на проведение аудита.

В этом разделе

5.20.1. Добавление учетной записи для доступа по SSH

► Чтобы добавить в MaxPatrol VM учетную запись для доступа к активу:

1. В главном меню в разделе **Сбор данных** выберите пункт **Учетные записи**.

   Откроется страница **Учетные записи**.

2. В панели инструментов нажмите кнопку **Добавить учетную запись** и в раскрывшемся меню выберите пункт **Логин — пароль**.

   Откроется страница **Добавление учетной записи**.

3. В поле **Название** введите название учетной записи.

   Примечание. В поле **Описание** вы можете ввести любой текстовый комментарий.

4. В раскрывающемся списке **Метки** установите флажок **Terminal**.
5. В поле **Логин** введите логин учетной записи.
6. В поле **Пароль** введите пароль и подтвердите его в поле **Подтверждение пароля**.
7. Нажмите кнопку **Сохранить**.

Учетная запись добавлена.

5.20.2. Создание задачи на аудит актива по SSH

► Чтобы создать задачу на проведение аудита актива:

1. В главном меню в разделе **Сбор данных** выберите пункт **Задачи**.

   Откроется страница **Задачи по сбору данных**.

2. В панели инструментов нажмите кнопку **Создать задачу** и в раскрывшемся меню выберите пункт **Сбор данных**.

   Откроется страница **Создание задачи на сбор данных**.

3. В поле **Название** введите название задачи.
4. Если требуется, добавьте подробное описание задачи по ссылке **Добавить описание**.
5. В раскрывающемся списке **Профиль** выберите **SSH Network Device Audit**.
6. В иерархическом списке выберите пункт **Сканирование систем** → **Через терминал: SSH и Telnet**.
7. В раскрывающемся списке **Учетная запись** выберите учетную запись для доступа к активу.
8. Если требуется, в раскрывающемся списке **Коллекторы** выберите коллекторы для сбора данных.

9. В панели **Цели сбора данных** на вкладке **Включить** в поле **Активы** введите IP-адрес или доменное имя (в формате FQDN) узла актива.

   Примечание. В панели **Расписание** вы можете включить и настроить автоматический запуск задачи по расписанию.

10. Нажмите кнопку **Сохранить**.

Задача на проведение аудита актива создана.

5.21. HPE Comware Software 5, 7: настройка актива

Настройку актива нужно выполнять от имени учетной записи с правом перехода в режим глобальной конфигурации.

Внимание! При использовании в IT-инфраструктуре организации межсетевого экрана или других средств для контроля сетевого трафика требуется настроить в них правила, разрешающие трафик в обоих направлениях между узлом актива и узлом MP 10 Collector. Для проведения аудита актива по протоколу SSH используется порт TCP 22.

Для проведения аудита на активе нужно создать учетную запись для доступа MP 10 Collector по протоколу SSH.

► Чтобы создать учетную запись для доступа к активу:

1. На узле, с которого производится настройка актива, запустите терминальный клиент, поддерживающий сетевые протоколы SSH и Telnet.
2. Авторизуйтесь на активе.
3. Перейдите в режим конфигурирования:
   ```
   system-view
   ```
4. Создайте учетную запись для доступа к активу:
   ```
   ocal-user <Логин>
   password simple <Пароль>
   authorization-attribute level 3
   service-type ssh
   ```
5. Выйдите из режима конфигурирования:
   ```
   quit
   ```
6. Сохраните изменения:
   ```
   save
   ```

Учетная запись создана.

5.22. HPE Comware Software 5, 7: настройка MaxPatrol VM

Для проведения аудита актива по протоколу SSH в MaxPatrol VM нужно добавить учетную запись для доступа к активу, создать и запустить задачу на проведение аудита.

В этом разделе

5.22.1. Добавление учетной записи для доступа по SSH

► Чтобы добавить в MaxPatrol VM учетную запись для доступа к активу:

1. В главном меню в разделе **Сбор данных** выберите пункт **Учетные записи**.

   Откроется страница **Учетные записи**.

2. В панели инструментов нажмите кнопку **Добавить учетную запись** и в раскрывшемся меню выберите пункт **Логин — пароль**.

   Откроется страница **Добавление учетной записи**.

3. В поле **Название** введите название учетной записи.

   Примечание. В поле **Описание** вы можете ввести любой текстовый комментарий.

4. В раскрывающемся списке **Метки** установите флажок **Terminal**.
5. В поле **Логин** введите логин учетной записи.
6. В поле **Пароль** введите пароль и подтвердите его в поле **Подтверждение пароля**.
7. Нажмите кнопку **Сохранить**.

Учетная запись добавлена.

5.22.2. Создание задачи на аудит актива по SSH

► Чтобы создать задачу на проведение аудита актива:

1. В главном меню в разделе **Сбор данных** выберите пункт **Задачи**.

   Откроется страница **Задачи по сбору данных**.

2. В панели инструментов нажмите кнопку **Создать задачу** и в раскрывшемся меню выберите пункт **Сбор данных**.

   Откроется страница **Создание задачи на сбор данных**.

3. В поле **Название** введите название задачи.
4. Если требуется, добавьте подробное описание задачи по ссылке **Добавить описание**.
5. В раскрывающемся списке **Профиль** выберите **SSH Network Device Audit**.
6. В иерархическом списке выберите пункт **Сканирование систем** → **Через терминал: SSH и Telnet**.

7. В раскрывающемся списке **Учетная запись** выберите учетную запись для доступа к активу.
8. Если требуется, в раскрывающемся списке **Коллекторы** выберите коллекторы для сбора данных.
9. В панели **Цели сбора данных** на вкладке **Включить** в поле **Активы** введите IP-адрес или доменное имя (в формате FQDN) узла актива.

   Примечание. В панели **Расписание** вы можете включить и настроить автоматический запуск задачи по расписанию.
10. Нажмите кнопку **Сохранить**.

Задача на проведение аудита актива создана.

5.23. Huawei VRP, серии AR, NE, S,: настройка актива

Настройку актива нужно выполнять от имени учетной записи с правом перехода в режим глобальной конфигурации.

Внимание! При использовании в IT-инфраструктуре организации межсетевого экрана или других средств для контроля сетевого трафика требуется настроить в них правила, разрешающие трафик в обоих направлениях между узлом актива и узлом MP 10 Collector. Для проведения аудита актива по протоколу SSH используется порт TCP 22, по протоколу SNMP — порт UDP 162.

Для проведения аудита на активе нужно создать учетную запись для доступа MP 10 Collector по протоколу SSH и пароль для доступа по протоколу SNMP.

В этом разделе

5.23.1. Создание учетной записи для доступа к активу по SSH

► Чтобы создать учетную запись для доступа к активу:

1. На узле, с которого производится настройка актива, запустите терминальный клиент, поддерживающий сетевые протоколы SSH и Telnet.
2. Авторизуйтесь на активе.
3. Перейдите в режим конфигурирования:

   ```
   system-view
   ```

4. Создайте учетную запись для доступа к активу:

```
aaa
local-user <Логин> password cipher <Пароль> privilege level 15
```

Примечание. Если для ограничения доступа к активу по протоколу SSH используется список доступа, добавьте IP-адрес узла MP 10 Collector в этот список.

5. Выйдите из режима конфигурирования:

```
quit
```

Учетная запись создана.

5.23.2. Создание пароля для доступа к активу по SNMP

► Чтобы создать пароль для доступа к активу:

1. На узле, с которого производится настройка актива, запустите терминальный клиент, поддерживающий сетевые протоколы SSH и Telnet.
2. Авторизуйтесь на активе.
3. Перейдите в режим конфигурирования:

```
system-view
```

4. Создайте список доступа для ограничения доступа по протоколу SNMP и добавьте IP-адрес узла MP 10 Collector в этот список:

```
acl number <Имя (номер) списка доступа>
rule 1 permit source <IP-адрес MP 10 Collector> 0.0.0.0
```

5. Включите версию протокола SNMPv2:

```
snmp-agent sys-info version v2c
```

6. Отключите версию протокола SNMPv3:

```
undo snmp-agent sys-info version v3
```

7. Создайте пароль для доступа к активу и добавьте его в список доступа:

```
snmp-agent community read <Пароль> <Имя (номер) списка доступа>
```

8. Выйдите из режима конфигурирования:

```
quit
```

Пароль создан.

5.24. Huawei VRP, серии AR, NE, S: настройка MaxPatrol VM

Для проведения аудита актива по протоколу SSH в MaxPatrol VM нужно добавить учетную запись для доступа к активу, создать и запустить задачу на проведение аудита.

Для проведения аудита по протоколу SNMP в MaxPatrol VM нужно добавить пароль для доступа к активу и создать задачу на проведение аудита.

В этом разделе

5.24.1. Добавление учетной записи для доступа по SSH

► Чтобы добавить в MaxPatrol VM учетную запись для доступа к активу:

1. В главном меню в разделе **Сбор данных** выберите пункт **Учетные записи**.

   Откроется страница **Учетные записи**.

2. В панели инструментов нажмите кнопку **Добавить учетную запись** и в раскрывшемся меню выберите пункт **Логин — пароль**.

   Откроется страница **Добавление учетной записи**.

3. В поле **Название** введите название учетной записи.

   Примечание. В поле **Описание** вы можете ввести любой текстовый комментарий.

4. В раскрывающемся списке **Метки** установите флажок **Terminal**.
5. В поле **Логин** введите логин учетной записи.
6. В поле **Пароль** введите пароль и подтвердите его в поле **Подтверждение пароля**.
7. Нажмите кнопку **Сохранить**.

Учетная запись добавлена.

5.24.2. Создание задачи на аудит актива по SSH

► Чтобы создать задачу на проведение аудита актива:

1. В главном меню в разделе **Сбор данных** выберите пункт **Задачи**.

   Откроется страница **Задачи по сбору данных**.

2. В панели инструментов нажмите кнопку **Создать задачу** и в раскрывшемся меню выберите пункт **Сбор данных**.

   Откроется страница **Создание задачи на сбор данных**.

3. В поле **Название** введите название задачи.
4. Если требуется, добавьте подробное описание задачи по ссылке **Добавить описание**.
5. В раскрывающемся списке **Профиль** выберите **SSH Network Device Audit**.

6. В иерархическом списке выберите пункт **Сканирование систем** → **Через терминал: SSH и Telnet**.
7. В раскрывающемся списке **Учетная запись** выберите учетную запись для доступа к активу.
8. Если требуется, в раскрывающемся списке **Коллекторы** выберите коллекторы для сбора данных.
9. В панели **Цели сбора данных** на вкладке **Включить** в поле **Активы** введите IP-адрес или доменное имя (в формате FQDN) узла актива.

   Примечание. В панели **Расписание** вы можете включить и настроить автоматический запуск задачи по расписанию.
10. Нажмите кнопку **Сохранить**.

Задача на проведение аудита актива создана.

5.24.3. Добавление пароля для доступа по SNMP

► Чтобы добавить в MaxPatrol VM пароль для доступа к активу:

1. В главном меню в разделе **Сбор данных** выберите пункт **Учетные записи**.

   Откроется страница **Учетные записи**.
2. В панели инструментов нажмите кнопку **Добавить учетную запись** и в раскрывшемся меню выберите пункт **Пароль**.

   Откроется страница **Добавление учетной записи**.
3. В поле **Название** введите название учетной записи.

   Примечание. В поле **Описание** вы можете ввести любой текстовый комментарий.
4. В раскрывающемся списке **Метки** установите флажок **SNMP**.
5. В поле **Пароль** введите пароль и подтвердите его в поле **Подтверждение пароля**.
6. Нажмите кнопку **Сохранить**.

Пароль добавлен.

5.24.4. Создание задачи на аудит актива по SNMP

► Чтобы создать задачу на проведение аудита актива:

1. В главном меню в разделе **Сбор данных** выберите пункт **Задачи**.

   Откроется страница **Задачи по сбору данных**.
2. В панели инструментов нажмите кнопку **Создать задачу** и в раскрывшемся меню выберите пункт **Сбор данных**.

Откроется страница **Создание задачи на сбор данных**.

3. В поле **Название** введите название задачи.
4. Если требуется, добавьте подробное описание задачи по ссылке **Добавить описание**.
5. В раскрывающемся списке **Профиль** выберите **SNMP Network Device Audit**.
6. В иерархическом списке выберите пункт **Сканирование систем** → **По протоколу SNMP**.
7. Если требуется, в раскрывающемся списке выберите другую версию протокола SNMP.
8. В раскрывающемся списке **Учетная запись** выберите учетную запись для доступа к активу.

   Внимание! При использовании протокола SNMP версии 3 пароль учетной записи должен содержать не менее 8 символов.
9. Если требуется, в раскрывающемся списке **Коллекторы** выберите коллекторы для сбора данных.
10. В панели **Цели сбора данных** на вкладке **Включить** в поле **Активы** введите IP-адрес или доменное имя (в формате FQDN) узла актива.

    Примечание. В панели **Расписание** вы можете включить и настроить автоматический запуск задачи по расписанию.
11. Нажмите кнопку **Сохранить**.

Задача на проведение аудита актива создана.

5.25. Juniper JunOS 11—19: настройка актива

Настройку актива нужно выполнять от имени учетной записи с правом перехода в режим глобальной конфигурации.

Внимание! При использовании в IT-инфраструктуре организации межсетевого экрана или других средств для контроля сетевого трафика требуется настроить в них правила, разрешающие трафик в обоих направлениях между узлом актива и узлом MP 10 Collector. Для проведения аудита актива по протоколу SSH используется порт TCP 22, по протоколу SNMP — порт UDP 162.

Для проведения аудита на активе нужно создать учетную запись для доступа MP 10 Collector по протоколу SSH и пароль для доступа по протоколу SNMP.

В этом разделе

5.25.1. Создание учетной записи для доступа к активу по SSH

► Чтобы создать учетную запись для доступа к активу:

1. На узле, с которого производится настройка актива, запустите терминальный клиент, поддерживающий сетевые протоколы SSH и Telnet.
2. Авторизуйтесь на активе.
3. Перейдите в режим конфигурирования:
   ```
   configure
   ```
4. Создайте учетную запись для доступа к активу:
   ```
   set system login user <Логин> authentication plain-text-password
   <Пароль>
   ```
5. Примените изменения и выйдите из режима конфигурирования:
   ```
   commit and-quit
   ```

Учетная запись создана.

5.25.2. Создание пароля для доступа к активу по SNMP

► Чтобы создать пароль для доступа к активу:

1. На узле, с которого производится настройка актива, запустите терминальный клиент, поддерживающий сетевые протоколы SSH и Telnet.
2. Авторизуйтесь на активе.
3. Перейдите в режим конфигурирования:
   ```
   configure
   ```
4. Создайте пароль для доступа к активу:
   ```
   edit snmp community <Пароль>
   ```
5. Настройте доступ с правом на чтение с IP-адрес узла MP 10 Collector:
   ```
   set clients <IP-адрес MP 10 Collector>/32
   set authorization read-only
   ```
6. Примените изменения и выйдите из режима конфигурирования:
   ```
   end
   ```

Пароль создан.

5.26. Juniper JunOS 11—19: настройка MaxPatrol VM

Для проведения аудита актива по протоколу SSH в MaxPatrol VM нужно добавить учетную запись для доступа к активу, создать и запустить задачу на проведение аудита.

Для проведения аудита по протоколу SNMP в MaxPatrol VM нужно добавить пароль для доступа к активу и создать задачу на проведение аудита.

В этом разделе

5.26.1. Добавление учетной записи для доступа по SSH

► Чтобы добавить в MaxPatrol VM учетную запись для доступа к активу:

1. В главном меню в разделе **Сбор данных** выберите пункт **Учетные записи**.

   Откроется страница **Учетные записи**.

2. В панели инструментов нажмите кнопку **Добавить учетную запись** и в раскрывшемся меню выберите пункт **Логин — пароль**.

   Откроется страница **Добавление учетной записи**.

3. В поле **Название** введите название учетной записи.

   Примечание. В поле **Описание** вы можете ввести любой текстовый комментарий.

4. В раскрывающемся списке **Метки** установите флажок **Terminal**.
5. В поле **Логин** введите логин учетной записи.
6. В поле **Пароль** введите пароль и подтвердите его в поле **Подтверждение пароля**.
7. Нажмите кнопку **Сохранить**.

Учетная запись добавлена.

5.26.2. Создание задачи на аудит актива по SSH

► Чтобы создать задачу на проведение аудита актива:

1. В главном меню в разделе **Сбор данных** выберите пункт **Задачи**.

   Откроется страница **Задачи по сбору данных**.

2. В панели инструментов нажмите кнопку **Создать задачу** и в раскрывшемся меню выберите пункт **Сбор данных**.

   Откроется страница **Создание задачи на сбор данных**.

3. В поле **Название** введите название задачи.

4. Если требуется, добавьте подробное описание задачи по ссылке **Добавить описание**.
5. В раскрывающемся списке **Профиль** выберите **SSH Network Device Audit**.
6. В иерархическом списке выберите пункт **Сканирование систем** → **Через терминал: SSH и Telnet**.
7. В раскрывающемся списке **Учетная запись** выберите учетную запись для доступа к активу.
8. Если требуется, в раскрывающемся списке **Коллекторы** выберите коллекторы для сбора данных.
9. В панели **Цели сбора данных** на вкладке **Включить** в поле **Активы** введите IP-адрес или доменное имя (в формате FQDN) узла актива.

   Примечание. В панели **Расписание** вы можете включить и настроить автоматический запуск задачи по расписанию.
10. Нажмите кнопку **Сохранить**.

Задача на проведение аудита актива создана.

5.26.3. Добавление пароля для доступа по SNMP

► Чтобы добавить в MaxPatrol VM пароль для доступа к активу:

1. В главном меню в разделе **Сбор данных** выберите пункт **Учетные записи**.

   Откроется страница **Учетные записи**.
2. В панели инструментов нажмите кнопку **Добавить учетную запись** и в раскрывшемся меню выберите пункт **Пароль**.

   Откроется страница **Добавление учетной записи**.
3. В поле **Название** введите название учетной записи.

   Примечание. В поле **Описание** вы можете ввести любой текстовый комментарий.
4. В раскрывающемся списке **Метки** установите флажок **SNMP**.
5. В поле **Пароль** введите пароль и подтвердите его в поле **Подтверждение пароля**.
6. Нажмите кнопку **Сохранить**.

Пароль добавлен.

5.26.4. Создание задачи на аудит актива по SNMP

► Чтобы создать задачу на проведение аудита актива:

1. В главном меню в разделе **Сбор данных** выберите пункт **Задачи**.

Откроется страница **Задачи по сбору данных**.

2. В панели инструментов нажмите кнопку **Создать задачу** и в раскрывшемся меню выберите пункт **Сбор данных**.

   Откроется страница **Создание задачи на сбор данных**.

3. В поле **Название** введите название задачи.
4. Если требуется, добавьте подробное описание задачи по ссылке **Добавить описание**.
5. В раскрывающемся списке **Профиль** выберите **SNMP Network Device Audit**.
6. В иерархическом списке выберите пункт **Сканирование систем** → **По протоколу SNMP**.
7. Если требуется, в раскрывающемся списке выберите другую версию протокола SNMP.
8. В раскрывающемся списке **Учетная запись** выберите учетную запись для доступа к активу.

   Внимание! При использовании протокола SNMP версии 3 пароль учетной записи должен содержать не менее 8 символов.

9. Если требуется, в раскрывающемся списке **Коллекторы** выберите коллекторы для сбора данных.
10. В панели **Цели сбора данных** на вкладке **Включить** в поле **Активы** введите IP-адрес или доменное имя (в формате FQDN) узла актива.

    Примечание. В панели **Расписание** вы можете включить и настроить автоматический запуск задачи по расписанию.

11. Нажмите кнопку **Сохранить**.

Задача на проведение аудита актива создана.

5.27. QTech QSW, модели 3450-28T, 6500-52F, 8300-52F: настройка актива

Проверка аудита производилась на ПО версии 7.0.3.5. Корректная работа аудита на других версиях не гарантируется.

Настройку актива нужно выполнять от имени учетной записи с правом перехода в режим глобальной конфигурации.

> **Внимание!** При использовании в IT-инфраструктуре организации межсетевого экрана или других средств для контроля сетевого трафика требуется настроить в них правила, разрешающие трафик в обоих направлениях между узлом актива и узлом MP 10 Collector. Для проведения аудита актива по протоколу SSH используется порт TCP 22.

Для проведения аудита на активе нужно создать учетную запись для доступа MP 10 Collector по протоколу SSH.

Внимание! Эта инструкция разработана для аутентификации пользователей на сетевом устройстве методом Local. В этом случае данные учетных записей хранятся на самом устройстве.

Для аутентификации пользователей методом Local в файле конфигурации сетевого устройства должны присутствовать строка:

```
authentication line vty login local
```

► Чтобы создать учетную запись для доступа к активу:

1. На узле, с которого производится настройка актива, запустите терминальный клиент, поддерживающий сетевые протоколы SSH и Telnet.
2. Авторизуйтесь на активе.
3. Перейдите в режим конфигурирования:
   ```
   configure terminal
   ```
4. Создайте учетную запись для доступа к активу:
   ```
   username <Логин> privilege 15 password <Пароль>
   ```
5. Если на активе ограничен доступ по IP-адресам, разрешите доступ с узла MP 10 Collector:
6. `authentication securityip <IP-адрес MP 10 Collector>`
7. Выйдите из режима конфигурирования:
   ```
   end
   ```
8. Сохраните изменения:
   ```
   write memory
   ```

Учетная запись создана.

5.28. QTech QSW, модели 3450-28T, 6500-52F, 8300-52F: настройка MaxPatrol VM

Для проведения аудита актива по протоколу SSH в MaxPatrol VM нужно добавить учетную запись для доступа к активу, создать и запустить задачу на проведение аудита.

В этом разделе

5.28.1. Добавление учетной записи для доступа по SSH

► Чтобы добавить в MaxPatrol VM учетную запись для доступа к активу:

1. В главном меню в разделе **Сбор данных** выберите пункт **Учетные записи**.

Откроется страница **Учетные записи**.

2. В панели инструментов нажмите кнопку **Добавить учетную запись** и в раскрывшемся меню выберите пункт **Логин — пароль**.

   Откроется страница **Добавление учетной записи**.

3. В поле **Название** введите название учетной записи.

   Примечание. В поле **Описание** вы можете ввести любой текстовый комментарий.

4. В раскрывающемся списке **Метки** установите флажок **Terminal**.
5. В поле **Логин** введите логин учетной записи.
6. В поле **Пароль** введите пароль и подтвердите его в поле **Подтверждение пароля**.
7. Нажмите кнопку **Сохранить**.

Учетная запись добавлена.

5.28.2. Создание задачи на аудит актива по SSH

► Чтобы создать задачу на проведение аудита актива:

1. В главном меню в разделе **Сбор данных** выберите пункт **Задачи**.

   Откроется страница **Задачи по сбору данных**.

2. В панели инструментов нажмите кнопку **Создать задачу** и в раскрывшемся меню выберите пункт **Сбор данных**.

   Откроется страница **Создание задачи на сбор данных**.

3. В поле **Название** введите название задачи.
4. Если требуется, добавьте подробное описание задачи по ссылке **Добавить описание**.
5. В раскрывающемся списке **Профиль** выберите **SSH Network Device Audit**.
6. В иерархическом списке выберите пункт **Сканирование систем** → **Через терминал: SSH и Telnet**.
7. В раскрывающемся списке **Учетная запись** выберите учетную запись для доступа к активу.
8. Если требуется, в раскрывающемся списке **Коллекторы** выберите коллекторы для сбора данных.
9. В панели **Цели сбора данных** на вкладке **Включить** в поле **Активы** введите IP-адрес или доменное имя (в формате FQDN) узла актива.

Примечание. В панели **Расписание** вы можете включить и настроить автоматический запуск задачи по расписанию.

10. Нажмите кнопку **Сохранить**.

Задача на проведение аудита актива создана.

6. Системы аутентификации, авторизации и учета

Раздел содержит инструкции для настройки аудита поддерживаемых в MaxPatrol VM систем аутентификации, авторизации и учета.

В этом разделе

6.1. Cisco ACS 5: настройка актива

Настройка актива выполняется аналогично Cisco ADE-OS (см. раздел 6.3).

6.2. Cisco ACS 5: настройка MaxPatrol VM

Настройка MaxPatrol VM для аудита актива выполняется аналогично Cisco ADE-OS (см. раздел 6.4).

6.3. Cisco ADE-OS: настройка актива

Настройку актива нужно выполнять от имени учетной записи с правом перехода в режим глобальной конфигурации.

> **Внимание!** При использовании в IT-инфраструктуре организации межсетевого экрана или других средств для контроля сетевого трафика требуется настроить в них правила, разрешающие трафик в обоих направлениях между узлом актива и узлом MP 10 Collector. Для проведения аудита актива по протоколу SSH используется порт TCP 22, по протоколу SNMP — порт UDP 162.

Для проведения аудита на активе нужно создать учетную запись для доступа MP 10 Collector по протоколу SSH и пароль для доступа по протоколу SNMP.

В этом разделе

6.3.1. Создание учетной записи для доступа к активу по SSH

► Чтобы создать учетную запись для доступа к активу:

1. На узле, с которого производится настройка актива, запустите терминальный клиент, поддерживающий сетевые протоколы SSH и Telnet.
2. Авторизуйтесь на активе.
3. Перейдите в режим конфигурирования:
   `configure terminal`
4. Создайте учетную запись для доступа к активу:
   `username <Логин> password plain <Пароль> role admin`
5. Выйдите из режима конфигурирования:
   `end`
6. Сохраните изменения:
   `write memory`

Учетная запись создана.

6.3.2. Создание пароля для доступа к активу по SNMP

► Чтобы создать пароль для доступа к активу:

1. На узле, с которого производится настройка актива, запустите терминальный клиент, поддерживающий сетевые протоколы SSH и Telnet.
2. Авторизуйтесь на активе.
3. Перейдите в режим конфигурирования:
   `configure terminal`
4. Создайте пароль для доступа к активу:
   `snmp-server community <Пароль> ro`
5. Выйдите из режима конфигурирования:
   `end`
6. Сохраните изменения:
   `write memory`

Пароль создан.

6.4. Cisco ADE-OS: настройка MaxPatrol VM

Для проведения аудита актива по протоколу SSH в MaxPatrol VM нужно добавить учетную запись для доступа к активу, пароль для повышения привилегий (перехода в привилегированный режим EXEC) и создать задачу на проведение аудита.

Для проведения аудита по протоколу SNMP в MaxPatrol VM нужно добавить пароль для доступа к активу и создать задачу на проведение аудита.

В этом разделе

6.4.1. Добавление учетной записи для доступа по SSH

► Чтобы добавить в MaxPatrol VM учетную запись для доступа к активу:

1. В главном меню в разделе **Сбор данных** выберите пункт **Учетные записи**.

   Откроется страница **Учетные записи**.

2. В панели инструментов нажмите кнопку **Добавить учетную запись** и в раскрывшемся меню выберите пункт **Логин — пароль**.

   Откроется страница **Добавление учетной записи**.

3. В поле **Название** введите название учетной записи.

   Примечание. В поле **Описание** вы можете ввести любой текстовый комментарий.

4. В раскрывающемся списке **Метки** установите флажок **Terminal**.
5. В поле **Логин** введите логин учетной записи.
6. В поле **Пароль** введите пароль и подтвердите его в поле **Подтверждение пароля**.
7. Нажмите кнопку **Сохранить**.

Учетная запись добавлена.

6.4.2. Создание задачи на аудит актива по SSH

► Чтобы создать задачу на проведение аудита актива:

1. В главном меню в разделе **Сбор данных** выберите пункт **Задачи**.

Откроется страница **Задачи по сбору данных**.

2. В панели инструментов нажмите кнопку **Создать задачу** и в раскрывшемся меню выберите пункт **Сбор данных**.

   Откроется страница **Создание задачи на сбор данных**.

3. В поле **Название** введите название задачи.
4. Если требуется, добавьте подробное описание задачи по ссылке **Добавить описание**.
5. В раскрывающемся списке **Профиль** выберите **SSH Network Device Audit**.
6. В иерархическом списке выберите пункт **Сканирование систем** → **Через терминал: SSH и Telnet**.
7. В раскрывающемся списке **Учетная запись** выберите учетную запись для доступа к активу.
8. Если требуется, в раскрывающемся списке **Коллекторы** выберите коллекторы для сбора данных.
9. В панели **Цели сбора данных** на вкладке **Включить** в поле **Активы** введите IP-адрес или доменное имя (в формате FQDN) узла актива.

   Примечание. В панели **Расписание** вы можете включить и настроить автоматический запуск задачи по расписанию.

10. Нажмите кнопку **Сохранить**.

Задача на проведение аудита актива создана.

6.4.3. Добавление пароля для доступа по SNMP

► Чтобы добавить в MaxPatrol VM пароль для доступа к активу:

1. В главном меню в разделе **Сбор данных** выберите пункт **Учетные записи**.

   Откроется страница **Учетные записи**.

2. В панели инструментов нажмите кнопку **Добавить учетную запись** и в раскрывшемся меню выберите пункт **Пароль**.

   Откроется страница **Добавление учетной записи**.

3. В поле **Название** введите название учетной записи.

   Примечание. В поле **Описание** вы можете ввести любой текстовый комментарий.

4. В раскрывающемся списке **Метки** установите флажок **SNMP**.
5. В поле **Пароль** введите пароль и подтвердите его в поле **Подтверждение пароля**.
6. Нажмите кнопку **Сохранить**.

Пароль добавлен.

6.4.4. Создание задачи на аудит актива по SNMP

► Чтобы создать задачу на проведение аудита актива:

1. В главном меню в разделе **Сбор данных** выберите пункт **Задачи**.

   Откроется страница **Задачи по сбору данных**.

2. В панели инструментов нажмите кнопку **Создать задачу** и в раскрывшемся меню выберите пункт **Сбор данных**.

   Откроется страница **Создание задачи на сбор данных**.

3. В поле **Название** введите название задачи.
4. Если требуется, добавьте подробное описание задачи по ссылке **Добавить описание**.
5. В раскрывающемся списке **Профиль** выберите **SNMP Network Device Audit**.
6. В иерархическом списке выберите пункт **Сканирование систем** → **По протоколу SNMP**.
7. Если требуется, в раскрывающемся списке выберите другую версию протокола SNMP.
8. В раскрывающемся списке **Учетная запись** выберите учетную запись для доступа к активу.

   Внимание! При использовании протокола SNMP версии 3 пароль учетной записи должен содержать не менее 8 символов.

9. Если требуется, в раскрывающемся списке **Коллекторы** выберите коллекторы для сбора данных.
10. В панели **Цели сбора данных** на вкладке **Включить** в поле **Активы** введите IP-адрес или доменное имя (в формате FQDN) узла актива.

    Примечание. В панели **Расписание** вы можете включить и настроить автоматический запуск задачи по расписанию.

11. Нажмите кнопку **Сохранить**.

Задача на проведение аудита актива создана.

6.5. Cisco Identity Services Engine (ISE) 2.3: настройка актива

Внимание! Указана версия ПО, на которой производилась проверка аудита. Корректная работа аудита на других версиях не гарантируется.

Настройка актива выполняется аналогично Cisco ADE-OS (см. раздел 6.3).

6.6. Cisco Identity Services Engine (ISE) 2.3: настройка MaxPatrol VM

Настройка MaxPatrol VM для аудита актива выполняется аналогично Cisco ADE-OS (см. раздел 6.4).

7. Системы виртуализации

Раздел содержит инструкции для настройки аудита поддерживаемых в MaxPatrol VM систем виртуализации.

В этом разделе

7.1. VMware vCenter Server 5.5—7.0: настройка актива

Настройку актива нужно выполнять от имени учетной записи, имеющей права локального администратора ОС и поддерживающей роль администратора VMware vCenter Server.

> **Внимание!** При использовании межсетевого экрана требуется настроить в нем правила, разрешающие внешние подключения к используемым портам TCP/IP. Для доступа к VMware vCenter Server по умолчанию используется порт 443/TCP.

Для проведения аудита на активе нужно:

1. Средствами ОС создать учетную запись локального пользователя ОС (см. раздел 15.1.2) для доступа MP 10 Collector.

   Примечание. Данные этой учетной записи нужно указать при добавлении учетной записи в MaxPatrol VM.

2. Добавить учетную запись в локальную (групповую) политику безопасности (см. раздел 15.1.3) «Доступ к компьютеру из сети» (Access this computer from the network).
3. Добавить учетную запись в список пользователей VMware vCenter Server.

В этом разделе

7.1.1. Добавление учетной записи в версиях 5.5, 6.0

► Чтобы добавить учетную запись ОС в список пользователей vCenter Server:

1. В адресной строке браузера введите IP-адрес или доменное имя сервера.
2. Авторизуйтесь под именем учетной записи администратора.

   Откроется страница **VMware vSphere Web Client**.

3. В иерархическом списке выберите узел сервера.

4. Выберите вкладку **Manage**.
5. Нажмите кнопку **Permissions**.
6. В панели инструментов нажмите ✚.

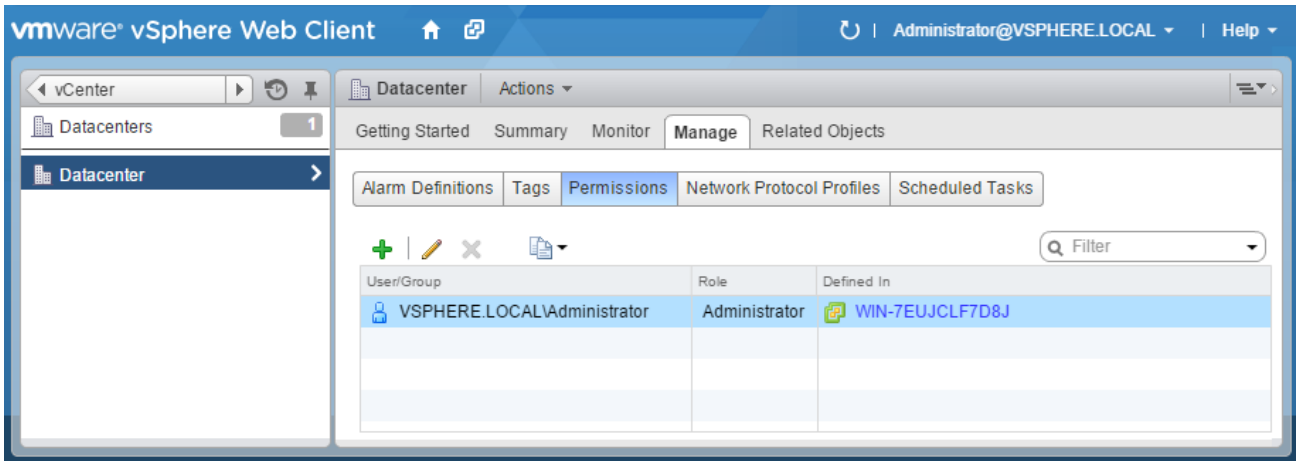

Рисунок 7. Выбор вкладки **Manage**

7. В открывшемся окне нажмите кнопку **Add**.

   Откроется окно **Select Users/Groups**.

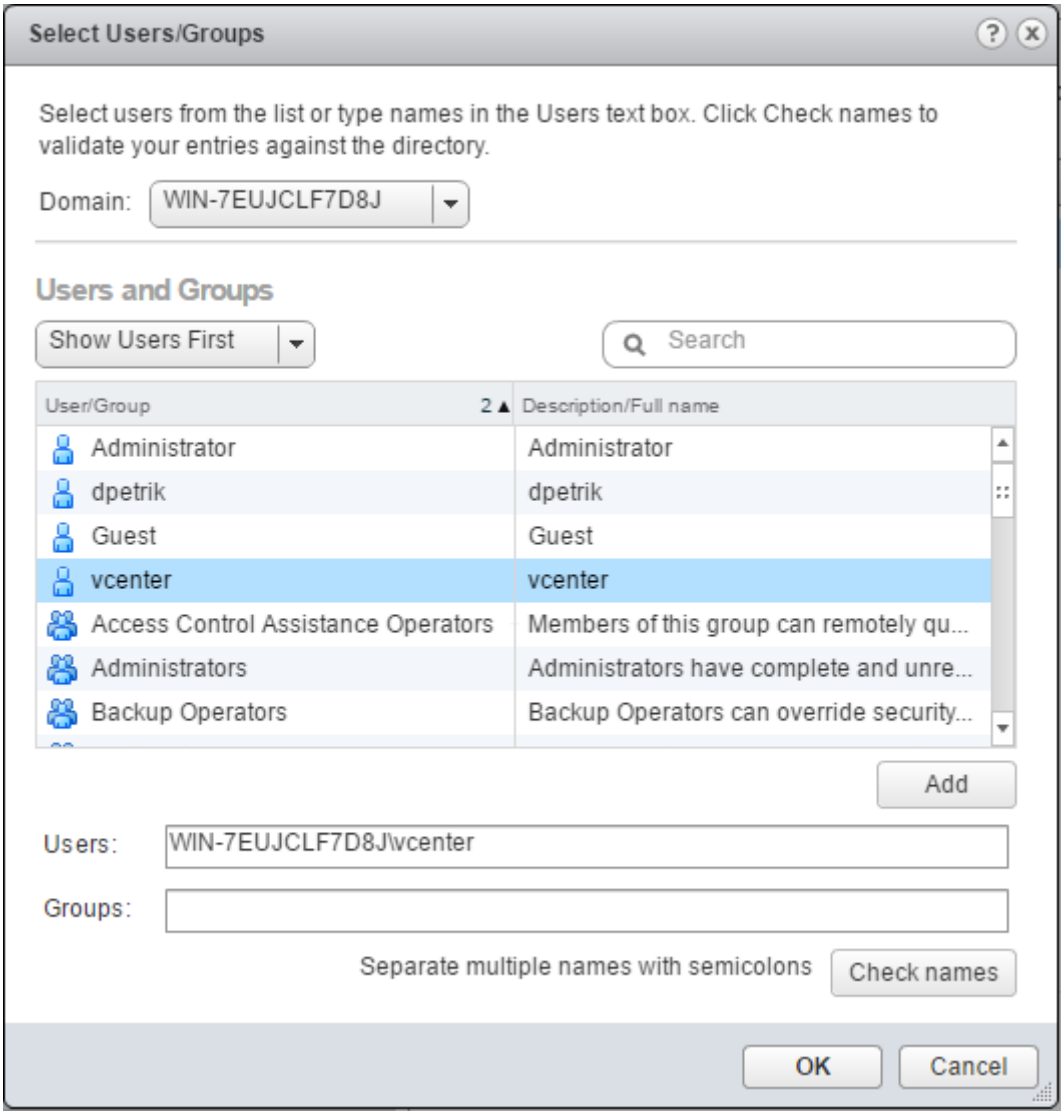

Рисунок 8. Выбор учетной записи ОС

8. Если используется доменная учетная запись, в раскрывающемся списке **Domain** выберите домен учетной записи.
9. В списке выберите учетную запись и нажмите кнопку **Add**.
10. Нажмите кнопку **OK**.
11. В окне **<Имя сервера> — Change Role On Permissions** в раскрывающемся списке выберите **Read-only**.

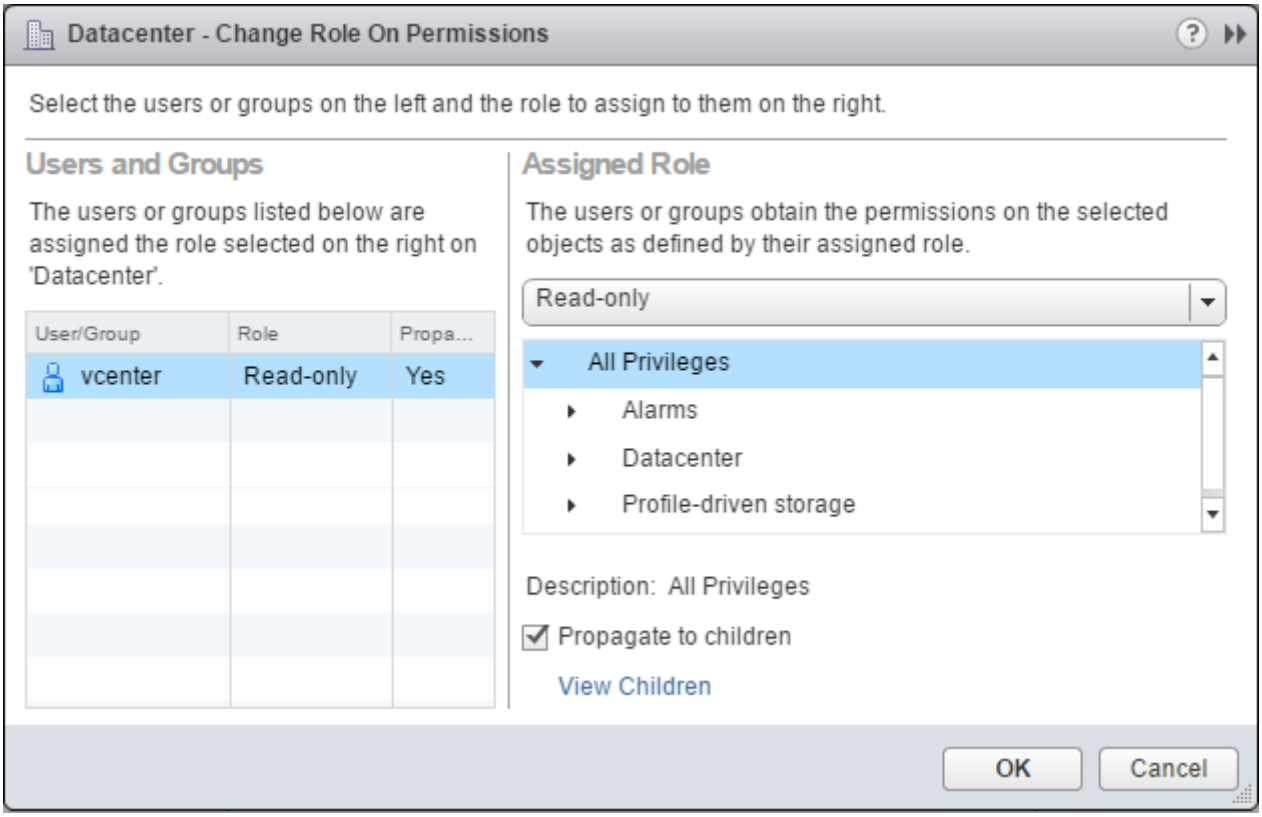

Рисунок 9. Назначение прав доступа учетной записи

12. Нажмите кнопку **OK**.

Учетная запись ОС добавлена в список пользователей vCenter Server.

7.1.2. Добавление учетной записи в версии 6.5

► Чтобы добавить учетную запись ОС в список пользователей vCenter Server:

1. В адресной строке браузера введите IP-адрес или доменное имя сервера.
2. Авторизуйтесь под именем учетной записи администратора.

   Откроется страница **VMware vSphere Web Client**.
3. В левой части страницы нажмите кнопку **Hosts and Clusters**.
4. В иерархическом списке выберите узел сервера.
5. Выберите вкладку **Permissions**.

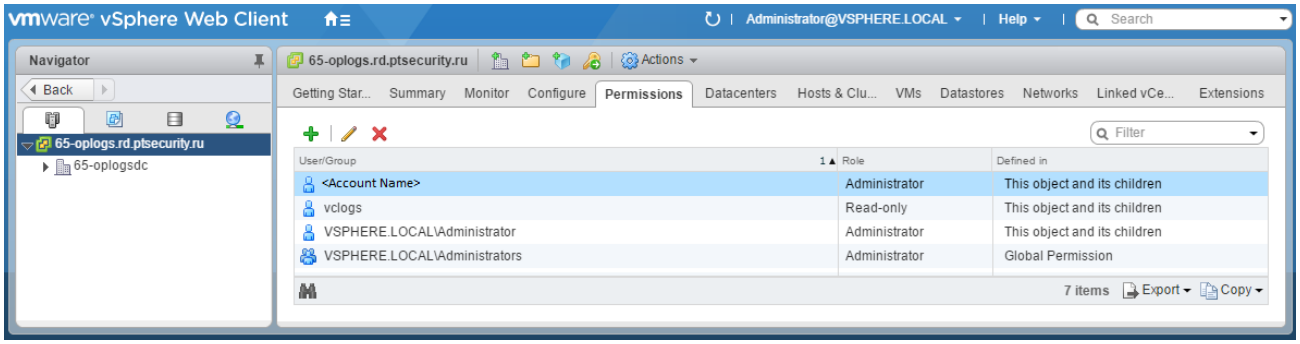

Рисунок 10. Выбор вкладки **Permissions**

6. В панели инструментов вкладки нажмите ✚.
7. В открывшемся окне нажмите кнопку **Add**.

   Откроется окно **Select Users/Groups**.

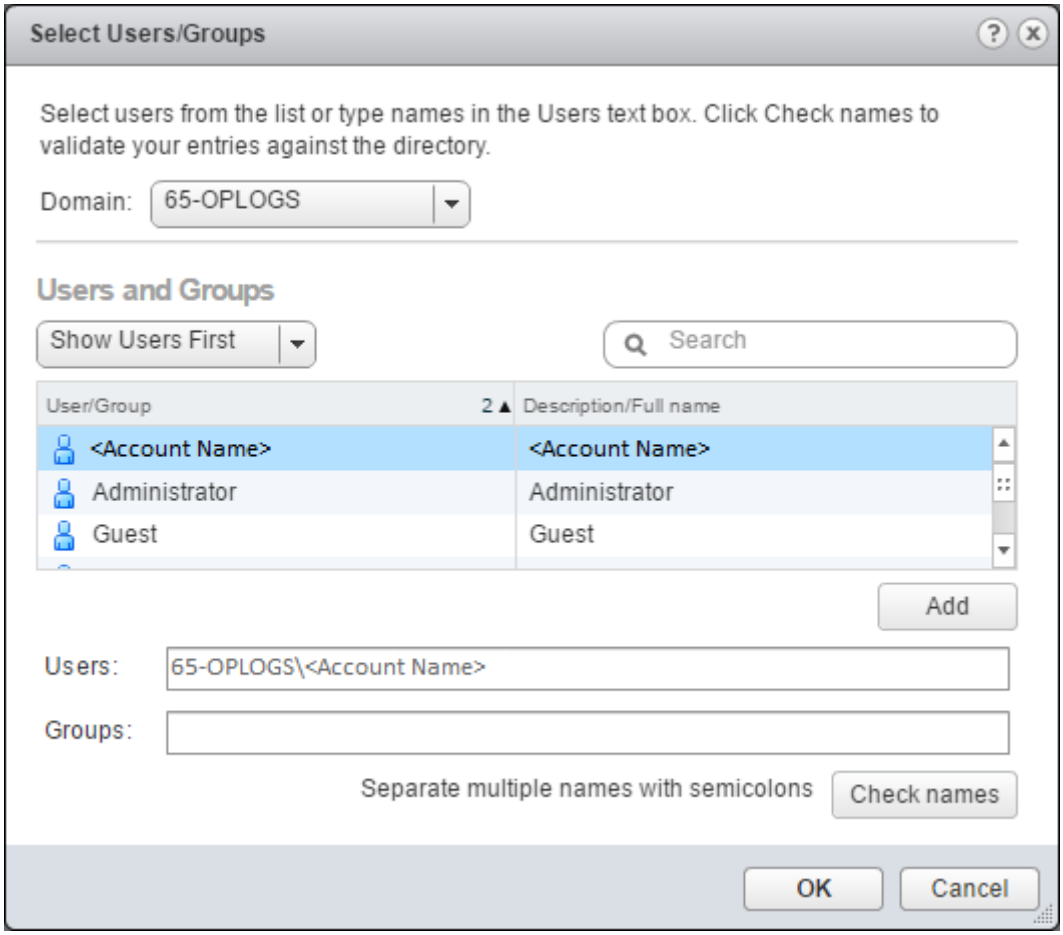

Рисунок 11. Выбор учетной записи ОС

8. Если используется доменная учетная запись, в раскрывающемся списке **Domain** выберите домен.

9. В списке выберите учетную запись и нажмите кнопку **Add**.
10. Нажмите кнопку **OK**.
11. В окне **<Имя сервера>** — **Add Permission** в раскрывающемся списке выберите **Read-only**.

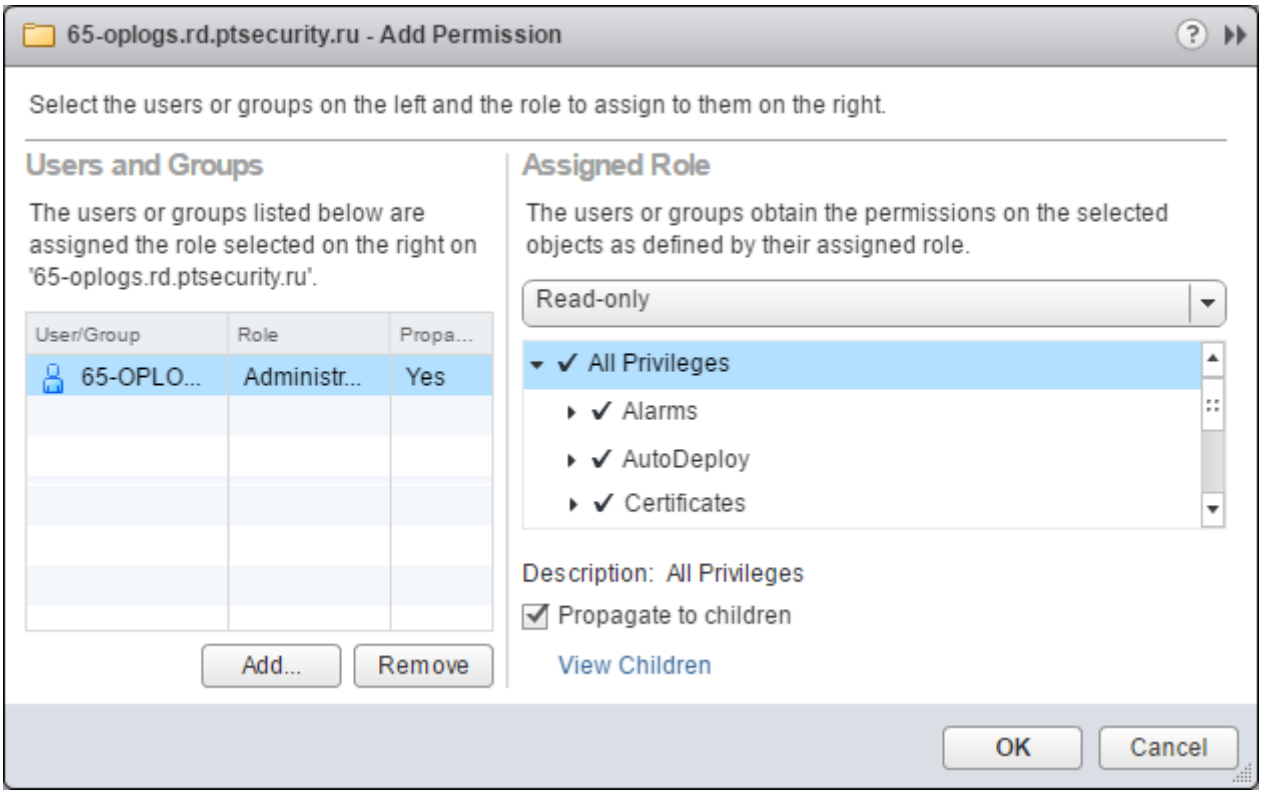

Рисунок 12. Назначение прав доступа учетной записи

12. Нажмите кнопку **OK**.

Учетная запись ОС добавлена в список пользователей vCenter Server.

7.1.3. Добавление учетной записи в версиях 6.7, 7.0

► Чтобы добавить учетную запись ОС в список пользователей vCenter Server:

1. В адресной строке браузера введите IP-адрес или доменное имя сервера.
2. Авторизуйтесь под именем учетной записи администратора.

   Откроется страница **VM vSphere Client**.
3. В левой части страницы нажмите кнопку **Hosts and Clusters**.
4. В иерархическом списке выберите узел сервера.
5. Выберите вкладку **Permissions**.

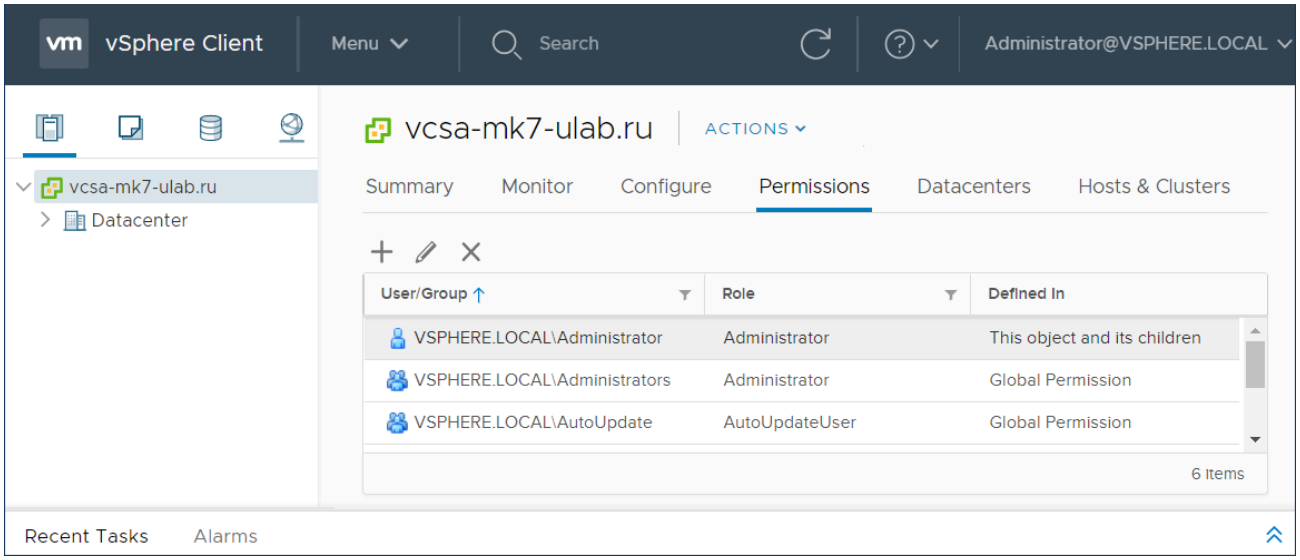

Рисунок 13. Выбор вкладки **Permissions**

6. В панели инструментов вкладки нажмите + .

   Откроется окно **Add Permission**.

7. В раскрывающемся списке **User** выберите домен и в поле ниже введите логин учетной записи.
8. В раскрывающемся списке **Role** выберите **Read-only**.
9. Установите флажок **Propagate to children**.

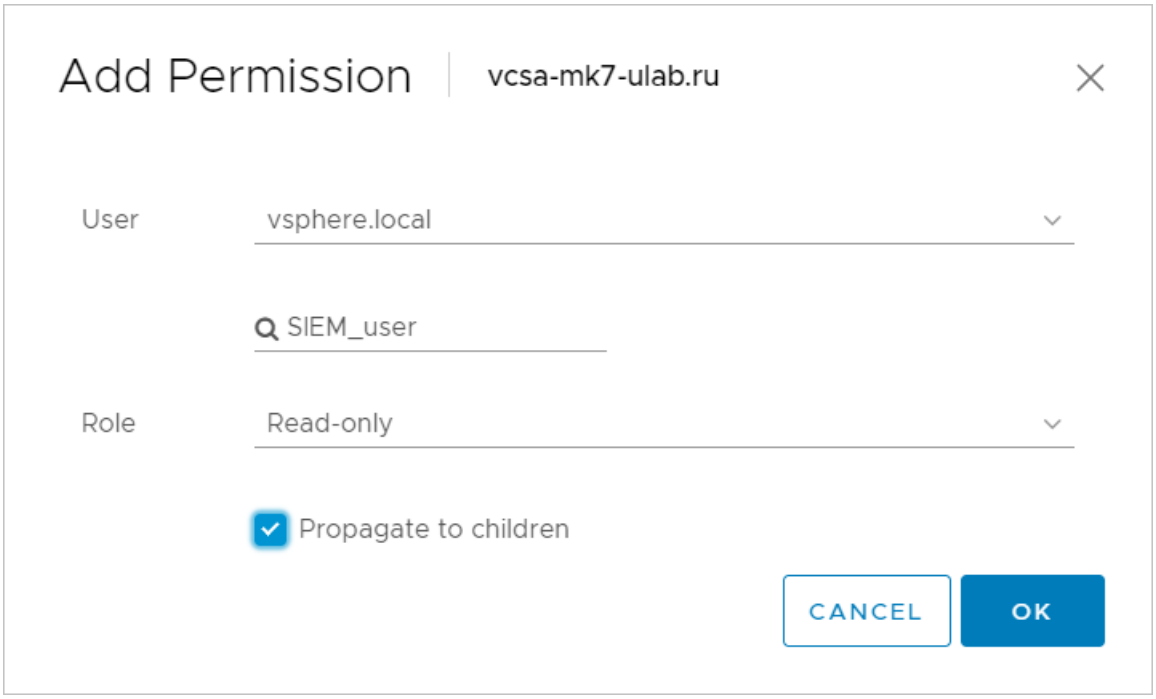

Рисунок 14. Назначение прав доступа учетной записи

10. Нажмите кнопку **OK**.

Учетная запись ОС добавлена в список пользователей vCenter Server.

7.2. VMware vCenter Server 5.5—7.0: настройка MaxPatrol VM

Для настройки аудита в MaxPatrol VM нужно добавить учетную запись для доступа к активу, создать и запустить задачу на сбор данных с профилем vSphere Audit.

Примечание. Для доступа на сервер VMware vCenter вы можете использовать сертификат SSL. Для этого на узле сервера необходимо выпустить сертификат (поле Subject Alternative Name должно содержать IP-адрес) и с помощью утилиты vSphere Certificate Manager добавить его в VMware Endpoint Certificate Store; на узле MP 10 Collector необходимо штатными средствами ОС добавить этот сертификат в хранилище сертификатов от доверенных корневых центров сертификации.

В этом разделе

7.2.1. Добавление учетной записи

► Чтобы добавить в MaxPatrol VM учетную запись для доступа к активу:

1. В главном меню в разделе **Сбор данных** выберите пункт **Учетные записи**.

   Откроется страница **Учетные записи**.

2. В панели инструментов нажмите кнопку **Добавить учетную запись** и в раскрывшемся меню выберите пункт **Логин — пароль**.

   Откроется страница **Добавление учетной записи**.

3. В поле **Название** введите название учетной записи.

   Примечание. В поле **Описание** вы можете ввести любой текстовый комментарий.

4. В раскрывающемся списке **Метки** установите флажок **vSphere_API**.

5. В поле **Логин** введите логин учетной записи.

6. Если требуется, в поле **Пароль** введите пароль и подтвердите его в поле **Подтверждение пароля**.

7. Если для доступа к источнику используется доменная учетная запись, в поле **Домен** введите имя домена.
8. Нажмите кнопку **Сохранить**.

Учетная запись добавлена.

7.2.2. Создание и запуск задачи на аудит актива

► Чтобы создать и запустить задачу на проведение аудита актива:

1. В главном меню в разделе **Сбор данных** выберите пункт **Задачи**.

   Откроется страница **Задачи по сбору данных**.
2. В панели инструментов нажмите кнопку **Создать задачу** и в раскрывшемся меню выберите пункт **Сбор данных**.

   Откроется страница **Создание задачи на сбор данных**.
3. В поле **Название** введите название задачи.
4. Если требуется, добавьте подробное описание задачи по ссылке **Добавить описание**.
5. В раскрывающемся списке **Профиль** выберите **vSphere Audit**.
6. В иерархическом списке выберите пункт **Сканирование систем** → **VMware vSphere**.
7. В раскрывающемся списке **Учетная запись** выберите учетную запись пользователя ОС.
8. Отключите проверку сертификата SSL.
9. Если требуется, в раскрывающемся списке **Коллекторы** выберите коллекторы для сбора данных.
10. В панели **Цели сбора данных** на вкладке **Включить** в поле **Активы** введите IP-адрес или доменное имя (в формате FQDN) узла актива.

    Примечание. В панели **Расписание** вы можете включить и настроить автоматический запуск задачи по расписанию.
11. Нажмите кнопку **Сохранить и запустить**.

Задача на проведение аудита актива создана и запущена.

8. Системы защиты сети

Раздел содержит инструкции для настройки аудита поддерживаемых в MaxPatrol VM систем защиты сети.

В этом разделе

8.1. Palo Alto Networks PAN-OS 6.1—8.1: настройка актива

Настройку актива нужно выполнять от имени учетной записи администратора устройства.

> **Внимание!** При использовании в IT-инфраструктуре организации межсетевого экрана или других средств для контроля сетевого трафика требуется настроить в них правила, разрешающие трафик в обоих направлениях между узлом актива и узлом MP 10 Collector. Для проведения аудита актива по протоколу SSH используется порт TCP 22.

Для проведения аудита на активе нужно создать учетную запись для доступа MP 10 Collector по протоколу SSH.

► Чтобы создать учетную запись для доступа к активу:

1. В адресной строке браузера введите IP-адрес или доменное имя актива.
2. Авторизуйтесь на активе.
3. Выберите вкладку **Device**.
4. В левой части страницы выберите **Administrators**.
5. В нижней части страницы нажмите кнопку **Add**.

   Откроется окно **Administrator**.
6. В поле **Name** введите логин учетной записи.
7. В поле **Password** введите пароль учетной записи и повторите его в поле **Confirm Password**.
8. Выберите **Role**: **Dynamic** и в раскрывающемся списке **Superuser (read-only)**.
9. Нажмите кнопку **OK**.

10. Нажмите кнопку **Save**.
11. Нажмите кнопку **Commit**.

Учетная запись создана.

8.2. Palo Alto Networks PAN-OS 6.1—8.1: настройка MaxPatrol VM

Для проведения аудита актива по протоколу SSH в MaxPatrol VM нужно добавить учетную запись для доступа к активу, создать и запустить задачу на проведение аудита.

В этом разделе

8.2.1. Добавление учетной записи для доступа по SSH

► Чтобы добавить в MaxPatrol VM учетную запись для доступа к активу:

1. В главном меню в разделе **Сбор данных** выберите пункт **Учетные записи**.

   Откроется страница **Учетные записи**.
2. В панели инструментов нажмите кнопку **Добавить учетную запись** и в раскрывшемся меню выберите пункт **Логин — пароль**.

   Откроется страница **Добавление учетной записи**.
3. В поле **Название** введите название учетной записи.

   Примечание. В поле **Описание** вы можете ввести любой текстовый комментарий.
4. В раскрывающемся списке **Метки** установите флажок **Terminal**.
5. В поле **Логин** введите логин учетной записи.
6. В поле **Пароль** введите пароль и подтвердите его в поле **Подтверждение пароля**.
7. Нажмите кнопку **Сохранить**.

Учетная запись добавлена.

8.2.2. Создание задачи на аудит актива по SSH

► Чтобы создать задачу на проведение аудита актива:

1. В главном меню в разделе **Сбор данных** выберите пункт **Задачи**.

Откроется страница **Задачи по сбору данных**.

2. В панели инструментов нажмите кнопку **Создать задачу** и в раскрывшемся меню выберите пункт **Сбор данных**.

   Откроется страница **Создание задачи на сбор данных**.

3. В поле **Название** введите название задачи.
4. Если требуется, добавьте подробное описание задачи по ссылке **Добавить описание**.
5. В раскрывающемся списке **Профиль** выберите **SSH Network Device Audit**.
6. В иерархическом списке выберите пункт **Сканирование систем** → **Через терминал: SSH и Telnet**.
7. В раскрывающемся списке **Учетная запись** выберите учетную запись для доступа к активу.
8. Если требуется, в раскрывающемся списке **Коллекторы** выберите коллекторы для сбора данных.
9. В панели **Цели сбора данных** на вкладке **Включить** в поле **Активы** введите IP-адрес или доменное имя (в формате FQDN) узла актива.

   Примечание. В панели **Расписание** вы можете включить и настроить автоматический запуск задачи по расписанию.

10. Нажмите кнопку **Сохранить**.

Задача на проведение аудита актива создана.

8.3. Positive Technologies MaxPatrol 8: настройка интеграции

Настройку интеграции нужно выполнять от имени учетной записи пользователя MP8, добавленной в группу Administrators. Настройку на узле MP8 нужно выполнять от имени учетной записи локального администратора ОС.

Внимание! При использовании в IT-инфраструктуре организации межсетевого экрана или других средств для контроля сетевого трафика требуется настроить в них правила, разрешающие трафик в обоих направлениях между узлом MP8 и узлом MP 10 Collector. Используются порты UDP 137, UDP 138, TCP 139, TCP 445.

Внимание! При использовании на узле MP8 межсетевого экрана Windows в нем нужно включить правило для входящих подключений (см. раздел 15.1.1) «Общий доступ к файлам и принтерам (входящий трафик SMB)» (File and Printer Sharing (SMB-In)).

В MaxPatrol VM предусмотрена возможность импорта активов под управлением Windows и ОС семейства Linux, обнаруженных MP8 при сканировании в режимах Pentest и Audit. Выполняется импорт данных о сетевой конфигурации, сетевых службах, установленных ОС и ПО, обнаруженных уязвимостях и аппаратном обеспечении активов.

Внимание! Для импорта активов в отчете MP8 должны быть указаны IP- и MAC-адрес каждого актива. Кроме того, для активов с Windows должны быть указаны имя узла, его FQDN и идентификатор системы (SystemID).

В MP8 для экспорта отчета нужно:

1. Добавить учетные записи для доступа в ОС Windows и Linux при сканировании в режиме Audit.
2. Создать пользовательский профиль для сканирования в режимах Pentest и Audit.
3. Создать и запустить задачу на сканирование.
4. Настроить доставку отчета в общую папку.
5. Создать шаблон отчета в формате MPX import (.xml) для экспорта в MaxPatrol VM.
6. Выполнить экспорт отчета в общую папку.

Для импорта данных отчета на узле MP8 нужно:

1. Средствами ОС создать учетную запись локального пользователя ОС (см. раздел 15.1.2) для доступа MP 10 Collector.

   Примечание. Данные этой учетной записи нужно указать при добавлении учетной записи в MaxPatrol VM.

2. Добавить учетную запись в локальную (групповую) политику безопасности (см. раздел 15.1.3) «Доступ к компьютеру из сети» (Access this computer from the network).
3. Настроить общий доступ к папке с отчетами и предоставить учетной записи права на чтение и запись файлов в этой папке.

В этом разделе

8.3.1. Добавление учетной записи

► Чтобы добавить учетную запись:

1. Запустите консоль MP8.
2. Выберите вкладку **Сканирования**.
3. В нижней части окна выберите вкладку **Учетные записи**.

4. В панели **Учетные записи** нажмите ✚.

   Откроется окно **Добавление учетной записи**.

5. В поле **Название** введите название учетной записи.
6. В поле **Имя пользователя** введите логин.
7. Если требуется, в поле **Пароль** введите пароль и подтвердите его в поле **Подтверждение пароля**.
8. Нажмите кнопку **OK**.

Учетная запись добавлена.

8.3.2. Создание профиля для сканирования

► Чтобы создать пользовательский профиль для сканирования:

1. Запустите консоль MP8.
2. Выберите вкладку **Сканирования**.
3. В нижней части окна выберите вкладку **Профили**.
4. В панели **Профили** нажмите ✚.

   Откроется окно **Редактирование профиля**.

5. В поле **Название профиля** введите название.
6. В левой части окна выберите узел **Профиль сканирования** → **Режимы сканирования**.
7. Снимите флажок **Выполнить сканирование в режиме Compliance** (должны быть установлены флажки **Выполнить сканирование в режиме PenTest** и **Выполнить сканирование в режиме Audit**).
8. В левой части окна выберите узел **Учетные записи** → **режим Audit** → **Windows**.
9. В раскрывающемся списке **Учетная запись** выберите название учетной записи для доступа в Windows.
10. В левой части окна выберите узел **Учетные записи** → **режим Audit** → **<ОС семейства Unix>**.
11. В раскрывающемся списке **Учетная запись** выберите название учетной записи для доступа в ОС семейства Unix.
12. Нажмите кнопку **OK**.

Пользовательский профиль создан.

8.3.3. Создание и запуск задачи на сканирование

► Чтобы создать и запустить задачу на сканирование:

1. Запустите консоль MP8.
2. Выберите вкладку **Сканирования**.
3. В нижней части окна выберите вкладку **Задачи**.
4. В панели **Задачи** нажмите .

   Откроется окно **Параметры задачи**.
5. В поле **Название** введите название задачи.
6. Если требуется, добавьте подробное описание задачи по ссылке **Добавить описание**.
7. В списке **Узлы** по ссылке **Добавить профиль** добавьте строку.
8. В колонке **Профиль и переопределения** в раскрывающемся списке выберите профиль сканирования.
9. В колонке **Узлы** введите через запятую IP-адреса узлов для сканирования.
10. Нажмите кнопку **OK**.
11. В панели **Задачи** нажмите .

    В панели **Активные сканы** появится строка статуса сканирования.

Задача на сканирование создана и запущена.

8.3.4. Настройка доставки отчетов

► Чтобы настроить доставку отчетов:

1. Запустите консоль MP8.
2. Выберите вкладку **Отчеты**.
3. В левой части окна выберите **Доставки**.
4. В панели **Доставки** нажмите .

   Откроется окно **Добавление доставки**.
5. В поле **Название** введите название доставки.
6. В поле **Имя файла отчета** введите шаблон имени файла в формате XML.
7. Выберите доставку в сетевой каталог.

8. В поле **Сетевой каталог** введите путь к общей папке для отчетов.
9. Нажмите кнопку **OK**.

Доставка отчетов настроена.

8.3.5. Создание шаблона отчета

► Чтобы создать шаблон отчета:

1. Запустите консоль MP8.
2. Выберите вкладку **Отчеты**.
3. В левой части окна выберите **Отчеты**.
4. В панели **Отчеты** нажмите .

   Откроется окно **Добавление отчета**.
5. В поле **Название** введите название шаблона.
6. В раскрывающемся списке **Формат** выберите **MPX import (.xml)**.
7. В блоке параметров **Тип отчета** выберите **Информация**.
8. В блоке параметров **Исходные данные** выберите **По скану**.
9. В раскрывающемся списке **Тип данных** установите флажки **PenTest** и **Audit**.
10. Нажмите кнопку **OK**.

Шаблон отчета создан.

8.3.6. Экспорт отчета

► Чтобы выполнить экспорт отчета по данным сканирования:

1. Запустите консоль MP8.
2. Выберите вкладку **История**.
3. В панели **Задачи** выберите задачу на сканирование.
4. В панели **Календарь** выберите узел с датой сканирования.
5. В панели **Сканы** в контекстном меню результата сканирования выберите **Отчет** → **<Название шаблона отчета>**.
6. Выберите вкладку **Отчеты**.
7. В панели **Отчеты** выберите отчет и нажмите .
8. В открывшемся окне выберите доставку и нажмите кнопку **Доставить**.

9. В открывшемся окне нажмите **OK**.
10. Нажмите кнопку **Закрыть**.

Экспорт отчета выполнен.

8.4. Positive Technologies MaxPatrol 8: настройка MaxPatrol VM

Для импорта отчета из общей папки на узле MP8 в MaxPatrol VM нужно добавить учетную запись для доступа на узел MP8, создать и запустить задачу на импорт отчета с профилем **MP8ScanImporter**.

Примечание. При обновлении данных об активах указываются дата и время импорта отчета.

В этом разделе

8.4.1. Добавление учетной записи

► Чтобы добавить в MaxPatrol VM учетную запись для доступа на узел MP8:

1. В главном меню в разделе **Сбор данных** выберите пункт **Учетные записи**.

   Откроется страница **Учетные записи**.
2. В панели инструментов нажмите кнопку **Добавить учетную запись** и в раскрывшемся меню выберите пункт **Логин — пароль**.

   Откроется страница **Добавление учетной записи**.
3. В поле **Название** введите название учетной записи.

   Примечание. В поле **Описание** вы можете ввести любой текстовый комментарий.
4. В раскрывающемся списке **Метки** установите флажок **SMB**.
5. В поле **Логин** введите логин учетной записи.
6. Если требуется, в поле **Пароль** введите пароль и подтвердите его в поле **Подтверждение пароля**.
7. Нажмите кнопку **Сохранить**.

Учетная запись добавлена.

8.4.2. Создание и запуск задачи на импорт отчета

► Чтобы создать и запустить задачу на импорт отчета:

1. В главном меню в разделе **Сбор данных** выберите пункт **Задачи**.

   Откроется страница **Задачи по сбору данных**.

2. В панели инструментов нажмите кнопку **Создать задачу** и в раскрывшемся меню выберите пункт **Сбор данных**.

   Откроется страница **Создание задачи на сбор данных**.

3. В поле **Название** введите название задачи.
4. Если требуется, добавьте подробное описание задачи по ссылке **Добавить описание**.
5. В раскрывающемся списке **Профиль** выберите **MP8ScanImporter**.
6. В раскрывающемся списке **Учетная запись** выберите учетную запись пользователя ОС.
7. В иерархическом списке выберите пункт **Сбор событий**.
8. В поле **Путь к общей папке** введите путь к папке с отчетами.
9. Если требуется, в раскрывающемся списке **Коллектор** выберите MP 10 Collector для сбора событий.
10. В панели **Цели сбора данных** на вкладке **Включить** в поле **Сетевые адреса** введите IP-адрес узла MP8.

    Примечание. В панели **Расписание** вы можете включить и настроить автоматический запуск задачи по расписанию.

11. Нажмите кнопку **Сохранить и запустить**.

Задача на импорт отчета создана и запущена.

9. Системы мониторинга сети

Раздел содержит инструкции для настройки аудита поддерживаемых в MaxPatrol VM систем мониторинга сети.

В этом разделе

9.1. Microsoft System Center Configuration Manager (SCCM) 2012—2019: настройка актива

Настройку актива нужно выполнять от имени учетной записи, имеющей права локального администратора ОС и поддерживающей в настраиваемом экземпляре СУБД роль sysadmin.

> **Внимание!** При использовании в IT-инфраструктуре организации межсетевого экрана или других средств для контроля сетевого трафика требуется настроить в них правила, разрешающие трафик в обоих направлениях между узлом актива и узлом MP 10 Collector. Для проведения аудита используется порт 1433/TCP.

Данные об узлах, зарегистрированных в Microsoft System Center Configuration Manager, сохраняются в БД (по умолчанию SCCM) под управлением СУБД Microsoft SQL Server. При проведении аудита эти узлы добавляются в MaxPatrol VM в качестве активов. Для каждого актива указывается информация о версии ОС и установленном ПО.

Для проведения аудита на активе нужно:

1. Создать локальную (см. раздел 15.1.2) или доменную (см. раздел 15.4.3) учетную запись пользователя Windows.

   Примечание. Данные этой учетной записи нужно указать при добавлении учетной записи в MaxPatrol VM.

2. Настроить локальную (см. раздел 15.4.2) или групповую (см. раздел 15.4.4) политику безопасности для удаленного доступа учетной записи.
3. Настроить локальную или групповую (см. раздел 15.3.6) политику безопасности для доступа учетной записи к разделам реестра.
4. На основе учетной записи пользователя Windows создать учетную запись СУБД и выдать ей права на просмотр определений объектов БД с данными для аудита. Вы можете сделать это вручную (см. раздел 9.1.1) или с помощью запроса (см. раздел 9.1.2).
5. Настроить порты TCP/IP для подключения к СУБД (см. раздел 15.4.6).
6. Настроить автоматический запуск SQL Server Browser (см. раздел 15.4.7).

В этом разделе

9.1.1. Создание учетной записи Microsoft SQL Server

При создании учетной записи СУБД для проведения аудита требуется на основе учетной записи пользователя Windows создать учетную запись с правом на чтение БД master и SCCM и в каждой из этих БД выдать учетной записи право на просмотр определений объектов.

Создание учетной записи

► Чтобы создать учетную запись СУБД на основе учетной записи пользователя Windows:

1. Запустите Microsoft SQL Server Management Studio.

   Откроется окно **Connect to Server**.

2. В раскрывающемся списке **Server name** выберите сервер и экземпляр СУБД.
3. Введите данные учетной записи администратора СУБД и нажмите кнопку **Connect**.

   Откроется окно Microsoft SQL Server Management Studio.

4. В панели **Object Explorer** в контекстном меню узла **<Имя экземпляра СУБД>** → **Security** → **Logins** выберите **New Login**.

   Откроется окно **Login — New**.

5. Выберите **Windows authentication** и нажмите кнопку **Search**.

   Откроется окно **Select User or Group**.

6. Нажмите кнопку **Locations**.
7. В открывшемся окне выберите:
   - если используется локальная учетная запись — имя узла;
   - если используется доменная учетная запись — имя домена.
8. Нажмите кнопку **OK**.
9. В поле **Enter the object name to select** введите логин учетной записи Windows и нажмите кнопку **Check Names**.
10. Нажмите кнопку **OK**.
11. В окне **Login — New** в раскрывающемся списке **Default database** выберите **master**.
12. В панели **Select a page** выберите **User Mapping**.

13. В списке **User mapped to this login** установите флажки в строках баз данных **master** и **SCCM**.
14. В списке **Database role membership** установите флажки для ролей **db_datareader** и **public**.
15. В панели **Select a page** выберите **Securables**.
16. Если список в панели **Securables** не содержит имени сервера СУБД, нажмите кнопку **Search**, в открывшемся окне выберете **The server <Имя сервера>** и нажмите кнопку **OK**.
17. В нижней части окна выберите вкладку **Explicit**.
18. В колонке **Gant** установите флажки в строках **Connect SQL**, **View server state** и **View any definition**.

    Примечание. При установке флажка **View any definition** учетной записи предоставляется доступ к определениям всех объектов сервера СУБД из таблиц sys.server_permissions, sys.server_principals и sys.sql_logins.
19. Нажмите кнопку **OK**.

Учетная запись СУБД создана.

Выдача прав на просмотр определений объектов БД

Инструкцию требуется выполнить для каждой БД с данными для аудита.

► Чтобы выдать учетной записи право на просмотр определений объектов БД:

1. Запустите Microsoft SQL Server Management Studio.

   Откроется окно **Connect to Server**.
2. В раскрывающемся списке **Server name** выберите сервер и экземпляр СУБД.
3. Введите данные учетной записи администратора СУБД и нажмите кнопку **Connect**.

   Откроется окно Microsoft SQL Server Management Studio.
4. В панели **Object Explorer** в контекстном меню узла **<Имя экземпляра СУБД>** → **Databases** → **System Databases** → **<Имя БД>** выберите **Properties**.

   Откроется окно **Databases Properties — <Имя БД>**.
5. В панели **Select a page** выберите **Permissions**.
6. В списке **Users or roles** выберите созданную ранее учетную запись.
7. В нижней части окна выберите вкладку **Explicit**.
8. В колонке **Gant** установите флажок в строке **View definition**.
9. Нажмите кнопку **OK**.

Право на просмотр определений объектов БД выдано учетной записи.

9.1.2. Создание учетной записи Microsoft SQL Server с помощью запроса

► Чтобы создать учетную запись СУБД на основе учетной записи пользователя Windows с помощью запроса:

1. Запустите Microsoft SQL Server Management Studio.

   Откроется окно **Connect to Server**.

2. В раскрывающемся списке **Server name** выберите сервер и экземпляр СУБД.

3. Введите данные учетной записи администратора СУБД и нажмите кнопку **Connect**.

   Откроется окно Microsoft SQL Server Management Studio.

4. В панели **Object Explorer** в контекстном меню узла **<Имя экземпляра СУБД>** выберите **New Query**.

   Откроется панель нового запроса.

5. Введите запрос:

```
use [master];
create login [<Домен>\<Логин>] from windows;
create user [<Домен>\<Логин>] for login [<Домен>\<Логин>]
grant select on information_schema.tables to [<Домен>\<Логин>]
grant select on sys.databases to [<Домен>\<Логин>]
grant select on sys.database_files to [<Домен>\<Логин>]
grant view server state to [<Домен>\<Логин>]
grant view definition to [<Домен>\<Логин>]
use [SCCM];
create user [<Домен>\<Логин>] for login [<Домен>\<Логин>]
grant select on SCCM.sys.database_files to [<Домен>\<Логин>]
grant select on SCCM.dbo.v_R_System_Valid to [<Домен>\<Логин>]
grant select on SCCM.SCCM_Ext.vex_GS_PROCESSOR to [<Домен>\<Логин>]
grant select on SCCM.dbo.v_GS_LOGICAL_DISK to [<Домен>\<Логин>]
grant select on SCCM.dbo.v_GS_COMPUTER_SYSTEM to [<Домен>\<Логин>]
grant select on SCCM.SCCM_Ext.vex_R_System to [<Домен>\<Логин>]
grant select on SCCM.dbo.System_DATA to [<Домен>\<Логин>]
grant select on SCCM.dbo.v_GS_OPERATING_SYSTEM to [<Домен>\<Логин>]
grant select on SCCM.dbo.v_GS_ADD_REMOVE_PROGRAMS to [<Домен>\<Логин>]
grant select on SCCM.dbo.v_GS_ADD_REMOVE_PROGRAMS_64 to [<Домен>\<Логин>]
grant select on SCCM.SCCM_Ext.vex_GS_NETWORK_ADAPTER to [<Домен>\<Логин>]
--Строка для таблицы Ext.vex_GS_NETWORK_ADAPTER_CONFIGUR
grant select on SCCM.SCCM_Ext.vex_GS_NETWORK_ADAPTER_CONFIGUR to [<Домен>\<Логин>]
--Строка для выдачи прав на просмотр определений объектов БД
grant view definition to [<Домен>\<Логин>]
```

6. Если вместо таблицы `Ext.vex_GS_NETWORK_ADAPTER_CONFIGUR` используется `Ext.vex_GS_NETWORK_ADAPTER_CONFIGURATION`, замените в запросе строку:

```
grant select on SCCM.SCCM_Ext.vex_GS_NETWORK_ADAPTER_CONFIGUR to [<Домен>\<Логин>]
```

на строку:

```
grant select on SCCM.SCCM_Ext.vex_GS_NETWORK_ADAPTER_CONFIGURATION to [<Домен>\<Логин>]
```

7. В панели инструментов нажмите кнопку **Execute**.

Учетная запись СУБД создана.

9.2. Microsoft System Center Configuration Manager (SCCM) 2012—2019: настройка MaxPatrol VM

Примечание. Для доступа в СУБД Microsoft SQL Server на узле MP 10 Collector требуется установить Microsoft ODBC Driver for SQL Server, версию для 32-разрядной архитектуры для MP 10 Collector на Windows или версию для 64-разрядной архитектуры для MP 10 Collector на Linux. Драйвер вы можете скачать с сайта microsoft.com.

Для проведения аудита в MaxPatrol VM нужно добавить учетную запись для доступа к активу, создать и запустить задачу на сбор данных с профилем MSSQL Audit.

В этом разделе

9.2.1. Добавление учетной записи для СУБД Microsoft SQL Server

► Чтобы добавить в MaxPatrol VM учетную запись для доступа к активу:

1. В главном меню в разделе **Сбор данных** выберите пункт **Учетные записи**.

   Откроется страница **Учетные записи**.

2. В панели инструментов нажмите кнопку **Добавить учетную запись** и в раскрывшемся меню выберите пункт **Логин — пароль**.

   Откроется страница **Добавление учетной записи**.

3. В поле **Название** введите название учетной записи.

   Примечание. В поле **Описание** вы можете ввести любой текстовый комментарий.

4. В раскрывающемся списке **Метки** установите флажки **DB_MSSQL** и **WindowsAudit**.

5. В поле **Логин** введите логин учетной записи.

6. Если требуется, в поле **Пароль** введите пароль и подтвердите его в поле **Подтверждение пароля**.

7. Если для доступа к источнику используется доменная учетная запись, в поле **Домен** введите имя домена.
8. Нажмите кнопку **Сохранить**.

Учетная запись добавлена.

9.2.2. Создание и запуск задачи на аудит актива

► Чтобы создать и запустить задачу на проведение аудита актива:

1. В главном меню в разделе **Сбор данных** выберите пункт **Задачи**.

   Откроется страница **Задачи по сбору данных**.
2. В панели инструментов нажмите кнопку **Создать задачу** и в раскрывшемся меню выберите пункт **Сбор данных**.

   Откроется страница **Создание задачи на сбор данных**.
3. В поле **Название** введите название задачи.
4. Если требуется, добавьте подробное описание задачи по ссылке **Добавить описание**.
5. В раскрывающемся списке **Профиль** выберите **MSSQL Audit**.
6. В иерархическом списке выберите пункт **Сканирование систем** → **Windows**.
7. В раскрывающемся списке **Учетная запись** выберите учетную запись пользователя ОС.
8. В иерархическом списке выберите пункт **Сканирование систем** → **Microsoft SQL Server**.
9. В раскрывающемся списке **Учетная запись** выберите учетную запись пользователя ОС.
10. В поле **Имя экземпляра СУБД** введите имя экземпляра.
11. Если требуется, в раскрывающемся списке **Коллекторы** выберите коллекторы для сбора данных.
12. В панели **Цели сбора данных** на вкладке **Включить** в поле **Активы** введите IP-адрес или доменное имя (в формате FQDN) узла актива.

    Примечание. В панели **Расписание** вы можете включить и настроить автоматический запуск задачи по расписанию.
13. Нажмите кнопку **Сохранить и запустить**.

Задача на проведение аудита актива создана и запущена.

10. Системы управления базами данных

Раздел содержит инструкции для настройки аудита поддерживаемых в MaxPatrol VM систем управления базами данных.

В этом разделе

10.1. Microsoft SQL Server 2008—2019: настройка актива

Настройку актива нужно выполнять от имени учетной записи, имеющей права локального администратора ОС и поддерживающей в настраиваемом экземпляре СУБД роль sysadmin.

> **Внимание!** При использовании в IT-инфраструктуре организации межсетевого экрана или других средств для контроля сетевого трафика требуется настроить в них правила, разрешающие трафик в обоих направлениях между узлом актива и узлом MP 10 Collector. Для проведения аудита используется порт 1433/TCP.

Для проведения аудита на активе нужно:

1. Создать локальную (см. раздел 15.1.2) или доменную (см. раздел 15.4.3) учетную запись пользователя Windows.

   Примечание. Данные этой учетной записи нужно указать при добавлении учетной записи в MaxPatrol VM.

2. Настроить локальную (см. раздел 15.4.2) или групповую (см. раздел 15.4.4) политику безопасности для удаленного доступа учетной записи.
3. Настроить локальную или групповую (см. раздел 15.3.6) политику безопасности для доступа учетной записи к разделам реестра.
4. На основе учетной записи пользователя Windows создать учетную запись СУБД и выдать ей права на просмотр определений объектов БД с данными для аудита. Вы можете сделать это вручную (см. раздел 10.1.1) или с помощью запроса (см. раздел 10.1.2).
5. Настроить порты TCP/IP для подключения к СУБД (см. раздел 15.4.6).
6. Настроить автоматический запуск SQL Server Browser (см. раздел 15.4.7).

В этом разделе

10.1.1. Создание учетной записи Microsoft SQL Server

При создании учетной записи СУБД для проведения аудита требуется на основе учетной записи пользователя Windows создать учетную запись с правом на чтение БД master, model, msdb, tempdb и в каждой из этих БД выдать учетной записи право на просмотр определений объектов.

Создание учетной записи

► Чтобы создать учетную запись СУБД на основе учетной записи пользователя Windows:

1. Запустите Microsoft SQL Server Management Studio.

   Откроется окно **Connect to Server**.

2. В раскрывающемся списке **Server name** выберите сервер и экземпляр СУБД.

3. Введите данные учетной записи администратора СУБД и нажмите кнопку **Connect**.

   Откроется окно Microsoft SQL Server Management Studio.

4. В панели **Object Explorer** в контекстном меню узла **<Имя экземпляра СУБД>** → **Security** → **Logins** выберите **New Login**.

   Откроется окно **Login — New**.

5. Выберите **Windows authentication** и нажмите кнопку **Search**.

   Откроется окно **Select User or Group**.

6. Нажмите кнопку **Locations**.

7. В открывшемся окне выберите:

   - если используется локальная учетная запись — имя узла;
   - если используется доменная учетная запись — имя домена.

8. Нажмите кнопку **OK**.

9. В поле **Enter the object name to select** введите логин учетной записи Windows и нажмите кнопку **Check Names**.

10. Нажмите кнопку **OK**.

11. В окне **Login — New** в раскрывающемся списке **Default database** выберите **master**.

12. В панели **Select a page** выберите **User Mapping**.

13. В списке **User mapped to this login** установите флажки в строках баз данных **master**, **model**, **msdb**, **tempdb**.

14. В списке **Database role membership** установите флажки для ролей **db_datareader** и **public**.

15. В панели **Select a page** выберите **Securables**.

16. Если список в панели **Securables** не содержит имени сервера СУБД, нажмите кнопку **Search**, в открывшемся окне выберете **The server <Имя сервера>** и нажмите кнопку **OK**.
17. В нижней части окна выберите вкладку **Explicit**.
18. В колонке **Gant** установите флажки в строках **Connect SQL**, **View server state** и **View any definition**.

    Примечание. При установке флажка **View any definition** учетной записи предоставляется доступ к определениям всех объектов сервера СУБД из таблиц sys.server_permissions, sys.server_principals и sys.sql_logins.
19. Нажмите кнопку **OK**.

Учетная запись СУБД создана.

Выдача прав на просмотр определений объектов БД

Инструкцию требуется выполнить для каждой БД с данными для аудита.

► Чтобы выдать учетной записи право на просмотр определений объектов БД:

1. Запустите Microsoft SQL Server Management Studio.

   Откроется окно **Connect to Server**.
2. В раскрывающемся списке **Server name** выберите сервер и экземпляр СУБД.
3. Введите данные учетной записи администратора СУБД и нажмите кнопку **Connect**.

   Откроется окно Microsoft SQL Server Management Studio.
4. В панели **Object Explorer** в контекстном меню узла **<Имя экземпляра СУБД>** → **Databases** → **System Databases** → **<Имя БД>** выберите **Properties**.

   Откроется окно **Databases Properties — <Имя БД>**.
5. В панели **Select a page** выберите **Permissions**.
6. В списке **Users or roles** выберите созданную ранее учетную запись.
7. В нижней части окна выберите вкладку **Explicit**.
8. В колонке **Gant** установите флажок в строке **View definition**.
9. Нажмите кнопку **OK**.

Право на просмотр определений объектов БД выдано учетной записи.

10.1.2. Создание учетной записи Microsoft SQL Server с помощью запроса

► Чтобы создать учетную запись СУБД на основе учетной записи пользователя Windows с помощью запроса:

1. Запустите Microsoft SQL Server Management Studio.

   Откроется окно **Connect to Server**.

2. В раскрывающемся списке **Server name** выберите сервер и экземпляр СУБД.

3. Введите данные учетной записи администратора СУБД и нажмите кнопку **Connect**.

   Откроется окно Microsoft SQL Server Management Studio.

4. В панели **Object Explorer** в контекстном меню узла **<Имя экземпляра СУБД>** выберите **New Query**.

   Откроется панель нового запроса.

5. Введите запрос:

```
use [master];
create login [<Домен>\<Логин>] from windows;
declare @db_user varchar(300)
select @db_user =
  'USE [?]
  create user [<Домен>\<Логин>] for login [<Домен>\<Логин>]'
exec sp_MSforeachdb @db_user
declare @db_priv varchar(600)
select @db_priv =
  'USE [?]
  grant select on sys.database_permissions to [<Домен>\<Логин>]
  grant select on sys.database_principals to [<Домен>\<Логин>]
  grant select on sys.database_files to [<Домен>\<Логин>]
  grant select on sys.database_role_members to [<Домен>\<Логин>]
  grant select on sys.all_objects to [<Домен>\<Логин>]
  grant select on sys.triggers to [<Домен>\<Логин>]
  grant view definition to [<Домен>\<Логин>]'
exec sp_MSforeachdb @db_priv
grant select on information_schema.tables to [<Домен>\<Логин>]
grant select on sys.databases to [<Домен>\<Логин>]
grant select on sys.server_permissions to [<Домен>\<Логин>]
grant select on sys.sql_logins to [<Домен>\<Логин>]
grant select on sys.server_principals to [<Домен>\<Логин>]
grant select on dbo.syscharsets to [<Домен>\<Логин>]
grant select on sys.database_files to [<Домен>\<Логин>]
grant select on sys.database_mirroring to [<Домен>\<Логин>]
grant select on sys.configurations to [<Домен>\<Логин>]
grant select on sys.servers to [<Домен>\<Логин>]
```

```
grant select on sys.assemblies to [<Домен>\<Логин>]
grant select on sys.server_role_members to [<Домен>\<Логин>]
grant select on sys.dm_os_loaded_modules to [<Домен>\<Логин>]
grant select on dbo.syscharsets to [<Домен>\<Логин>]
grant view server state to [<Домен>\<Логин>]
--Сторка для выдачи прав на просмотр определений объектов БД
grant view any definition to [<Домен>\<Логин>]
```

6. В панели инструментов нажмите кнопку **Execute**.

Учетная запись СУБД создана.

10.2. Microsoft SQL Server 2008—2019: настройка MaxPatrol VM

Примечание. Для доступа в СУБД Microsoft SQL Server на узле MP 10 Collector требуется установить Microsoft ODBC Driver for SQL Server, версию для 32-разрядной архитектуры для MP 10 Collector на Windows или версию для 64-разрядной архитектуры для MP 10 Collector на Linux. Драйвер вы можете скачать с сайта microsoft.com.

Для проведения аудита в MaxPatrol VM нужно добавить учетную запись для доступа к активу, создать и запустить задачу на проведение аудита с профилем MSSQL Audit.

В этом разделе

10.2.1. Добавление учетной записи для СУБД Microsoft SQL Server

► Чтобы добавить в MaxPatrol VM учетную запись для доступа к активу:

1. В главном меню в разделе **Сбор данных** выберите пункт **Учетные записи**.

   Откроется страница **Учетные записи**.

2. В панели инструментов нажмите кнопку **Добавить учетную запись** и в раскрывшемся меню выберите пункт **Логин — пароль**.

   Откроется страница **Добавление учетной записи**.

3. В поле **Название** введите название учетной записи.

   Примечание. В поле **Описание** вы можете ввести любой текстовый комментарий.

4. В раскрывающемся списке **Метки** установите флажки **DB_MSSQL** и **WindowsAudit**.

5. В поле **Логин** введите логин учетной записи.

6. Если требуется, в поле **Пароль** введите пароль и подтвердите его в поле **Подтверждение пароля**.
7. Если для доступа к источнику используется доменная учетная запись, в поле **Домен** введите имя домена.
8. Нажмите кнопку **Сохранить**.

Учетная запись добавлена.

10.2.2. Создание и запуск задачи на аудит актива

► Чтобы создать и запустить задачу на проведение аудита актива:

1. В главном меню в разделе **Сбор данных** выберите пункт **Задачи**.

   Откроется страница **Задачи по сбору данных**.
2. В панели инструментов нажмите кнопку **Создать задачу** и в раскрывшемся меню выберите пункт **Сбор данных**.

   Откроется страница **Создание задачи на сбор данных**.
3. В поле **Название** введите название задачи.
4. Если требуется, добавьте подробное описание задачи по ссылке **Добавить описание**.
5. В раскрывающемся списке **Профиль** выберите **MSSQL Audit**.
6. В иерархическом списке выберите пункт **Сканирование систем** → **Windows**.
7. В раскрывающемся списке **Учетная запись** выберите учетную запись пользователя ОС.
8. В иерархическом списке выберите пункт **Сканирование систем** → **Microsoft SQL Server**.
9. В раскрывающемся списке **Учетная запись** выберите учетную запись пользователя ОС.
10. В поле **Имя экземпляра СУБД** введите имя экземпляра.
11. Если требуется, в раскрывающемся списке **Коллекторы** выберите коллекторы для сбора данных.
12. В панели **Цели сбора данных** на вкладке **Включить** в поле **Активы** введите IP-адрес или доменное имя (в формате FQDN) узла актива.

    Примечание. В панели **Расписание** вы можете включить и настроить автоматический запуск задачи по расписанию.
13. Нажмите кнопку **Сохранить и запустить**.

Задача на проведение аудита актива создана и запущена.

11. Системы управления серверами

Раздел содержит инструкции для настройки аудита поддерживаемых в MaxPatrol VM систем управления серверами.

В этом разделе

11.1. Dell iDRAC 7—9: настройка актива

Настройку актива нужно выполнять от имени учетной записи администратора устройства.

> **Внимание!** При использовании в IT-инфраструктуре организации межсетевого экрана или других средств для контроля сетевого трафика требуется настроить в них правила, разрешающие трафик в обоих направлениях между узлом актива и узлом MP 10 Collector. Для проведения аудита актива по протоколу SSH используется порт TCP 22.

Для проведения аудита на активе нужно включить доступ по протоколу SSH и создать учетную запись для доступа MP 10 Collector.

В этом разделе

11.1.1. Включение доступа к активу по протоколу SSH

► Чтобы включить доступ к активу по протоколу SSH:

1. Войдите в веб-интерфейс контроллера Dell iDRAC под учетной записью администратора.
2. В главном меню выберите **iDRAC Settings** → **Services**.

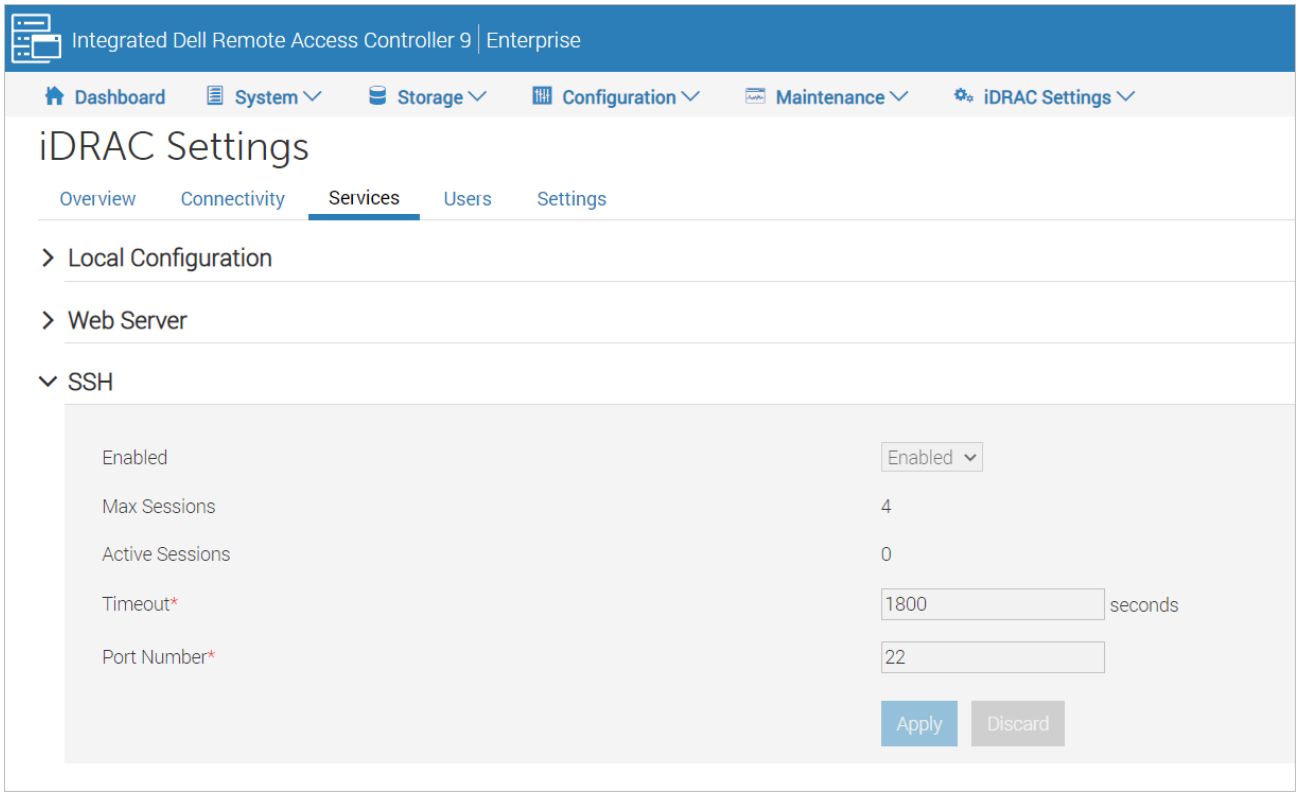

Рисунок 15. Включение доступа к активу по протоколу SSH

3. В раскрывающемся блоке **SSH** в раскрывающемся списке **Enabled** выберите значение **Enabled**.
4. Нажмите кнопку **Apply**.

Доступ к активу по протоколу SSH включен.

11.1.2. Создание учетной записи для доступа к активу

► Чтобы создать учетную запись для доступа к активу:

1. Войдите в веб-интерфейс контроллера Dell iDRAC под учетной записью администратора.
2. В главном меню выберите **iDRAC Settings** → **Users**.
3. В раскрывающемся блоке **Local Users** нажмите кнопку **Add**.

   Откроется окно создания учетной записи.
4. В поле **User Name** укажите логин учетной записи.
5. В полях **Password** и **Confirm Password** укажите пароль учетной записи.
6. В раскрывающемся списке **User Role** выберите значение **Operator**.

7. Установите флажки **Login to iDRAC** и **Execute Debug Commands**.
8. Нажмите кнопку **Save**.

Учетная запись для доступа к активу создана.

11.2. Dell iDRAC 7—9: настройка MaxPatrol VM

Для проведения аудита актива по протоколу SSH в MaxPatrol VM нужно добавить учетную запись для доступа к активу, создать и запустить задачу на проведение аудита.

11.3. HPE iLO 3—5: настройка актива

Настройку актива нужно выполнять от имени учетной записи администратора устройства.

> **Внимание!** При использовании в IT-инфраструктуре организации межсетевого экрана или других средств для контроля сетевого трафика требуется настроить в них правила, разрешающие трафик в обоих направлениях между узлом актива и узлом MP 10 Collector. Для проведения аудита актива по протоколу SSH используется порт TCP 22.

Для проведения аудита на активе нужно включить доступ по протоколу SSH и создать учетную запись для доступа MP 10 Collector.

В этом разделе

11.3.1. Включение доступа к активу по протоколу SSH

► Чтобы включить доступ к активу по протоколу SSH:

1. Войдите в веб-интерфейс программы HPE iLO под учетной записью с правами Configure iLO Settings.
2. В левой части страницы выберите **Administration** → **Access Settings**.

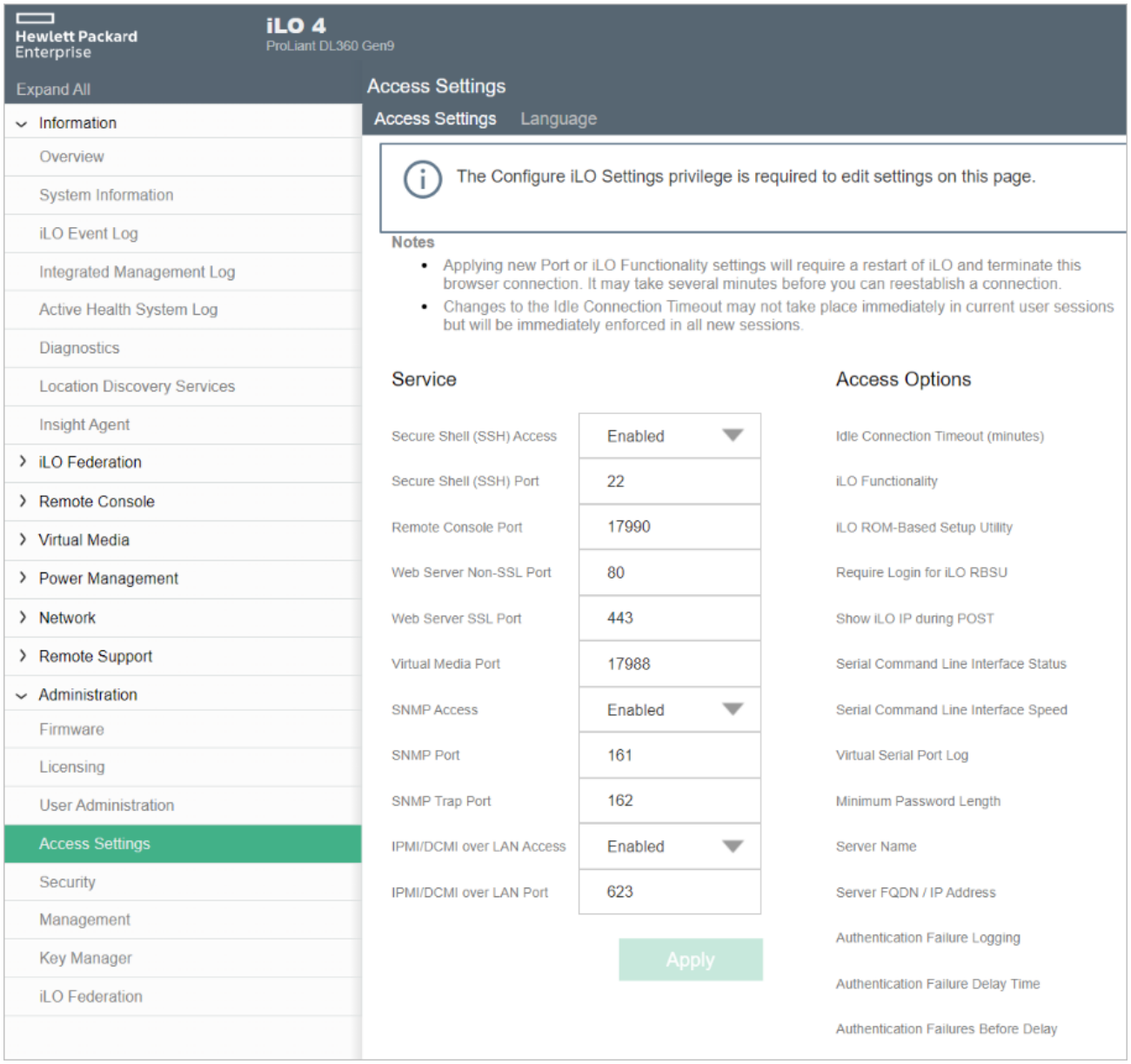

Рисунок 16. Включение доступа к активу по протоколу SSH

3. В раскрывающемся списке **Secure Shell (SSH) Access** выберите значение **Enabled**.
4. Нажмите кнопку **Apply**.

Доступ к активу по протоколу SSH включен.

11.3.2. Создание учетной записи для доступа к активу

Для проведения аудита на активе нужно создать учетную запись для доступа MP 10 Collector по протоколу SSH.

► Чтобы создать учетную запись для доступа к активу:

1. Войдите в веб-интерфейс контроллера HPE iLO под учетной записью с правами Administer User Accounts.
2. В левой части страницы выберите **Administration** → **User Administration**.
3. В блоке параметров **Local Users** нажмите кнопку **New**.

   Откроется окно создания учетной записи пользователя.
4. В поле **User Name** укажите имя пользователя, которое будет использоваться при отображении учетной записи в интерфейсе HPE iLO.
5. В поле **Login Name** укажите логин учетной записи.
6. В полях **Password** и **Password Confirm** укажите пароль учетной записи.
7. Установите флажок **Login**.
8. Нажмите кнопку **Add User**.

Учетная запись для доступа к активу создана.

11.4. HPE iLO 3—5: настройка MaxPatrol VM

Для проведения аудита актива по протоколу SSH в MaxPatrol VM нужно добавить учетную запись для доступа к активу, создать и запустить задачу на проведение аудита.

12. Службы каталогов

Раздел содержит инструкции для настройки аудита поддерживаемых в MaxPatrol VM служб каталогов.

В этом разделе

12.1. Microsoft Active Directory в Windows Server 2003—2019: настройка актива

Настройку актива нужно выполнять от имени учетной записи, имеющей права администратора домена Active Directory.

> **Внимание!** При использовании в IT-инфраструктуре организации межсетевого экрана или других средств для контроля сетевого трафика требуется настроить в них правила, разрешающие трафик в обоих направлениях между узлом источника и узлом MP 10 Collector. В Windows Server версии 2003 и 2003 R2 используются динамические TCP-порты 1025—5000[2], в версиях от 2008 до 2019 используются TCP-порты 135, 139, 389, 445, 636, динамические TCP-порты 49152—65535[2] и UDP-порты 135, 137, 138, 445.

Для проведения аудита на активе нужно создать учетную запись администратора домена Active Directory для доступа к активу MP 10 Collector. Данные этой учетной записи нужно указать при добавлении учетной записи в MaxPatrol VM.

> **Примечание.** Вы можете детально настроить учетную запись, предоставив ей права на выполнение команд для проведения аудита (см. приложение).

12.2. Microsoft Active Directory в Windows Server 2003—2019: настройка MaxPatrol VM

Для аудита актива в MaxPatrol VM нужно добавить учетную запись для доступа к активу, создать и запустить задачу на проведение аудита с профилем Microsoft Active Directory Audit.

В этом разделе

---

2 Диапазон динамических портов может быть изменен в ОС.

12.2.1. Добавление учетной записи ОС

► Чтобы добавить в MaxPatrol VM учетную запись для доступа к источнику:

1. В главном меню в разделе **Сбор данных** выберите пункт **Учетные записи**.

   Откроется страница **Учетные записи**.

2. В панели инструментов нажмите кнопку **Добавить учетную запись** и в раскрывшемся меню выберите пункт **Логин — пароль**.

   Откроется страница **Добавление учетной записи**.

3. В поле **Название** введите название учетной записи.

   Примечание. В поле **Описание** вы можете ввести любой текстовый комментарий.

4. В раскрывающемся списке **Метки** установите флажок **LDAP**.
5. В поле **Логин** введите логин учетной записи.
6. Если требуется, в поле **Пароль** введите пароль и подтвердите его в поле **Подтверждение пароля**.
7. Если для доступа к источнику используется доменная учетная запись, в поле **Домен** введите имя домена.
8. Нажмите кнопку **Сохранить**.

Учетная запись добавлена.

12.2.2. Создание и запуск задачи на аудит актива

► Чтобы создать и запустить задачу на проведение аудита актива:

1. В главном меню в разделе **Сбор данных** выберите пункт **Задачи**.

   Откроется страница **Задачи по сбору данных**.

2. В панели инструментов нажмите кнопку **Создать задачу** и в раскрывшемся меню выберите пункт **Сбор данных**.

   Откроется страница **Создание задачи на сбор данных**.

3. В поле **Название** введите название задачи.
4. Если требуется, добавьте подробное описание задачи по ссылке **Добавить описание**.
5. В раскрывающемся списке **Профиль** выберите **Microsoft Active Directory Audit**.
6. В иерархическом списке выберите пункт **Сканирование систем** → **По протоколу LDAP**.
7. В раскрывающемся списке **Учетная запись** выберите учетную запись.

8. Если требуется, в раскрывающемся списке **Коллекторы** выберите коллекторы для сбора данных.
9. В панели **Цели сбора данных** на вкладке **Включить** в поле **Активы** введите IP-адрес или доменное имя (в формате FQDN) узла актива.

   Примечание. В панели **Расписание** вы можете включить и настроить автоматический запуск задачи по расписанию.

10. Нажмите кнопку **Сохранить и запустить**.

Задача на проведение аудита актива создана и запущена.

13. Устройства беспроводной сети

Раздел содержит инструкции для настройки аудита поддерживаемых в MaxPatrol VM устройств беспроводной сети.

В этом разделе

13.1. Cisco AireOS Wireless Controller 7.4, 7.6: настройка актива

Настройку актива нужно выполнять от имени учетной записи с правом перехода в режим глобальной конфигурации.

> **Внимание!** При использовании в IT-инфраструктуре организации межсетевого экрана или других средств для контроля сетевого трафика требуется настроить в них правила, разрешающие трафик в обоих направлениях между узлом актива и узлом MP 10 Collector. Для проведения аудита актива по протоколу SSH используется порт TCP 22.

Для проведения аудита на активе нужно создать учетную запись для доступа MP 10 Collector по протоколу SSH.

► Чтобы создать учетную запись для доступа к активу:

1. На узле, с которого производится настройка актива, запустите терминальный клиент, поддерживающий сетевые протоколы SSH и Telnet.
2. Авторизуйтесь на активе.
3. Создайте учетную запись для доступа к активу:
   ```
   config mgmtuser add <Логин> <Пароль> read-only
   ```
4. Сохраните изменения:
   ```
   save config
   ```

Учетная запись создана.

13.2. Cisco AireOS Wireless Controller 7.4, 7.6: настройка MaxPatrol VM

Для проведения аудита актива по протоколу SSH в MaxPatrol VM нужно добавить учетную запись для доступа к активу, создать и запустить задачу на проведение аудита.

В этом разделе

13.2.1. Добавление учетной записи для доступа по SSH

► Чтобы добавить в MaxPatrol VM учетную запись для доступа к активу:

1. В главном меню в разделе **Сбор данных** выберите пункт **Учетные записи**.

   Откроется страница **Учетные записи**.

2. В панели инструментов нажмите кнопку **Добавить учетную запись** и в раскрывшемся меню выберите пункт **Логин — пароль**.

   Откроется страница **Добавление учетной записи**.

3. В поле **Название** введите название учетной записи.

   Примечание. В поле **Описание** вы можете ввести любой текстовый комментарий.

4. В раскрывающемся списке **Метки** установите флажок **Terminal**.
5. В поле **Логин** введите логин учетной записи.
6. В поле **Пароль** введите пароль и подтвердите его в поле **Подтверждение пароля**.
7. Нажмите кнопку **Сохранить**.

Учетная запись добавлена.

13.2.2. Создание задачи на аудит актива по SSH

► Чтобы создать задачу на проведение аудита актива:

1. В главном меню в разделе **Сбор данных** выберите пункт **Задачи**.

   Откроется страница **Задачи по сбору данных**.

2. В панели инструментов нажмите кнопку **Создать задачу** и в раскрывшемся меню выберите пункт **Сбор данных**.

   Откроется страница **Создание задачи на сбор данных**.

3. В поле **Название** введите название задачи.
4. Если требуется, добавьте подробное описание задачи по ссылке **Добавить описание**.
5. В раскрывающемся списке **Профиль** выберите **SSH Network Device Audit**.
6. В иерархическом списке выберите пункт **Сканирование систем** → **Через терминал: SSH и Telnet**.

7. В раскрывающемся списке **Учетная запись** выберите учетную запись для доступа к активу.
8. Если требуется, в раскрывающемся списке **Коллекторы** выберите коллекторы для сбора данных.
9. В панели **Цели сбора данных** на вкладке **Включить** в поле **Активы** введите IP-адрес или доменное имя (в формате FQDN) узла актива.

   Примечание. В панели **Расписание** вы можете включить и настроить автоматический запуск задачи по расписанию.
10. Нажмите кнопку **Сохранить**.

Задача на проведение аудита актива создана.

14. Другие активы

Раздел содержит инструкции для настройки аудита других активов, поддерживаемых в MaxPatrol VM.

В этом разделе

14.1. Atlassian Confluence 7.13 и выше: настройка актива

Настройку актива нужно выполнять от имени учетной записи администратора устройства.

> **Внимание!** При использовании в IT-инфраструктуре организации межсетевого экрана или других средств для контроля сетевого трафика требуется настроить в них правила, разрешающие трафик в обоих направлениях между узлом актива и узлом MP 10 Collector. Для проведения аудита актива по протоколу SSH используется порт TCP 22.

Для настройки актива необходимо настроить удаленный доступ к СУБД и создать учетную запись СУБД с правом на чтение базы данных актива.

Настройка СУБД MySQL для сканирования

Данные актива сохраняются в базу данных (по умолчанию confluence) под управлением СУБД MySQL.

► Чтобы настроить СУБД MySQL для сканирования:

1. Настройте удаленный доступ к СУБД.
2. В интерфейсе терминала запустите консоль MySQL с правами суперпользователя (root):
   ```
   mysql -u root -p
   ```
3. Переключитесь на базу данных confluence:
   ```
   USE confluence;
   ```
4. Создайте учетную запись пользователя с правами удаленного доступа к базе данных:
   ```
   CREATE USER 'ptsiem'@'%' IDENTIFIED BY 'P@ssw0rd';
   ```

   Примечание. Логин и пароль созданной учетной записи необходимо будет указать при добавлении учетной записи в MaxPatrol VM.
5. Предоставьте учетной записи права на чтение таблиц, в которых хранятся данные об активе:
   ```
   GRANT SELECT ON confluence.BANDANA TO 'ptsiem'@'%';
   GRANT SELECT ON confluence.CONTENT TO 'ptsiem'@'%';
   GRANT SELECT ON confluence.CONTENT_PERM TO 'ptsiem'@'%';
   ```

```
GRANT SELECT ON confluence.CONTENT_PERM_SET TO 'ptsiem'@'%';
GRANT SELECT ON confluence.cwd_directory TO 'ptsiem'@'%';
GRANT SELECT ON confluence.cwd_directory_attribute TO 'ptsiem'@'%';
GRANT SELECT ON confluence.cwd_directory_operation TO 'ptsiem'@'%';
GRANT SELECT ON confluence.cwd_group TO 'ptsiem'@'%';
GRANT SELECT ON confluence.cwd_membership TO 'ptsiem'@'%';
GRANT SELECT ON confluence.cwd_user TO 'ptsiem'@'%';
GRANT SELECT ON confluence.SPACES TO 'ptsiem'@'%';
GRANT SELECT ON confluence.SPACEPERMISSIONS TO 'ptsiem'@'%';
GRANT SELECT ON confluence.user_mapping TO 'ptsiem'@'%';
```

6. Примените внесенные изменения:

   ```
   FLUSH PRIVILEGES;
   ```

7. Завершите сеанс работы с консолью MySQL:

   ```
   EXIT;
   ```

СУБД MySQL настроена для сканирования.

14.2. Atlassian Confluence 7.13 и выше: настройка MaxPatrol VM

Для проведения аудита актива по протоколу SSH в MaxPatrol VM нужно добавить учетную запись для доступа к активу, создать профиль для сканирования актива, создать и запустить задачу на проведение аудита.

В этом разделе

14.2.1. Добавление учетной записи СУБД MySQL

► Чтобы добавить в MaxPatrol VM учетную запись для доступа к БД с данными актива:

1. В главном меню в разделе **Сбор данных** выберите пункт **Учетные записи**.

   Откроется страница **Учетные записи**.

2. В панели инструментов нажмите кнопку **Добавить учетную запись** и в раскрывшемся меню выберите пункт **Логин — пароль**.

   Откроется страница **Добавление учетной записи**.

3. В поле **Название** введите название учетной записи.

   Примечание. В поле **Описание** вы можете ввести любой текстовый комментарий.

4. В раскрывающемся списке **Метки** установите флажок **DB_MySQL**.

5. В поле **Логин** введите логин созданной ранее учетной записи.
6. В поле **Пароль** введите пароль созданной ранее учетной записи и подтвердите его в поле **Подтверждение пароля**.
7. Если для доступа к активу используется доменная учетная запись, в поле **Домен** введите имя домена.
8. Нажмите кнопку **Сохранить**.

Учетная запись добавлена.

14.2.2. Создание профиля для сканирования

► Чтобы добавить в MaxPatrol VM профиль для сканирования актива:

1. В главном меню в разделе **Сбор данных** выберите пункт **Профили**.

   Откроется страница **Профили**.
2. В рабочей области выберите профиль **Unix Audit**.
3. В панели инструментов нажмите кнопку **Создать** и в раскрывшемся меню выберите пункт **На базе выбранного профиля**.

   Откроется страница **Новый профиль**.
4. В поле **Название** введите название профиля.

   Примечание. В поле **Описание** вы можете ввести любой текстовый комментарий.
5. В панели **Параметры профиля** в раскрывающемся списке **Сканирование систем** выберите пункт **Oracle MySQL**.
6. Нажмите кнопку **Сохранить**.

Профиль для сканирования актива добавлен.

14.2.3. Создание и запуск задачи на аудит актива

► Чтобы создать задачу на проведение аудита актива:

1. В главном меню в разделе **Сбор данных** выберите пункт **Задачи**.

   Откроется страница **Задачи по сбору данных**.
2. В панели инструментов нажмите кнопку **Создать задачу** и в раскрывшемся меню выберите пункт **Сбор данных**.

   Откроется страница **Создание задачи на сбор данных**.
3. В поле **Название** введите название задачи.
4. Если требуется, добавьте подробное описание задачи по ссылке **Добавить описание**.

5. В панели **Параметры сбора данных** в раскрывающемся списке **Профиль** выберите профиль, созданный ранее.
6. В иерархическом списке пункт **Сканирование систем** → **Oracle MySQL**.
7. В раскрывающемся списке **Учетная запись** выберите созданную ранее учетную запись для доступа к СУБД MySQL.
8. В иерархическом списке выберите пункт **Сканирование систем** → **Через терминал: SSH**.
9. Настройте сканирование ОС актива (см. раздел 3).
10. Если требуется, в раскрывающемся списке **Коллекторы** выберите коллекторы для сбора данных.
11. Если в системе заведено больше одной инфраструктуры, в раскрывающемся списке **Инфраструктура** выберите инфраструктуру.
12. В панели **Цели сбора данных** на вкладке **Включить** в поле **Активы** введите IP-адрес или доменное имя (в формате FQDN) узла актива.

    Примечание. В панели **Расписание** вы можете включить и настроить автоматический запуск задачи по расписанию.
13. Нажмите кнопку **Сохранить**.

Задача на проведение аудита актива создана.

15. Стандартные операции для настройки активов

Раздел содержит инструкции для стандартных операций, выполняемых при настройке аудита активов.

В этом разделе

15.1. Стандартные операции в Windows

Раздел содержит инструкции для стандартных операций, выполняемых в Windows.

В этом разделе

15.1.1. Включение правила межсетевого экрана Windows

► Чтобы включить правило межсетевого экрана Windows:

1. Откройте панель управления Windows.
2. Запустите брандмауэр Windows.
3. В левой части окна выберите узел **Монитор брандмауэра Защитника Windows в режиме повышенной безопасности** → **<Категория правила>**.
4. Выберите правило.

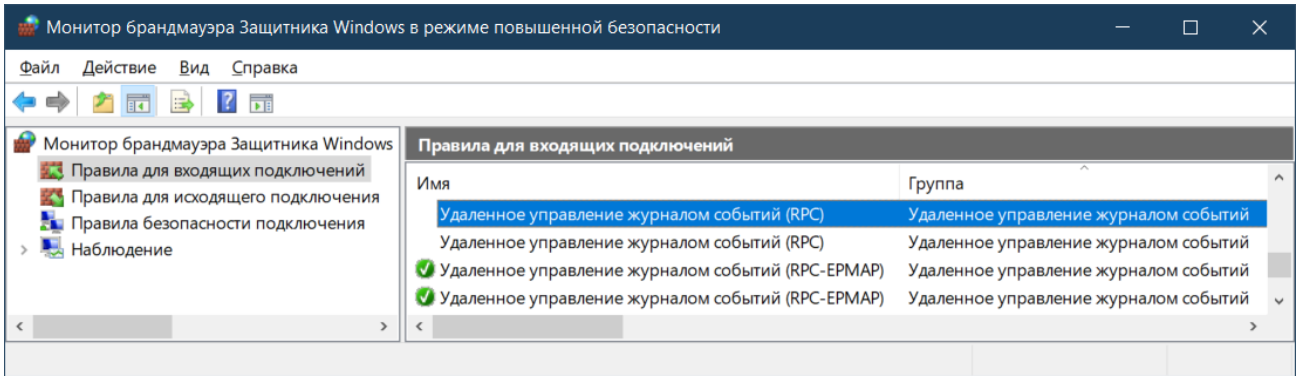

Рисунок 17. Выбор правила межсетевого экрана

5. В главном меню выберите **Действия** → **Включить правило**.

Правило включено.

15.1.2. Создание учетной записи ОС

► Чтобы создать учетную запись пользователя ОС:

1. Откройте панель управления Windows.
2. Выберите **Администрирование** → **Управление компьютером**.
3. В левой части окна выберите узел **Управление компьютером** → **Локальные пользователи и группы** → **Пользователи**.

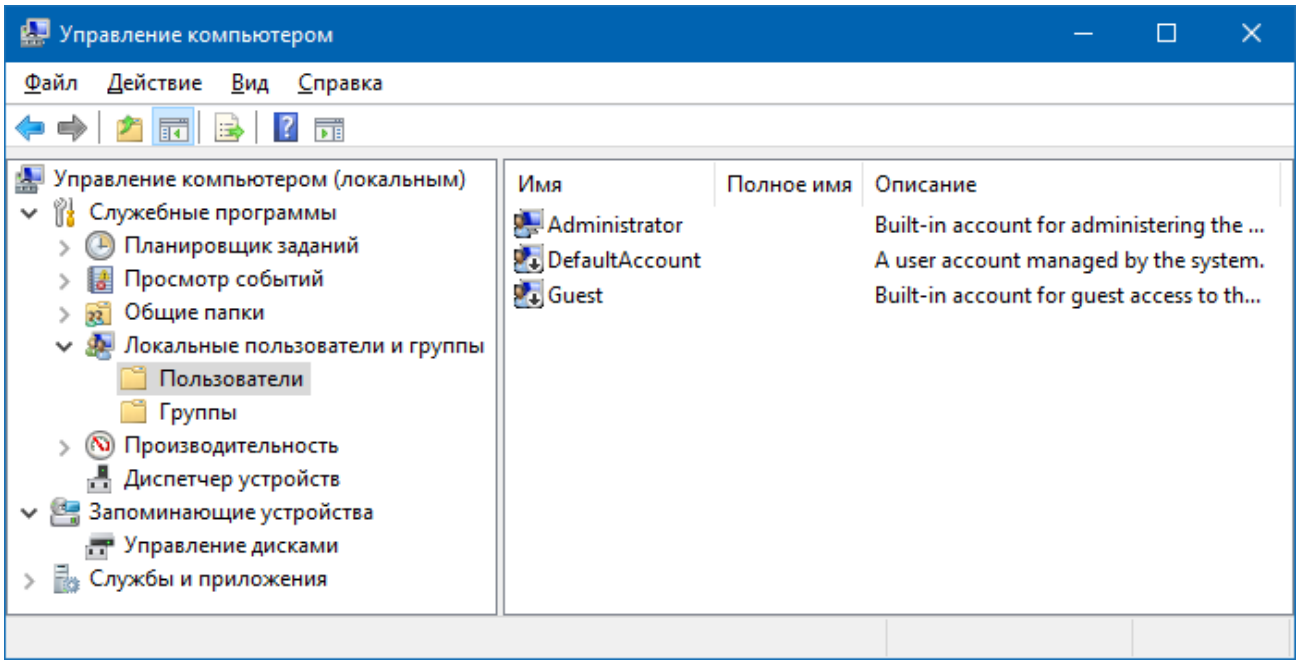

Рисунок 18. Выбор узла **Пользователи**

4. В главном меню выберите **Действие** → **Новый пользователь**.
5. В открывшемся окне в поле **Пользователь** введите логин учетной записи.
6. Установите флажок **Запретить смену пароля пользователем**.
7. Установите флажок **Срок действия пароля не ограничен**.
8. В поле **Пароль** введите пароль и подтвердите его в поле **Подтверждение**.

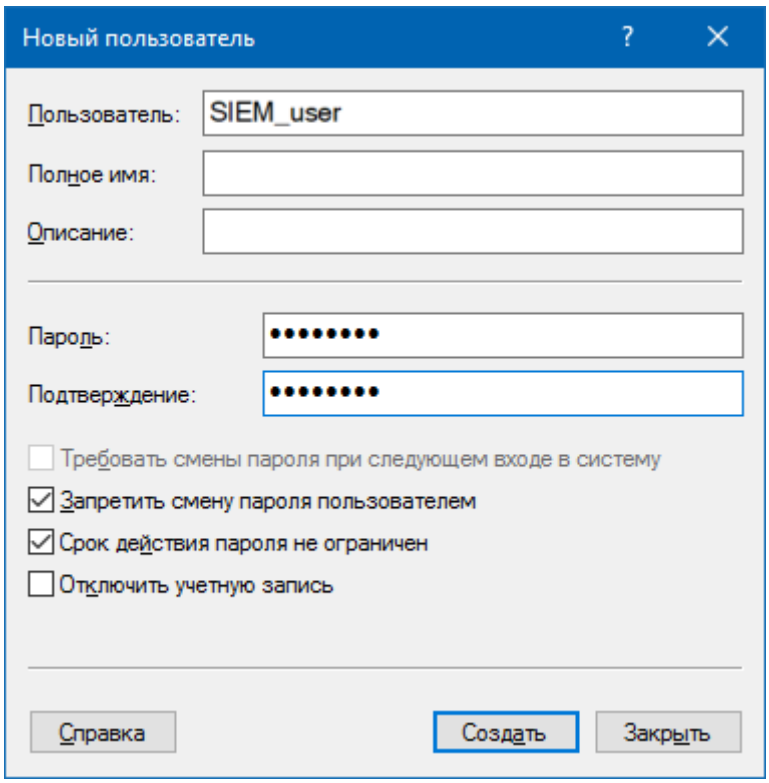

Рисунок 19. Настройка параметров учетной записи

9. Нажмите кнопку **Создать**.

Учетная запись создана.

15.1.3. Добавление учетной записи в локальную политику безопасности

► Чтобы добавить учетную запись в локальную политику безопасности:

1. Откройте панель управления Windows.
2. Выберите **Администрирование** → **Локальная политика безопасности**.
3. В левой части окна выберите узел **Параметры безопасности** → **Локальные политики** → **Назначение прав пользователя**.

4. Выберите политику, к которой нужно добавить учетную запись.

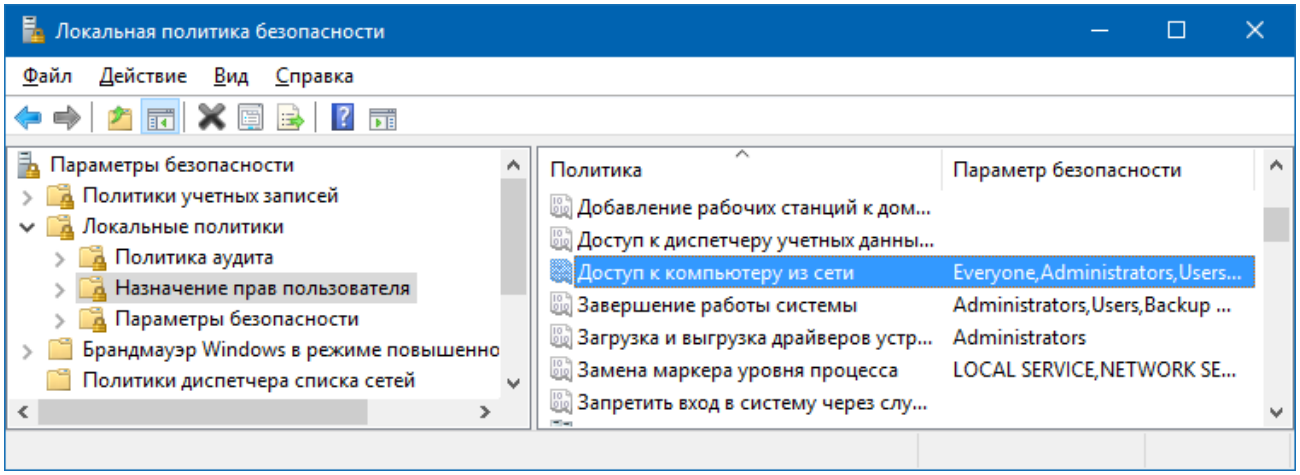

Рисунок 20. Выбор локальной политики безопасности

5. В главном меню выберите **Действие** → **Свойства**.
6. В открывшемся окне нажмите кнопку **Добавить пользователя или группу**.
7. В открывшемся окне нажмите кнопку **Размещение**.
8. В открывшемся окне выберите:
   - если используется локальная учетная запись — имя узла;
   - если используется доменная учетная запись — имя домена.
9. Нажмите кнопку **OK**.
10. В поле **Введите имена выбираемых объектов** введите логин учетной записи и нажмите кнопку **OK**.
11. В окне **Свойства <Имя политики>** нажмите кнопку **OK**.

Учетная запись добавлена в локальную политику безопасности.

15.1.4. Добавление учетной записи в локальную группу пользователей ОС

► Чтобы добавить учетную запись в локальную группу пользователей ОС:

1. Откройте панель управления Windows.
2. Выберите **Администрирование** → **Управление компьютером**.
3. В левой части окна выберите узел **Локальные пользователи и группы** → **Группы**.
4. Выберите группу, в которую нужно добавить учетную запись.

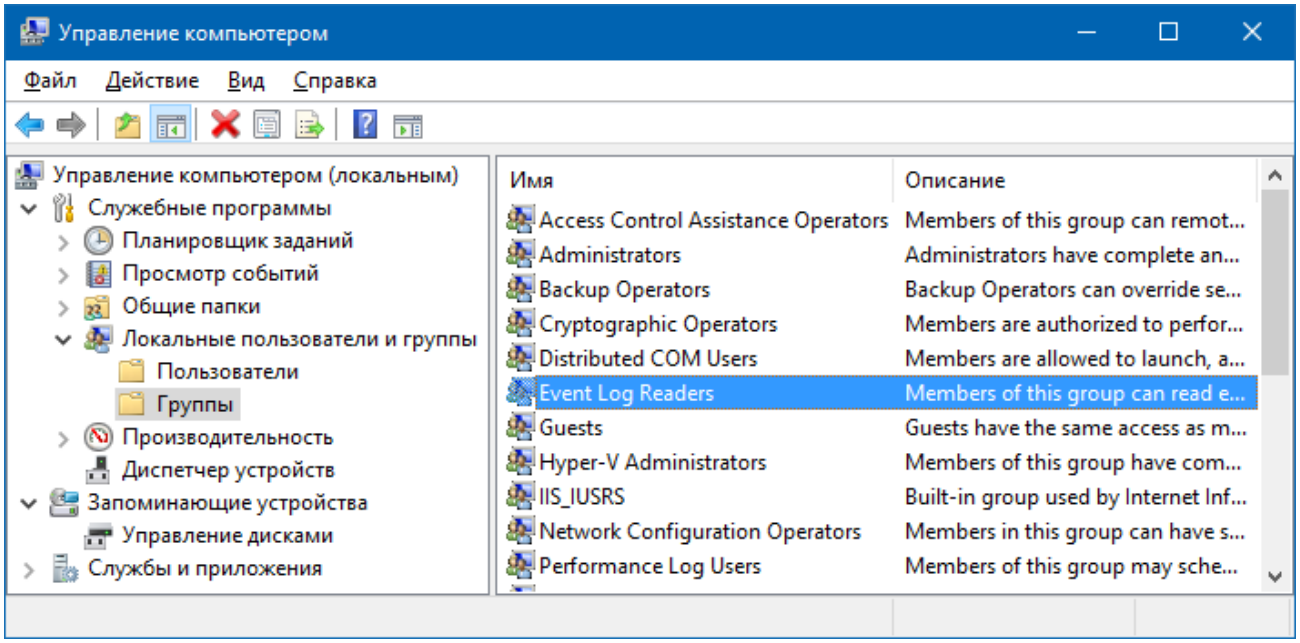

Рисунок 21. Выбор группы пользователей

5. В главном меню выберите **Действие** → **Добавить в группу**.
6. В открывшемся окне нажмите кнопку **Добавить**.
7. В открывшемся окне нажмите кнопку **Размещение**.
8. В открывшемся окне выберите:
   - если используется локальная учетная запись — имя узла;
   - если используется доменная учетная запись — имя домена.
9. Нажмите кнопку **OK**.
10. В поле **Введите имена выбираемых объектов** введите логин учетной записи и нажмите кнопку **OK**.
11. В окне **Свойства <Имя группы>** нажмите кнопку **OK**.

Учетная запись добавлена в группу.

15.2. Стандартные операции в ОС семейства Unix

Раздел содержит инструкции для стандартных операций, выполняемых в ОС семейства Unix.

В этом разделе

15.2.1. Создание учетной записи в ОС семейства Unix

Внимание! Инструкцию нужно выполнять от имени учетной записи root.

► Чтобы создать учетную запись с правом доступа к каталогу с файлами журнала:

1. Создайте учетную запись с неограниченным сроком действия:
   `useradd -m <Логин>`
2. Укажите пароль учетной записи:
   `passwd <Пароль>`
3. Определите группу владения каталога с файлами журнала:
   `ls -ld <Каталог>`

   На экране появятся разрешения каталога, логин владельца и название группы владения.
4. Добавьте учетную запись в группу владения каталога:
   `usermod -G <Группа владения> <Логин>`

Учетная запись создана.

После создания учетной записи в ОС AIX нужно войти в ОС под именем этой учетной записи и сменить пароль.

15.2.2. Определение используемой службы журналирования

► Чтобы определить используемую на источнике службу журналирования,

выполните команду:

- если установлена операционная система ALT Linux:
  `rpm -qa | grep syslog`
- если Astra Linux, Debian или Ubuntu:
  `dpkg --list | grep syslog`
- если CentOS, Oracle Linux или Red Hat Enterprise Linux:
  `rpm -qa *syslog*`
- если SUSE Linux Enterprise Server:
  `zypper search *syslog* --installed-only | grep 'i |'`

  На экране появится название используемой службы.

15.2.3. Перезапуск службы в ОС семейства Unix

► Чтобы перезапустить службу в ОС семейства Unix,

выполните команду:

- если в ОС используется система инициализации SysV:
  `/etc/init.d/<Имя службы> restart`
- если используется BSD-style init:
  `/etc/rc.d/<Имя службы> restart`
- если Upstart:
  `service <Имя службы> restart`
- если systemd:
  `systemctl restart <Имя службы>`

Служба перезапущена.

15.3. Использование доменной учетной записи для доступа к реестру Windows

Внимание! При использовании в IT-инфраструктуре организации межсетевого экрана или других средств для контроля сетевого трафика требуется настроить в них правила, разрешающие трафик в обоих направлениях между узлом MP 10 Collector и узлом актива. Используются системный TCP-порт 135 и динамические TCP-порты 49152—65535.

Для сбора данных из реестра Windows на активах нужно на контроллере домена:

1. Создать доменную группу учетных записей, используемых для сбора данных.
2. Создать доменную учетную запись для доступа MP 10 Collector на активы.
3. Добавить учетную запись в доменную группу.
4. Создать групповую политику учетных записей для сбора данных.
5. Настроить групповую политику для удаленного доступа.

   Примечание. Вы можете не настраивать групповую политику для удаленного доступа, если на контроллере домена и на всех рабочих станциях, к которым применяется групповая политика, в группу Users добавлен пользователь Authenticated Users и в политику безопасности «Доступ к компьютеру из сети» добавлена группа Users или Everyone.
6. Настроить групповую политику для раздела реестра `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg`.
7. Назначить групповую политику активам, с которых нужно собирать данные.

В этом разделе

Настройка групповой политики для удаленного доступа (см. раздел 15.3.5)

Настройка групповой политики для раздела реестра (см. раздел 15.3.6)

Назначение групповой политики (см. раздел 15.3.7)

15.3.1. Создание доменной группы пользователей

► Чтобы создать доменную группу пользователей:

1. Откройте панель управления Windows.
2. Выберите **Администрирование** → **Пользователи и компьютеры Active Directory**.

   Запустится оснастка «Active Directory — пользователи и компьютеры».

   Примечание. Вы можете запустить оснастку «Active Directory — пользователи и компьютеры» выполнив команду `dsa.msc`.
3. В левой части окна выберите объект **Пользователи и компьютеры Active Directory** → **<Имя домена>** → **Users**.
4. В главном меню выберите **Действие** → **Создать** → **Группа**.

   Откроется окно **Новый объект — Группа**.
5. В поле **Имя группы** введите название.

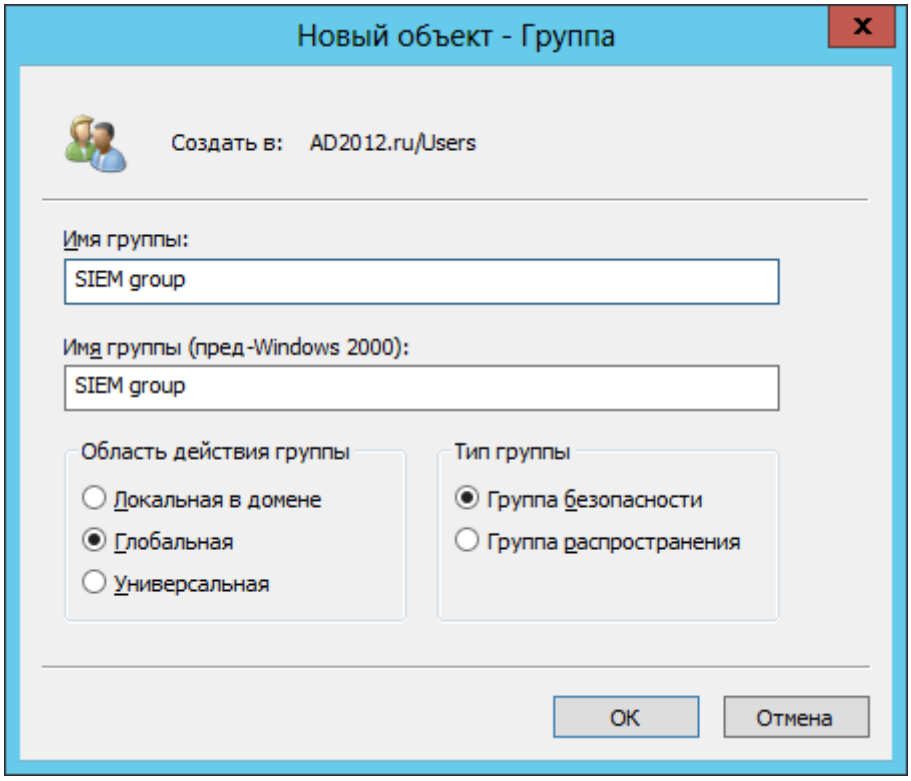

Рисунок 22. Создание доменной группы пользователей

6. Нажмите кнопку **OK**.

Доменная группа пользователей создана.

15.3.2. Создание доменной учетной записи

► Чтобы создать доменную учетную запись:

1. Откройте панель управления Windows.
2. Выберите **Администрирование** → **Пользователи и компьютеры Active Directory**.

   Запустится оснастка «Active Directory — пользователи и компьютеры».

   Примечание. Вы можете запустить оснастку «Active Directory — пользователи и компьютеры» выполнив команду `dsa.msc`.

3. В левой части окна выберите **Пользователи и компьютеры Active Directory** → **<Имя домена>** → **Users**.

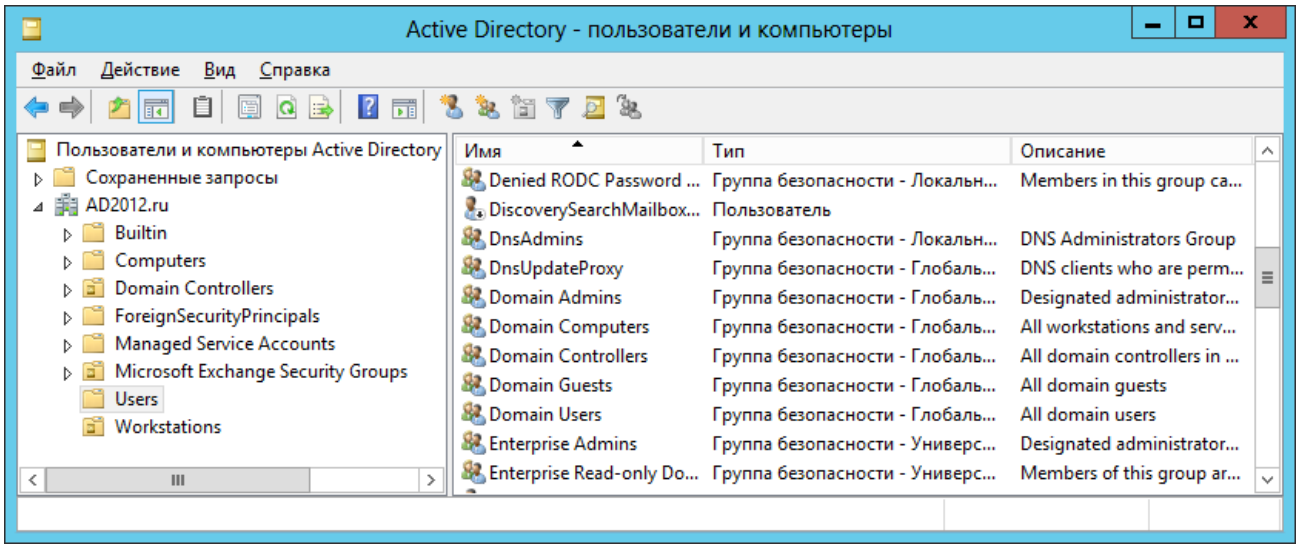

Рисунок 23. Выбор объект **Users**

4. В главном меню выберите **Действие** → **Создать** → **Пользователь**.

   Запустится мастер создания учетной записи пользователя.

5. В поле **Имя** введите имя пользователя.
6. В поле **Имя входа пользователя** введите логин учетной записи.

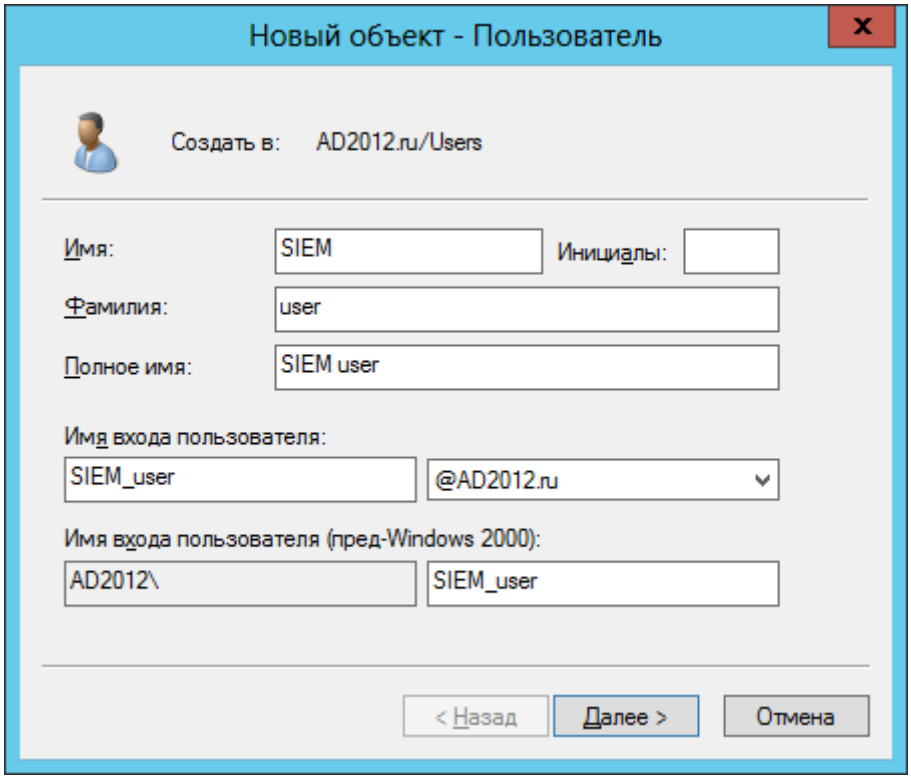

Рисунок 24. Ввод логина учетной записи

7. Нажмите кнопку **Далее**.
8. В поле **Пароль** введите пароль учетной записи и подтвердите его в поле **Подтверждение**.
9. Снимите флажок **Требовать смены пароля при следующем входе в систему**.
10. Установите флажок **Срок действия пароля не ограничен**.

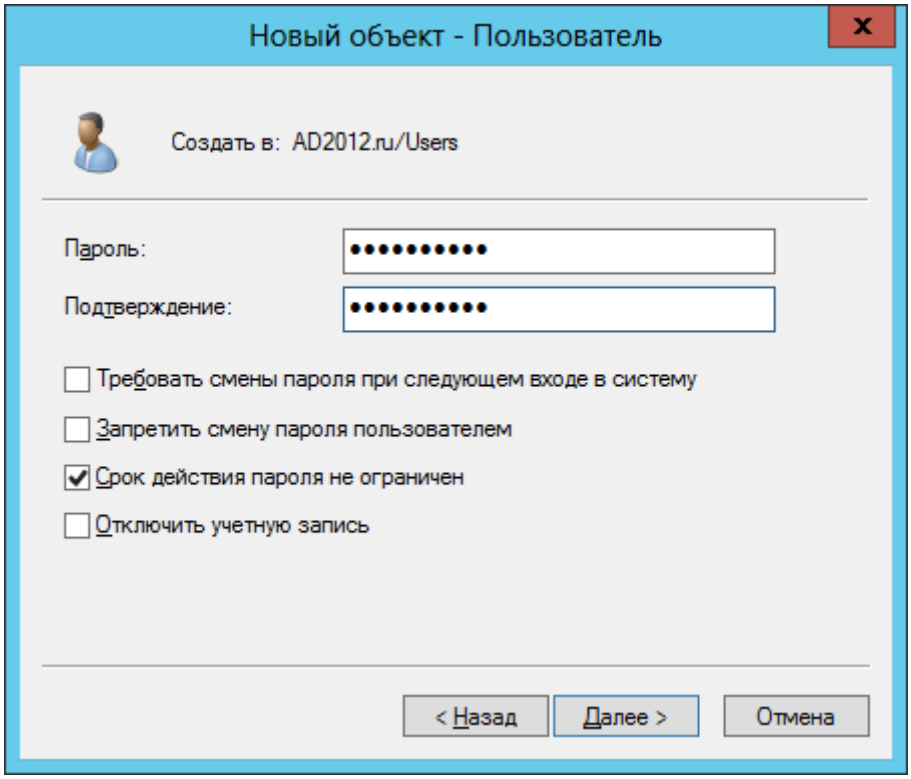

Рисунок 25. Ввод пароля учетной записи

11. Нажмите кнопку **Далее**.
12. Нажмите кнопку **Готово**.

Доменная учетная запись создана.

15.3.3. Добавление учетной записи в доменную группу пользователей

► Чтобы добавить доменную учетную запись в доменную группу пользователей:

1. Откройте панель управления Windows.
2. Выберите **Администрирование** → **Пользователи и компьютеры Active Directory**.

   Запустится оснастка «Active Directory — пользователи и компьютеры».

   Примечание. Вы можете запустить оснастку «Active Directory — пользователи и компьютеры» выполнив команду `dsa.msc`.
3. В левой части окна выберите **Пользователи и компьютеры Active Directory** → **<Имя домена>** → **Users**.
4. В списке выберите учетную запись.
5. В главном меню выберите **Действие** → **Свойства**.

Откроется окно **Свойства: <Логин>**.

6. Выберите вкладку **Член групп**.
7. Нажмите кнопку **Добавить**.

   Откроется окно **Выбор: "Группы"**.

8. В поле **Введите имена выбираемых объектов** введите название группы.

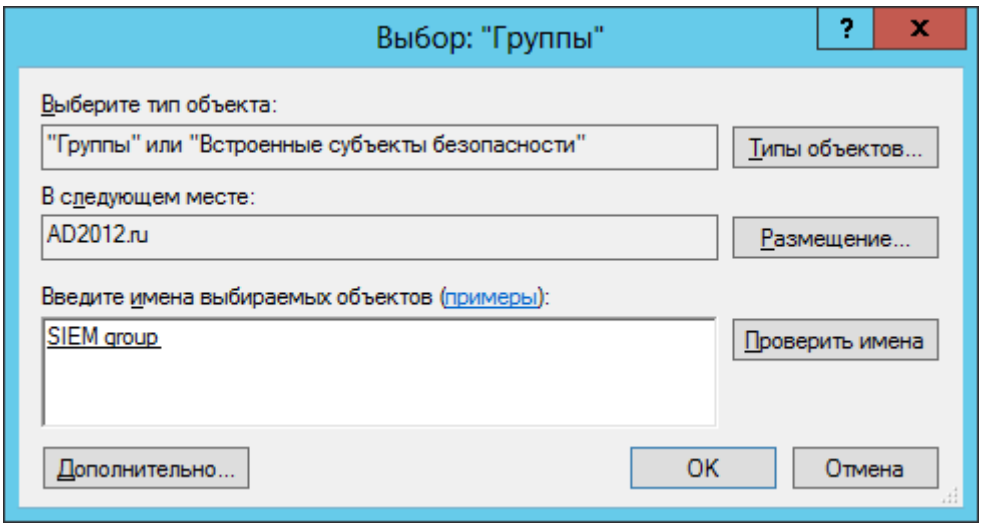

Рисунок 26. Выбор группы пользователей

9. Нажмите кнопку **OK**.
10. В списке **Член групп** выберите добавленную группу и нажмите кнопку **Задать основную группу**.

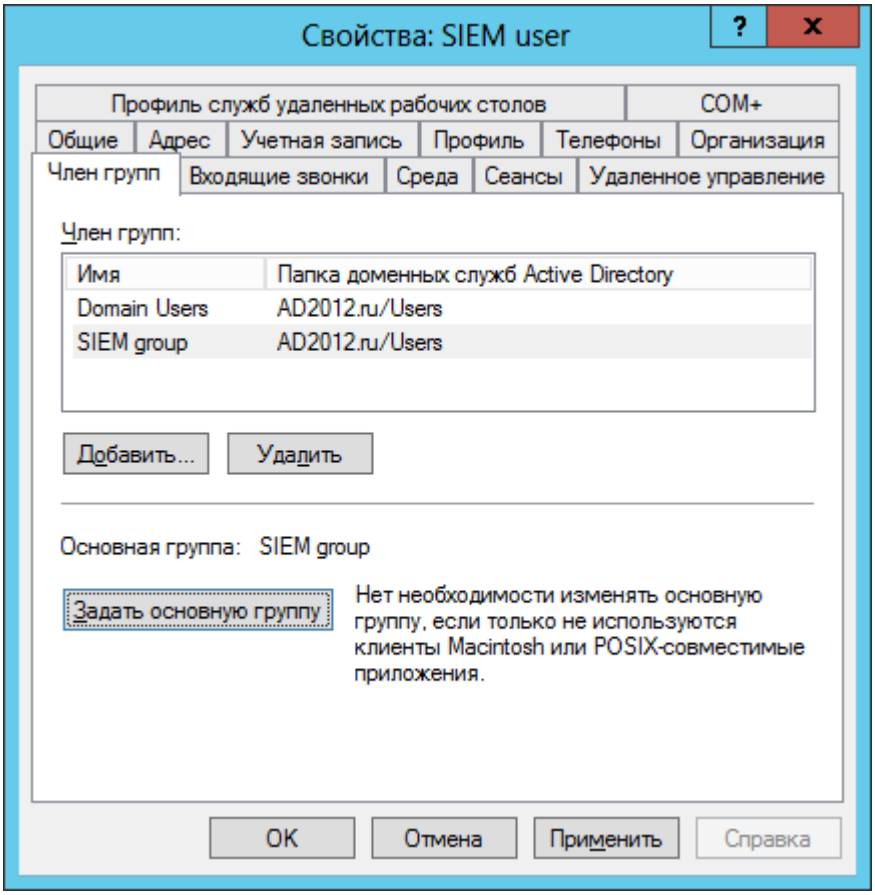

Рисунок 27. Выбор основной группы

11. В списке **Член групп** выберите группу Domain Users и нажмите кнопку **Удалить**.
12. В окне **Свойства: <Логин>** нажмите кнопку **OK**.

Учетная запись добавлена в доменную группу пользователей.

15.3.4. Создание групповой политики

► Чтобы создать групповую политику:

1. Откройте панель управления Windows.
2. Выберите **Администрирование** → **Управление групповой политикой**.

   Запустится консоль управления групповыми политиками.

   Примечание. Вы можете запустить консоль управления групповыми политиками выполнив команду `gpmc.msc`.

3. В левой части окна выберите **Управление групповой политикой** → **Лес: <Имя леса>** → **Домены** → **<Имя домена>** → **Объекты групповой политики**.

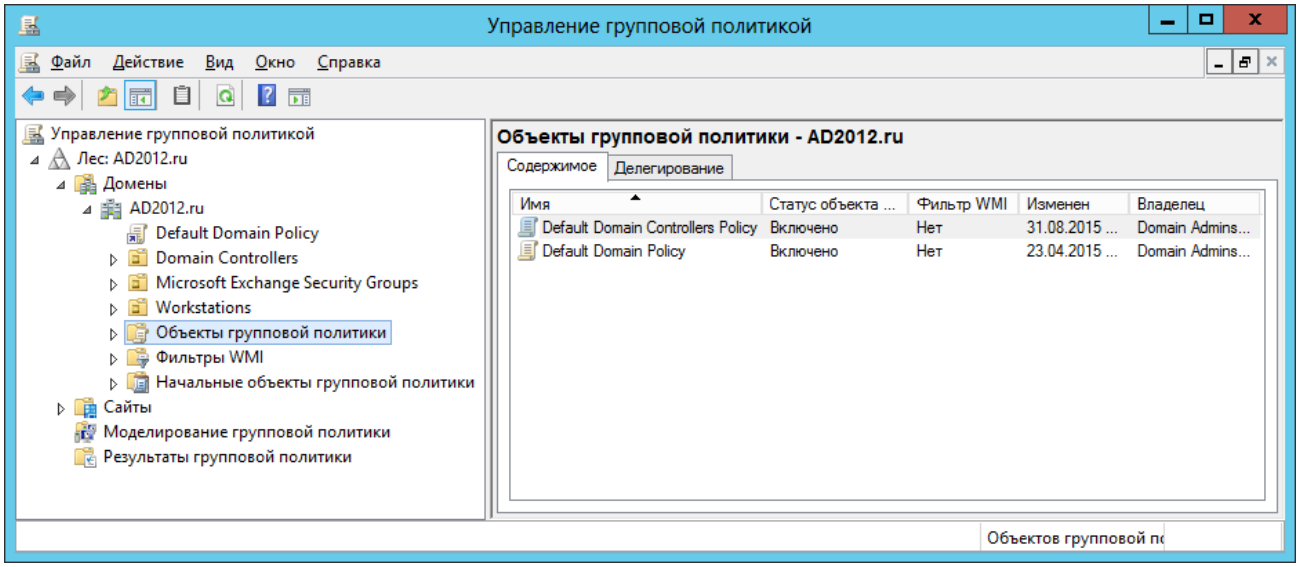

Рисунок 28. Выбор узла **Объекты групповой политики**

4. В главном меню выберите **Действие** → **Создать**.

   Откроется окно **Новый объект групповой политики**.

5. В поле **Имя** введите имя групповой политики.
6. Нажмите кнопку **OK**.

Групповая политика создана.

15.3.5. Настройка групповой политики для удаленного доступа

Примечание. Вы можете не выполнять инструкцию, если на контроллере домена и на всех рабочих станциях, к которым применяется групповая политика, в группу Users добавлен пользователь Authenticated Users и в политику безопасности «Доступ к компьютеру из сети» добавлена группа Users или Everyone.

► Чтобы настроить групповую политику для удаленного доступа:

1. Откройте панель управления Windows.
2. Выберите **Администрирование** → **Управление групповой политикой**.

   Запустится консоль управления групповыми политиками.

   Примечание. Вы можете запустить консоль управления групповыми политиками выполнив команду `gpmc.msc`.

3. В левой части окна выберите **Управление групповой политикой** → **Лес: <Имя леса>** → **Домены** → **<Имя домена>** → **Объекты групповой политики** → **<Имя групповой политики>**.

4. В главном меню выберите **Действие** → **Изменить**.

   Откроется окно **Редактор управления групповыми политиками**.

5. В левой части окна выберите **Политика <Имя групповой политики>** → **Конфигурация компьютера** → **Политики** → **Конфигурация Windows** → **Параметры безопасности** → **Локальные политики** → **Назначение прав пользователя**.

6. В списке выберите политику **Доступ к компьютеру из сети**.

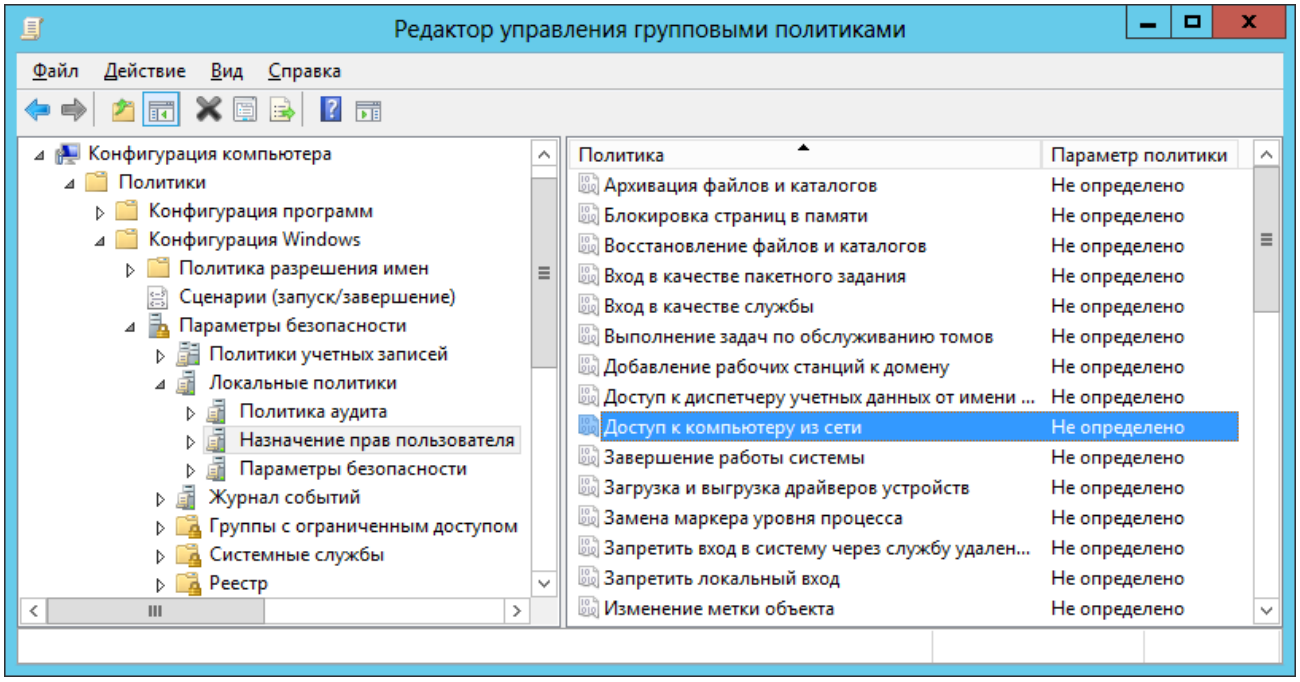

Рисунок 29. Выбор политики **Доступ к компьютеру из сети**

7. В главном меню выберите **Действие** → **Свойства**.

   Откроется окно **Свойства: Доступ к компьютеру из сети**.

8. Установите флажок **Определить следующие параметры политики**.

9. Нажмите кнопку **Добавить пользователя или группу**.

   Откроется окно **Добавление пользователя или группы**.

10. Нажмите кнопку **Обзор**.

    Откроется окно **Выбор: "Пользователи", "Учетные записи служб" или "Группы"**.

11. В поле **Введите имена выбираемых объектов** введите название группы.

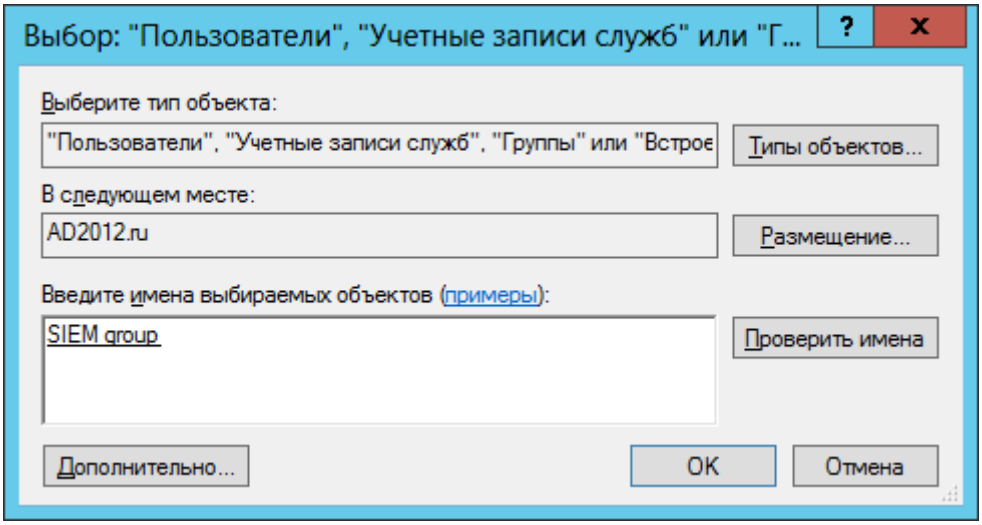

Рисунок 30. Выбор группы пользователей

12. Нажмите кнопку **OK**.
13. В окне **Добавление пользователя или группы** нажмите кнопку **OK**.
14. В окне **Свойства: Доступ к компьютеру из сети** нажмите кнопку **OK**.

Групповая политика для удаленного доступа настроена.

15.3.6. Настройка групповой политики для раздела реестра

► Чтобы настроить групповую политику для раздела реестра:

1. Откройте панель управления Windows.
2. Выберите **Администрирование** → **Управление групповой политикой**.

   Запустится консоль управления групповыми политиками.

   Примечание. Вы можете запустить консоль управления групповыми политиками выполнив команду `gpmc.msc`.

3. В левой части окна выберите **Управление групповой политикой** → **Лес: <Имя леса>** → **Домены** → **<Имя домена>** → **Объекты групповой политики** → **<Имя групповой политики>**.
4. В главном меню выберите **Действие** → **Изменить**.

   Откроется окно **Редактор управления групповыми политиками**.

5. В левой части окна выберите **Политика <Имя групповой политики>** → **Конфигурация компьютера** → **Политики** → **Конфигурация Windows** → **Параметры безопасности** → **Реестр**.

6. В главном меню выберите **Действие** → **Добавить раздел**.

   Откроется окно **Выбор раздела реестра**.

7. В поле **Реестр** выберите **MACHINE** → **SYSTEM** → **CurrentControlSet** → **Control** → **SecurePipeServers** → **winreg**.

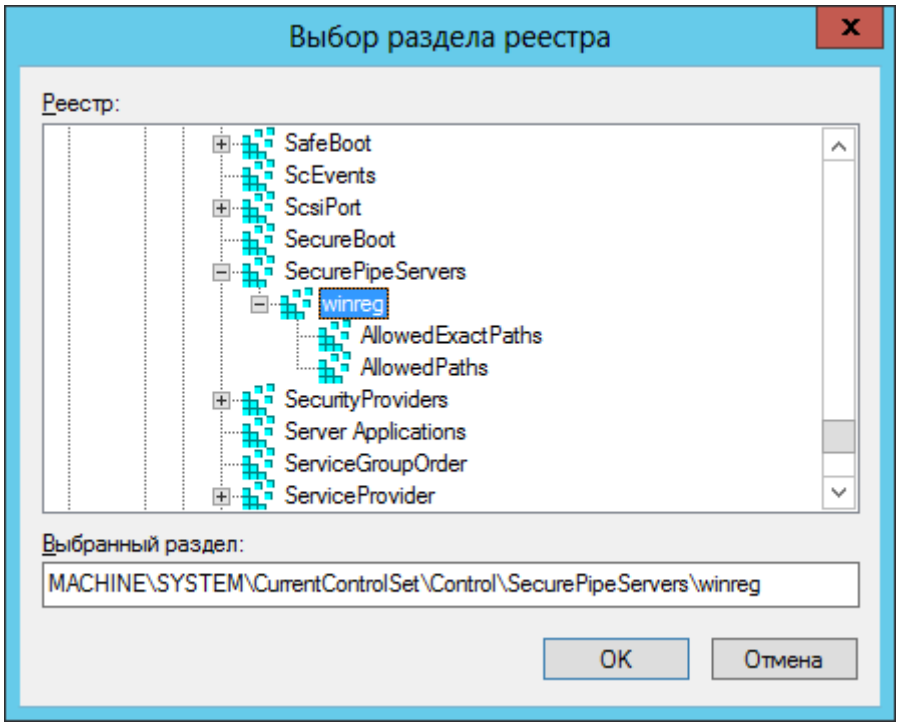

Рисунок 31. Выбор раздела реестра

8. Нажмите кнопку **OK**.

   Откроется окно **Безопасность базы данных для MACHINE**.

9. Нажмите кнопку **Дополнительно**.

   Откроется окно **Дополнительные параметры безопасности для "MACHINE"**.

10. Нажмите кнопку **Добавить**.

    Откроется окно **Элемент разрешения для "MACHINE"**.

11. По ссылке **Выберите субъект** откройте окно **Выбор: "Пользователи", "Учетные записи служб" или "Группы"**.

12. В поле **Введите имена выбираемых объектов** введите название группы.

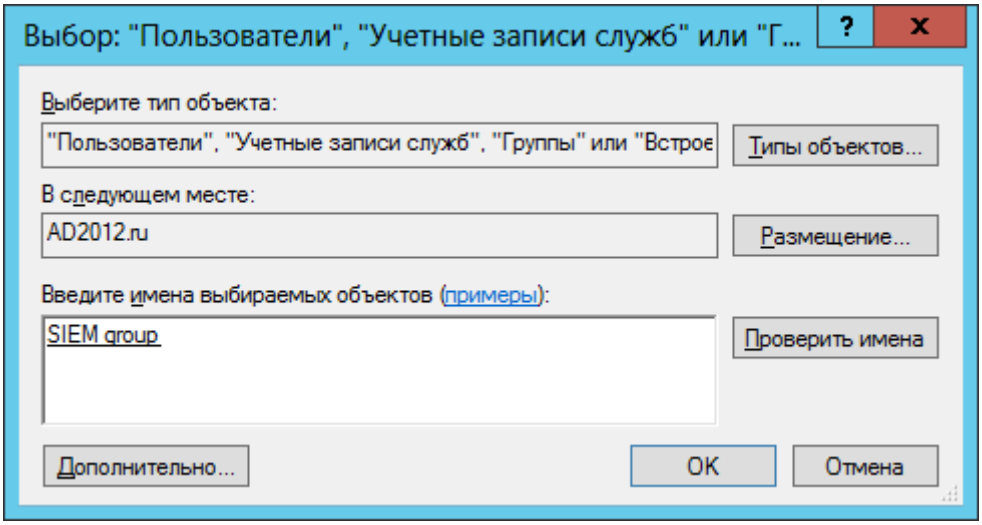

Рисунок 32. Выбор группы пользователей

13. Нажмите кнопку **OK**.
14. В раскрывающемся списке **Применяется к** выберите **Этот объект**.
15. Нажмите ссылку **Отображение дополнительных разрешений**.
16. Установите флажки **Уведомление**, **Чтение разрешений**.

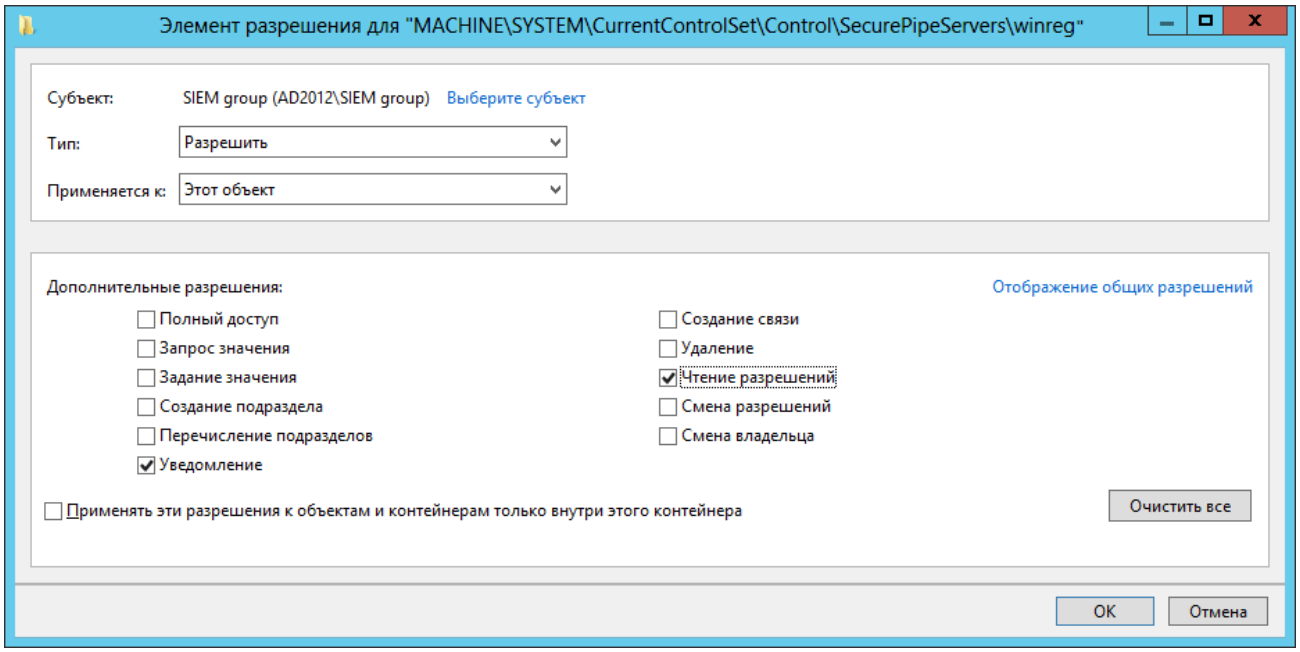

Рисунок 33. Настройка разрешений на раздел реестра

17. Нажмите кнопку **OK**.
18. В окне **Дополнительные параметры безопасности для "MACHINE"** нажмите кнопку **OK**.

19. В окне **Безопасность базы данных для MACHINE** нажмите кнопку **OK**.
20. В окне **Добавление объекта** нажмите кнопку **OK**.

Групповая политика для раздела реестра настроена.

15.3.7. Назначение групповой политики

► Чтобы назначить групповую политику:

1. Откройте панель управления Windows.
2. Выберите **Администрирование** → **Управление групповой политикой**.

   Запустится консоль управления групповыми политиками.

   Примечание. Вы можете запустить консоль управления групповыми политиками выполнив команду `gpmc.msc`.

3. В левой части окна консоли управления выберите объект, соответствующий узлу, с которого нужно собирать события.
4. В главном меню выберите **Действие** → **Связать существующий объект групповой политики**.

   Откроется окно **Выбор объекта групповой политики**.

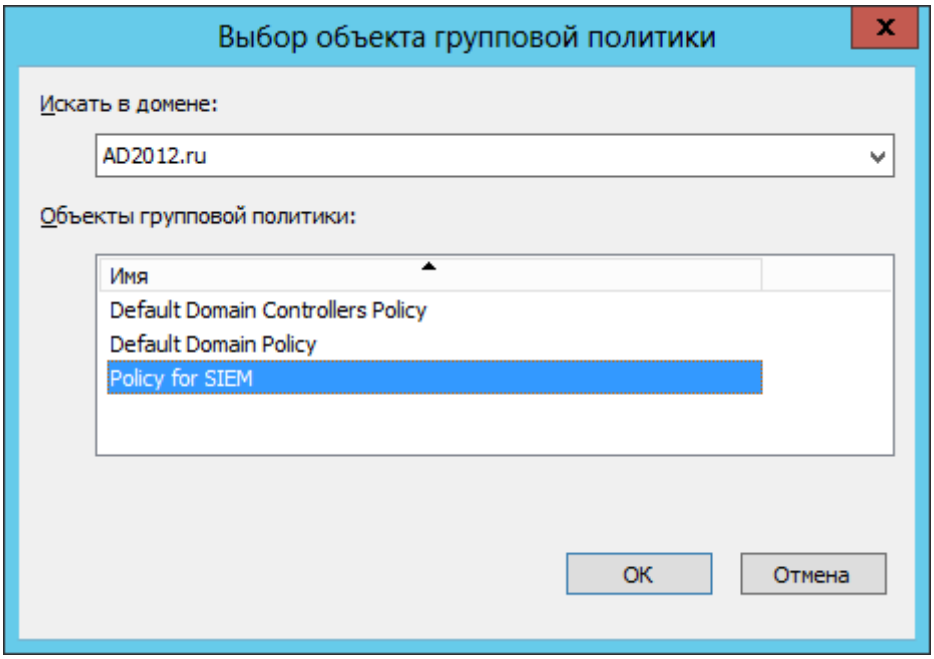

Рисунок 34. Выбор групповой политики

5. В списке **Объекты групповой политики** выберите созданную для объекта политику.
6. Нажмите кнопку **OK**.

Групповая политика назначена.

15.4. Настройка доступа в СУБД Microsoft SQL Server

Внимание! При использовании на узле источника межсетевого экрана требуется настроить в нем правила, разрешающие внешние подключения к используемым портам TCP/IP. Для подключения к СУБД Microsoft SQL Server по умолчанию используется порт 1433.

Для настройки доступа MP 10 Collector к БД под управлением СУБД Microsoft SQL Server нужно:

1. Создать локальную (см. раздел 15.4.1) или доменную (см. раздел 15.4.3) учетную запись пользователя Windows.

   Примечание. Данные этой учетной записи нужно указать при добавлении учетной записи в MaxPatrol VM.

2. Настроить локальную (см. раздел 15.4.2) или групповую (см. раздел 15.4.4) политику безопасности для удаленного доступа учетной записи.
3. На основе учетной записи пользователя Windows создать учетную запись СУБД с правом на чтение БД источника (см. раздел 15.4.5).
4. Настроить порты TCP/IP для подключения к СУБД (см. раздел 15.4.6).
5. Настроить автоматический запуск SQL Server Browser (см. раздел 15.4.7).

При использовании на активе отказоустойчивого кластера Microsoft SQL Server в качестве IP-адреса актива с СУБД автоматически определяется IP-адрес прослушивателя кластера. В задаче на сбор данных из БД вместо этого адреса необходимо ввести IP-адрес одного из узлов с Microsoft SQL Server.

В этом разделе

15.4.1. Создание учетной записи ОС

► Чтобы создать учетную запись пользователя ОС:

1. Откройте панель управления Windows.
2. Выберите **Администрирование** → **Управление компьютером**.
3. В левой части окна выберите узел **Управление компьютером** → **Локальные пользователи и группы** → **Пользователи**.

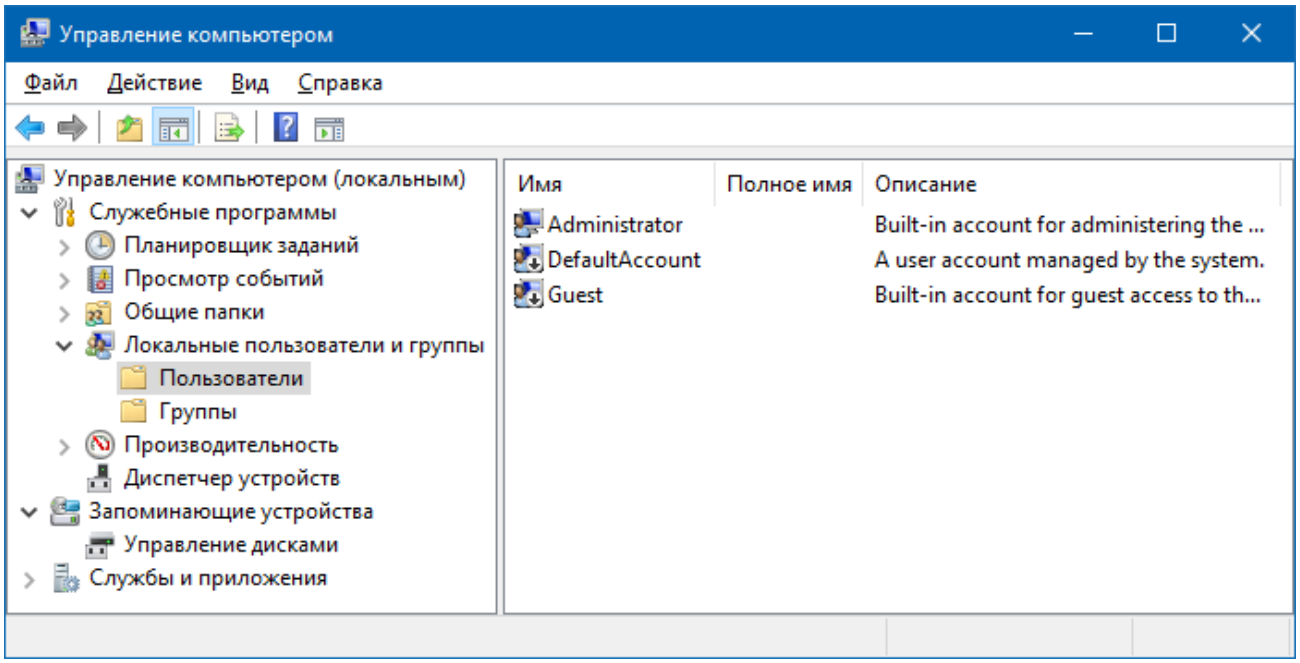

Рисунок 35. Выбор узла **Пользователи**

4. В главном меню выберите **Действие** → **Новый пользователь**.
5. В открывшемся окне в поле **Пользователь** введите логин учетной записи.
6. Установите флажок **Запретить смену пароля пользователем**.
7. Установите флажок **Срок действия пароля не ограничен**.
8. В поле **Пароль** введите пароль и подтвердите его в поле **Подтверждение**.

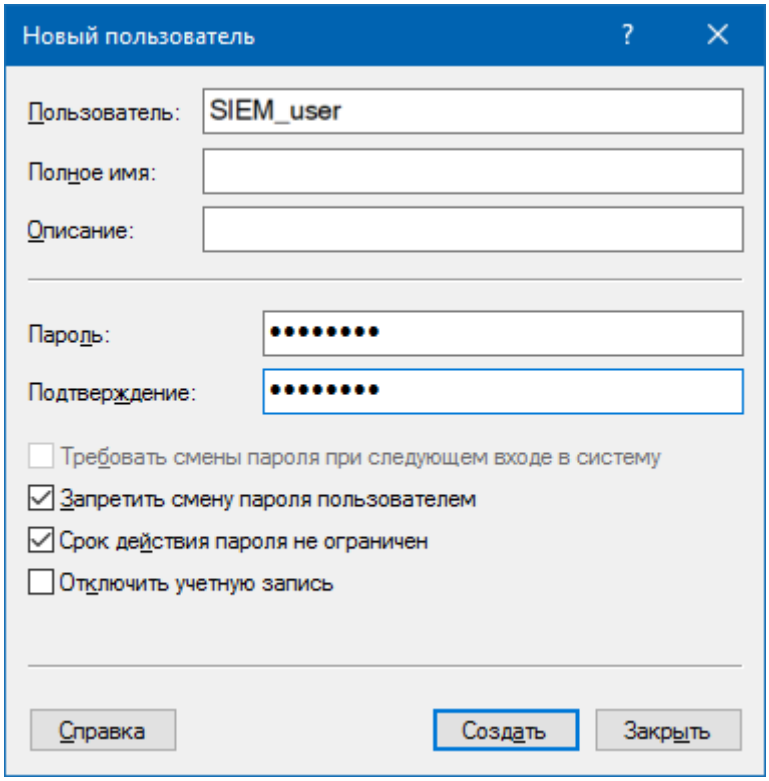

Рисунок 36. Настройка параметров учетной записи

9. Нажмите кнопку **Создать**.

Учетная запись создана.

15.4.2. Настройка локальной политики безопасности для удаленного доступа

► Чтобы настроить локальную политику безопасности для удаленного доступа учетной записи:

1. Откройте панель управления Windows.
2. Выберите **Администрирование** → **Локальная политика безопасности**.
3. В левой части окна выберите узел **Параметры безопасности** → **Локальные политики** → **Назначение прав пользователя**.
4. Выберите политику **Доступ к компьютеру из сети**.

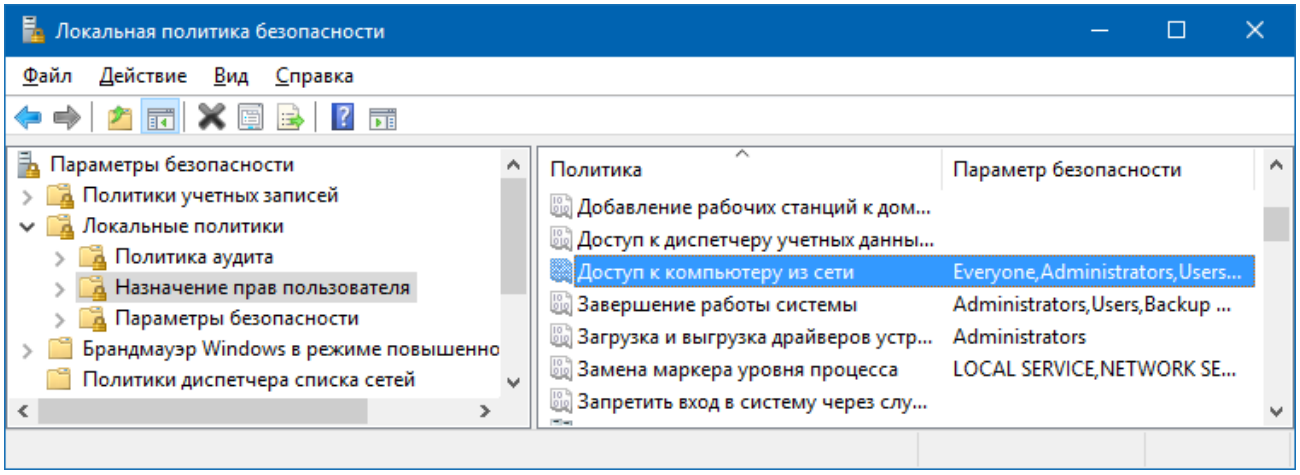

Рисунок 37. Выбор локальной политики безопасности

5. В главном меню выберите **Действие** → **Свойства**.
6. В открывшемся окне нажмите кнопку **Добавить пользователя или группу**.
7. В открывшемся окне нажмите кнопку **Размещение**.
8. В открывшемся окне выберите:
   - если используется локальная учетная запись — имя узла;
   - если используется доменная учетная запись — имя домена.
9. Нажмите кнопку **OK**.
10. В поле **Введите имена выбираемых объектов** введите имя учетной записи и нажмите кнопку **Проверить имена**.

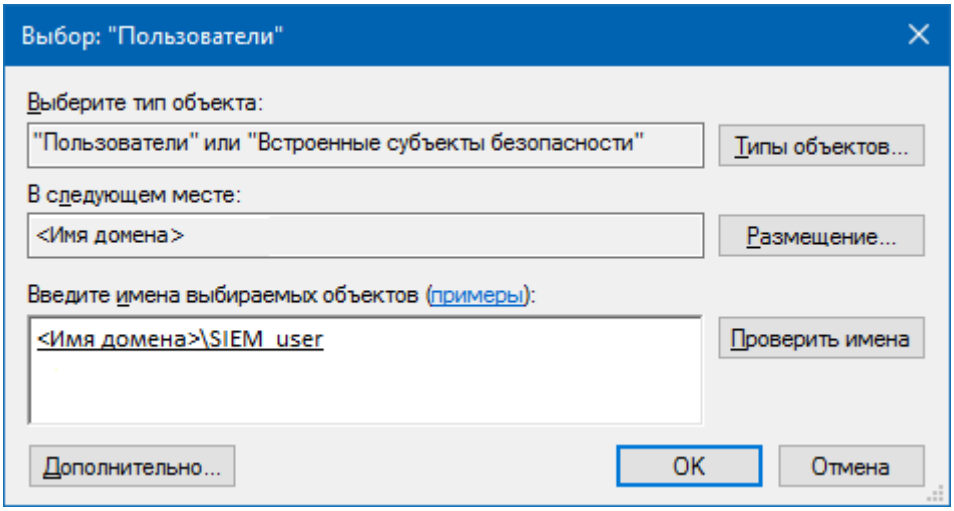

Рисунок 38. Выбор учетной записи

11. Нажмите кнопку **OK**.
12. В окне **Свойства: Доступ к компьютеру из сети** нажмите кнопку **OK**.

Локальная политика безопасности настроена.

15.4.3. Создание доменной учетной записи

► Чтобы создать доменную учетную запись:

1. Откройте панель управления Windows.
2. Выберите **Администрирование** → **Пользователи и компьютеры Active Directory**.

   Запустится оснастка «Active Directory — пользователи и компьютеры».

   Примечание. Вы можете запустить оснастку «Active Directory — пользователи и компьютеры» выполнив команду `dsa.msc`.

3. В левой части окна выберите **Пользователи и компьютеры Active Directory** → **<Имя домена>** → **Users**.

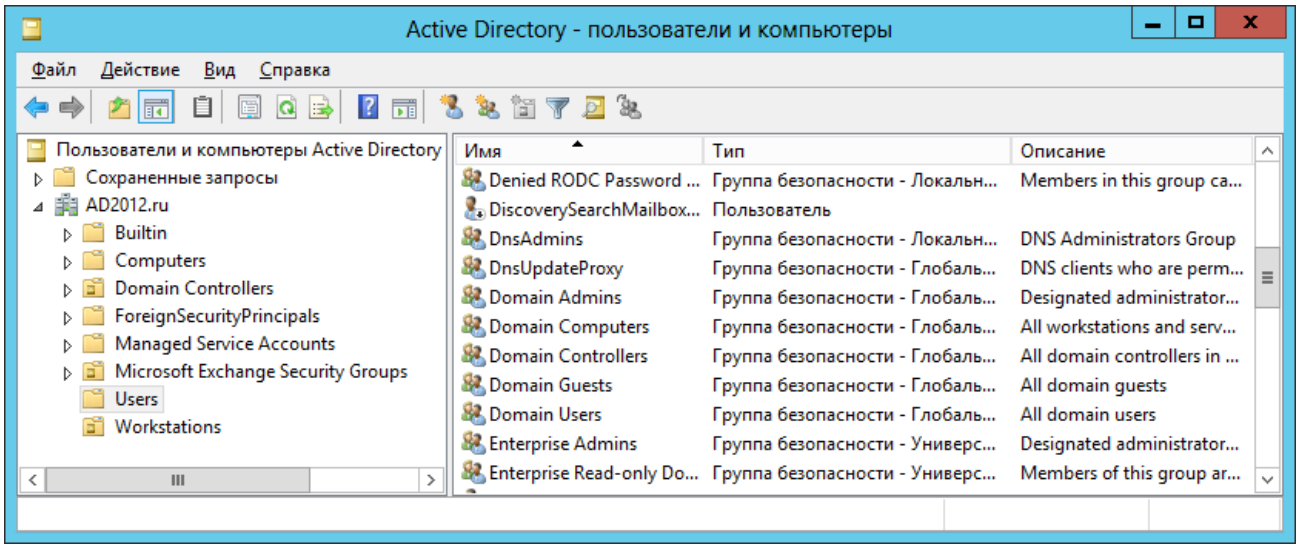

Рисунок 39. Выбор объект **Users**

4. В главном меню выберите **Действие** → **Создать** → **Пользователь**.

   Запустится мастер создания учетной записи пользователя.

5. В поле **Имя** введите имя пользователя.
6. В поле **Имя входа пользователя** введите логин учетной записи.

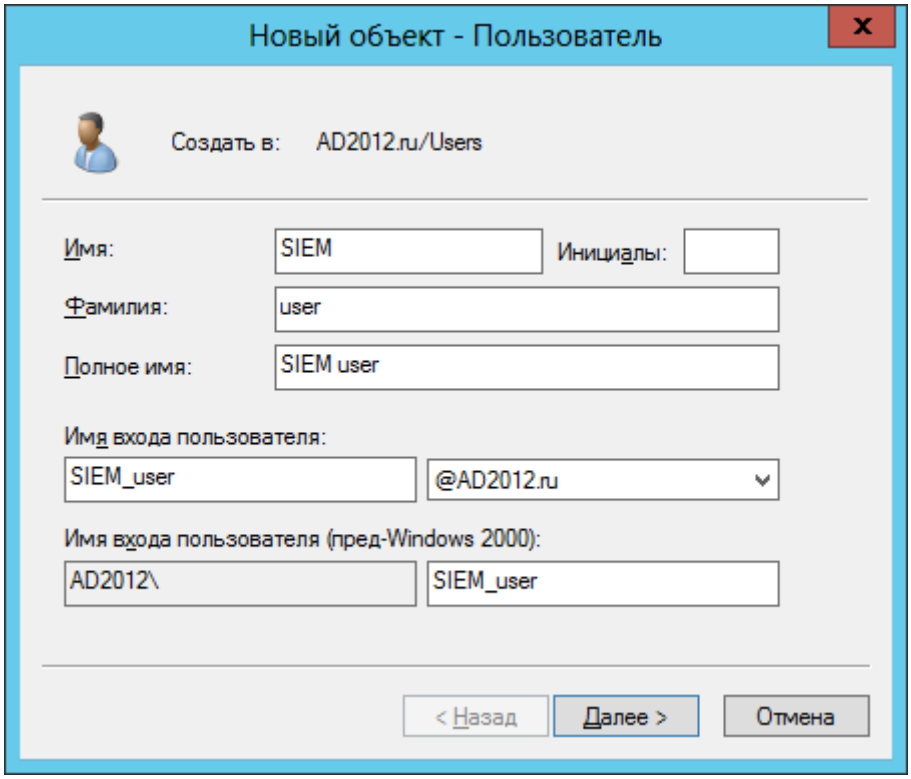

Рисунок 40. Ввод логина учетной записи

7. Нажмите кнопку **Далее**.
8. В поле **Пароль** введите пароль учетной записи и подтвердите его в поле **Подтверждение**.
9. Снимите флажок **Требовать смены пароля при следующем входе в систему**.
10. Установите флажок **Срок действия пароля не ограничен**.

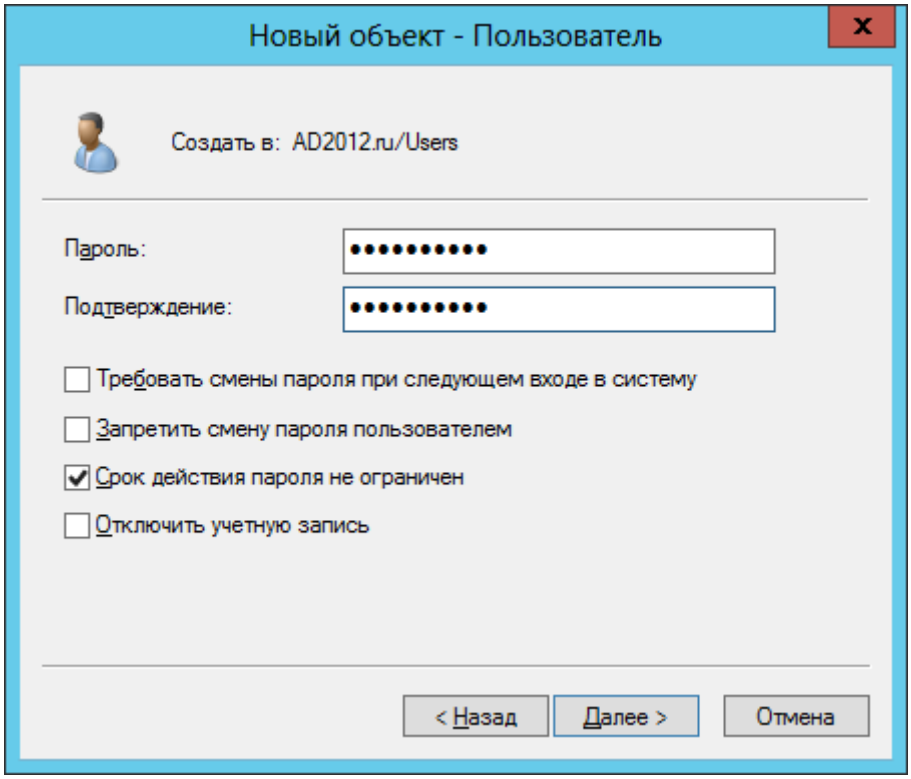

Рисунок 41. Ввод пароля учетной записи

11. Нажмите кнопку **Далее**.
12. Нажмите кнопку **Готово**.

Доменная учетная запись создана.

15.4.4. Настройка групповой политики для удаленного доступа

► Чтобы настроить групповую политику для удаленного доступа учетной записи:

1. Откройте панель управления Windows.
2. Выберите **Администрирование** → **Управление групповой политикой**.

   Запустится консоль управления групповыми политиками.

   Примечание. Вы можете запустить консоль управления групповыми политиками выполнив команду `gpmc.msc`.

3. В левой части окна выберите **Политика <Имя групповой политики>** → **Конфигурация компьютера** → **Политики** → **Конфигурация Windows** → **Параметры безопасности** → **Локальные политики** → **Назначение прав пользователя**.
4. В списке выберите политику **Доступ к компьютеру из сети**.

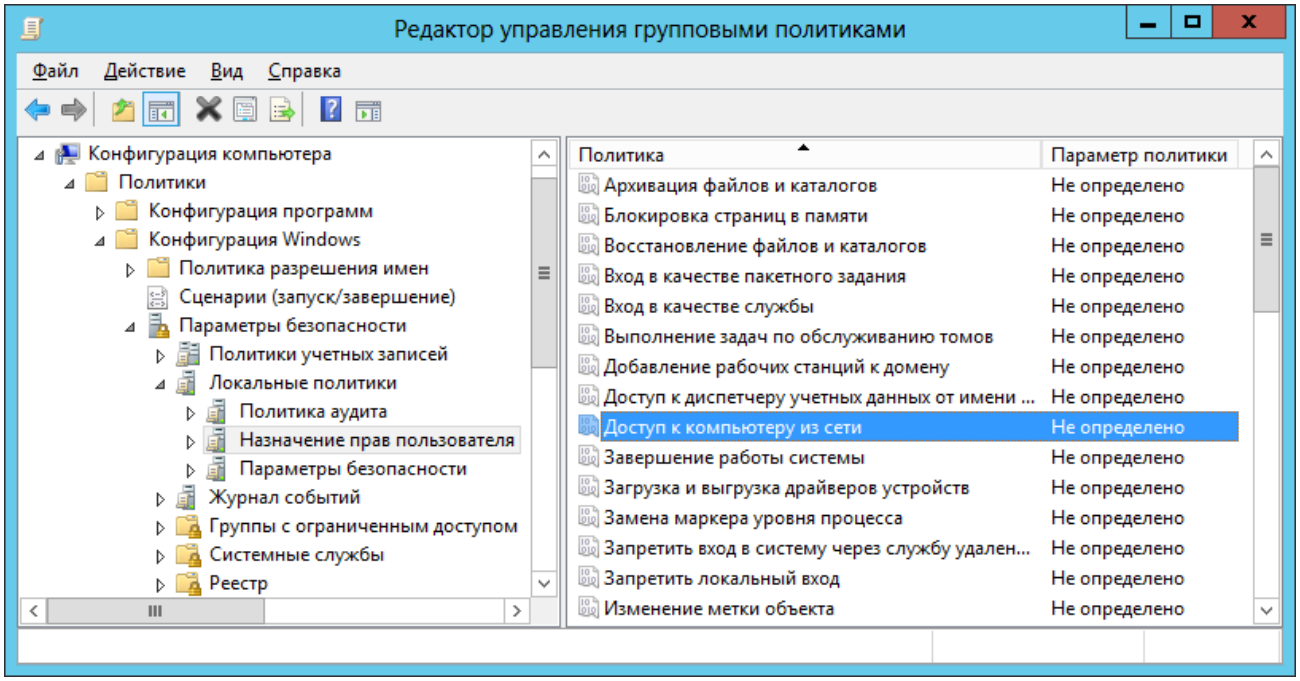

Рисунок 42. Выбор политики **Доступ к компьютеру из сети**

5. В главном меню выберите **Действие** → **Свойства**.

   Откроется окно **Свойства: Доступ к компьютеру из сети**.

6. Установите флажок **Определить следующие параметры политики**.

7. Нажмите кнопку **Добавить пользователя или группу**.

   Откроется окно **Добавление пользователя или группы**.

8. Нажмите кнопку **Обзор**.

   Откроется окно **Выбор: "Пользователи", "Учетные записи служб" или "Группы"**.

9. В поле **Введите имена выбираемых объектов** введите логин учетной записи.

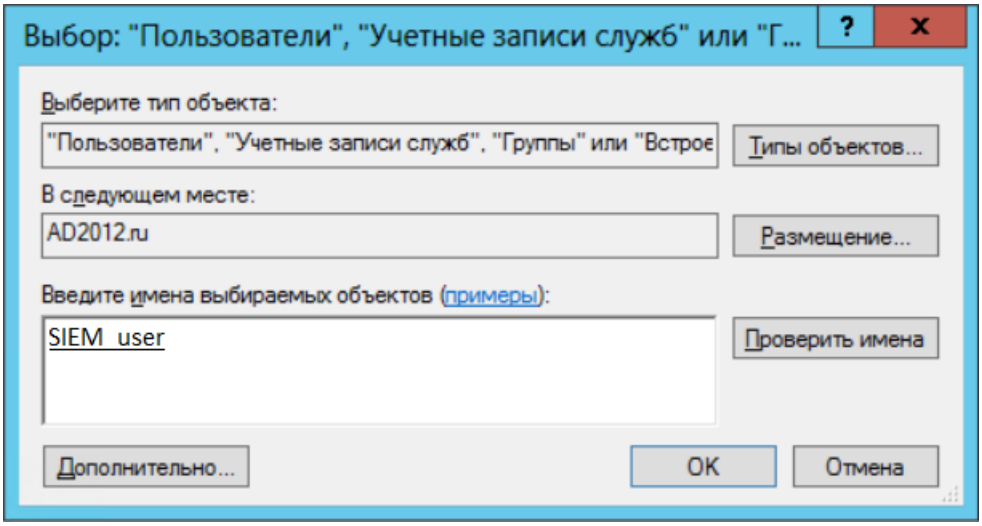

Рисунок 43. Выбор учетной записи

10. Нажмите кнопку **OK**.
11. В окне **Добавление пользователя или группы** нажмите кнопку **OK**.
12. В окне **Свойства: Доступ к компьютеру из сети** нажмите кнопку **OK**.

Групповая политика для удаленного доступа настроена.

15.4.5. Создание учетной записи Microsoft SQL Server

► Чтобы создать учетную запись пользователя СУБД на основе учетной записи Windows:

1. Запустите Microsoft SQL Server Management Studio.

   Откроется окно **Connect to Server**.

Рисунок 44. Подключение к СУБД

2. В раскрывающемся списке **Server name** выберите сервер и экземпляр СУБД.
3. Введите данные учетной записи администратора СУБД и нажмите кнопку **Connect**.

   Откроется окно Microsoft SQL Server Management Studio.
4. В панели **Object Explorer** в контекстном меню узла **<Имя экземпляра СУБД>** → **Security** выберите **New** → **Login**.

   Откроется окно **Login — New**.
5. Выберите **Windows authentication** и нажмите кнопку **Search**.

   Откроется окно **Select User or Group**.

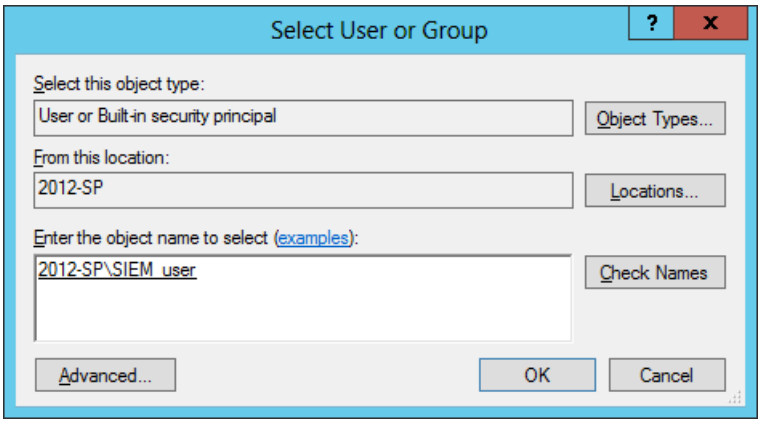

Рисунок 45. Выбор учетной записи

6. Нажмите кнопку **Locations**.
7. В открывшемся окне выберите:
   - если используется локальная учетная запись — имя узла;
   - если используется доменная учетная запись — имя домена.
8. Нажмите кнопку **OK**.
9. В поле **Enter the object name to select** введите логин созданной ранее учетной записи Windows и нажмите кнопку **Check Names**.
10. Нажмите кнопку **OK**.
11. В окне **Login — New** в раскрывающемся списке **Default database** выберите название БД источника.

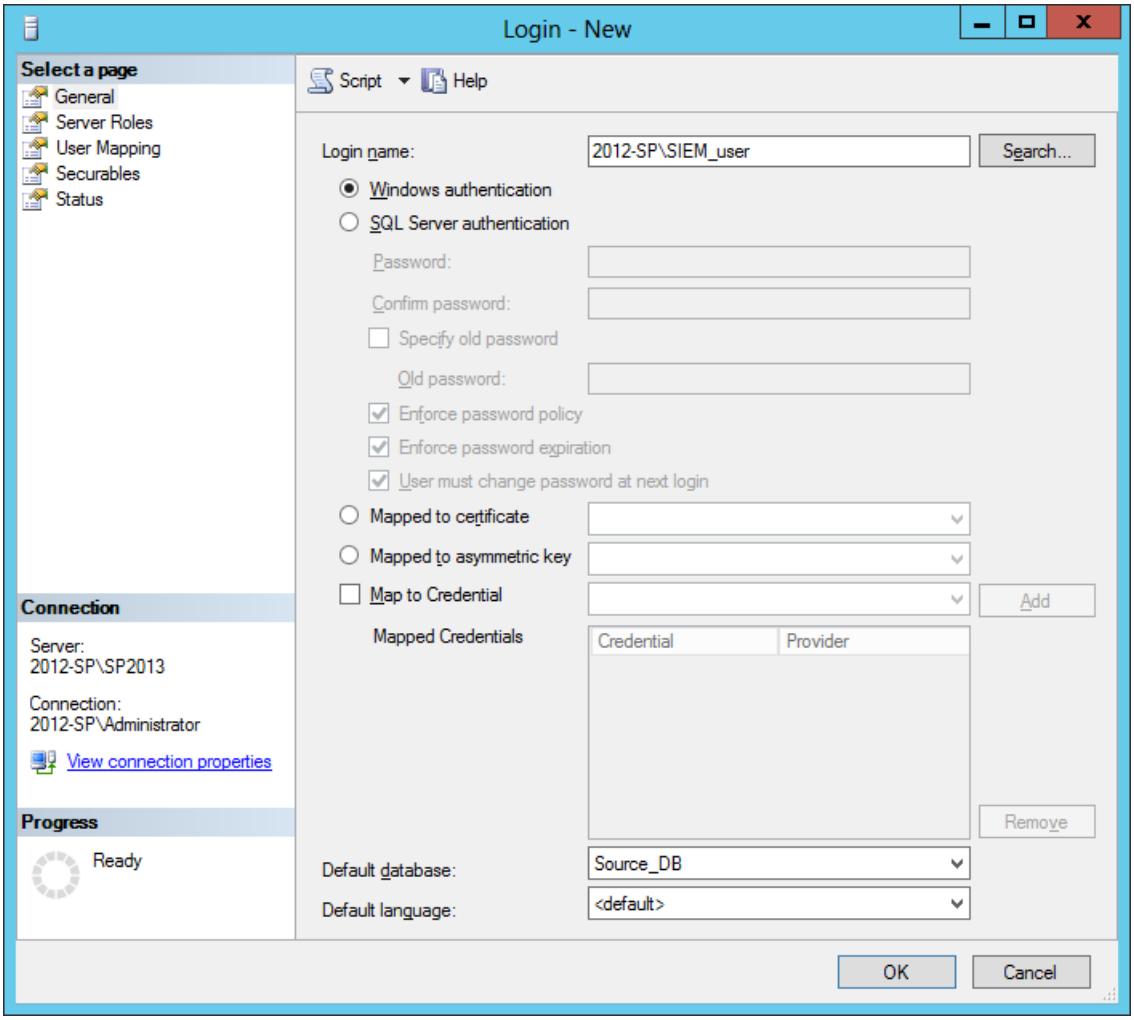

Рисунок 46. Настройка общих параметров учетной записи СУБД

12. В левой части окна выберите **User Mapping**.
13. В списке **User mapped to this login** установите флажок в строке с названием БД источника.
14. В списке **Database role membership** установите флажки для ролей **db_datareader** и **public**.

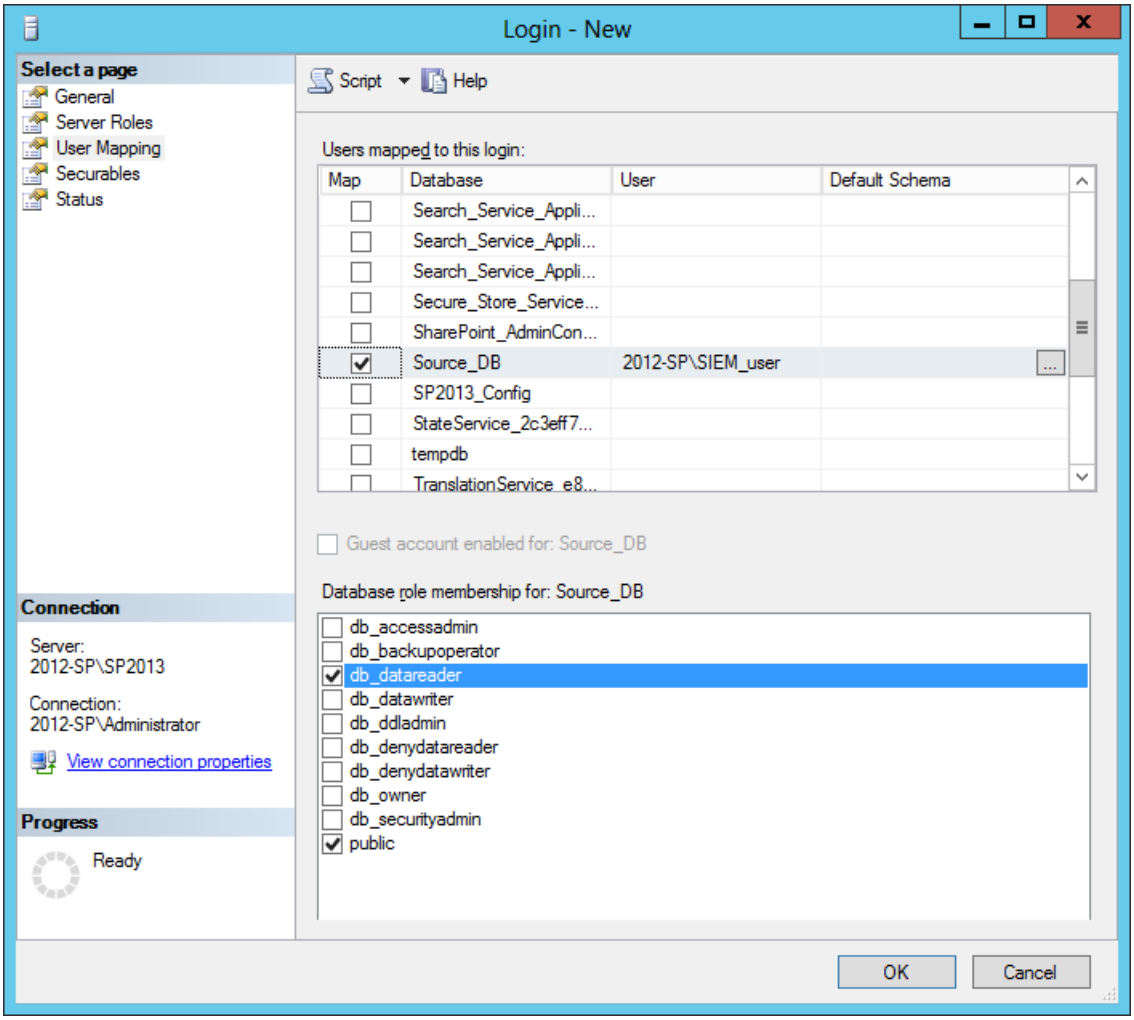

Рисунок 47. Выбор ролей пользователя СУБД

15. Нажмите кнопку **OK**.

Учетная запись пользователя СУБД создана.

15.4.6. Настройка портов TCP/IP

► Чтобы настроить порты TCP/IP для подключения к СУБД:

1. Запустите SQL Server Configuration Manager.
2. В левой части открывшегося окна выберите узел **SQL Server Configuration Manager (Local)** → **SQL Server Network Configuration** → **Protocols for <Имя экземпляра СУБД>**.
3. В контекстном меню протоколов передачи данных TCP/IP выберите пункт **Enable**.

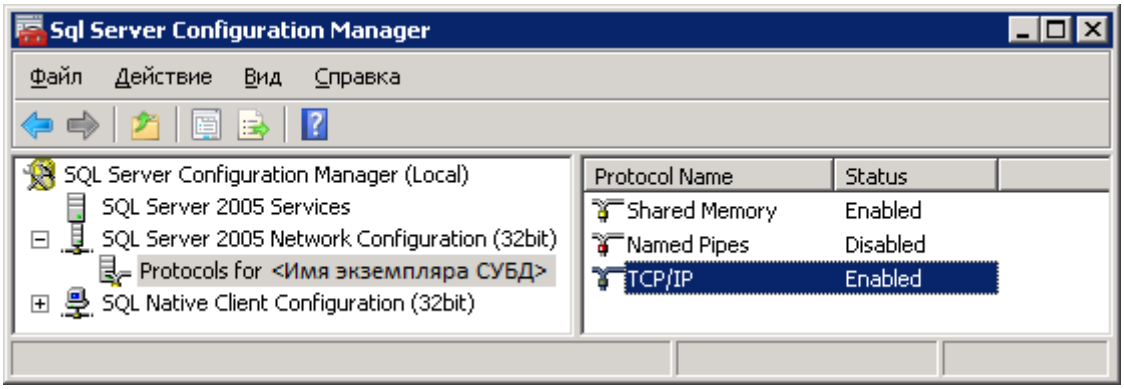

Рисунок 48. Включение протокола TCP/IP

4. В контекстном меню протоколов передачи данных TCP/IP выберите пункт **Свойства**.
5. В открывшемся окне **Свойства: TCP/IP** выберите вкладку **IP Addresses**.

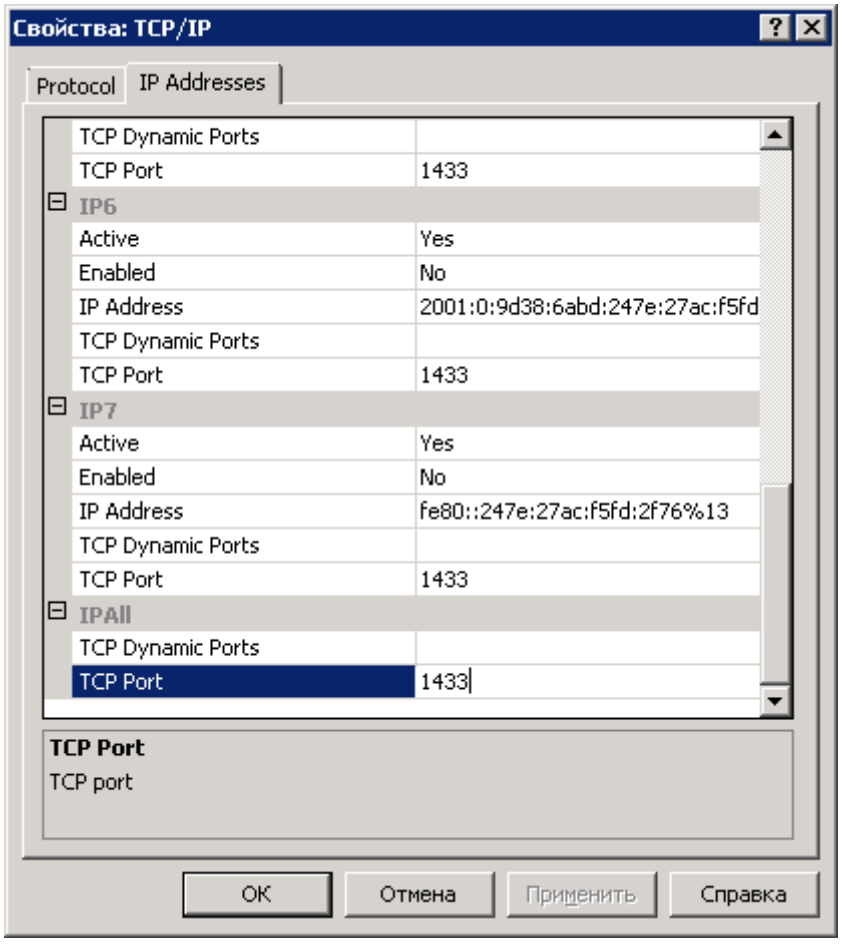

Рисунок 49. Ввод номера порта

6. Укажите порты для подключения к СУБД:

   Примечание. По умолчанию для доступа к СУБД используется TCP-порт **1433**.

- Если используется единственный порт, то в поле **TCP Port** секции **IPAll** укажите значение порта по умолчанию **1433**.
- В ином случае в полях **TCP Port** секции **IPAll** и секциях всех активных сетевых интерфейсов (**IP1**, **IP2**, ...) укажите номер любого свободного порта больше **1024**.

7. Нажмите кнопку **OK**.

Порты TCP/IP настроены. При использовании межсетевого экрана требуется настроить в нем правила, разрешающие внешние подключения к используемым портам TCP/IP.

15.4.7. Запуск SQL Server Browser

► Чтобы настроить автоматический запуск службы SQL Server Browser:

1. Запустите SQL Server Configuration Manager.
2. В левой части открывшегося окна выберите узел **SQL Server Configuration Manager (Local)** → **SQL Server Services**.

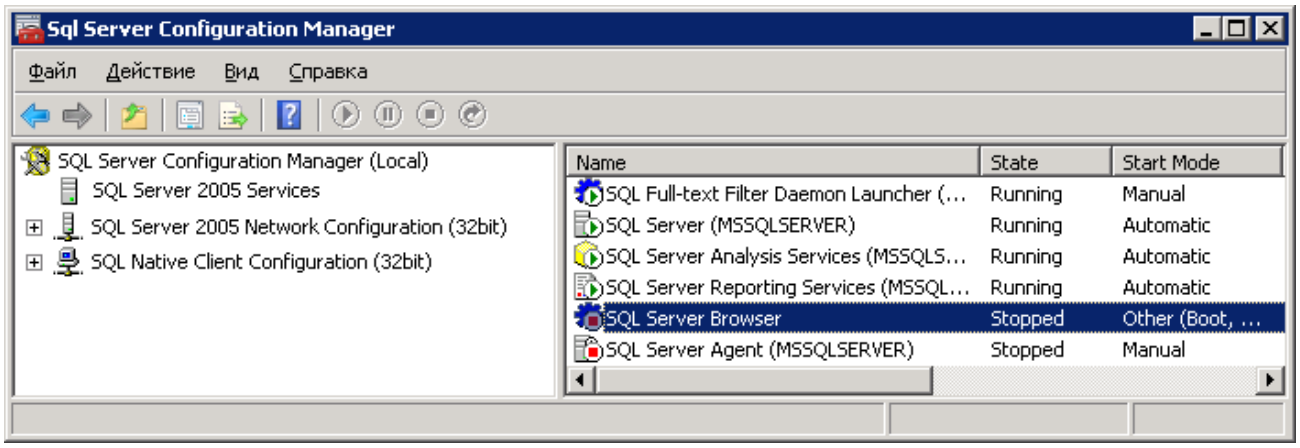

Рисунок 50. Выбор SQL Server Browser

3. В контекстном меню **SQL Server Browser** выберите пункт **Свойства**.
4. В открывшемся окне **Свойства: SQL Server Browser** выберите вкладку **Service**.
5. В раскрывающемся списке **Start Mode** выберите **Automatic**.

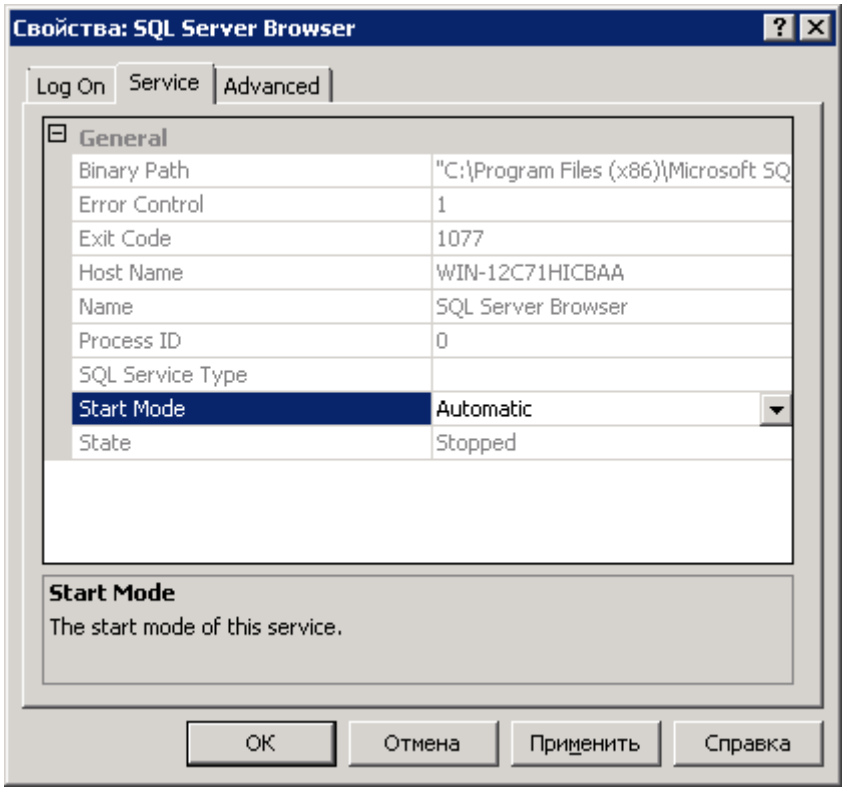

Рисунок 51. Выбор режима запуска SQL Server Browser

6. Выберите вкладку **Log On**.

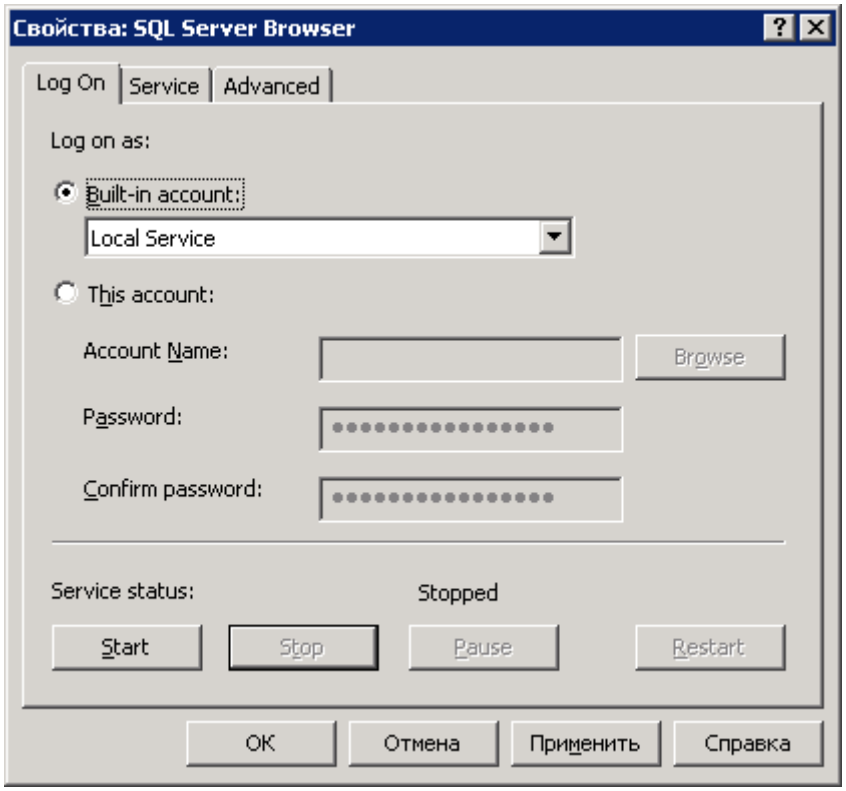

Рисунок 52. Запуск SQL Server Browser

7. Нажмите кнопку **Start** для запуска службы SQL Server Browser.
8. Нажмите кнопку **OK**.
9. Перезапустите СУБД.

Автоматический запуск службы SQL Server Browser настроен.

16. Параметры модулей

Раздел содержит описание параметров работы модулей MP 10 Collector для сканирования активов.

В этом разделе

16.1. Модули для аудита активов

Раздел содержит описание параметров модулей для сбора информации об активах.

> **Внимание!** Если MP 10 Collector установлен на Linux, MaxPatrol VM не сможет проводить аудит активов с Microsoft Windows по протоколу SMBv1, собирать события с профилем CheckpointOpsecLog, собирать данные по протоколам SMB, DCE и RPC в режиме пентеста, а также использовать протокол Kerberos. Производительность работы MP 10 Collector, установленного на Linux, в режиме пентеста на 15—40% ниже, чем на Microsoft Windows.

В этом разделе

16.1.1. Модуль Audit

Модуль предназначен для аудита активов методом белого ящика. В параметрах профиля нужно указать учетную запись, которой предоставлены права на выполнение команд для сбора данных об активе (см. приложение). Для модуля созданы стандартные профили:

— Checkpoint Management Server SSH Audit — для аудита систем информационной безопасности Check Point по протоколу SSH.

— Checkpoint OPSEC Audit — для аудита систем информационной безопасности Check Point через API OPSEC.

— Microsoft Active Directory Audit — для аудита ресурсов службы каталогов Microsoft Active Directory по протоколу LDAP.

Внимание! Для просмотра данных аудита, полученных в результате сканирования с профилями Microsoft Active Directory Audit или Windows DC Audit, необходимо создать динамическую группу активов по условию `ActiveDirectory`.

— MSSQL Audit — для аудита СУБД Microsoft SQL Server.

— Oracle Audit — для аудита СУБД Oracle Database.

Примечание. При использовании профиля Oracle Audit для снижения нагрузки на сервер рекомендуется очищать в сканируемой СУБД Oracle Database таблицу SYS.AUD$ (в пространстве SYSTEM) не реже чем раз в три месяца.

— SNMP Network Device Audit — для аудита сетевых устройств по протоколу SNMP.

— SSH Cisco Audit in Enable Mode — для аудита сетевых устройств компании Cisco по протоколу SSH.

Примечание. При проведении аудита с профилем SSH Cisco Audit in Enable Mode для повышения привилегий на активе (до уровня 15) нужно указать учетную запись типа «пароль» для выполнения команды `enable` и перехода в привилегированный режим EXEC.

— SSH Network Device Audit — для аудита сетевых устройств по протоколам SSH.

— Unix Audit — для аудита ОС семейства Unix.

Примечание. При проведении аудита ОС семейства Unix с профилем Unix Audit активы не будут обнаружены и добавлены, если в ОС используется ядро Linux версии 2.6.38 или ниже. Активы также не будут обнаружены и добавлены, если в ОС используется утилита dmidecode версии 2.8 или ниже.

— vSphere Audit — для аудита платформ виртуализации VMware vSphere.

— Web API Audit — для аудита систем через веб-API. Например, систем Check Point, JetBrains TeamCity, JFrog Artifactory и Zabbix.

— Windows Audit — для аудита Windows.

Внимание! Адаптивный контроль аномалий Kaspersky Endpoint Security блокирует возможность сбора данных механизмом WMI (например, в профиле Windows Audit). Для проведения аудита учетную запись, которая используется для доступа в ОС, требуется добавить в исключения правила адаптивного контроля аномалий «Запуск Windows PowerShell с помощью WMI».

— Windows Audit Vulnerabilities Discovery — для сбора данных о приложениях и ОС, необходимых для поиска уязвимостей на узлах с Windows.

— Windows DC Audit — для сбора данных о ресурсах службы каталогов Microsoft Active Directory и аудита Windows.

Примечание. Профиль Windows DC Audit использует протоколы LDAP, WMI и RPC.

— Windows Updates Discovery — для обновления данных о приложениях и ОС, необходимых для поиска уязвимостей на узлах с Windows.

Настраивать параметры модуля вы можете при создании пользовательского профиля на базе стандартного или задачи на сбор данных. Для этого в панели с параметрами профиля в иерархическом списке нужно выбрать секцию параметров и настроить необходимые. Далее приводятся описания параметров в каждой секции.

В этом разделе

16.1.1.1. Сканирование систем — Check Point через OPSEC

Секция содержит следующие параметры для настройки сбора данных с сервера управления системы информационной безопасности Check Point через Check Point Management Interface (CPMI):

— **Учетная запись** — раскрывающийся список для выбора учетной записи типа «сертификат» (в кодировке Base64) для аутентификации клиента на сервере. Используется для типов аутентификации **SSLCA** и **SSLCA_COMP**.

— **Учетная запись CPMI** — раскрывающийся список для выбора учетной записи администратора сервера управления.

— **Имя сервера управления** — поле для вводи SIC-имени сервера в виде `CN=<Имя>,O=<Домен>`.

— **Порт** — поле для ввода номера порта сервера для сбора данных (по умолчанию 18190/TCP).

— **Порт аутентификации CPMI** — дополнительное поле для ввода номера порта сервера для аутентификации через CPMI (по умолчанию 18190/TCP).

— **Тип аутентификации клиента на сервере управления** — дополнительный раскрывающийся список для выбора типа аутентификации клиента на сервере:

- **SSLCA** — клиент предоставляет сертификат, выданный сервером (по умолчанию);
- **SSLCA_COMP** — клиент предоставляет сертификат, выданный сервером (передается в сжатом виде);
- **ASYM_SSLCA** — сертификат клиента не требуется;
- **ASYM_SSLCA_COMP** — сертификат клиента не требуется (сертификат от сервера передается клиенту в сжатом виде);
- **NONE** — аутентификация не требуется.

— **Тайм-аут ответа** — дополнительное поле для ввода максимального времени ответа сервера в секундах (`0` — время не ограничено).

16.1.1.2. Сканирование систем — Microsoft SQL Server

Секция содержит следующие параметры для настройки сбора данных из СУБД Microsoft SQL Server:

— **Использовать аутентификацию Windows** — при включении для аутентификации в СУБД используется учетная запись пользователя Windows.

— **Учетная запись** — раскрывающийся список для выбора учетной записи, которая будет использоваться MP 10 Collector при аутентификации в СУБД.

— **Имя экземпляра СУБД** — поле для ввода имени экземпляра СУБД, к которому выполняется подключение.

— **Имя базы данных** — поле для ввода имени БД.

— **Порт** — дополнительное поле для ввода номера порта подключения к СУБД (по умолчанию 1433/TCP).

— **Кодировка** — дополнительное поле для ввода названия кодировки символов в СУБД.

— **Тайм-аут подключения** — дополнительное поле для ввода максимального времени ожидания ответа на запрос к СУБД.

— **Тайм-аут аутентификации** — дополнительное поле для ввода максимального времени ожидания ответа на запрос об аутентификации в СУБД.

16.1.1.3. Сканирование систем — Oracle Database

Секция содержит следующие параметры для настройки сбора данных из СУБД Oracle Database:

- **Учетная запись** — раскрывающийся список для выбора учетной записи, которая будет использоваться MP 10 Collector при аутентификации в СУБД.
- **Тип имени экземпляра СУБД** — раскрывающийся список для выбора типа имени экземпляра СУБД:
  - **SID** — системный идентификатор экземпляра;
  - **SERVICE_NAME** — псевдоним Transparent Network Substrate.
- **Имя экземпляра СУБД** — поле для ввода имени экземпляра СУБД, к которому выполняется подключение.
- **Порт** — дополнительное поле для ввода номера порта подключения к СУБД (по умолчанию 1521/TCP).
- **Кодировка** — дополнительное поле для ввода названия кодировки символов в СУБД.
- **Тайм-аут подключения** — дополнительное поле для ввода максимального времени ожидания ответа на запрос к СУБД.
- **Тайм-аут аутентификации** — дополнительное поле для ввода максимального времени ожидания ответа на запрос об аутентификации в СУБД.
- **Значение переменной окружения NLS_LANG** — дополнительное поле для ввода значения переменной окружения NLS_LANG (по умолчанию RUSSIAN_CIS.UTF8).

16.1.1.4. Сканирование систем — Oracle MySQL

Секция содержит следующие параметры для настройки сбора данных из СУБД Oracle MySQL:

- **Учетная запись** — раскрывающийся список для выбора учетной записи, которая будет использоваться MP 10 Collector при аутентификации в СУБД.
- **Порт** — дополнительное поле для ввода номера порта подключения к СУБД (по умолчанию 3306/TCP).
- **Кодировка** — дополнительное поле для ввода названия кодировки символов в СУБД.
- **Тайм-аут подключения** — дополнительное поле для ввода максимального времени ожидания ответа на запрос к СУБД.
- **Тайм-аут аутентификации** — дополнительное поле для ввода максимального времени ожидания ответа на запрос об аутентификации в СУБД.

16.1.1.5. Сканирование систем — SAP через RFC

Секция содержит следующие параметры для настройки сбора данных с сервера приложений (или сервера сообщений) системы SAP через интерфейс RFC:

- **Учетная запись** — раскрывающийся список для выбора учетной записи, которая будет использоваться MP 10 Collector при аутентификации на сервере.
- **Номер мандата клиента** — поле для ввода номера мандата клиента SAP.
- **Номер экземпляра сервера приложений** — поле для ввода номера системы SAP.
- **Строка подключения к SAProuter** — поле для ввода строки подключения SAProuter.
- **Использовать сервер сообщений вместо сервера приложений** — при включении для сбора данных используются параметры сервера сообщений.
- **Имя экземпляра** — поле для ввода имени экземпляра при использовании сервера сообщений.
- **Имя логической группы** — поле для ввода имени логической группы системы SAP при использовании сервера сообщений.
- **Папка для отладочных файлов** — дополнительное поле для ввода пути к папке для сохранения отладочных файлов.
- **Максимальное количество записей, считываемых из таблицы** — дополнительное поле для ввода максимального количества записей, считываемых из таблицы.
- **Тайм-аут сбора** — дополнительное поле для ввода максимального времени сбора в секундах.

16.1.1.6. Сканирование систем — VMware vSphere

Секция содержит следующие параметры для настройки сбора данных с VMware vCenter Server:

- **Учетная запись** — раскрывающийся список для выбора учетной записи, которая будет использоваться MP 10 Collector при аутентификации на сервере.
- **Порт** — дополнительное поле для ввода номера порта подключения к серверу (по умолчанию 443).
- **Использовать протокол SSL** — при включении используется протокол SSL.
- **Проверять сертификат SSL** — при включении для аутентификации на сервере используется сертификат SSL.

  Примечание. Для использования сертификата на узле VMware vCenter Server необходимо выпустить сертификат (поле Subject Alternative Name должно содержать IP-адрес) и с помощью утилиты vSphere Certificate Manager добавить его в VMware Endpoint Certificate Store; на узле MP 10 Collector необходимо штатными средствами ОС добавить этот сертификат в хранилище сертификатов от доверенных корневых центров сертификации.

16.1.1.7. Сканирование систем — Windows

Секция содержит параметры для настройки сбора данных из Windows с помощью следующих механизмов:

— WMI — инструменты управления Windows;

— RPC — удаленный вызова процедур;

— Remote Engine (RE) — удаленное выполнения сценариев (требуется WMI).

WMI

При выборе **WMI** доступны следующие параметры:

— **Учетная запись** — раскрывающийся список для выбора учетной записи, которая будет использоваться MP 10 Collector при аутентификации в ОС.

— **Пространство имен WMI** — поле для ввода пространства имен WMI, в котором выполняется WQL-запрос.

— **Уровень проверки подлинности WBEM** — дополнительный раскрывающийся список для выбора уровня проверки подлинности при удаленном вызове процедур (RPC):

- **None** — не выполняется;
- **Connect** — при подключении;
- **Pocket** — при получении данных;
- **PacketPrivacy** — шифрование значения аргумента.

— **Разрядность архитектуры ОС** — дополнительный раскрывающийся список для выбора разрядности архитектуры ОС.

— **Тайм-аут выполнения команд** — дополнительное поле для ввода тайм-аута выполнения команд в секундах.

— **Тайм-аут ответа на WQL-запрос** — дополнительное поле для ввода тайм-аута выполнения WQL-запросов в секундах.

RPC и Remote Engine

При выборе дополнительных механизмов сбора данных **RPC** и (или) **RE** также доступны раскрывающиеся списки для выбора приоритета использования механизмов сбора данных при сканировании файловой системы, реестра Windows и сбора данных службы безопасности Windows (вызов Windows API).

16.1.1.8. Сканирование систем — По протоколу LDAP

Секция содержит следующие параметры для настройки сбора данных из Windows через LDAP:

- **Учетная запись** — раскрывающийся список для выбора учетной записи, которая будет использоваться MP 10 Collector при аутентификации в ОС.
- **Порт** — дополнительное поле для ввода номера порта подключения к Windows (по умолчанию 389/TCP).
- **Использовать протокол SSL** — при включении для подключения по LDAP используется SSL-соединение.

  Примечание. Для SSL-соединения в дополнительном поле **Порт** требуется указать используемый порт. Обычно для такого соединения используется порт 636.
- **Тайм-аут ответа актива на эхо-запрос** — дополнительное поле для ввода тайм-аута ответа портов на эхо-запрос в секундах.
- **Тайм-аут поиска активов** — дополнительное поле для ввода тайм-аута получения одной страницы результата поиска в секундах.

16.1.1.9. Сканирование систем — По протоколу SNMP

Секция содержит раскрывающийся список для выбора версии протокола SNMP.

SNMP версий 1 и 2

При выборе версий 1 или 2 доступен параметр **Учетная запись типа «пароль»** — раскрывающийся список для выбора учетной записи типа «пароль», которая будет использоваться клиентом для аутентификации на сервере MP 10 Collector.

SNMP версии 3

При выборе версии 3 доступны следующие параметры:

- **Учетная запись** — раскрывающийся список для выбора учетной записи, которая будет использоваться клиентом для аутентификации на сервере MP 10 Collector.

Внимание! При использовании протокола SNMP версии 3 пароль учетной записи должен содержать не менее 8 символов.

— **Аутентификация** — при включении используется аутентификация.

  - **Алгоритм аутентификации** — раскрывающийся список для выбора алгоритма подсчета хеш-суммы ключа аутентификации **MD5**, **SHA_1**, **SHA_224**, **SHA_256**, **SHA_384** или **SHA_512**.

— **Шифрование** — при включении используется шифрование передаваемых данных.

  - **Учетная запись** — раскрывающийся список для выбора учетной записи.
  - **Алгоритм шифрования** — раскрывающийся список для выбора алгоритма шифрования данных **DES**, **AES_128**, **AES_192**, **AES_256**, **AES_192_CISCO** или **AES_256_CISCO**.

Параметры сбора данных (дополнительные параметры)

Блок доступен для всех версий протокола и содержит следующие параметры:

— **Повторное подключение: максимальное количество попыток** — поле для ввода максимального количества попыток восстановить связь с клиентом в случае ее разрыва.

— **Повторное подключение: интервал между попытками** — поле для ввода времени в секундах между попытками сервера восстановить связь с клиентом.

16.1.1.10. Сканирование систем — Через веб-API

Секция содержит следующие параметры для настройки сбора данных через веб-API:

— **Тип аутентификации** — раскрывающийся список для выбора типа аутентификации на сервере системы через веб-API:

  - **Учетные данные** — в заголовке запроса передаются логин и пароль учетной записи;
  - **Токен доступа Bearer** — в заголовке запроса передается токен доступа типа Bearer (аутентификация по протоколу OAuth);
  - **Ключ API** — в запросе передается ключ API.

— **Учетная запись** — раскрывающийся список для выбора учетной записи, которая будет использоваться MP 10 Collector при аутентификации на сервере.

— **Порт** — дополнительное поле для ввода номера порта подключения к серверу.

— **Использовать протокол SSL** — при включении используется протокол SSL.

— **Проверять сертификат SSL** — при включении для аутентификации на сервере используется сертификат SSL.

— **Тайм-аут ответа на запрос** — дополнительное поле для ввода максимального времени ожидания ответа на запрос.

16.1.1.11. Сканирование систем — Через терминал

Секция содержит раскрывающийся список для выбора используемого терминального протокола SSH, Telnet или обоих протоколов одновременно.

Подключение

Блок содержит следующие параметры:

— **Учетная запись** — раскрывающийся список для выбора учетной записи, которая будет использоваться MP 10 Collector при аутентификации на узле.

  Внимание! При аутентификации на узле с помощью SSH-ключей поддерживаются только ключи в формате OpenSSH.

— **Порт** — дополнительное поле для ввода номера порта подключения по SSH (по умолчанию для протокола SSH используется порт 22/TCP, для протокола Telnet — 23/TCP).

— **Способ повышения привилегий** — раскрывающийся список для выбора способа повышения привилегий при локальной аутентификации:

  - **sudo** — при выполнении каждой команды;
  - **su** — выполняется команда `su`;
  - **su_minus** — выполняется команда `su -`;
  - **enable** — выполняется команда `enable` (используется для некоторых устройств Cisco);
  - **expert** — выполняется команда `expert` (используется для систем Check Point);
  - **Другой** — выполняется команда, указанная в поле **Команда**.

— **Учетная запись для повышения привилегий** — раскрывающийся список для выбора учетной записи, которая будет использоваться MP 10 Collector для повышения привилегий на источнике.

— **Ожидать приглашение на ввод логина** — дополнительный параметр, при включении при локальной аутентификации ожидается ввод логина.

— **Ожидать приглашение на ввод пароля** — дополнительный параметр, при включении при локальной аутентификации ожидается ввод пароля.

Параметры SSH

Секция содержит следующие параметры для настройки выполнения команд SSH:

— **Регулярное выражение для баннера** — поле для ввода регулярного выражения для формата сообщения SSH (баннера). Используется для сообщений с динамическим содержимым (например, счетчиков или часов).

— **Тайм-аут ожидания ошибок аутентификации** — поле для ввода тайм-аута ожидания ошибок аутентификации в секундах.

- **Префикс команд** — поле для ввода префикса команд.
- **Тайм-аут выполнения команд** — поле для ввода тайм-аута выполнения команд в секундах.
- **Тайм-аут подключения** — поле для ввода тайм-аута подключения в секундах.
- **История командной оболочки** — при включении сохраняется история команд используемого интерпретатора команд.
- **Тайм-аут дополнительной аутентификации** — поле для ввода тайм-аута дополнительной аутентификации в секундах.
- **Интервал проверки активности сервера** — поле для ввода интервала отправки эхо-запросов в секундах (`0` — отправка пакетов отключена).
- **Тип псевдотерминала** — поле для ввода типа псевдотерминала.
- **Высота окна псевдотерминала** — поле для ввода высоты окна псевдотерминала.
- **Ширина окна псевдотерминала** — поле для ввода ширины окна псевдотерминала.
- **Папка временных файлов** — поле для ввода имени папки с временными файлами ОС. Если папка не указана, автоматически выбираются `$TMPDIR`, `$TMP`, `$TEMP`, `$TEMPDIR`, `/tmp`, `$HOME` или `~SSH.LOGIN`.
- **Тип терминального протокола** — раскрывающийся список для выбора типа терминального протокола (если ничего не выбрано, тип определяется автоматически):
  - **Unix** — для ОС семейства Unix;
  - **NetworkDevice** — для сетевых устройств;
  - **Checkpoint** — для сетевых устройств Check Point;
  - **Netware** — для сетевых устройств с операционной системой Novell NetWare;
  - **DionisNX** — для сетевых устройств Dionis-NX.
- **Тайм-аут загрузки данных в файл** — поле для ввода тайм-аута загрузки данных в файл в секундах.
- **Используемая командная оболочка** — выбор используемого интерпретатора команд:
  - **Определяется модулем** — для ОС используются следующие интерпретаторы команд: AIX — Korn shell; Darwin — Bash; FreeBSD — Bourne shell; HP-UX — Bourne shell; Linux — Bash; IBM OS/400 — Bash; Sun — Bourne shell; Sun 5.11 — Korn shell.
  - **По умолчанию для ОС** — используется командный интерпретатор ОС по умолчанию.

    Внимание! Модуль не поддерживает работу с интерпретатором команд C shell. Если по умолчанию в ОС используется C shell, работа модуля будет остановлена с ошибкой.

— **Используемая реализация DH-алгоритма** — выбор используемой версии криптографического протокола Диффи — Хеллмана:

- **Режим совместимости** — используется версия pre-RFC4419 SSH-2 diffie-hellman-group-exchange;
- **Актуальная реализация** — используется актуальная версия.

Параметры SSH → Разрешенные команды

Секция содержит кнопку **Добавить**. По кнопке вы можете добавить поля для ввода разрешенных команд. Поддерживаются регулярные выражения. Если ни одной команды не добавлено, все команды считаются разрешенными. Если есть добавленные команды, но среди них нет выполняемой команды, работа модуля завершается с ошибкой.

Параметры SSH → Запрещенные команды

Секция содержит кнопку **Добавить**. По кнопке вы можете добавить поля для ввода запрещенных команд. Поддерживаются регулярные выражения. Если выполняемая команда добавлена, то работа модуля завершается с ошибкой.

Параметры SSH → Отпечатки ключей SSH

Секция содержит кнопку **Добавить**. По кнопке вы можете добавить поля для ввода адресов узлов и отпечатков их ключей SSH.

Параметры SSH → Команды перед инициализацией сканирования

Секция содержит кнопку **Добавить**. По кнопке вы можете добавить поля для ввода команд выполняемых перед инициализацией сканирования.

Параметры SSH → Команды после инициализации сканирования

Секция содержит кнопку **Добавить**. По кнопке вы можете добавить поля для ввода команд выполняемых после инициализации сканирования.

Параметры SSH → Приглашения сервера

Секция содержит следующие параметры для настройки правил диалога с сервером:

— **Ввод логинов** — по кнопке **Добавить** вы можете добавить секции параметров для определения приглашений сервера на ввод логина. Каждая секция содержит раскрывающийся список для выбора формата запроса (**Строка** или **Регулярное выражение**) и поле для ввода запроса.

— **Ввод паролей** — по кнопке **Добавить** вы можете добавить секции параметров для определения приглашений сервера на ввод пароля. Каждая секция содержит раскрывающийся список для выбора формата запроса (**Строка** или **Регулярное выражение**) и поле для ввода запроса.

— **Продолжение вывода команды** — по кнопке **Добавить** вы можете добавить секции параметров для определения приглашений сервера на продолжение вывода команд. Каждая секция содержит параметры:

- **Название события** — поле для ввода названия события.
- **Фаза соединения** — раскрывающийся список для выбора этапа соединения: **Login**, **Session**, **Logout**.
- **Команды серверу** — по кнопке **Добавить** вы можете добавить секции параметров для настройки команд серверу. Каждая секция содержит раскрывающийся список для выбора формата команды, поле для ввода команды, а также следующие параметры:

  Включить эхо команд — при включении в течение времени, указанного в поле **Пауза после выполнения**, ожидается эхо команды от сервера.

  Пауза после выполнения — поле для ввода времени задержки после выполнения команды в миллисекундах.
- **Ответы сервера** — по кнопке **Добавить** вы можете добавить секции параметров для определения ответа сервера. Каждая секция содержит раскрывающийся список для выбора формата запроса (**Строка** или **Регулярное выражение**) и поле для ввода запроса.

— **Произвольные события** — по кнопке **Добавить** вы можете добавить секции параметров для определения произвольных событий. Каждая секция содержит параметры:

- **Название события** — поле для ввода названия события.
- **Фаза соединения** — раскрывающийся список для выбора этапа соединения: **Login**, **Session**, **Logout**.
- **Команды серверу** — по кнопке **Добавить** вы можете добавить секции параметров для настройки команд серверу. Каждая секция содержит раскрывающийся список для выбора формата команды, поле для ввода команды, а также следующие параметры:

  Включить эхо команд — при включении в течение времени, указанного в поле **Пауза после выполнения**, ожидается эхо команды от сервера.

Пауза после выполнения — поле для ввода времени задержки после выполнения команды в миллисекундах.

- **Ответы сервера** — по кнопке **Добавить** вы можете добавить секции параметров для определения ответа сервера. Каждая секция содержит раскрывающийся список для выбора формата запроса (**Строка** или **Регулярное выражение**) и поле для ввода запроса.

— **Ошибки доступа** — по кнопке **Добавить** вы можете добавить секции параметров для определения ответов сервера об ошибках доступа к файлу или ресурсу. Каждая секция содержит раскрывающийся список для выбора формата запроса (**Строка** или **Регулярное выражение**) и поле для ввода запроса.

— **Неправильный пароль** — по кнопке **Добавить** вы можете добавить секции параметров для определения ответов сервера об ошибках неверного пароля. Каждая секция содержит раскрывающийся список для выбора формата запроса (**Строка** или **Регулярное выражение**) и поле для ввода запроса.

— **Ошибки sudo** — по кнопке **Добавить** вы можете добавить секции параметров для определения ответов сервера об ошибках sudo. Каждая секция содержит раскрывающийся список для выбора формата запроса (**Строка** или **Регулярное выражение**) и поле для ввода запроса.

— **Ошибки команд** — по кнопке **Добавить** вы можете добавить секции параметров для определения ответов сервера об ошибках команд. Каждая секция содержит раскрывающийся список для выбора формата запроса (**Строка** или **Регулярное выражение**) и поле для ввода запроса.

16.1.1.12. Дополнительная экспертиза для аудита

Содержит раскрывающийся список **Дополнительная экспертиза для аудита**, в котором по умолчанию выбран справочник audit_expertise_extension с обновлениями экспертных данных для аудита, получаемых с сервера обновлений Positive Technologies. Данные из справочника используются для обнаружения ПО, которого нет в модели актива, что позволяет быстрее находить трендовые уязвимости.

Примечание. Использование справочника audit_expertise_extension поддерживают профили Windows Audit, Windows Audit Vulnerabilities Discovery и Unix Audit.

16.1.1.13. Особенности сканирования систем (дополнительные параметры)

Секция содержит следующие параметры для учета особенностей систем при сканировании:

— **Check Point** — блок параметров для настройки сканирования систем Check Point через терминал или через веб-API:

- **Количество элементов на странице ответа** — поле для ввода максимального количества элементов на странице в ответе на запрос.

16.1.1.14. Объем занимаемой памяти (дополнительные параметры)

Секция содержит следующие параметры для настройки работы модуля с памятью на узле MP 10 Collector:

- **Выделенный объем памяти** — поле для ввода объема памяти, выделяемой модулю на узле при его запуске, в мегабайтах.
- **Максимальный объем памяти** — поле для ввода максимального объема используемой модулем памяти в мегабайтах.
- **Шаг увеличения объема памяти** — поле для ввода объема памяти, на который будет увеличиваться выделяемая модулю память в случае ее нехватки. Шаг может быть от 16 до 1024 байт (нужно указывать степень двойки).

16.1.1.15. Работа модуля (дополнительные параметры)

Секция содержит следующие параметры для настройки работы модуля:

- **Собирать события как устаревшие** — не используется.
- **Интервал отправки уведомлений о состоянии** — поле для ввода интервала отправки уведомлений об активности модуля на MP 10 Collector в миллисекундах.
- **Повторное подключение: максимальное количество попыток** — поле для ввода максимального количества попыток модуля восстановить связь с MP 10 Collector в случае ее разрыва.
- **Повторное подключение: интервал между попытками** — поле для ввода времени между попытками модуля восстановить связь с MP 10 Collector в миллисекундах.
- **Справочник с параметрами журналирования** — раскрывающийся список для выбора справочника MaxPatrol VM с параметрами журналирования работы модуля (см. раздел 16.3).
- **Сохранять статистику сбора данных** — при включении в журнале модуля сохраняется информация об объеме собранных модулем данных (в байтах), количестве пакетов с данными, отправленных модулем на MP 10 Collector, и их объеме (в байтах).

16.1.1.16. Отправка данных в систему (дополнительные параметры)

Секция содержит следующие параметры для настройки отправки данных в MaxPatrol VM:

— **Максимальное количество событий в пакете** — поле для ввода максимального количества событий в пакете.

— **Тип отправляемых данных** — раскрывающийся список для выбора типа отправляемых данных:

  - **raw** — необработанные события;
  - **normalized** — нормализованные события;
  - **retro_normalized** — события для ретроспективной корреляции;
  - **asset_events** — данные для модели активов.

— **Интервал отправки пакетов** — поле для ввода интервала отправки пакетов в миллисекундах.

16.1.1.17. Отладка сканирования (дополнительные параметры)

Секция содержит следующие параметры для отладки сбора данных об активах:

— **Сохранять дамп данных сканирования** — при включении данные сканирования сохраняются в файле.

— **Использовать SQLite для хранения данных при сканировании** — при включении данные сканирования сохраняются не в памяти узла MP 10 Collector, а во временной базе SQLite. Это увеличивает время сканирования, но позволяет собирать большие объемы данных.

— **Частичное сканирование** — при включении собираются только указанные данные об активах:

  - **По маскам модели активов** — фильтрация данных при заполнении модели активов выполняется по маскам для классов и методам модели активов. Для этого вида сканирования доступно поле **Маски** для ввода масок.
  - **По классам модели активов** — фильтрация данных при заполнении модели активов выполняется по именам классов модели и используемым при сканировании методам. Для этого вида сканирования доступны параметры:

    Имена заполняемых классов — имена классов модели активов, которые будут заполняться при частичном сканировании. Несколько имен нужно указывать через точку с запятой.

Имена пропускаемых классов — имена классов модели активов, которые не будут заполняться при частичном сканировании. Несколько имен нужно указывать через точку с запятой.

Имена пропускаемых методов — имена методов сбора данных (сценариев), которые не будут использоваться при частичном сканировании. Несколько имен нужно указывать через точку с запятой.

16.1.2. Модуль HostDiscovery

Внимание! Данные, полученные модулем hostdiscovery при проведении аудита того узла, с которого выполняется этот аудит, будут недостоверными.

Модуль предназначен для поиска активов в IT-инфраструктуре организации. Для проверки доступности активов используются ICMP ping, TCP ping или оба метода одновременно. Для модуля созданы стандартные профили:

- HostDiscovery — базовый профиль для поиска активов. Актив обнаруживается по открытым на нем TCP-портам из списка часто используемых или ответу на запрос по протоколу ICMP.
- Inventory Profile — для поиска активов. Актив обнаруживается по открытым на нем TCP-портам или ответу на запрос по протоколу ICMP.
- Os Detection Profile — для поиска активов и определения версий, установленных на них операционных систем. Актив обнаруживается по открытым на нем TCP-портам. Для определения ОС необходимо, чтобы хотя бы один из проверяемых на активе портов был открыт и хотя бы один был закрыт. Определяются следующие версии ОС: Windows 7, 10; Windows Server 2012, 2012 R2, 2016; Debian 3.x, 4; Oracle Solaris 9.x, 10.x; Ubuntu (Linux) 8, 10, 14, 15, 16, 17.
- PortScan Full Range — для поиска открытых на активе TCP-портов в диапазоне от 1 до 65535.

Настраивать параметры модуля вы можете при создании пользовательского профиля на базе стандартного или задачи на сбор данных. Для этого в панели с параметрами профиля в иерархическом списке нужно выбрать секцию параметров и настроить необходимые. Далее приводятся описания параметров в каждой секции.

В этом разделе

16.1.2.1. Способы проверки узлов

Секция содержит параметры для настройки проверки портов. Успех хотя бы одной проверки, указывает на активность узла. Доступны следующие параметры:

- **Проводить проверку с помощью эхо-запроса ICMP** — при включении выполняется проверка портов эхо-запросами по протоколу ICMP.
- **Порты TCP для проверки с помощью SYN-пакетов** — поле для ввода номеров TCP-портов, проверяемых с синхронизацией номеров последовательности. Несколько портов нужно вводить через запятую, диапазон портов через дефис. Например: `80, 443, 1024-2000`.
- **Порты TCP для проверки с помощью ACK-пакетов** — дополнительное поле для ввода номеров TCP-портов, проверяемых с подтверждением. Несколько портов нужно вводить через запятую, диапазон портов через дефис.
- **Порты TCP для проверки с помощью RST-пакетов** — дополнительное поле для ввода номеров TCP-портов. Несколько портов нужно вводить через запятую, диапазон портов через дефис.
- **Порты UDP для проверки** — дополнительное поле для ввода номеров проверяемых UDP-портов. Несколько портов нужно вводить через запятую, диапазон портов через дефис.

16.1.2.2. Параметры проверки узлов

Секция содержит следующие параметры для настройки проверок портов:

- **Определение операционной системы** — при включении на активных узлах проводится определение версии ОС.
- **Проверка с помощью ARP-запросов** — дополнительный параметр при включении которого проводится проверка проводится проверка с помощью ARP-запросов. Отключение может увеличить общее время проверки узлов.
- **Считать узел активным при ответе на ARP-запрос** — дополнительный параметр при включении которого узел считается активным при ответе ARP-запрос.
- **Считать узел активным при любом ответе** — дополнительный параметр при включении которого узел считается активным при ожидаемом ответе.
- **Сканирование активных узлов** — дополнительное параметр при включении которого выполняется сканирование портов на активных узлах.
- **Максимальное количество неудачных проверок** — дополнительное поле для ввода максимального количества неудачных проверок каждого узла.

  Интервал между проверками — дополнительное поле для ввода времени между проверками в миллисекундах. Используется, если истекло время, указанное в поле **Тайм-аут ответа**.

— **Тайм-аут ответа** — дополнительное поле для ввода максимального время ожидания ответа при проверке в миллисекундах.

— **Максимальная скорость отправки ARP-запросов** — дополнительное поле для ввода максимального количества ARP-запросов, отправляемых при проверках в секунду.

  Примечание. Большое количество ARP-запросов одного узла может быть принято за сетевую атаку (ARP-storm, ARP-flood, ARP-spoofing).

— **Максимальная скорость отправки пакетов** — дополнительное поле для ввода максимального количества пакетов, отправляемых при проверках в секунду.

16.1.2.3. Объем занимаемой памяти (дополнительные параметры)

Секция содержит следующие параметры для настройки работы модуля с памятью на узле MP 10 Collector:

— **Выделенный объем памяти** — поле для ввода объема памяти, выделяемой модулю на узле при его запуске, в мегабайтах.

— **Максимальный объем памяти** — поле для ввода максимального объема используемой модулем памяти в мегабайтах.

— **Шаг увеличения объема памяти** — поле для ввода объема памяти, на который будет увеличиваться выделяемая модулю память в случае ее нехватки. Шаг может быть от 16 до 1024 байт (нужно указывать степень двойки).

16.1.2.4. Работа модуля (дополнительные параметры)

Секция содержит следующие параметры для настройки работы модуля:

— **Собирать события как устаревшие** — не используется.

— **Интервал отправки уведомлений о состоянии** — поле для ввода интервала отправки уведомлений об активности модуля на MP 10 Collector в миллисекундах.

— **Повторное подключение: максимальное количество попыток** — поле для ввода максимального количества попыток модуля восстановить связь с MP 10 Collector в случае ее разрыва.

— **Повторное подключение: интервал между попытками** — поле для ввода времени между попытками модуля восстановить связь с MP 10 Collector в миллисекундах.

— **Справочник с параметрами журналирования** — раскрывающийся список для выбора справочника MaxPatrol VM с параметрами журналирования работы модуля (см. раздел 16.3).

— **Сохранять статистику сбора данных** — при включении в журнале модуля сохраняется информация об объеме собранных модулем данных (в байтах), количестве пакетов с данными, отправленных модулем на MP 10 Collector, и их объеме (в байтах).

16.1.3. Модуль MP8ScanImporter

Модуль предназначен для импорта информации об активах обнаруженных MP8. Импорт выполняется из файлов отчетов формата XML, расположенных в папке на узле MP8. Для модуля создан стандартный профиль MP8ScanImporter.

Настраивать параметры модуля вы можете при создании пользовательского профиля на базе стандартного или задачи на сбор данных. Для этого в панели с параметрами профиля в иерархическом списке нужно выбрать секцию параметров и настроить необходимые. Далее приводятся описания параметров в каждой секции.

В этом разделе

16.1.3.1. Подключение

Секция содержит следующий параметр для настройки подключения к узлу MP8:

— **Учетная запись** — раскрывающийся список для выбора учетной записи, которая будет использоваться MP 10 Collector при аутентификации на узле.

16.1.3.2. Сбор событий

Секция содержит следующие параметры для настройки сбора отчетов с узла MP8:

— **Путь к общей папке** — поле для ввода пути к общей папке с файлами отчетов.

— **Параметры преобразования** — поле для ввода параметров для отладки модуля.

16.1.3.3. Работа модуля (дополнительные параметры)

Секция содержит следующие параметры для настройки работы модуля:

— **Собирать события как устаревшие** — не используется.

— **Интервал отправки уведомлений о состоянии** — поле для ввода интервала отправки уведомлений об активности модуля на MP 10 Collector в миллисекундах.

— **Повторное подключение: максимальное количество попыток** — поле для ввода максимального количества попыток модуля восстановить связь с MP 10 Collector в случае ее разрыва.

— **Повторное подключение: интервал между попытками** — поле для ввода времени между попытками модуля восстановить связь с MP 10 Collector в миллисекундах.

— **Справочник с параметрами журналирования** — раскрывающийся список для выбора справочника MaxPatrol VM с параметрами журналирования работы модуля (см. раздел 16.3).

— **Сохранять статистику сбора данных** — при включении в журнале модуля сохраняется информация об объеме собранных модулем данных (в байтах), количестве пакетов с данными, отправленных модулем на MP 10 Collector, и их объеме (в байтах).

16.1.4. Модуль Pentest

Модуль предназначен для аудита активов без использования данных учетных записей на источнике (методом черного ящика). Позволяет проводить тестирование на проникновение, поиск уязвимостей и информации о связанном с ними ПО. Для модуля созданы следующие стандартные профили:

— Bruteforce PenTest — для подбора учетных записей.

— Database Discovery — для проверки БД.

— Fast PenTest — для быстрого поиска уязвимостей.

— Full PenTest — для поиска уязвимостей.

— Http Servers Discovery — для сканирования веб-ресурсов.

— Mail Servers Discovery — для проверки почтовых служб.

— Remote Management Discovery — для проверки удаленного подключения.

— Safe PenTest — для тестирования на проникновение.

— SAP Discovery — для проверки продуктов компании SAP.

— Service Discovery — для обнаружения активных узлов, поиска на них открытых портов и определения работающих служб.

— Service Discovery on well-known ports — для быстрого обнаружения активных узлов, открытых на них портов и определения служб.

— SNMP Scan — для проверки с использованием протокола SNMP.

— Unsafe PenTest — для тестирования на проникновение.

— Windows Discovery — для обнаружения активных узлов с Windows, поиска на них открытых портов и определения работающих служб.

Настраивать параметры модуля вы можете при создании пользовательского профиля на базе стандартного или задачи на сбор данных. Для этого в панели с параметрами профиля в иерархическом списке нужно выбрать секцию параметров и настроить необходимые. Далее приводятся описания параметров в каждой секции.

В этом разделе

Работа модуля (дополнительные параметры) (см. раздел 16.1.4.30)

Отправка данных в систему (дополнительные параметры) (см. раздел 16.1.4.31)

16.1.4.1. Общие параметры сканирования

Секция содержит следующие параметры для настройки общих параметров сканирования портов и определения использующих их служб:

— **Метод сканирования портов** — выбор метода определения открытых портов:

- **SYN-пакеты** — состояние порта определяется на основании ответа на SYN-пакет, без полного соединения. При этом операционная система не участвует в установлении соединения, что дает возможность уменьшить время сканировать. Этот метод сканирования менее заметен для некоторых сетевых устройств.
- **Подключение** — состояние порта определяются через установку TCP-соединения. При этом соединения используются механизмы, предоставляемые операционной системой. Этот метод сканирования является самым достоверным, но увеличивает время сканирования.

— **Искать сетевые принтеры** — при включении выполняется предварительный поиск сетевых принтеров. Порты сетевых принтеров не сканируются.

— **Учитывать приоритет использования портов** — дополнительное поле для ввода приоритета от 0 до 100. Если указан 0, при сканировании порта проверяются все поддерживаемые модулем службы, если 100 — только службы, по умолчанию использующие этот порт.

— **Минимальный интервал между подключениями** — дополнительное поле для ввода минимального времени между подключениями к портам в секундах. Задержка между подключениями позволяет снизить нагрузку на сеть, сканируемое оборудование и обойти некоторые средства защиты, но значительно увеличивает время сканирования.

— **Тайм-аут ответа TCP-портов** — дополнительное поле для ввода максимального времени ответа при подключении к TCP-портам в секундах.

— **Тайм-аут ответа UDP-портов** — дополнительное поле для ввода максимального времени ответа при подключении к UDP-портам в секундах.

16.1.4.2. Сканирование портов

Секция содержит следующие параметры сканирования портов:

- **Порты** — поле для ввода номеров сканируемых TCP-портов. Номера портов нужно вводить с постфиксом `/tcp`. Несколько портов нужно вводить через точку с запятой, диапазон портов через дефис. Например: `1-1674/tcp;1698-2028/tcp`.
- **Использовать эвристический метод определения открытых портов** — дополнительный параметр, при включении для определений открытых на узле портов используется информация, предоставляемая службами, например RPC, SNMP, UPnP. Метод позволяет получить дополнительную информацию об открытых портах вне указанного диапазона сканируемых портов.
- **Тайм-аут подключения** — поле для ввода максимального времени ответа на SYN-пакет в секундах.
- **Максимальное количество потоков** — дополнительное поле для ввода максимального количества одновременных соединений для одного сканируемого узла.

16.1.4.3. Сканирование UDP-служб

Секция содержит параметры для настройки обнаружения служб, которые используют UDP-порты. Это может замедлять процесс сканирования, особенно если в сети запрещены ICMP-пакеты «Порт недоступен». Ответ службы ожидается в течение времени, указанного в параметре **Тайм-аут ответа UDP-портов**. Доступны следующие параметры для включения обнаружения служб на указанных портах:

- **CA BrightStor ARCServe Backup (порт 41524)**;
- **Character Generator Protocol (порт 19)**;
- **Daytime (порт 13)**;
- **DB2 DAS (порт 523)**;
- **DHCP (порта 67)**;
- **DNS (порт 53)**;
- **ECHO (порт 7)**;
- **GTP (порты 2123, 2152, 3386)**;
- **ICQ (порт 4000)**;
- **IKE (порт 500)**;
- **IKE NAT-T (порт 4500)**;
- **IPMI (порт 623)**;
- **LLMNR (порт 5355)**;

- **mDNS (порт 5353)**;
- **Microsoft Remote Desktop Gateway**;
- **Порт RDG** — поле для ввода номера порта службы Microsoft Remote Desktop Gateway (по умолчанию 3391/UDP).
- **Microsoft RPC Port Mapper (порт 135)**;
- **Microsoft SQL Server (порт 1434)**;
- **NetBIOS Name (порт 137)**;
- **NTP (порт 123)**;
- **ONC RPC portmap (порт 111)**;
- **OpenVPN (порт 1194)**;
- **pcAnyWhere (порт 5632)**;
- **Quota (порт 17)**;
- **SIP (порт 5060)**;
- **SLP (порт 427)**;
- **SNMP (порт 161)**;
- **Teredo (порт 3544)**;
- **TFTP (порт 69)**;
- **Unreal Tournament (порт 7777)**;
- **UPNP (порт 1900)**;
- **XDMCP (порт 177)**;
- **Memcached (порт 11211)**.

16.1.4.4. Поиск уязвимостей

Секция содержит раскрывающийся список для выбора режима поиска уязвимостей.

Полная проверка

При выборе **Полная проверка** выполняются все проверки для поиска уязвимостей из базы данных Knowledge Base. При этом доступны вложенные секции для настройки различных типов проверок и следующие параметры для настройки поиска уязвимостей:

- **Проверять на устойчивость к известным DoS-атакам** — при включении выполняется имитация атаки типа «отказ в обслуживании». Остановка службы или влияние атаки на ее работу указывает на наличие уязвимости (в случае проблем со связью возможны ложные срабатывания).

Внимание! Проверка является небезопасной и может привести к временной недоступности отдельных служб или узлов.

— **Использовать эвристический метод определения версий служб** — при включении для определения версии служб используется информация, получаемая из анализа ответов серверов на нестандартные запросы. Метод существенно повышает достоверность сканирования, но работает только для некоторых популярных протоколов, например DNS, HTTP, SMTP, SSH.

Частичная проверка

При выборе **Частичная проверка** выполняется проверки только с указанными идентификаторами для поиск уязвимостей из базы данных Knowledge Base. Доступны следующие параметры для настройки поиска уязвимостей:

— **Добавить порты для проверок** — поле для ввода номеров дополнительных портов для проверок. Сначала будет выполнен поиск уязвимостей на стандартных, характерных для них портах. Затем, если уязвимости не найдены, используются указанные порты.

— **Исключить порты для проверок** — поле для ввода номеров портов, которые будут исключены из проверок.

— **Идентификаторы проверок** — по кнопке **Добавить** вы можете добавить поля для ввода идентификаторов проверок, выполняемых при поиске уязвимостей.

16.1.4.5. Поиск уязвимостей — Подбор учетных данных — IBM DB2

Секция содержит следующие параметры для настройки подбора учетных данных пользователей СУБД IBM DB2:

— **Подбирать учетные данные** — при включении выполняется подбор учетных данных.

— **Имена баз данных** — по кнопке **Добавить** вы можете добавить поля для ввода имен БД, для которых будут подбираться учетные данные.

— **Справочники для подбора учетных данных** — раскрывающийся список для выбора справочников, которые будут использоваться при подборе учетных данных.

- **Справочник с логинами** — раскрывающийся список для выбора справочника MaxPatrol VM с логинами.
- **Справочник с паролями** — раскрывающийся список для выбора справочника MaxPatrol VM с паролями.
- **Справочник с парами «логин — пароль»** — раскрывающийся список для выбора справочника MaxPatrol VM с парами «логин — пароль».

— **Подбирать имена баз данных** — по кнопке **Добавить** вы можете добавить поля для ввода имен, среди которым будет выполнятся поиск имен БД, доступных в СУБД.

— **Максимальное количество потоков** — поле для ввода максимального количества параллельных потоков для подбора учетных данных.

16.1.4.6. Поиск уязвимостей — Подбор учетных данных — Microsoft SQL Server

Секция содержит следующие параметры для настройки подбора учетных данных пользователей СУБД Microsoft SQL Server:

— **Базовый справочник с парами «логин — пароль»** — раскрывающийся список для выбора справочника MaxPatrol VM с парами «логин — пароль».

— **Справочники для подбора учетных данных** — раскрывающийся список для выбора справочников, которые будут использоваться при подборе учетных данных.

- **Справочник с логинами** — раскрывающийся список для выбора справочника MaxPatrol VM с логинами.
- **Справочник с паролями** — раскрывающийся список для выбора справочника MaxPatrol VM с паролями.
- **Справочник с парами «логин — пароль»** — раскрывающийся список для выбора справочника MaxPatrol VM с парами «логин — пароль».

— **Максимальное количество потоков** — поле для ввода максимального количества параллельных потоков для подбора учетных данных.

16.1.4.7. Поиск уязвимостей — Подбор учетных данных — Oracle Database

Секция содержит следующие параметры для настройки подбора учетных данных пользователей СУБД Oracle Database:

— **Имена экземпляров СУБД** — по кнопке **Добавить** вы можете добавить поля для ввода имен экземпляров СУБД, для которых будут подбираться учетные данные.

— **Подбирать пароли для указанных SID** — при включении выполняется подбор паролей для SID или SERVICE_NAME, указанных в выбранных справочниках MaxPatrol VM (в секции параметров **Oracle Database, подбор SID**).

— **Подбирать пароли для найденных SID** — при включении выполняется подбор паролей для найденных SID или SERVICE_NAME.

— **Базовый справочник с парами «логин — пароль»** — раскрывающийся список для выбора справочника MaxPatrol VM с парами «логин — пароль».

— **Справочники для подбора учетных данных** — раскрывающийся список для выбора справочников, которые будут использоваться при подборе учетных данных.

  - **Справочник с логинами** — раскрывающийся список для выбора справочника MaxPatrol VM с логинами.
  - **Справочник с паролями** — раскрывающийся список для выбора справочника MaxPatrol VM с паролями.
  - **Справочник с парами «логин — пароль»** — раскрывающийся список для выбора справочника MaxPatrol VM с парами «логин — пароль».

— **Максимальное количество потоков** — поле для ввода максимального количества параллельных потоков для подбора учетных данных.

16.1.4.8. Поиск уязвимостей — Подбор учетных данных — Oracle Database, подбор SID

Секция содержит следующие параметры для настройки подбора SID или SERVICE_NAME для СУБД Oracle Database:

— **Базовый справочник с SID или SERVICE_NAME** — раскрывающийся список для выбора справочника MaxPatrol VM с SID или SERVICE_NAME.

— **Дополнительный справочник с SID или SERVICE_NAME** — раскрывающийся список для выбора справочника MaxPatrol VM с дополнительными SID или SERVICE_NAME.

— **Максимальное количество потоков** — поле для ввода максимального количества параллельных потоков для подбора SID или SERVICE_NAME.

16.1.4.9. Поиск уязвимостей — Подбор учетных данных — Oracle MySQL

Секция содержит следующие параметры для настройки подбора учетных данных пользователей СУБД Oracle MySQL:

— **Справочник с логинами** — раскрывающийся список для выбора справочника MaxPatrol VM с логинами.

— **Справочник с паролями** — раскрывающийся список для выбора справочника MaxPatrol VM с паролями.

— **Максимальное количество потоков** — поле для ввода максимального количества параллельных потоков для подбора учетных данных.

16.1.4.10. Поиск уязвимостей — Подбор учетных данных — SAP Sybase ASE

Секция содержит следующие параметры для настройки подбора учетных данных пользователей СУБД SAP Sybase ASE:

— **Справочники для подбора учетных данных** — раскрывающийся список для выбора справочников, которые будут использоваться при подборе учетных данных.

- **Справочник с логинами** — раскрывающийся список для выбора справочника MaxPatrol VM с логинами.
- **Справочник с паролями** — раскрывающийся список для выбора справочника MaxPatrol VM с паролями.
- **Справочник с парами «логин — пароль»** — раскрывающийся список для выбора справочника MaxPatrol VM с парами «логин — пароль».

16.1.4.11. Поиск уязвимостей — Подбор учетных данных — SAP через DIAG

Секция содержит следующие параметры для настройки подбора учетных данных пользователей систем SAP по протоколу DIAG:

— **Проверить номера мандатов клиентов** — по кнопке **Добавить** вы можете добавить поля для ввода номеров мандатов клиентов SAP, для которых будут подбираться учетные данные.

— **Проверить все номера мандатов от 000 до 999** — при включении учетные данные подбираются для клиентов SAP с любыми мандатами.

— **Справочники для подбора учетных данных** — раскрывающийся список для выбора справочников, которые будут использоваться при подборе учетных данных.

- **Справочник с логинами** — раскрывающийся список для выбора справочника MaxPatrol VM с логинами.
- **Справочник с паролями** — раскрывающийся список для выбора справочника MaxPatrol VM с паролями.
- **Справочник с парами «логин — пароль»** — раскрывающийся список для выбора справочника MaxPatrol VM с парами «логин — пароль».

— **Максимальное количество потоков** — поле для ввода максимального количества параллельных потоков для подбора учетных данных.

16.1.4.12. Поиск уязвимостей — Подбор учетных данных — SAP через RFC

Секция содержит следующие параметры для настройки подбора учетных данных пользователей систем SAP через интерфейс RFC:

— **Проверить номера мандатов клиентов** — по кнопке **Добавить** вы можете добавить поля для ввода номеров мандатов клиентов SAP, для которых будут подбираться учетные данные.

— **Проверить все номера мандатов от 000 до 999** — при включении учетные данные подбираются для клиентов SAP с любыми мандатами.

— **Справочники для подбора учетных данных** — раскрывающийся список для выбора справочников, которые будут использоваться при подборе учетных данных.

- **Справочник с логинами** — раскрывающийся список для выбора справочника MaxPatrol VM с логинами.
- **Справочник с паролями** — раскрывающийся список для выбора справочника MaxPatrol VM с паролями.
- **Справочник с парами «логин — пароль»** — раскрывающийся список для выбора справочника MaxPatrol VM с парами «логин — пароль».

— **Максимальное количество потоков** — поле для ввода максимального количества параллельных потоков для подбора учетных данных.

16.1.4.13. Поиск уязвимостей — Подбор учетных данных — Symantec pcAnywhere

Секция содержит следующие параметры для настройки подбора учетных данных пользователей Symantec pcAnywhere:

— **Справочники для подбора учетных данных** — раскрывающийся список для выбора справочников, которые будут использоваться при подборе учетных данных.

- **Справочник с логинами** — раскрывающийся список для выбора справочника MaxPatrol VM с логинами.
- **Справочник с паролями** — раскрывающийся список для выбора справочника MaxPatrol VM с паролями.
- **Справочник с парами «логин — пароль»** — раскрывающийся список для выбора справочника MaxPatrol VM с парами «логин — пароль».

— **Максимальное количество потоков** — поле для ввода максимального количества параллельных потоков для подбора учетных данных.

16.1.4.14. Поиск уязвимостей — Подбор учетных данных — Virtual Network Computing

Секция содержит следующие параметры для настройки подбора учетных данных пользователей система удаленного доступа Virtual Network Computing:

— **Базовый справочник с парами «логин — пароль»** — раскрывающийся список для выбора справочника MaxPatrol VM с парами «логин — пароль».

— **Справочники для подбора учетных данных** — раскрывающийся список для выбора справочников, которые будут использоваться при подборе учетных данных.

- **Справочник с логинами** — раскрывающийся список для выбора справочника MaxPatrol VM с логинами.
- **Справочник с паролями** — раскрывающийся список для выбора справочника MaxPatrol VM с паролями.
- **Справочник с парами «логин — пароль»** — раскрывающийся список для выбора справочника MaxPatrol VM с парами «логин — пароль».

16.1.4.15. Поиск уязвимостей — Подбор учетных данных — VMware vSphere

Секция содержит следующие параметры для настройки подбора учетных данных пользователей систем VMware vSphere:

— **Справочники для подбора учетных данных** — раскрывающийся список для выбора справочников, которые будут использоваться при подборе учетных данных.

- **Справочник с логинами** — раскрывающийся список для выбора справочника MaxPatrol VM с логинами.
- **Справочник с паролями** — раскрывающийся список для выбора справочника MaxPatrol VM с паролями.
- **Справочник с парами «логин — пароль»** — раскрывающийся список для выбора справочника MaxPatrol VM с парами «логин — пароль».

16.1.4.16. Поиск уязвимостей — Подбор учетных данных — По протоколу FTP

Секция содержит следующие параметры для настройки подбора учетных данных пользователей по протоколу FTP:

— **Справочник с логинами** — раскрывающийся список для выбора справочника MaxPatrol VM с логинами.

— **Справочник с паролями** — раскрывающийся список для выбора справочника MaxPatrol VM с паролями.

16.1.4.17. Поиск уязвимостей — Подбор учетных данных — По протоколу NetBIOS

Секция содержит следующие параметры для настройки подбора учетных данных по протоколу NetBIOS:

— **Справочники для подбора учетных данных** — раскрывающийся список для выбора справочников, которые будут использоваться при подборе учетных данных.

- **Справочник с логинами** — раскрывающийся список для выбора справочника MaxPatrol VM с логинами.
- **Справочник с паролями** — раскрывающийся список для выбора справочника MaxPatrol VM с паролями.
- **Справочник с парами «логин — пароль»** — раскрывающийся список для выбора справочника MaxPatrol VM с парами «логин — пароль».

— **Подбирать пароли для найденных логинов** — при включении выполняется поиск паролей для найденных логинов.

16.1.4.18. Поиск уязвимостей — Подбор учетных данных — По протоколу POP3

Секция содержит следующие параметры для настройки подбора учетных данных по протоколу POP3:

— **Базовый справочник с парами «логин — пароль»** — раскрывающийся список для выбора справочника MaxPatrol VM с парами «логин — пароль».

— **Справочники для подбора учетных данных** — раскрывающийся список для выбора справочников, которые будут использоваться при подборе учетных данных.

- **Справочник с логинами** — раскрывающийся список для выбора справочника MaxPatrol VM с логинами.
- **Справочник с паролями** — раскрывающийся список для выбора справочника MaxPatrol VM с паролями.
- **Справочник с парами «логин — пароль»** — раскрывающийся список для выбора справочника MaxPatrol VM с парами «логин — пароль».

16.1.4.19. Поиск уязвимостей — Подбор учетных данных — По протоколу RDP

Секция содержит следующие параметры для настройки подбора учетных данных по протоколу RDP:

— **Базовый справочник с парами «логин — пароль»** — раскрывающийся список для выбора справочника MaxPatrol VM с парами «логин — пароль».

— **Справочники для подбора учетных данных** — раскрывающийся список для выбора справочников, которые будут использоваться при подборе учетных данных.

- **Справочник с логинами** — раскрывающийся список для выбора справочника MaxPatrol VM с логинами.
- **Справочник с паролями** — раскрывающийся список для выбора справочника MaxPatrol VM с паролями.
- **Справочник с парами «логин — пароль»** — раскрывающийся список для выбора справочника MaxPatrol VM с парами «логин — пароль».

16.1.4.20. Поиск уязвимостей — Подбор учетных данных — По протоколу SIP

Секция содержит следующие параметры для настройки подбора учетных данных по протоколу SIP:

— **Справочники для подбора учетных данных** — раскрывающийся список для выбора справочников, которые будут использоваться при подборе учетных данных.

- **Справочник с логинами** — раскрывающийся список для выбора справочника MaxPatrol VM с логинами.
- **Справочник с паролями** — раскрывающийся список для выбора справочника MaxPatrol VM с паролями.
- **Справочник с парами «логин — пароль»** — раскрывающийся список для выбора справочника MaxPatrol VM с парами «логин — пароль».

16.1.4.21. Поиск уязвимостей — Подбор учетных данных — По протоколу SMTP

Секция содержит следующие параметры для настройки подбора учетных данных по протоколу SMTP:

— **Справочники для подбора учетных данных** — раскрывающийся список для выбора справочников, которые будут использоваться при подборе учетных данных.

- **Справочник с логинами** — раскрывающийся список для выбора справочника MaxPatrol VM с логинами.
- **Справочник с паролями** — раскрывающийся список для выбора справочника MaxPatrol VM с паролями.
- **Справочник с парами «логин — пароль»** — раскрывающийся список для выбора справочника MaxPatrol VM с парами «логин — пароль».

16.1.4.22. Поиск уязвимостей — Подбор учетных данных — По протоколу SNMP

Секция содержит блоки параметров для настройки подбора учетных данных пользователей с использованием различных версий протокола SNMP.

Версия 2

Для протокола версии 2 доступен параметр:

— **Справочник с паролями** — раскрывающийся список для выбора справочника MaxPatrol VM с паролями.

Версия 3

Для протокола версии 3 доступны следующие параметры:

— **Справочник с логинами** — раскрывающийся список для выбора справочника MaxPatrol VM с логинами.

— **Справочник с паролями** — раскрывающийся список для выбора справочника MaxPatrol VM с паролями.

16.1.4.23. Поиск уязвимостей — Подбор учетных данных — По протоколу SSH

Секция содержит следующие параметры для настройки подбора учетных данных по протоколу SSH:

— **Базовый справочник с парами «логин — пароль»** — раскрывающийся список для выбора справочника MaxPatrol VM с парами «логин — пароль».

— **Справочники для подбора учетных данных** — раскрывающийся список для выбора справочников, которые будут использоваться при подборе учетных данных.

- **Справочник с логинами** — раскрывающийся список для выбора справочника MaxPatrol VM с логинами.
- **Справочник с паролями** — раскрывающийся список для выбора справочника MaxPatrol VM с паролями.
- **Справочник с парами «логин — пароль»** — раскрывающийся список для выбора справочника MaxPatrol VM с парами «логин — пароль».

16.1.4.24. Поиск уязвимостей — Подбор учетных данных — По протоколу Telnet

Секция содержит следующие параметры для настройки подбора учетных данных по протоколу Telnet:

— **Базовый справочник с парами «логин — пароль»** — раскрывающийся список для выбора справочника MaxPatrol VM с парами «логин — пароль».

— **Приглашения сервера на ввод логина** — раскрывающийся список для выбора справочника MaxPatrol VM содержащего запросы для определения приглашений сервера на ввод логина.

— **Приглашения сервера на ввод пароля** — раскрывающийся список для выбора справочника MaxPatrol VM содержащего запросы для определения приглашений сервера на ввод пароля.

— **Справочники для подбора учетных данных** — раскрывающийся список для выбора справочников, которые будут использоваться при подборе учетных данных.

- **Справочник с логинами** — раскрывающийся список для выбора справочника MaxPatrol VM с логинами.
- **Справочник с паролями** — раскрывающийся список для выбора справочника MaxPatrol VM с паролями.
- **Справочник с парами «логин — пароль»** — раскрывающийся список для выбора справочника MaxPatrol VM с парами «логин — пароль».

16.1.4.25. Поиск уязвимостей — Подбор учетных данных — Фаматек RAdmin

Секция содержит следующие параметры для настройки подбора учетных данных пользователей ПО Фаматек RAdmin:

— **Базовый справочник с парами «логин — пароль»** — раскрывающийся список для выбора справочника MaxPatrol VM с парами «логин — пароль».

— **Справочники для подбора учетных данных** — раскрывающийся список для выбора справочников, которые будут использоваться при подборе учетных данных.

- **Справочник с логинами** — раскрывающийся список для выбора справочника MaxPatrol VM с логинами.
- **Справочник с паролями** — раскрывающийся список для выбора справочника MaxPatrol VM с паролями.
- **Справочник с парами «логин — пароль»** — раскрывающийся список для выбора справочника MaxPatrol VM с парами «логин — пароль».

16.1.4.26. Поиск уязвимостей — Поиск файлов

Секция содержит следующие параметры для настройки поиска файлов:

— **Максимальное количество проверяемых файлов** — поле для ввода максимального количества файлов.

— **Глубина поиска во вложенных папках** — поле для ввода максимальной глубины вложенных папок при поиске файлов.

— Параметры для настройки поиска файлов по названию:

  - **Справочник с регулярными выражениями для имен файлов** — раскрывающийся список для выбора справочника MaxPatrol VM с регулярными выражениями для имен и расширений файлов (по умолчанию filenames).
  - **Справочник с именами файлов для поиска через TFTP** — раскрывающийся список для выбора справочника MaxPatrol VM с названиями файлов.
  - **Искать скрытые папки FTP** — при включении выполняется поиск скрытых каталогов по словарю. Значительно замедляет сканирование FTP-серверов.

— **Поиска файлов по содержимому** — при включении выполняется поиск файлов по содержимому. Доступны следующие параметры:

  - **Регулярные выражения для содержимого файлов** — по кнопке **Добавить** вы можете добавить поля для ввода регулярные выражений для содержимого файлов.
  - **Маска имен файлов** — дополнительное поле для ввода маски имен проверяемых файлов.
  - **Минимальный размер файла** — дополнительное поле для ввода минимального размера проверяемых файлов в байтах.
  - **Максимальный размер файла** — дополнительное поле для ввода максимального размера проверяемых файлов в байтах.

16.1.4.27. Поиск уязвимостей — Сканирование по LDAP

Секция содержит следующие параметры для настройки сканирования по LDAP:

— **Максимальное количество атрибутов имени** — поле для ввода максимального количества значений атрибутов, используемых при сканировании. Это позволяет ограничить количество информации, получаемой со сканируемого LDAP-сервера.

— **Максимальное количество RDN первого уровня** — поле для ввода максимального количество записей Relative Distinguished Name, используемых сканировании.

16.1.4.28. Отладка сканирования (дополнительные параметры)

Секция содержит следующие параметры для отладки сбора данных об активах:

— **Сохранять дамп данных сканирования** — при включении данные сканирования сохраняются в файле.

— **Использовать SQLite для хранения данных при сканировании** — при включении данные сканирования сохраняются не в памяти узла MP 10 Collector, а во временной базе SQLite. Это увеличивает время сканирования, но позволяет собирать большие объемы данных.

— **Частичное сканирование** — при включении собираются только указанные данные об активах:

- **По маскам модели активов** — фильтрация данных при заполнении модели активов выполняется по маскам для классов и методам модели активов. Для этого вида сканирования доступно поле **Маски** для ввода масок.
- **По классам модели активов** — фильтрация данных при заполнении модели активов выполняется по именам классов модели и используемым при сканировании методам. Для этого вида сканирования доступны параметры:

  Имена заполняемых классов — имена классов модели активов, которые будут заполняться при частичном сканировании. Несколько имен нужно указывать через точку с запятой.

  Имена пропускаемых классов — имена классов модели активов, которые не будут заполняться при частичном сканировании. Несколько имен нужно указывать через точку с запятой.

  Имена пропускаемых методов — имена методов сбора данных (сценариев), которые не будут использоваться при частичном сканировании. Несколько имен нужно указывать через точку с запятой.

16.1.4.29. Объем занимаемой памяти (дополнительные параметры)

Секция содержит следующие параметры для настройки работы модуля с памятью на узле MP 10 Collector:

— **Выделенный объем памяти** — поле для ввода объема памяти, выделяемой модулю на узле при его запуске, в мегабайтах.

— **Максимальный объем памяти** — поле для ввода максимального объема используемой модулем памяти в мегабайтах.

— **Шаг увеличения объема памяти** — поле для ввода объема памяти, на который будет увеличиваться выделяемая модулю память в случае ее нехватки. Шаг может быть от 16 до 1024 байт (нужно указывать степень двойки).

16.1.4.30. Работа модуля (дополнительные параметры)

Секция содержит следующие параметры для настройки работы модуля:

— **Собирать события как устаревшие** — не используется.

— **Интервал отправки уведомлений о состоянии** — поле для ввода интервала отправки уведомлений об активности модуля на MP 10 Collector в миллисекундах.

— **Повторное подключение: максимальное количество попыток** — поле для ввода максимального количества попыток модуля восстановить связь с MP 10 Collector в случае ее разрыва.

— **Повторное подключение: интервал между попытками** — поле для ввода времени между попытками модуля восстановить связь с MP 10 Collector в миллисекундах.

— **Справочник с параметрами журналирования** — раскрывающийся список для выбора справочника MaxPatrol VM с параметрами журналирования работы модуля (см. раздел 16.3).

— **Сохранять статистику сбора данных** — при включении в журнале модуля сохраняется информация об объеме собранных модулем данных (в байтах), количестве пакетов с данными, отправленных модулем на MP 10 Collector, и их объеме (в байтах).

16.1.4.31. Отправка данных в систему (дополнительные параметры)

Секция содержит следующие параметры для настройки отправки данных в MaxPatrol VM:

— **Максимальное количество событий в пакете** — поле для ввода максимального количества событий в пакете.

— **Тип отправляемых данных** — раскрывающийся список для выбора типа отправляемых данных:

- **raw** — необработанные события;
- **normalized** — нормализованные события;
- **retro_normalized** — события для ретроспективной корреляции;
- **asset_events** — данные для модели активов.

— **Интервал отправки пакетов** — поле для ввода интервала отправки пакетов в миллисекундах.

16.2. Модуль для выполнения сценария на удаленных узлах, RemoteExecutor

Модуль предназначен для выполнения сценария на удаленных узлах. Для модуля созданы стандартные профили:

— PowershellExecutor — для выполнение указанного сценария с помощью Windows PowerShell и получения результата выполнения.

— RemoteExecutor — для выполнения указанного сценария на удаленном узле и получения результата выполнения.

Настраивать параметры модуля вы можете при создании пользовательского профиля на базе стандартного или задачи на сбор данных. Для этого в панели с параметрами профиля в иерархическом списке нужно выбрать секцию параметров и настроить необходимые. Далее приводятся описания параметров в каждой секции.

В этом разделе

16.2.1. Подключение

Секция содержит следующий параметр для настройки подключения к источнику:

— **Учетная запись** — раскрывающийся список для выбора учетной записи, которая будет использоваться MP 10 Collector при аутентификации на источнике.

16.2.2. Запуск сценария

Секция содержит следующие параметры для настройки запуска сценария:

— **Собирать результат выполнения сценария** — при включении если после выполнения сценария папка с результатом пуста, модуль завершается с ошибкой.

— **Тип файла сценария** — раскрывающийся список для выбора типа сценария:

- **Сценарий ком. строки** — сценарий командной оболочки Windows. Для этого типа доступен параметр:

  Справочник со сценарием — раскрывающийся список для выбора справочника со сценарием.

- **Сценарий PowerShell** — сценарий Windows PowerShell. Для этого типа доступен параметр:

Версия PowerShell — поле для ввода номера версии Windows PowerShell, которая необходима для выполнения сценария.

- **ZIP-архив со сценарием** — архиве должен содержать файл `run.cmd`, принимающий как аргумент путь к папке с результатами выполнения. Для этого типа доступны параметры:

  Путь к файлу архива — поле для ввода пути к файлу ZIP-архива со сценариями, которые надо выполнить на удаленных узлах.

  Контрольная сумма файла архива (MD5) — поле для ввода хеш-суммы файла архива, рассчитанная по алгоритму MD5.

  Контрольная сумма файла архива (SHA-1) — поле для ввода хеш-суммы файла архива, рассчитанная по алгоритму SHA-1.

- **Исполняемый файл** — исполняемый файл, будет скопирован на удаленный узел и запущен с указанными аргументами. Для этого типа доступны параметры:

  Путь к исполняемому файлу — поле для ввода пути к исполняемому файлу сценария.

  Аргументы команды запуска — поле для ввода аргументов команды запуска исполняемого файла.

— **Название файла с результатом выполнения** — поле для ввода пути к файлу в который будет перенаправлен стандартный поток вывода данных при выполнении сценария (stdout).

— **Название файла с ошибками** — поле для ввода пути к файлу, в который будет перенаправлен стандартный поток ошибок при выполнении сценария (stderr).

— **Дополнительные файлы** — по кнопке **Добавить** вы можете указать дополнительные файлы, необходимые для выполнении сценария.

— **Максимальное количество потоков** — дополнительное поле для ввода максимального количества одновременных сеансов с разными узлами. Позволяет ограничить нагрузку на ресурсы узла MP 10 Collector.

— **Тайм-аут выполнения сценария** — дополнительное поле для ввода максимального времени выполнения сценария в минутах.

16.2.3. Объем занимаемой памяти (дополнительные параметры)

Секция содержит следующие параметры для настройки работы модуля с памятью на узле MP 10 Collector:

- **Выделенный объем памяти** — поле для ввода объема памяти, выделяемой модулю на узле при его запуске, в мегабайтах.
- **Максимальный объем памяти** — поле для ввода максимального объема используемой модулем памяти в мегабайтах.
- **Шаг увеличения объема памяти** — поле для ввода объема памяти, на который будет увеличиваться выделяемая модулю память в случае ее нехватки. Шаг может быть от 16 до 1024 байт (нужно указывать степень двойки).

16.2.4. Работа модуля (дополнительные параметры)

Секция содержит следующие параметры для настройки работы модуля:

- **Собирать события как устаревшие** — не используется.
- **Интервал отправки уведомлений о состоянии** — поле для ввода интервала отправки уведомлений об активности модуля на MP 10 Collector в миллисекундах.
- **Повторное подключение: максимальное количество попыток** — поле для ввода максимального количества попыток модуля восстановить связь с MP 10 Collector в случае ее разрыва.
- **Повторное подключение: интервал между попытками** — поле для ввода времени между попытками модуля восстановить связь с MP 10 Collector в миллисекундах.
- **Справочник с параметрами журналирования** — раскрывающийся список для выбора справочника MaxPatrol VM с параметрами журналирования работы модуля (см. раздел 16.3).
- **Сохранять статистику сбора данных** — при включении в журнале модуля сохраняется информация об объеме собранных модулем данных (в байтах), количестве пакетов с данными, отправленных модулем на MP 10 Collector, и их объеме (в байтах).

16.3. Параметры журналирования работы модулей

Параметры журналирования работы модулей MP 10 Collector и их компонентов настраиваются с помощью справочников MaxPatrol VM. По умолчанию для всех модулей используются параметры, указанные в справочнике logging_settings.

Для изменения параметров журналирования одного или нескольких модулей нужно создать пользовательский справочник и настроить в нем параметры журналирования в формате XML (по аналогии со справочником logging_settings). Справочник должен содержать объекты

`params` и `root`. В объекте `params` вы можете настроить параметры файлов журналов. В объекте `root` вы можете настроить параметры журналирования отдельных модулей и компонентов. Название созданного справочника нужно указать в профиле в разделе с дополнительными параметрами **Работа модуля** в параметре **Справочник с параметрами журналирования**.

> **Примечание.** Журналы модулей сохраняются в папке установки MP 10 Collector в папке `\log\modules\<Название модуля>`.

Структура справочника logging_settings:

```
<?xml version="1.0" encoding="utf-8"?>
<config>
  <root>
    <Logger level="INFO"/>
    <ModuleHost level="INFO"/>
    <Pipe level="INFO"/>
    <libnet level="INFO"/>
    <Parser level="INFO"/>
    <Impersonater level="INFO"/>
    <AgentClient level="INFO"/>
    <Profile level="INFO"/>
    <MP9 level="INFO"/>
    <Scanner level="INFO"/>
    <Pentest level="INFO"/>
    <PythonInterpreter level="INFO"/>
    <PyEventCollector level="INFO"/>
    <CustomEventCollector level="INFO"/>
    <vSphereEventCollector level="INFO"/>
    <BatchEventSearch level="INFO"/>
    <RetroCorrelator level="INFO"/>
    <NetFlow level="INFO"/>
    <WMILog level="INFO"/>
    <WMINotification level="INFO"/>
    <SapRfcEventCollector level="INFO"/>
    <SnmpTrapCollector level="INFO"/>
    <NetSNMP level="INFO"/>
    <SSHEventCollector level="INFO"/>
    <libssh level="INFO"/>
    <wineventlog level="INFO"/>
    <SysLog level="INFO"/>
    <odbclog level="INFO"/>
    <FileMonitor level="INFO"/>
    <DPICollector level="INFO"/>
    <OpsecLog level="INFO"/>
    <MSExchangeEventCollector level="INFO"/>
    <HostDiscovery level="INFO"/>
    <Transports>
        <LDAP level="INFO"/>
```

```
        <LDAP2 level="INFO"/>
        <NodeB level="INFO"/>
        <NotesRPC level="INFO"/>
        <ODBC level="INFO"/>
        <OPSEC level="INFO"/>
        <RPC level="INFO"/>
        <SAPGUI level="INFO"/>
        <SAPRFC level="INFO"/>
        <SNMP level="INFO"/>
        <netsnmp level="INFO"/>
        <SSH level="INFO"/>
        <Telnet level="INFO"/>
        <WMI level="INFO"/>
        <Minister level="INFO"/>
    </Transports>
  </root>
  <params max_file_size="100" max_backup_index="50"/>
</config>
```

params

Объект содержит параметры для настройки журнала модуля:

— `max_file_size`

  Параметр для выбора максимального размера файла журнала в мегабайтах (по умолчанию 100 МБ).

— `max_backup_index`

  Параметр для выбора максимального количества журналов для одной задачи (по умолчанию 50). После достижения указанного количества наиболее старый журнал удаляется.

root

Объект содержит параметры для выбора режима журналирования работы модулей и их компонентов. Каждому из модулей (компонентов) соответствует параметр для выбора режима журналирования (см. таблицу ниже). По умолчанию для всех модулей установлен режим `INFO`. Вы можете выбрать один из следующих режимов:

— `NOTSET` — журналирования отключено;

— `FATAL` — ошибки, влияющие на корректный запуск и остановку компонента;

— `ERROR` — ошибки в работе компонента;

— `WARN` — предупреждения, связанные некорректной настройкой модуля;

— `INFO` — информационные сообщения о работе компонента;

— `DEBUG` — информационные сообщения о деталях работы компонента;

— `TRACE` — информационные сообщения обо всех деталях работы компонента.

Таблица 1. Параметры для выбора режима журналирования

Параметр	Модуль (компонент)
`AgentClient`	Служебный компонент MP 10 Collector
`BatchEventSearch`	Модуль BatchEventSearch
`CustomEventCollector`	Модуль Custom Event Collector
`DallasLockCollector`	Сценарий сбора событий, используемый профилем Dallas Lock events collector
`DPICollector`	Модуль NADSensor
`FileMonitor`	Модуль FileMonitor
`HostDiscovery`	Модуль HostDiscovery
`Impersonater`	Служебный компонент MP 10 Collector
`IncapsulaEventCollector`	Сценарий сбора событий, используемый профилем Imperva Incapsula
`libnet`	Компонент, обеспечивающий работу модулей с компьютерной сетью
`libssh`	Компонент модуля SshEventCollector для сбора данных по протоколу SSH
`Logger`	Компонент для журналирования работы модулей
`ModuleHost`	Служебный компонент, обеспечивающий запуск модулей MP 10 Collector
`MP9`	Служебный компонент MP 10 Collector, обеспечивающий сбор данных модулями Audit и Pentest
`MSExchangeEventCollector`	Сценарии сбора событий, используемые профилями Microsoft Exchange 2010 (mailbox audit) и Microsoft Exchange 2013 (mailbox logon)
`NetFlow`	Модуль NetFlow
`NetSNMP`	Компонент модуля SnmpTrapCollector для работы с компьютерной сетью
`odbclog`	Модуль OdbcLog
`OpsecLog`	Модуль OpsecLog
`Parser`	Компонент, используемый в модулях FileMonitor, FileImporter и SapRfcEventCollector для дополнительной обработки строк полученных событий (парсер)

Параметр	Модуль (компонент)
`Pentest`	Модуль Pentest
`Pipe`	Компонент, обеспечивающий канал связи между модулем и MP 10 Collector
`Profile`	Служебный компонент MP 10 Collector
`PyEventCollector`	Компонент MP 10 Collector для запуска пользовательских модулей на языке программирования Python
`PythonInterpreter`	Компонент MP 10 Collector для работы пользовательских модулей на языке программирования Python
`RetroCorrelator`	Модуля RetroCorrelator
`SapRfcEventCollector`	Модуль SapRfcEventCollector
`Scanner`	Модуль Audit
`SnmpTrapCollector`	Модуль snmptrapcollector
`SSHEventCollector`	Модуль ssheventcollector
`SysLog`	Модуль syslog
`Transports`	Механизмы сбора данных. Вы можете изменить режим журналирования одновременно для всех механизмов или, используя соответствующий параметр, для групп или отдельных механизмов сбора данных: — `LDAP` и `LDAP2` — сбор по протоколу LDAP; — `Minister` — служебный компонент MP 10 Collector, обеспечивающий работу механизмов сбора данных; — `NodeB` — для сетевых устройств Huawei NodeB; — `NotesRPC` — технология RPC для сбора с Windows; — `ODBC` — группа механизмов для сбора данных из СУБД; — `OPSEC` — для систем Check Point через API OPSEC; — `RPC` — технология RPC для сбора с Windows; — `SAPRFC` — для систем SAP через RFC; — `SNMP` — по протоколу SNMP; — `SSH` и `Telnet` — для терминальных протоколов; — `WMI` — технология WMI для сбора с Windows
`vSphereEventCollector`	Модуль vSphereEventLog
`wineventlog`	Модуль WinEventLog
`WMILog`	Модуль WmiLog

Параметр	Модуль (компонент)
`WMINotification`	Модуль WmiNotification

17. Обращение в службу технической поддержки

Техническая поддержка продукта включает в себя следующие услуги:

- решение вопросов эксплуатации продукта, помощь в использовании его функциональных возможностей;
- диагностику сбоев продукта, включая поиск причины сбоя и информирование клиента о найденных проблемах;
- разрешение проблем с продуктом, предоставление решений или возможностей обойти проблему с сохранением всей необходимой производительности;
- устранение ошибок в продукте (в рамках выпуска обновлений к продукту).

Вы можете получать техническую поддержку на портале.

Этот раздел содержит информацию о способах и условиях получения технической поддержки.

В этом разделе

17.1. Техническая поддержка на портале

Портал предоставляет вам возможность создавать запросы на техническую поддержку.

Вы можете создать учетную запись на портале, используя адреса электронной почты, расположенные на официальном домене вашей организации. Вы также можете указывать другие адреса электронной почты для учетной записи в качестве дополнительных. Для оперативной связи укажите в профиле учетной записи название вашей организации и контактный телефон.

Портал содержит статьи базы знаний, новости обновлений продуктов Positive Technologies, ответы на часто задаваемые вопросы пользователей. Для доступа к базе знаний и всем новостям нужно создать на портале учетную запись.

Техническая поддержка на портале предоставляется на русском и английском языках.

17.2. Время работы службы технической поддержки

На портале технической поддержки вы можете круглосуточно создавать и обновлять запросы, читать новости продуктов и пользоваться базой знаний.

17.3. Как служба технической поддержки работает с запросами

При получении вашего запроса специалист службы технической поддержки классифицирует его (присваивает запросу тип и уровень значимости) и выполняет дальнейшие шаги по выполнению запроса.

В этом разделе

17.3.1. Предоставление информации для технической поддержки

При обращении за технической поддержкой по первому требованию специалиста Positive Technologies нужно предоставить:

— номер лицензии на использование продукта;

— файлы журналов и другие наборы диагностических данных, хранящихся в продукте;

— снимки экрана;

— результаты выполнения рекомендаций специалиста технической поддержки;

— каналы для удаленного доступа к продукту (по взаимному согласованию оптимального канала диагностики).

Positive Technologies не несет обязательств по оказанию технической поддержки в случае отказа предоставить указанную выше информацию.

Если информация по обращению не предоставлена в течение значительного времени (от двух недель с момента последней активности), специалист технической поддержки имеет право считать ваше обращение неактуальным и, уведомив вас, закрыть запрос.

17.3.2. Типы запросов

Специалист технической поддержки относит ваш запрос к одному из следующих типов.

Вопросы по установке, повторной установке и предстартовой настройке продукта

Подразумевается помощь в подготовке продукта к работе, ответы на вопросы на данном этапе эксплуатации продукта. Техническая поддержка по этим вопросам доступна в течение 30 дней с момента активации продукта.

Вопросы по администрированию и настройке продукта

Включают в себя вопросы, возникающие в процессе эксплуатации продукта, рекомендации по оптимизации и настройке параметров продукта.

Восстановление работоспособности продукта

В случае критического сбоя и потери доступа к основной функциональности продукта специалист Positive Technologies оказывает помощь в восстановлении работоспособности продукта. Восстановление заключается либо в помощи по установке продукта заново с потенциальной потерей накопленных до сбоя данных, либо в откате продукта на доступную резервную копию (резервное копирование должно быть настроено заблаговременно). Positive Technologies не несет ответственность за потерю данных в случае неверно настроенного резервного копирования.

Обновление продукта

Positive Technologies поставляет пакеты обновления в течение срока обновления, указанного в лицензии на продукт.

Positive Technologies не несет ответственности за проблемы, возникшие при нарушении регламентированного процесса обновления.

Устранение дефектов продукта

Если по результатам диагностики обнаружен дефект продукта, Positive Technologies обязуется предпринять разумные усилия по предоставлению обходного решения (если возможно), а также включить исправление дефекта в ближайшие возможные обновления продукта.

17.3.3. Время реакции и приоритизация запросов

Время реакции на запрос рассчитывается с момента получения запроса до первичного ответа специалиста технической поддержки с уведомлением о взятии запроса в работу.

Время обработки запроса рассчитывается с момента отправки уведомления о взятии вашего запроса в работу до предоставления описания дальнейших шагов по устранению проблемы либо классификации вопроса, указанного в запросе, как дефекта ПО и передачи запроса ответственным лицам для исправления дефекта.

Время реакции и время обработки зависят от указанного вами уровня значимости запроса (см. таблицу 2).

Специалист службы технической поддержки оставляет за собой право переопределять уровень значимости запроса по приведенным ниже критериям. Указанные сроки являются целевыми и подразумевают стремление и разумные усилия исполнителя для их соблюдения, но возможны отклонения от данных сроков по объективным причинам.

Таблица 2. Время реакции на запрос и время его обработки

Уровень значимости запроса	**Критерии значимости запроса**	**Время реакции на запрос**	**Время обработки запроса**
Критический	Аварийные сбои, полностью препятствующие штатной работе продукта (исключая первоначальную установку) либо оказывающие критическое влияние на бизнес	До 4 часов	Не ограничено
Высокий	Сбои, затрагивающие часть функциональности продукта и проявляющиеся в любых условиях эксплуатации либо оказывающие значительное влияние на бизнес	До 24 часов	Не ограничено
Обычный	Сбои, проявляющиеся в специфических условиях эксплуатации продукта либо не оказывающие значительного влияния на бизнес	До 24 часов	Не ограничено
Низкий	Вопросы информационного характера либо сбои, не влияющие на эксплуатацию продукта	До 24 часов	Не ограничено

Указанные часы относятся только к рабочему времени специалистов технической поддержки (времени обработки запроса).

17.3.4. Выполнение работ по запросу

По мере выполнения работ по вашему запросу специалист технической поддержки сообщает вам:

— о диагностике проблемы и ее результатах;

— о поиске решения или возможности обойти причины возникновения проблемы;

— о планировании и выпуске обновления продукта (если требуется для устранения проблемы).

Если по итогам обработки запроса необходимо внести изменения в продукт, Positive Technologies включает работы по исправлению в ближайшее возможное плановое обновление продукта (в зависимости от сложности изменений).

Работы по запросу считаются выполненными, если:

— предоставлено решение или возможность обойти проблему, не влияющая на производительность и критически важную функцию продукта;

— диагностирован дефект продукта, собрана техническая информация о дефекте и условиях его воспроизведения; исправление дефекта запланировано к выходу в рамках планового обновления продукта;

— проблема вызвана программными продуктами или оборудованием сторонних производителей, не подпадающих под гарантийные обязательства по продукту;

— проблема классифицирована как неподдерживаемая.

Приложение. Команды, выполняемые при аудите активов

Аудит активов выполняется модулем audit с профилем, выбираемым в зависимости от установленной на активе операционной системы. Для получения данных об активе на нем выполняются команды, указанные ниже. Для выполнения команд и сбора полученной информации используются порты, указанные в таблице. В параметрах профиля нужно указать учетную запись, которой предоставлены права на выполнение команд, перечисленных для актива.

Примечание. Команды могут содержать переменные, значения которых (например, пути к файлам, IP-адреса интерфейсов, номера портов) определяются и подставляются при проведении аудита. Имена переменных начинаются со знака вопроса. Вопросительные знаки в командах удваиваются для экранирования.

Таблица 3. Стандартные профили для аудита активов

Актив	Версия	Профиль	Порт по умолчанию
«Базальт СПО», «Альт СП»	8	Unix Audit	TCP 22
«Базальт СПО», «Альт Рабочая станция»	9, 10	Unix Audit	TCP 22
«РЕД СОФТ», «РЕД ОС»	7.1—7.3	Unix Audit	TCP 22
Alcatel OmniSwitch	6.4.4 [3]	SSH Network Device Audit, SNMP Network Device Audit [4]	TCP 22, UDP 162
Avaya (Nortel) NOS, серия ERS	5.1.0.015 [3]	SSH Network Device Audit, SNMP Network Device Audit [4]	TCP 22, UDP 162
Canonical Ubuntu	14.04, 16.04, 18.04	Unix Audit	TCP 22
CentOS	6, 7	Unix Audit	TCP 22
Check Point GAiA OS	76, 77.10—81.10	Checkpoint Management Server SSH Audit, Checkpoint OPSEC Audit	TCP 22, 18190

3 Указаны версии ПО, на которых производилась проверка аудита. Корректная работа аудита на других версиях не гарантируется.

4 Рекомендуется выбирать профиль для аудита по протоколу SSH. В случае блокировки доступа на актив по протоколу SSH необходимо использовать профиль для аудита по протоколу SNMP.

Актив	Версия	Профиль	Порт по умолчанию
Check Point SPLAT	R75.40[3]	SSH Network Device Audit, Checkpoint OPSEC Audit	TCP 22, 18190
Cisco ACS	5	SSH Network Device Audit, SNMP Network Device Audit[4]	TCP 22, UDP162
Cisco ADE-OS	—	SSH Network Device Audit, SNMP Network Device Audit[4]	TCP 22, UDP 162
Cisco AireOS Wireless Controller	7.4.100, 7.6.130[3]	SSH Network Device Audit	TCP 22
Cisco ASA	8, 9	SSH Cisco Audit in Enable Mode	TCP 22, UDP 162
Cisco IOS	12, 15, 16	SSH Cisco Audit in Enable Mode, SNMP Network Device Audit[4]	TCP 22, UDP 162
Cisco IOS XE	12, 15, 16	SSH Cisco Audit in Enable Mode, SNMP Network Device Audit[4]	TCP 22, UDP 162
Cisco IOS XR, серия ASR9000	4.3.4, 6.1.1, 6.4.2[3]	SSH Network Device Audit	TCP 22
Cisco ISE (Identity Services Engine)	2.3.0[3]	SSH Network Device Audit, SNMP Network Device Audit[4]	TCP 22, UDP 162
Cisco NX-OS	4—7	SSH Network Device Audit, SNMP Network Device Audit[4]	TCP 22, UDP 162
Debian	7, 8 ,9	Unix Audit	TCP 22
Eltex, маршрутизаторы серии ESR	1.4.4[3]	SSH Network Device Audit	TCP 22
Eltex, коммутаторы серий MES 1xxx, 2xxx, 3xxx, 51xx, 52xx	1.1.44, 4.0.9.3[3]	SSH Network Device Audit	TCP 22
FortiNet FortiOS	5.4.2, 6.0.1[3]	SSH Network Device Audit	TCP 22
FreeBSD	8—11	Unix Audit	TCP 22
HPE Comware Software	5, 7	SSH Network Device Audit	TCP 22
HPE UX	11.31[3]	Unix Audit	TCP 22, 23

Актив	Версия	Профиль	Порт по умолчанию
Huawei VRP, коммутаторы серии S, маршрутизаторы серий AR и NE	—	SSH Network Device Audit, SNMP Network Device Audit [4]	TCP 22, UDP 162
IBM AIX	5.3, 6.1, 7.1, 7.2	Unix Audit	TCP 22, 23
Juniper JunOS	11—19	SSH Network Device Audit, SNMP Network Device Audit [4]	TCP 22, UDP 162
Microsoft Windows	XP	Windows Audit	TCP 1025—5000 [5]
Microsoft Windows Server	2003, 2003 R2	Windows Audit	
Microsoft Windows	Vista, 7, 8, 8.1, 10	Windows Audit	TCP 135, 139, 389, 445, 636 49152—65535 [5]; UDP 135, 137, 138, 445
Microsoft Windows Server	2008, 2008 R2, 2012, 2012 R2, 2016, 2019	Windows Audit	
Oracle Linux	6, 7	Unix Audit	TCP 22
Oracle Solaris	9, 10, 11	Unix Audit	TCP 22, 23
Palo Alto Networks PAN-OS	6.1—8.1 [3]	SSH Network Device Audit	TCP 22
Qtech QSW, модели 3450-28T, 6500-52F, 8300-52F	—	SSH Network Device Audit	TCP 22
Red Hat Enterprise Linux	6—9	Unix Audit	TCP 22
SUSE Linux Enterprise Server	11, 12	Unix Audit	TCP 22
VMware vSphere Hypervisor (ESXi)	5.5, 6.0, 6.5, 6.7 [3]	vSphere Audit	TCP 443

5 Диапазон динамических портов может быть изменен в ОС.

Команды для определения ОС на активе

При проведении аудита через терминал модуль audit выполняет на активе следующие команды для определения установленной ОС:

```
- cpstat os
- display version
- esxcli system version get
- fw ver -k
- get system status
- ifconfig -a
- ip addr show
- ip address
- racadm getversion
- rpm -qa '*release*' 2>/dev/null
- show /map1
- show /map1/dnsendpt1
- show banner static
- show inventory
- show run-config
- show system
- show system info
- show system info | match model
- show version
- show version brief
- show version | no-more
- terminal length 0
- terminal pager 0
- uname
- uname -a
- uname -a > /dev/null
- uname -s
- ver
```

«Базальт СПО». «Альт 8 СП», «Альт Рабочая станция»

При проведении аудита модуль audit выполняет на активе следующие команды:

```
- /etc/init.d/?service_name status 2>/dev/null
- /sbin/blkid ?filesystem
- /sbin/runlevel 2>/dev/null
- /usr/sbin/ifconfig -a
- ?path --version
- ?path -V
- ?which_path ?command
- PATH=?path; ?which_path ?command
- arch
- arp -n
```

```
- at -l
- auditctl -l
- auditctl -v
- chkconfig --list
- df -kP
- df /
- dhcpcd --dumplease ?interface
- dhcpcd --dumplease ?interface_id
- dhcpcd --version | head -n1
- dmesg
- dmidecode
- dmidecode --string system-uuid
- docker container ls --all --no-trunc --format='{{ .ID}}' | xargs -r docker inspect
- docker image ls --all --no-trunc --format='{{json .ID}}' | uniq | xargs -r docker
    inspect
- docker info --format='{{json .}}'
- docker ps --no-trunc -f "ancestor=?image_id" --format="{{.ID}}" | head -n 1 | xargs
    -r docker inspect --format="{{.State.Pid}}"
- echo $LOGNAME
- env
- fdisk -l
- file -bL ?path
- find -H /etc/rc*.d
- find -H ?mask
- find ?path -type f -follow
- free
- getfacl --skip-base --absolute-names ?path
- |-
    gitlab-rails runner '
    class MemberForExport
      attr_accessor :id
      attr_accessor :type
      attr_accessor :access_level
    end
    class GroupForExport
      attr_accessor :id
      attr_accessor :name
      attr_accessor :full_name
      attr_accessor :full_path
      attr_accessor :visibility
      attr_accessor :parent_id
      attr_accessor :group_members
      def fill_members(group)
        @group_members = []
        group.members.each do |member|
          pm = MemberForExport.new
```

```
          pm.id = member.user_id
          pm.access_level = member.access_level
          pm.type = "User"
          @group_members << pm
        end
        group.shared_with_group_links.each do |group_member|
          pm = MemberForExport.new
          pm.id = group_member.shared_with_group_id
          pm.access_level = group_member.group_access
          pm.type = "Group"
          @group_members << pm
        end
      end
    end
    groups_for_export = []
    Group.all.each do |group|
      gr = GroupForExport.new
      gr.id = group.id
      gr.name = group.name
      gr.full_name = group.full_name
      gr.full_path = group.full_path
      gr.visibility = group.visibility
      gr.parent_id = group.parent.try(:id)
      gr.fill_members(group)
      groups_for_export << gr
    end
    puts groups_for_export.to_json
    '
- "gitlab-rails runner '\nclass
ProjectMemberForExport\n  attr_accessor :id\n  attr_accessor
    :type\n  attr_accessor :access_level\nend\n\nclass
ProjectForExport\n  attr_accessor
    :id\n  attr_accessor :name\n  attr_accessor :full_name\n  attr_accessor :full_pat
h\n
    \
attr_accessor :visibility\n  attr_accessor :owner\n  attr_accessor :project_members\n
\n
    \ def fill_members(project)\n    @owner =
ProjectMemberForExport.new\n    @owner.id
    = project.owner.id\n    @owner.access_level = 50\n    @owner.type =
project.owner.class.name\n
    \   \n    @project_members = [@owner]\n\n    project.members.each do |member|\n
    \     next if @owner.type == \"User\" && member.user_id == @owner.id\n\n      pm
    = ProjectMemberForExport.new\n      pm.id = member.user_id\n      pm.access_level
    = member.access_level\n      pm.type = \"User\"\n\n      @project_members << pm\n
    \   end\n\n    project.project_group_links.each do |group_member|\n      pm =
    ProjectMemberForExport.new\n      pm.id =
group_member.group_id\n      pm.access_level
```

```
    = group_member.group_access\n      pm.type = \"Group\"\n\n      @project_members
    << pm\n    end\n  end\nend\n\nproject_for_export = []\n\nProject.all.each do |
project|\n
    \ pr = ProjectForExport.new\n  pr.id = project.id\n  pr.name = project.name\n
    \ pr.full_name = project.full_name\n  pr.full_path =
project.full_path\n  pr.visibility
    = project.visibility\n\n  pr.fill_members(project)\n\n  project_for_export <<
    pr\nend\n\nputs project_for_export.to_json\n'"
- |-
    gitlab-rails runner '
    class SettingForExport
      attr_accessor :signup_enabled
      attr_accessor :password_authentication_enabled_for_web
      attr_accessor :password_authentication_enabled_for_git
    end
    setting = ApplicationSetting.current
    setting_for_export = SettingForExport.new
    setting_for_export.signup_enabled = setting.signup_enabled
    setting_for_export.password_authentication_enabled_for_web =
      setting.password_authentication_enabled_for_web
    setting_for_export.password_authentication_enabled_for_git =
      setting.password_authentication_enabled_for_git
    puts setting_for_export.to_json
    '
- |-
    gitlab-rails runner '
    class UserForExport
      attr_accessor :id
      attr_accessor :username
      attr_accessor :name
      attr_accessor :admin
      attr_accessor :state
      attr_accessor :otp_required_for_login
      attr_accessor :type
      attr_accessor :identities
      attr_accessor :key_fingerprints
    end
    users_for_export = []
    User.all.each do |user|
      us = UserForExport.new
      us.id = user.id
      us.username = user.username
      us.name = user.name
      us.admin = user.admin
      us.state = user.state
      us.otp_required_for_login = user.otp_required_for_login
      us.type = user.user_type
```

```
      us.identities = user.identities
      us.key_fingerprints = user.keys.map { |key| key.fingerprint }
      users_for_export << us
    end
    puts users_for_export.to_json
    '
- gitlab-rake gitlab:env:info
- host ?host_field
- hostname
- hostname -f 2>/dev/null
- hostname -s
- ifconfig -a
- initctl list
- initctl show-config
- ip -4 route show
- ip -6 route show
- ip addr show
- ip address
- ip neigh show
- iptables-save
- ls -l /dev/disk/by-uuid/
- ls -l /proc/*/exe 2>/dev/null
- ls -l ?path
- ls -lLd ?path
- ls -lZdL ?path
- lsblk -o UUID,MOUNTPOINT
- lspci
- lsusb 2>/dev/null
- lvdisplay 2>/dev/null
- mount
- netstat -vpntua 2>/dev/null
- networkctl list
- nmcli connection show ?interface_id
- nsenter -t ?container_pid -m /bin/cat /etc/SuSE-release
- nsenter -t ?container_pid -m /bin/cat /etc/centos-release
- nsenter -t ?container_pid -m /bin/cat /etc/debian_version
- nsenter -t ?container_pid -m /bin/cat /etc/enterprise-release
- nsenter -t ?container_pid -m /bin/cat /etc/lsb-release
- nsenter -t ?container_pid -m /bin/cat /etc/oracle-release
- nsenter -t ?container_pid -m /bin/cat /etc/os-release
- nsenter -t ?container_pid -m /bin/cat /etc/redhat-release
- nsenter -t ?container_pid -m rpm -qa '*release*' 2>/dev/null
- pargs ?pid
- pgrep -l -x 'dhclient|systemd-network|NetworkManager|dhcpcd|wickedd-dhcp4'
- ps -e -o pid,ppid,tty,user,group,etime,comm
- ps -eo lstart -o ";%p;%P;%U;%G;%y;" -o label -o ";%c;%a"
```

```
- pvdisplay 2>/dev/null
- rpm -qa '*release*' 2>/dev/null
- rpm -qa --qf '%{NAME}|%{EPOCH}:%{VERSION}-%{RELEASE}\n' | sed 's/(none)/0/g'
- rpm -qf --qf '%{NAME}\n' ?path 2>/dev/null
- ss -tupan 2>/dev/null
- sysctl -a
- systemctl get-default
- systemctl list-unit-files -t target --no-pager --no-legend
- systemctl list-units -a --type target --no-pager --no-legend
- systemctl list-units -t service --all --no-pager --no-legend
- test -d ?path; echo $??
- test -e /proc/self/status && cat /proc/self/status
- test -e ?path; echo $??
- test -f ?path; echo $??
- uname
- uname -m
- uname -n
- uname -p
- uname -r
- uname -s
- vgdisplay 2>/dev/null
- who -r
- wicked test dhcp4 ?interface_id
```

«РЕД СОФТ» «РЕД ОС»

При проведении аудита модуль audit выполняет на активе следующие команды:

```
- |4
    ls -1tr /var/lib/{dhcp,dhclient}/dhclient*.lease* 2>/dev/null |
    xargs cat 2>/dev/null | awk '
    BEGIN {block = ""; do_flag = 0; ifname = "";} {
        if ($0 ~ /\}/) {
            do_flag = 0;
            if (ifname) lease_arr[ifname] = block;
        }
        if (do_flag) {
            block = (block "\n" $0);
            if ($0 ~ /^[[:space:]]*interface[[:space:]]+".*";/) {
                ifname = gensub(/^[^"]*"|";.*/, "", "g", $0);
            }
        }
        if ($0 ~ /^lease/) {
            do_flag = 1;
            block = "";
        }
    }
```

```
    END {
        for (i in lease_arr) {
            print lease_arr[i];
        }
    }'
- /etc/init.d/?service_name status 2>/dev/null
- /sbin/blkid ?filesystem
- /sbin/runlevel 2>/dev/null
- /usr/sbin/ifconfig -a
- ?path --version
- ?path -V
- ?which_path ?command
- PATH=?path; ?which_path ?command
- arch
- arp -n
- at -l
- auditctl -l
- auditctl -v
- chkconfig --list
- df -kP
- df /
- dhcpcd --dumplease ?interface_id
- dhcpcd --version | head -n1
- dmesg
- dmidecode
- dmidecode --string system-uuid
- docker container ls --all --no-trunc --format='{{ .ID}}' | xargs -r docker inspect
- docker image ls --all --no-trunc --format='{{json .ID}}' | uniq | xargs -r docker
    inspect
- docker info --format='{{json .}}'
- docker ps --no-trunc -f "ancestor=?image_id" --format="{{.ID}}" | head -n 1 | xargs
    -r docker inspect --format="{{.State.Pid}}"
- echo $LOGNAME
- egrep -i 'ORA_HOME|ORACLE_HOME' /etc/rc*/* /etc/init.d/* /home/*/.oraenv /home/
*/.bash_profile
    -s -l 2>/dev/null
- env
- fdisk -l
- file -bL ?path
- find -H /etc/rc*.d
- find -H ?mask
- find ?oracle_home/dbs -type f \( -iname 'init*.ora' ! -iname 'init.ora' \)
- find ?oracle_home/dbs -type f \( -iname 'spfile*.ora' \)
- find ?path -type f -follow
- free
- getfacl --skip-base --absolute-names ?path
```

```
- |-
    gitlab-rails runner '
    class MemberForExport
      attr_accessor :id
      attr_accessor :type
      attr_accessor :access_level
    end
    class GroupForExport
      attr_accessor :id
      attr_accessor :name
      attr_accessor :full_name
      attr_accessor :full_path
      attr_accessor :visibility
      attr_accessor :parent_id
      attr_accessor :group_members
      def fill_members(group)
        @group_members = []
        group.members.each do |member|
          pm = MemberForExport.new
          pm.id = member.user_id
          pm.access_level = member.access_level
          pm.type = "User"
          @group_members << pm
        end
        group.shared_with_group_links.each do |group_member|
          pm = MemberForExport.new
          pm.id = group_member.shared_with_group_id
          pm.access_level = group_member.group_access
          pm.type = "Group"
          @group_members << pm
        end
      end
    end
    groups_for_export = []
    Group.all.each do |group|
      gr = GroupForExport.new
      gr.id = group.id
      gr.name = group.name
      gr.full_name = group.full_name
      gr.full_path = group.full_path
      gr.visibility = group.visibility
      gr.parent_id = group.parent.try(:id)
      gr.fill_members(group)
      groups_for_export << gr
    end
    puts groups_for_export.to_json
```

```
    '
- "gitlab-rails runner '\nclass
ProjectMemberForExport\n  attr_accessor :id\n  attr_accessor
    :type\n  attr_accessor :access_level\nend\n\nclass
ProjectForExport\n  attr_accessor
    :id\n  attr_accessor :name\n  attr_accessor :full_name\n  attr_accessor :full_pat
h\n
    \
attr_accessor :visibility\n  attr_accessor :owner\n  attr_accessor :project_members\n
\n
    \ def fill_members(project)\n    @owner =
ProjectMemberForExport.new\n    @owner.id
    = project.owner.id\n    @owner.access_level = 50\n    @owner.type =
project.owner.class.name\n
    \   \n    @project_members = [@owner]\n\n    project.members.each do |member|\n
    \     next if @owner.type == \"User\" && member.user_id == @owner.id\n\n      pm
    = ProjectMemberForExport.new\n      pm.id = member.user_id\n      pm.access_level
    = member.access_level\n      pm.type = \"User\"\n\n      @project_members << pm\n
    \   end\n\n    project.project_group_links.each do |group_member|\n      pm =
    ProjectMemberForExport.new\n      pm.id =
group_member.group_id\n      pm.access_level
    = group_member.group_access\n      pm.type = \"Group\"\n\n      @project_members
    << pm\n    end\n  end\nend\n\nproject_for_export = []\n\nProject.all.each do |
project|\n
    \ pr = ProjectForExport.new\n  pr.id = project.id\n  pr.name = project.name\n
    \ pr.full_name = project.full_name\n  pr.full_path =
project.full_path\n  pr.visibility
    = project.visibility\n\n  pr.fill_members(project)\n\n  project_for_export <<
    pr\nend\n\nputs project_for_export.to_json\n'"
- |-
    gitlab-rails runner '
    class SettingForExport
      attr_accessor :signup_enabled
      attr_accessor :password_authentication_enabled_for_web
      attr_accessor :password_authentication_enabled_for_git
    end
    setting = ApplicationSetting.current
    setting_for_export = SettingForExport.new
    setting_for_export.signup_enabled = setting.signup_enabled
    setting_for_export.password_authentication_enabled_for_web =
      setting.password_authentication_enabled_for_web
    setting_for_export.password_authentication_enabled_for_git =
      setting.password_authentication_enabled_for_git
    puts setting_for_export.to_json
    '
- |-
    gitlab-rails runner '
    class UserForExport
```

```
      attr_accessor :id
      attr_accessor :username
      attr_accessor :name
      attr_accessor :admin
      attr_accessor :state
      attr_accessor :otp_required_for_login
      attr_accessor :type
      attr_accessor :identities
      attr_accessor :key_fingerprints
    end
    users_for_export = []
    User.all.each do |user|
      us = UserForExport.new
      us.id = user.id
      us.username = user.username
      us.name = user.name
      us.admin = user.admin
      us.state = user.state
      us.otp_required_for_login = user.otp_required_for_login
      us.type = user.user_type
      us.identities = user.identities
      us.key_fingerprints = user.keys.map { |key| key.fingerprint }
      users_for_export << us
    end
    puts users_for_export.to_json
    '
- gitlab-rake gitlab:env:info
- grubby --info ALL
- host ?host_field
- hostname
- hostname -f 2>/dev/null
- hostname -s
- ifconfig -a
- initctl list
- initctl show-config
- ip -4 route show
- ip -6 route show
- ip addr show
- ip address
- ip neigh show
- iptables-save
- ls -l /dev/disk/by-uuid/
- ls -l /proc/*/exe 2>/dev/null
- ls -l ?path
- ls -lLd ?path
- ls -lZdL ?path
```

```
- lsblk -o UUID,MOUNTPOINT
- lsnrctl status
- lspci
- lsusb 2>/dev/null
- lvdisplay 2>/dev/null
- mount
- netstat -vpntua 2>/dev/null
- networkctl list
- nmcli connection show ?interface_id
- nsenter -t ?container_pid -m /bin/cat /etc/SuSE-release
- nsenter -t ?container_pid -m /bin/cat /etc/centos-release
- nsenter -t ?container_pid -m /bin/cat /etc/debian_version
- nsenter -t ?container_pid -m /bin/cat /etc/enterprise-release
- nsenter -t ?container_pid -m /bin/cat /etc/lsb-release
- nsenter -t ?container_pid -m /bin/cat /etc/oracle-release
- nsenter -t ?container_pid -m /bin/cat /etc/os-release
- nsenter -t ?container_pid -m /bin/cat /etc/redhat-release
- nsenter -t ?container_pid -m rpm -qa '*release*' 2>/dev/null
- pargs ?pid
- pgrep -l -x 'dhclient|systemd-network|NetworkManager|dhcpcd|wickedd-dhcp4'
- ps -e -o pid,ppid,tty,user,group,etime,comm
- ps -ef
- ps -eo lstart -o ";%p;%P;%U;%G;%y;" -o label -o ";%c;%a"
- pvdisplay 2>/dev/null
- rpm -qa '*release*' 2>/dev/null
- rpm -qa --qf 'Name=%{NAME}\nEpoch=%{EPOCH}\nVersion=%{VERSION}\nRelease=%{RELEASE}
\n\n'
    |  sed 's/(none)://g'
- rpm -qf --qf '%{NAME}\n' ?path
- ss -tupan 2>/dev/null
- sysctl -a
- systemctl get-default
- systemctl list-unit-files -t target --no-pager --no-legend
- systemctl list-units -a --type target --no-pager --no-legend
- systemctl list-units -t service --all --no-pager --no-legend
- test -d ?path; echo $??
- test -e /proc/self/status && cat /proc/self/status
- test -e ?path; echo $??
- test -f ?path; echo $??
- uname
- uname -m
- uname -n
- uname -p
- uname -r
- uname -s
- vgdisplay 2>/dev/null
```

```
- who -r
- wicked test dhcp4 ?interface_id
```

Alcatel-Lucent AOS

При проведении аудита модуль audit выполняет на активе следующие команды:

```
- show arp
- show chassis
- show configuration snapshot
- show interfaces
- show interfaces flood rate
- show interfaces port
- show interfaces status
- show ip bgp
- show ip helper dhcp-snooping port
- show ip interface
- show ip managed-interface
- show ip ospf
- show ip route
- show ip service
- show lldp config
- show mac-address-table
- show port-security
- show session config
- show swlog
- show system
- show user
- show vlan port
- show vlan router mac status
```

Astra Linux Common Edition

При проведении аудита модуль audit выполняет на активе следующие команды:

```
- /etc/init.d/?service_name status 2>/dev/null
- /sbin/blkid ?filesystem
- /sbin/runlevel 2>/dev/null
- /usr/sbin/ifconfig -a
- ?path --version
- ?path -V
- ?which_path ?command
- PATH=?path; ?which_path ?command
- arch
- arp -n
- at -l
- auditctl -l
- auditctl -v
```

```
- chkconfig --list
- df -kP
- df /
- dhcpcd --dumplease ?interface_id
- dhcpcd --version | head -n1
- dmesg
- dmidecode
- dmidecode --string system-uuid
- docker container ls --all --no-trunc --format='{{ .ID}}' | xargs -r docker inspect
- docker image ls --all --no-trunc --format='{{json .ID}}' | uniq | xargs -r docker
    inspect
- docker info --format='{{json .}}'
- docker ps --no-trunc -f "ancestor=?image_id" --format="{{.ID}}" | head -n 1 | xargs
    -r docker inspect --format="{{.State.Pid}}"
- dpkg -S ?path
- dpkg-query --show  -f='${Package}\t${Version}\n'  2>/dev/null
- echo $LOGNAME
- env
- fdisk -l
- file -bL ?path
- find -H /etc/rc*.d
- find -H ?mask
- find ?path -type f -follow
- free
- getfacl --skip-base --absolute-names ?path
- |-
    gitlab-rails runner '
    class MemberForExport
      attr_accessor :id
      attr_accessor :type
      attr_accessor :access_level
    end
    class GroupForExport
      attr_accessor :id
      attr_accessor :name
      attr_accessor :full_name
      attr_accessor :full_path
      attr_accessor :visibility
      attr_accessor :parent_id
      attr_accessor :group_members
      def fill_members(group)
        @group_members = []
        group.members.each do |member|
          pm = MemberForExport.new
          pm.id = member.user_id
          pm.access_level = member.access_level
```

```
          pm.type = "User"
          @group_members << pm
        end
        group.shared_with_group_links.each do |group_member|
          pm = MemberForExport.new
          pm.id = group_member.shared_with_group_id
          pm.access_level = group_member.group_access
          pm.type = "Group"
          @group_members << pm
        end
      end
    end
    groups_for_export = [
    Group.all.each do |group|
      gr = GroupForExport.new
      gr.id = group.id
      gr.name = group.name
      gr.full_name = group.full_name
      gr.full_path = group.full_path
      gr.visibility = group.visibility
      gr.parent_id = group.parent.try(:id)
      gr.fill_members(group)
      groups_for_export << gr
    end
    puts groups_for_export.to_json
    '
- "gitlab-rails runner '\nclass
ProjectMemberForExport\n  attr_accessor :id\n  attr_accessor
    :type\n  attr_accessor :access_level\nend\n\nclass
ProjectForExport\n  attr_accessor
    :id\n  attr_accessor :name\n  attr_accessor :full_name\n  attr_accessor :full_pat
h\n
    \
attr_accessor :visibility\n  attr_accessor :owner\n  attr_accessor :project_members\n
\n
    \ def fill_members(project)\n    @owner =
ProjectMemberForExport.new\n    @owner.id
    = project.owner.id\n    @owner.access_level = 50\n    @owner.type =
project.owner.class.name\n
    \   \n    @project_members = [@owner]\n\n    project.members.each do |member|\n
    \     next if @owner.type == \"User\" && member.user_id == @owner.id\n\n      pm
    = ProjectMemberForExport.new\n      pm.id = member.user_id\n      pm.access_level
    = member.access_level\n      pm.type = \"User\"\n\n      @project_members << pm\n
    \   end\n\n    project.project_group_links.each do |group_member|\n      pm =
    ProjectMemberForExport.new\n      pm.id =
group_member.group_id\n      pm.access_level
    = group_member.group_access\n      pm.type = \"Group\"\n\n      @project_members
```

```
    << pm\n    end\n  end\nend\n\nproject_for_export = []\n\nProject.all.each do |
project|\n
    \ pr = ProjectForExport.new\n  pr.id = project.id\n  pr.name = project.name\n
    \ pr.full_name = project.full_name\n  pr.full_path =
project.full_path\n  pr.visibility
    = project.visibility\n\n  pr.fill_members(project)\n\n  project_for_export <<
    pr\nend\n\nputs project_for_export.to_json\n'"
- |-
    gitlab-rails runner '
    class SettingForExport
      attr_accessor :signup_enabled
      attr_accessor :password_authentication_enabled_for_web
      attr_accessor :password_authentication_enabled_for_git
    end
    setting = ApplicationSetting.current
    setting_for_export = SettingForExport.new
    setting_for_export.signup_enabled = setting.signup_enabled
    setting_for_export.password_authentication_enabled_for_web =
      setting.password_authentication_enabled_for_web
    setting_for_export.password_authentication_enabled_for_git =
      setting.password_authentication_enabled_for_git
    puts setting_for_export.to_json
    '
- |-
    gitlab-rails runner '
    class UserForExport
      attr_accessor :id
      attr_accessor :username
      attr_accessor :name
      attr_accessor :admin
      attr_accessor :state
      attr_accessor :otp_required_for_login
      attr_accessor :type
      attr_accessor :identities
      attr_accessor :key_fingerprints
    end
    users_for_export = []
    User.all.each do |user|
      us = UserForExport.new
      us.id = user.id
      us.username = user.username
      us.name = user.name
      us.admin = user.admin
      us.state = user.state
      us.otp_required_for_login = user.otp_required_for_login
      us.type = user.user_type
      us.identities = user.identities
```

```
      us.key_fingerprints = user.keys.map { |key| key.fingerprint }
      users_for_export << us
    end
    puts users_for_export.to_json
    '
- gitlab-rake gitlab:env:info
- host ?host_field
- hostname
- hostname -f 2>/dev/null
- hostname -s
- ifconfig -a
- initctl list
- initctl show-config
- ip -4 route show
- ip -6 route show
- ip addr show
- ip address
- ip neigh show
- iptables-save
- ls -l /dev/disk/by-uuid/
- ls -l /proc/*/exe 2>/dev/null
- ls -l ?path
- ls -lLd ?path
- ls -lZdL ?path
- lsblk -o UUID,MOUNTPOINT
- lspci
- lsusb 2>/dev/null
- lvdisplay 2>/dev/null
- mount
- netstat -vpntua 2>/dev/null
- networkctl list
- nmcli connection show ?interface_id
- nsenter -t ?container_pid -m /bin/cat /etc/SuSE-release
- nsenter -t ?container_pid -m /bin/cat /etc/centos-release
- nsenter -t ?container_pid -m /bin/cat /etc/debian_version
- nsenter -t ?container_pid -m /bin/cat /etc/enterprise-release
- nsenter -t ?container_pid -m /bin/cat /etc/lsb-release
- nsenter -t ?container_pid -m /bin/cat /etc/oracle-release
- nsenter -t ?container_pid -m /bin/cat /etc/os-release
- nsenter -t ?container_pid -m /bin/cat /etc/redhat-release
- nsenter -t ?container_pid -m rpm -qa '*release*' 2>/dev/null
- pargs ?pid
- pgrep -l -x 'dhclient|systemd-network|NetworkManager|dhcpcd|wickedd-dhcp4'
- ps -e -o pid,ppid,tty,user,group,etime,comm
- ps -eo lstart -o ";%p;%P;%U;%G;%y;" -o label -o ";%c;%a"
- pvdisplay 2>/dev/null
```

```
- rpm -qa '*release*' 2>/dev/null
- ss -tupan 2>/dev/null
- sysctl -a
- systemctl get-default
- systemctl list-unit-files -t target --no-pager --no-legend
- systemctl list-units -a --type target --no-pager --no-legend
- systemctl list-units -t service --all --no-pager --no-legend
- test -d ?path; echo $??
- test -e /proc/self/status && cat /proc/self/status
- test -e ?path; echo $??
- test -f ?path; echo $??
- uname
- uname -i
- uname -m
- uname -n
- uname -p
- uname -r
- uname -s
- vgdisplay 2>/dev/null
- who -r
- wicked test dhcp4 ?interface_id
```

Astra Linux Special Edition

При проведении аудита модуль audit выполняет на активе следующие команды:

```
- /etc/init.d/?service_name status 2>/dev/null
- /sbin/blkid ?filesystem
- /sbin/runlevel 2>/dev/null
- /usr/sbin/ifconfig -a
- ?path --version
- ?path -V
- ?which_path ?command
- PATH=?path; ?which_path ?command
- arch
- arp -n
- at -l
- auditctl -l
- auditctl -v
- chkconfig --list
- df -kP
- df /
- dhcpcd --dumplease ?interface_id
- dhcpcd --version | head -n1
- dmesg
- dmidecode
- dmidecode --string system-uuid
```

```
- docker container ls --all --no-trunc --format='{{ .ID}}' | xargs -r docker inspect
- docker image ls --all --no-trunc --format='{{json .ID}}' | uniq | xargs -r docker
    inspect
- docker info --format='{{json .}}'
- docker ps --no-trunc -f "ancestor=?image_id" --format="{{.ID}}" | head -n 1 | xargs
    -r docker inspect --format="{{.State.Pid}}"
- dpkg -S ?path
- dpkg-query --show  -f='${Package}\t${Version}\n'  2>/dev/null
- echo $LOGNAME
- env
- fdisk -l
- file -bL ?path
- find -H /etc/rc*.d
- find -H ?mask
- find ?path -type f -follow
- free
- getfacl --skip-base --absolute-names ?path
- |-
    gitlab-rails runner '
    class MemberForExport
      attr_accessor :id
      attr_accessor :type
      attr_accessor :access_level
    end
    class GroupForExport
      attr_accessor :id
      attr_accessor :name
      attr_accessor :full_name
      attr_accessor :full_path
      attr_accessor :visibility
      attr_accessor :parent_id
      attr_accessor :group_members
      def fill_members(group)
        @group_members = []
        group.members.each do |member|
          pm = MemberForExport.new
          pm.id = member.user_id
          pm.access_level = member.access_level
          pm.type = "User"
          @group_members << pm
        end
        group.shared_with_group_links.each do |group_member|
          pm = MemberForExport.new
          pm.id = group_member.shared_with_group_id
          pm.access_level = group_member.group_access
          pm.type = "Group"
```

```
          @group_members << pm
        end
      end
    end
    groups_for_export = []
    Group.all.each do |group|
      gr = GroupForExport.new
      gr.id = group.id
      gr.name = group.name
      gr.full_name = group.full_name
      gr.full_path = group.full_path
      gr.visibility = group.visibility
      gr.parent_id = group.parent.try(:id)
      gr.fill_members(group)
      groups_for_export << gr
    end
    puts groups_for_export.to_json
    '
- "gitlab-rails runner '\nclass
ProjectMemberForExport\n  attr_accessor :id\n  attr_accessor
    :type\n  attr_accessor :access_level\nend\n\nclass
ProjectForExport\n  attr_accessor
    :id\n  attr_accessor :name\n  attr_accessor :full_name\n  attr_accessor :full_pat
h\n
    \
attr_accessor :visibility\n  attr_accessor :owner\n  attr_accessor :project_members\n
\n
    \ def fill_members(project)\n    @owner =
ProjectMemberForExport.new\n    @owner.id
    = project.owner.id\n    @owner.access_level = 50\n    @owner.type =
project.owner.class.name\n
    \   \n    @project_members = [@owner]\n\n    project.members.each do |member|\n
    \     next if @owner.type == \"User\" && member.user_id == @owner.id\n\n      pm
    = ProjectMemberForExport.new\n      pm.id = member.user_id\n      pm.access_level
    = member.access_level\n      pm.type = \"User\"\n\n      @project_members << pm\n
    \   end\n\n    project.project_group_links.each do |group_member|\n      pm =
    ProjectMemberForExport.new\n      pm.id =
group_member.group_id\n      pm.access_level
    = group_member.group_access\n      pm.type = \"Group\"\n\n      @project_members
    << pm\n    end\n  end\nend\n\nproject_for_export = []\n\nProject.all.each do |
project|\n
    \ pr = ProjectForExport.new\n  pr.id = project.id\n  pr.name = project.name\n
    \ pr.full_name = project.full_name\n  pr.full_path =
project.full_path\n  pr.visibility
    = project.visibility\n\n  pr.fill_members(project)\n\n  project_for_export <<
    pr\nend\n\nputs project_for_export.to_json\n'"
- |-
    gitlab-rails runner '
```

```
    class SettingForExport
      attr_accessor :signup_enabled
      attr_accessor :password_authentication_enabled_for_web
      attr_accessor :password_authentication_enabled_for_git
    end
    setting = ApplicationSetting.current
    setting_for_export = SettingForExport.new
    setting_for_export.signup_enabled = setting.signup_enabled
    setting_for_export.password_authentication_enabled_for_web =
      setting.password_authentication_enabled_for_web
    setting_for_export.password_authentication_enabled_for_git =
      setting.password_authentication_enabled_for_git
    puts setting_for_export.to_json
    '
- |-
    gitlab-rails runner '
    class UserForExport
      attr_accessor :id
      attr_accessor :username
      attr_accessor :name
      attr_accessor :admin
      attr_accessor :state
      attr_accessor :otp_required_for_login
      attr_accessor :type
      attr_accessor :identities
      attr_accessor :key_fingerprints
    end
    users_for_export = []
    User.all.each do |user|
      us = UserForExport.new
      us.id = user.id
      us.username = user.username
      us.name = user.name
      us.admin = user.admin
      us.state = user.state
      us.otp_required_for_login = user.otp_required_for_login
      us.type = user.user_type
      us.identities = user.identities
      us.key_fingerprints = user.keys.map { |key| key.fingerprint }
      users_for_export << us
    end
    puts users_for_export.to_json
    '
- gitlab-rake gitlab:env:info
- host ?host_field
- hostname
```

```
- hostname -f 2>/dev/null
- hostname -s
- ifconfig -a
- initctl list
- initctl show-config
- ip -4 route show
- ip -6 route show
- ip addr show
- ip address
- ip neigh show
- iptables-save
- ls -l /dev/disk/by-uuid/
- ls -l /proc/*/exe 2>/dev/null
- ls -l ?path
- ls -lLd ?path
- ls -lZdL ?path
- lsblk -o UUID,MOUNTPOINT
- lspci
- lsusb 2>/dev/null
- lvdisplay 2>/dev/null
- mount
- netstat -vpntua 2>/dev/null
- networkctl list
- nmcli connection show ?interface_id
- nsenter -t ?container_pid -m /bin/cat /etc/SuSE-release
- nsenter -t ?container_pid -m /bin/cat /etc/centos-release
- nsenter -t ?container_pid -m /bin/cat /etc/debian_version
- nsenter -t ?container_pid -m /bin/cat /etc/enterprise-release
- nsenter -t ?container_pid -m /bin/cat /etc/lsb-release
- nsenter -t ?container_pid -m /bin/cat /etc/oracle-release
- nsenter -t ?container_pid -m /bin/cat /etc/os-release
- nsenter -t ?container_pid -m /bin/cat /etc/redhat-release
- nsenter -t ?container_pid -m rpm -qa '*release*' 2>/dev/null
- pargs ?pid
- pgrep -l -x 'dhclient|systemd-network|NetworkManager|dhcpcd|wickedd-dhcp4'
- ps -e -o pid,ppid,tty,user,group,etime,comm
- ps -eo lstart -o ";%p;%P;%U;%G;%y;" -o label -o ";%c;%a"
- pvdisplay 2>/dev/null
- rpm -qa '*release*' 2>/dev/null
- ss -tupan 2>/dev/null
- sysctl -a
- systemctl get-default
- systemctl list-unit-files -t target --no-pager --no-legend
- systemctl list-units -a --type target --no-pager --no-legend
- systemctl list-units -t service --all --no-pager --no-legend
- test -d ?path; echo $??
```

```
- test -e /proc/self/status && cat /proc/self/status
- test -e ?path; echo $??
- test -f ?path; echo $??
- uname
- uname -i
- uname -m
- uname -n
- uname -p
- uname -r
- uname -s
- vgdisplay 2>/dev/null
- who -r
- wicked test dhcp4 ?interface_id
```

Avaya (Nortel) NOS

При проведении аудита модуль audit выполняет на активе следующие команды:

```
- show arp
- show banner static
- show http-port
- show interfaces
- show interfaces name
- show ip route
- show ip routing
- show ipv6 global
- show lacp port
- show mac-address-table vid ?vlan_id
- show mac-security config
- show mac-security mac-address-table
- show mac-security port
- show mac-security security-lists
- show mlt
- show running-config
- show snmp-server user
- show snmp-server view
- show sntp
- show ssh global
- show ssl
- show sys-info
- show telnet-access
- show vlan
- show vlan interface info
- show vlan ip
- show web-server
```

Canonical Ubuntu

При проведении аудита модуль audit выполняет на активе следующие команды:

```
- /etc/init.d/?service_name status 2>/dev/null
- /sbin/blkid ?filesystem
- /sbin/runlevel 2>/dev/null
- /usr/sbin/ifconfig -a
- ?path --version
- ?path -V
- ?which_path ?command
- PATH=?path; ?which_path ?command
- arch
- arp -n
- at -l
- auditctl -l
- auditctl -v
- chkconfig --list
- df -kP
- df /
- dhcpcd --dumplease ?interface_id
- dhcpcd --version | head -n1
- dmesg
- dmidecode
- dmidecode --string system-uuid
- docker container ls --all --no-trunc --format='{{ .ID}}' | xargs -r docker inspect
- docker image ls --all --no-trunc --format='{{json .ID}}' | uniq | xargs -r docker
    inspect
- docker info --format='{{json .}}'
- docker ps --no-trunc -f "ancestor=?image_id" --format="{{.ID}}" | head -n 1 | xargs
    -r docker inspect --format="{{.State.Pid}}"
- dpkg -S ?path
- dpkg -l
- dpkg-query --show  -f='${Package}\t${Version}\n'  2>/dev/null
- echo $LOGNAME
- env
- fdisk -l
- file -bL ?path
- find -H /etc/rc*.d
- find -H ?mask
- find ?path -type f -follow
- free
- getfacl --skip-base --absolute-names ?path
- |-
    gitlab-rails runner '
    class MemberForExport
      attr_accessor :id
```

```
      attr_accessor :type
      attr_accessor :access_level
    end
    class GroupForExport
      attr_accessor :id
      attr_accessor :name
      attr_accessor :full_name
      attr_accessor :full_path
      attr_accessor :visibility
      attr_accessor :parent_id
      attr_accessor :group_members
      def fill_members(group)
        @group_members = []
        group.members.each do |member|
          pm = MemberForExport.new
          pm.id = member.user_id
          pm.access_level = member.access_level
          pm.type = "User"
          @group_members << pm
        end
        group.shared_with_group_links.each do |group_member|
          pm = MemberForExport.new
          pm.id = group_member.shared_with_group_id
          pm.access_level = group_member.group_access
          pm.type = "Group"
          @group_members << pm
        end
      end
    end
    groups_for_export = []
    Group.all.each do |group|
      gr = GroupForExport.new
      gr.id = group.id
      gr.name = group.name
      gr.full_name = group.full_name
      gr.full_path = group.full_path
      gr.visibility = group.visibility
      gr.parent_id = group.parent.try(:id)
      gr.fill_members(group)
      groups_for_export << gr
    end
    puts groups_for_export.to_json
    '
- "gitlab-rails runner '\nclass
ProjectMemberForExport\n  attr_accessor :id\n  attr_accessor
    :type\n  attr_accessor :access_level\nend\n\nclass
ProjectForExport\n  attr_accessor
```

```
    :id\n  attr_accessor :name\n  attr_accessor :full_name\n  attr_accessor :full_pat
h\n
    \
attr_accessor :visibility\n  attr_accessor :owner\n  attr_accessor :project_members\n
\n
    \ def fill_members(project)\n    @owner =
ProjectMemberForExport.new\n    @owner.id
    = project.owner.id\n    @owner.access_level = 50\n    @owner.type =
project.owner.class.name\n
    \   \n    @project_members = [@owner]\n\n    project.members.each do |member|\n
    \     next if @owner.type == \"User\" && member.user_id == @owner.id\n\n      pm
    = ProjectMemberForExport.new\n      pm.id = member.user_id\n      pm.access_level
    = member.access_level\n      pm.type = \"User\"\n\n      @project_members << pm\n
    \   end\n\n    project.project_group_links.each do |group_member|\n      pm =
    ProjectMemberForExport.new\n      pm.id =
group_member.group_id\n      pm.access_level
    = group_member.group_access\n      pm.type = \"Group\"\n\n      @project_members
    << pm\n    end\n  end\nend\n\nproject_for_export = []\n\nProject.all.each do |
project|\n
    \ pr = ProjectForExport.new\n  pr.id = project.id\n  pr.name = project.name\n
    \ pr.full_name = project.full_name\n  pr.full_path =
project.full_path\n  pr.visibility
    = project.visibility\n\n  pr.fill_members(project)\n\n  project_for_export <<
    pr\nend\n\nputs project_for_export.to_json\n'"
- |-
    gitlab-rails runner '
    class SettingForExport
      attr_accessor :signup_enabled
      attr_accessor :password_authentication_enabled_for_web
      attr_accessor :password_authentication_enabled_for_git
    end
    setting = ApplicationSetting.current
    setting_for_export = SettingForExport.new
    setting_for_export.signup_enabled = setting.signup_enabled
    setting_for_export.password_authentication_enabled_for_web =
      setting.password_authentication_enabled_for_web
    setting_for_export.password_authentication_enabled_for_git =
      setting.password_authentication_enabled_for_git
    puts setting_for_export.to_json
    '
- |-
    gitlab-rails runner '
    class UserForExport
      attr_accessor :id
      attr_accessor :username
      attr_accessor :name
      attr_accessor :admin
      attr_accessor :state
```

```
      attr_accessor :otp_required_for_login
      attr_accessor :type
      attr_accessor :identities
      attr_accessor :key_fingerprints
    end
    users_for_export = []
    User.all.each do |user|
      us = UserForExport.new
      us.id = user.id
      us.username = user.username
      us.name = user.name
      us.admin = user.admin
      us.state = user.state
      us.otp_required_for_login = user.otp_required_for_login
      us.type = user.user_type
      us.identities = user.identities
      us.key_fingerprints = user.keys.map { |key| key.fingerprint }
      users_for_export << us
    end
    puts users_for_export.to_json
    '
  - gitlab-rake gitlab:env:info
  - host ?host_field
  - hostname
  - hostname -f 2>/dev/null
  - hostname -s
  - ifconfig -a
  - initctl list
  - initctl show-config
  - ip -4 route show
  - ip -6 route show
  - ip addr show
  - ip address
  - ip neigh show
  - iptables-save
  - ls -1 -Q ?path
  - ls -l /dev/disk/by-uuid/
  - ls -l /proc/*/exe 2>/dev/null
  - ls -l ?path
  - ls -lLd ?path
  - ls -lZdL ?path
  - lsblk -o UUID,MOUNTPOINT
  - lspci
  - lsusb 2>/dev/null
  - lvdisplay 2>/dev/null
  - mount
```

```
- netstat -vpntua 2>/dev/null
- networkctl list
- nmcli connection show ?interface_id
- nsenter -t ?container_pid -m /bin/cat /etc/SuSE-release
- nsenter -t ?container_pid -m /bin/cat /etc/centos-release
- nsenter -t ?container_pid -m /bin/cat /etc/debian_version
- nsenter -t ?container_pid -m /bin/cat /etc/enterprise-release
- nsenter -t ?container_pid -m /bin/cat /etc/lsb-release
- nsenter -t ?container_pid -m /bin/cat /etc/oracle-release
- nsenter -t ?container_pid -m /bin/cat /etc/os-release
- nsenter -t ?container_pid -m /bin/cat /etc/redhat-release
- nsenter -t ?container_pid -m rpm -qa '*release*' 2>/dev/null
- openvpn --version
- pargs ?pid
- pgrep -l -x 'dhclient|systemd-network|NetworkManager|dhcpcd|wickedd-dhcp4'
- ps -e -o pid,ppid,tty,user,group,etime,comm
- ps -eo lstart -o ";%p;%P;%U;%G;%y;" -o label -o ";%c;%a"
- pvdisplay 2>/dev/null
- rpm -qa '*release*' 2>/dev/null
- ss -tupan 2>/dev/null
- stat -L ?filepath
- sysctl -a
- systemctl cat openvpn-server@.service
- systemctl cat openvpn@.service
- systemctl get-default
- systemctl list-unit-files -t target --no-pager --no-legend
- systemctl list-units -a --type target --no-pager --no-legend
- systemctl list-units -t service --all --no-pager --no-legend
- systemctl status openvpn*
- test -d ?path; echo $??
- test -e /proc/self/status && cat /proc/self/status
- test -e ?path; echo $??
- test -f ?path; echo $??
- uname
- uname -i
- uname -m
- uname -n
- uname -p
- uname -r
- uname -s
- uname -v
- vgdisplay 2>/dev/null
- who -r
- wicked test dhcp4 ?interface_id
```

CentOS

При проведении аудита модуль audit выполняет на активе следующие команды:

```
- |4
    ls -1tr /var/lib/{dhcp,dhclient}/dhclient*.lease* 2>/dev/null |
    xargs cat 2>/dev/null | awk '
    BEGIN {block = ""; do_flag = 0; ifname = "";} {
        if ($0 ~ /\}/) {
            do_flag = 0;
            if (ifname) lease_arr[ifname] = block;
        }
        if (do_flag) {
            block = (block "\n" $0);
            if ($0 ~ /^[[:space:]]*interface[[:space:]]+".*";/) {
                ifname = gensub(/^[^"]*"|";.*/, "", "g", $0);
            }
        }
        if ($0 ~ /^lease/) {
            do_flag = 1;
            block = "";
        }
    }
    END {
        for (i in lease_arr) {
            print lease_arr[i];
        }
    }'
- /etc/init.d/?service_name status 2>/dev/null
- /sbin/blkid ?filesystem
- /sbin/runlevel 2>/dev/null
- /usr/sbin/ifconfig -a
- ?path --version
- ?path -V
- ?which_path ?command
- PATH=?path; ?which_path ?command
- arch
- arp -n
- at -l
- auditctl -l
- auditctl -v
- chkconfig --list
- df -kP
- df /
- dhcpcd --dumplease ?interface_id
- dhcpcd --version | head -n1
- dmesg
```

```
- dmidecode
- dmidecode --string system-uuid
- docker container ls --all --no-trunc --format='{{ .ID}}' | xargs -r docker inspect
- docker image ls --all --no-trunc --format='{{json .ID}}' | uniq | xargs -r docker
    inspect
- docker info --format='{{json .}}'
- docker ps --no-trunc -f "ancestor=?image_id" --format="{{.ID}}" | head -n 1 | xargs
    -r docker inspect --format="{{.State.Pid}}"
- echo $LOGNAME
- egrep -i 'ORA_HOME|ORACLE_HOME' /etc/rc*/* /etc/init.d/* /home/*/.oraenv /home/
*/.bash_profile
    -s -l 2>/dev/null
- env
- fdisk -l
- file -bL ?path
- find -H /etc/rc*.d
- find -H ?mask
- find ?oracle_home/dbs -type f \( -iname 'init*.ora' ! -iname 'init.ora' \)
- find ?oracle_home/dbs -type f \( -iname 'spfile*.ora' \)
- find ?path -type f -follow
- free
- getfacl --skip-base --absolute-names ?path
- |-
    gitlab-rails runner '
    class MemberForExport
      attr_accessor :id
      attr_accessor :type
      attr_accessor :access_level
    end
    class GroupForExport
      attr_accessor :id
      attr_accessor :name
      attr_accessor :full_name
      attr_accessor :full_path
      attr_accessor :visibility
      attr_accessor :parent_id
      attr_accessor :group_members
      def fill_members(group)
        @group_members = []
        group.members.each do |member|
          pm = MemberForExport.new
          pm.id = member.user_id
          pm.access_level = member.access_level
          pm.type = "User"
          @group_members << pm
        end
```

```
        group.shared_with_group_links.each do |group_member|
          pm = MemberForExport.new
          pm.id = group_member.shared_with_group_id
          pm.access_level = group_member.group_access
          pm.type = "Group"
          @group_members << pm
        end
      end
    end
    groups_for_export = []
    Group.all.each do |group|
      gr = GroupForExport.new
      gr.id = group.id
      gr.name = group.name
      gr.full_name = group.full_name
      gr.full_path = group.full_path
      gr.visibility = group.visibility
      gr.parent_id = group.parent.try(:id)
      gr.fill_members(group)
      groups_for_export << gr
    end
    puts groups_for_export.to_json
    '
- "gitlab-rails runner '\nclass
ProjectMemberForExport\n  attr_accessor :id\n  attr_accessor
    :type\n  attr_accessor :access_level\nend\n\nclass
ProjectForExport\n  attr_accessor
    :id\n  attr_accessor :name\n  attr_accessor :full_name\n  attr_accessor :full_pat
h\n
    \
attr_accessor :visibility\n  attr_accessor :owner\n  attr_accessor :project_members\n
\n
    \ def fill_members(project)\n    @owner =
ProjectMemberForExport.new\n    @owner.id
    = project.owner.id\n    @owner.access_level = 50\n    @owner.type =
project.owner.class.name\n
    \   \n    @project_members = [@owner]\n\n    project.members.each do |member|\n
    \     next if @owner.type == \"User\" && member.user_id == @owner.id\n\n      pm
    = ProjectMemberForExport.new\n      pm.id = member.user_id\n      pm.access_level
    = member.access_level\n      pm.type = \"User\"\n\n      @project_members << pm\n
    \   end\n\n    project.project_group_links.each do |group_member|\n      pm =
    ProjectMemberForExport.new\n      pm.id =
group_member.group_id\n      pm.access_level
    = group_member.group_access\n      pm.type = \"Group\"\n\n      @project_members
    << pm\n    end\n  end\nend\n\nproject_for_export = []\n\nProject.all.each do |
project|\n
    \ pr = ProjectForExport.new\n  pr.id = project.id\n  pr.name = project.name\n
```

```
    \ pr.full_name = project.full_name\n  pr.full_path =
project.full_path\n  pr.visibility
    = project.visibility\n\n  pr.fill_members(project)\n\n  project_for_export <<
    pr\nend\n\nputs project_for_export.to_json\n'"
- |-
    gitlab-rails runner '
    class SettingForExport
      attr_accessor :signup_enabled
      attr_accessor :password_authentication_enabled_for_web
      attr_accessor :password_authentication_enabled_for_git
    end
    setting = ApplicationSetting.current
    setting_for_export = SettingForExport.new
    setting_for_export.signup_enabled = setting.signup_enabled
    setting_for_export.password_authentication_enabled_for_web =
      setting.password_authentication_enabled_for_web
    setting_for_export.password_authentication_enabled_for_git =
      setting.password_authentication_enabled_for_git
    puts setting_for_export.to_json
    '
- |-
    gitlab-rails runner '
    class UserForExport
      attr_accessor :id
      attr_accessor :username
      attr_accessor :name
      attr_accessor :admin
      attr_accessor :state
      attr_accessor :otp_required_for_login
      attr_accessor :type
      attr_accessor :identities
      attr_accessor :key_fingerprints
    end
    users_for_export = []
    User.all.each do |user|
      us = UserForExport.new
      us.id = user.id
      us.username = user.username
      us.name = user.name
      us.admin = user.admin
      us.state = user.state
      us.otp_required_for_login = user.otp_required_for_login
      us.type = user.user_type
      us.identities = user.identities
      us.key_fingerprints = user.keys.map { |key| key.fingerprint }
      users_for_export << us
```

```
    end
    puts users_for_export.to_json
    '
- gitlab-rake gitlab:env:info
- grubby --info ALL
- host ?host_field
- hostname
- hostname -f 2>/dev/null
- hostname -s
- ifconfig -a
- initctl list
- initctl show-config
- ip -4 route show
- ip -6 route show
- ip addr show
- ip address
- ip neigh show
- iptables-save
- ls -l /dev/disk/by-uuid/
- ls -l /proc/*/exe 2>/dev/null
- ls -l ?path
- ls -lLd ?path
- ls -lZdL ?path
- lsblk -o UUID,MOUNTPOINT
- lsnrctl status
- lspci
- lsusb 2>/dev/null
- lvdisplay 2>/dev/null
- mount
- netstat -vpntua 2>/dev/null
- networkctl list
- nmcli connection show ?interface_id
- nsenter -t ?container_pid -m /bin/cat /etc/SuSE-release
- nsenter -t ?container_pid -m /bin/cat /etc/centos-release
- nsenter -t ?container_pid -m /bin/cat /etc/debian_version
- nsenter -t ?container_pid -m /bin/cat /etc/enterprise-release
- nsenter -t ?container_pid -m /bin/cat /etc/lsb-release
- nsenter -t ?container_pid -m /bin/cat /etc/oracle-release
- nsenter -t ?container_pid -m /bin/cat /etc/os-release
- nsenter -t ?container_pid -m /bin/cat /etc/redhat-release
- nsenter -t ?container_pid -m rpm -qa '*release*' 2>/dev/null
- openvpn --version
- pargs ?pid
- pgrep -l -x 'dhclient|systemd-network|NetworkManager|dhcpcd|wickedd-dhcp4'
- ps -e -o pid,ppid,tty,user,group,etime,comm
- ps -ef
```

```
- ps -eo lstart -o ";%p;%P;%U;%G;%y;" -o label -o ";%c;%a"
- pvdisplay 2>/dev/null
- rpm -qa '*release*' 2>/dev/null
- rpm -qa --qf 'Name=%{NAME}\nVersion=%{VERSION}\nRelease=%{RELEASE}\n\n'
- rpm -qf --qf '%{NAME}\n' ?path
- ss -tupan 2>/dev/null
- stat -L ?filepath
- sysctl -a
- systemctl cat openvpn-server@.service
- systemctl cat openvpn@.service
- systemctl get-default
- systemctl list-unit-files -t target --no-pager --no-legend
- systemctl list-units -a --type target --no-pager --no-legend
- systemctl list-units -t service --all --no-pager --no-legend
- systemctl status openvpn*
- test -d ?path; echo $??
- test -e /proc/self/status && cat /proc/self/status
- test -e ?path; echo $??
- test -f ?path; echo $??
- uname
- uname -m
- uname -n
- uname -p
- uname -r
- uname -s
- uname -v
- vgdisplay 2>/dev/null
- who -r
- wicked test dhcp4 ?interface_id
```

Check Point GAiA OS

При проведении аудита модуль audit выполняет на активе следующие команды:

```
- cpstat fw
- cpstat os
- cpstat vpn
- fw ver -k
- netstat -ien
- show arp dynamic all
- show arp static all
- show asset all
- show bgp summary
- show configuration
- show interfaces all
- show ipv6-state
- show mfc summary
```

```
- show password-controls all
- show rip interfaces
- show route
- show router-id
- show snmp usm user ?username
- show vrrp interfaces
- ver
```

Check Point Generic OS

При проведении аудита модуль audit выполняет на активе следующие команды:

```
- cpstat fw
- cpstat os
- cpstat vpn
- fw ver -k
- ver
```

Check Point SPLAT

При проведении аудита модуль audit выполняет на активе следующие команды:

```
- arp -n
- cpstat fw
- cpstat os
- cpstat vpn
- fw ver -k
- hostname
- idle
- ifconfig -a
- lockout show
- netstat -nr
- snmp service stat
- snmp user show
- snmp user show ?username
- ver
```

Cisco ACS

При проведении аудита модуль audit выполняет на активе следующие команды:

```
- show application
- show cdp neighbors
- show interface
- show inventory
- show ip route
- show logging internal
- show ntp
```

```
- show ports
- show running-config
- show version
```

Cisco ADE-OS

При проведении аудита модуль audit выполняет на активе следующие команды:

```
- show cdp neighbors
- show interface
- show inventory
- show ip route
- show logging internal
- show ntp
- show ports
- show running-config
- show version
```

Cisco AireOS Wireless Controller

При проведении аудита модуль audit выполняет на активе следующие команды:

```
- show advanced rate
- show arp switch
- show cdp neighbors detail
- show client detail ?mac_address
- show client summary
- show inventory
- show logging
- show route kernel
- show route summary
- show run-config
- show sessions
- show snmpcommunity
- show snmptrap
- show snmpv3user
- show snmpversion
- show sysinfo
```

Cisco ASA

При проведении аудита модуль audit выполняет на активе следующие команды:

```
- failover exec active show failover
- failover exec active show interface
- failover exec active show inventory
- failover exec active show ipv6 interface
- failover exec active show ipv6 route
```

```
- failover exec active show route
- failover exec standby show interface
- failover exec standby show inventory
- failover exec standby show ipv6 interface
- show arp
- show context
- show eigrp interfaces
- show eigrp topology
- show failover
- show firewall
- show hostname
- show hostname fqdn
- show interface
- show inventory
- show ipv6 interface
- show ipv6 route
- show logging | exclude \%
- show mode
- show ntp status
- show ospf
- show ospf interface
- show rip database
- show route
- show running-config
- show running-config all
- show snmp group
- show snmp host
- show snmp user
- show ssh
- show startup-config
- show version
```

Cisco IOS

При проведении аудита модуль audit выполняет на активе следующие команды:

```
- show archive
- show arp
- show bgp all summary
- show bgp vrf ?vrf all summary
- show cdp interface
- show cdp neighbors detail
- show dhcp lease
- show etherchannel detail
- show hosts
- show interfaces
- show interfaces switchport
```

```
- show inventory
- show ip access-lists
- show ip arp vrf ?vrf
- show ip dhcp snooping binding
- show ip eigrp ?as_number interfaces
- show ip eigrp vrf ?vrf ?as_number interfaces
- show ip interface
- show ip ospf
- show ip ospf interface
- show ip protocols
- show ip protocols vrf ?vrf
- show ip route vrf *
- show ip ssh
- show ipv6 interface
- show ipv6 route
- show ipv6 route vrf ?vrf
- show key chain
- show lldp interface
- show lldp neighbors
- show lldp neighbors ?port detail
- show logging | exclude \%
- show mac address-table
- show mac-address-table
- show ntp status
- show running-config
- show running-config all
- show running-config view full
- show snmp
- show snmp community
- show snmp context mapping
- show snmp group
- show snmp user
- show snmp view
- show spanning-tree
- show spanning-tree detail
- show standby
- show startup-config
- show version
- show vlan brief
- show vrf
- show vrrp
```

Cisco IOS XE

При проведении аудита модуль audit выполняет на активе следующие команды:

```
- show archive
- show arp
- show bgp all summary
- show bgp vrf ?vrf all summary
- show cdp interface
- show cdp neighbors detail
- show dhcp lease
- show etherchannel detail
- show hosts
- show interfaces
- show interfaces switchport
- show inventory
- show ip access-lists
- show ip arp vrf ?vrf
- show ip dhcp snooping binding
- show ip eigrp ?as_number interfaces
- show ip eigrp vrf ?vrf ?as_number interfaces
- show ip interface
- show ip ospf
- show ip ospf interface
- show ip protocols
- show ip protocols vrf ?vrf
- show ip route vrf *
- show ip ssh
- show ipv6 interface
- show ipv6 route
- show ipv6 route vrf ?vrf
- show key chain
- show lldp interface
- show lldp neighbors
- show lldp neighbors ?port detail
- show logging | exclude \%
- show mac address-table
- show mac-address-table
- show ntp status
- show running-config
- show running-config all
- show running-config view full
- show snmp
- show snmp community
- show snmp context mapping
- show snmp group
- show snmp user
```

```
- show snmp view
- show spanning-tree
- show spanning-tree detail
- show standby
- show startup-config
- show version
- show vlan brief
- show vrf
- show vrrp
```

Cisco IOS XR

При проведении аудита модуль audit выполняет на активе следующие команды:

```
- admin show diag chassis
- admin show running-config
- show arp vrf ?vrf
- show bundle
- show cdp interface
- show cdp neighbors detail
- show hosts
- show hsrp detail
- show install active summary
- show interfaces
- show ipv4 vrf all interface
- show ipv6 vrf all interface
- show lldp interface
- show lldp neighbors detail
- show logging last 1
- show route vrf ?vrf
- show route vrf ?vrf ipv6
- show running-config
- show snmp
- show snmp group
- show snmp view
- show version brief
- show vrf all
- show vrrp detail
```

Cisco ISE (Identity Services Engine)

При проведении аудита модуль audit выполняет на активе следующие команды:

```
- show application
- show cdp neighbors
- show interface
- show inventory
- show ip route
```

```
- show logging internal
- show ntp
- show ports
- show running-config
- show version
```

Cisco NX-OS

При проведении аудита модуль audit выполняет на активе следующие команды:

```
- show cdp neighbors detail
- show feature
- show hsrp
- show http-server
- show interface
- show interface switchport
- show inventory
- show ip arp vrf ?vrf
- show ip dhcp snooping binding
- show ip eigrp vrf all
- show ip interface vrf all
- show ip ospf vrf all
- show ip rip vrf all
- show ip route vrf all
- show ipv6 eigrp vrf all
- show ipv6 interface vrf all
- show ipv6 route vrf all
- show key chain
- show lldp neighbors detail
- show logging info
- show mac address-table
- show ntp peers
- show ntp status
- show port-channel summary
- show role
- show running-config
- show running-config all | no-more
- show spanning-tree detail
- show startup-config
- show version
- show vlan
- show vpc role
- show vpc | no-more
- show vrf all
- show vrrp detail
- show vrrpv3 detail
```

Debian

При проведении аудита модуль audit выполняет на активе следующие команды:

```
- /etc/init.d/?service_name status 2>/dev/null
- /sbin/blkid ?filesystem
- /sbin/runlevel 2>/dev/null
- /usr/sbin/ifconfig -a
- ?path --version
- ?path -V
- ?which_path ?command
- PATH=?path; ?which_path ?command
- arch
- arp -n
- at -l
- auditctl -l
- auditctl -v
- chkconfig --list
- df -kP
- df /
- dhcpcd --dumplease ?interface_id
- dhcpcd --version | head -n1
- dmesg
- dmidecode
- dmidecode --string system-uuid
- docker container ls --all --no-trunc --format='{{ .ID}}' | xargs -r docker inspect
- docker image ls --all --no-trunc --format='{{json .ID}}' | uniq | xargs -r docker
    inspect
- docker info --format='{{json .}}'
- docker ps --no-trunc -f "ancestor=?image_id" --format="{{.ID}}" | head -n 1 | xargs
    -r docker inspect --format="{{.State.Pid}}"
- dpkg -S ?path
- dpkg-query --show  -f='${Package}\t${Version}\n'  2>/dev/null
- echo $LOGNAME
- env
- fdisk -l
- file -bL ?path
- find -H /etc/rc*.d
- find -H ?mask
- find ?path -type f -follow
- free
- getfacl --skip-base --absolute-names ?path
- |-
    gitlab-rails runner '
    class MemberForExport
      attr_accessor :id
      attr_accessor :type
```

```
      attr_accessor :access_level
    end
    class GroupForExport
      attr_accessor :id
      attr_accessor :name
      attr_accessor :full_name
      attr_accessor :full_path
      attr_accessor :visibility
      attr_accessor :parent_id
      attr_accessor :group_members
      def fill_members(group)
        @group_members = []
        group.members.each do |member|
          pm = MemberForExport.new
          pm.id = member.user_id
          pm.access_level = member.access_level
          pm.type = "User"
          @group_members << pm
        end
        group.shared_with_group_links.each do |group_member|
          pm = MemberForExport.new
          pm.id = group_member.shared_with_group_id
          pm.access_level = group_member.group_access
          pm.type = "Group"
          @group_members << pm
        end
      end
    end
    groups_for_export = []
    Group.all.each do |group|
      gr = GroupForExport.new
      gr.id = group.id
      gr.name = group.name
      gr.full_name = group.full_name
      gr.full_path = group.full_path
      gr.visibility = group.visibility
      gr.parent_id = group.parent.try(:id)
      gr.fill_members(group)
      groups_for_export << gr
    end
    puts groups_for_export.to_json
    '
- "gitlab-rails runner '\nclass
ProjectMemberForExport\n  attr_accessor :id\n  attr_accessor
    :type\n  attr_accessor :access_level\nend\n\nclass
ProjectForExport\n  attr_accessor
```

```
    :id\n  attr_accessor :name\n  attr_accessor :full_name\n  attr_accessor :full_pat
h\n
    \
attr_accessor :visibility\n  attr_accessor :owner\n  attr_accessor :project_members\n
\n
    \ def fill_members(project)\n    @owner =
ProjectMemberForExport.new\n    @owner.id
    = project.owner.id\n    @owner.access_level = 50\n    @owner.type =
project.owner.class.name\n
    \   \n    @project_members = [@owner]\n\n    project.members.each do |member|\n
    \     next if @owner.type == \"User\" && member.user_id == @owner.id\n\n      pm
    = ProjectMemberForExport.new\n      pm.id = member.user_id\n      pm.access_level
    = member.access_level\n      pm.type = \"User\"\n\n      @project_members << pm\n
    \   end\n\n    project.project_group_links.each do |group_member|\n      pm =
    ProjectMemberForExport.new\n      pm.id =
group_member.group_id\n      pm.access_level
    = group_member.group_access\n      pm.type = \"Group\"\n\n      @project_members
    << pm\n    end\n  end\nend\n\nproject_for_export = []\n\nProject.all.each do |
project|\n
    \ pr = ProjectForExport.new\n  pr.id = project.id\n  pr.name = project.name\n
    \ pr.full_name = project.full_name\n  pr.full_path =
project.full_path\n  pr.visibility
    = project.visibility\n\n  pr.fill_members(project)\n\n  project_for_export <<
    pr\nend\n\nputs project_for_export.to_json\n'"
- |-
    gitlab-rails runner '
    class SettingForExport
      attr_accessor :signup_enabled
      attr_accessor :password_authentication_enabled_for_web
      attr_accessor :password_authentication_enabled_for_git
    end
    setting = ApplicationSetting.current
    setting_for_export = SettingForExport.new
    setting_for_export.signup_enabled = setting.signup_enabled
    setting_for_export.password_authentication_enabled_for_web =
      setting.password_authentication_enabled_for_web
    setting_for_export.password_authentication_enabled_for_git =
      setting.password_authentication_enabled_for_git
    puts setting_for_export.to_json
    '
- |-
    gitlab-rails runner '
    class UserForExport
      attr_accessor :id
      attr_accessor :username
      attr_accessor :name
      attr_accessor :admin
      attr_accessor :state
```

```
      attr_accessor :otp_required_for_login
      attr_accessor :type
      attr_accessor :identities
      attr_accessor :key_fingerprints
    end
    users_for_export = []
    User.all.each do |user|
      us = UserForExport.new
      us.id = user.id
      us.username = user.username
      us.name = user.name
      us.admin = user.admin
      us.state = user.state
      us.otp_required_for_login = user.otp_required_for_login
      us.type = user.user_type
      us.identities = user.identities
      us.key_fingerprints = user.keys.map { |key| key.fingerprint }
      users_for_export << us
    end
    puts users_for_export.to_json
    '
- gitlab-rake gitlab:env:info
- host ?host_field
- hostname
- hostname -f 2>/dev/null
- hostname -s
- ifconfig -a
- initctl list
- initctl show-config
- ip -4 route show
- ip -6 route show
- ip addr show
- ip address
- ip neigh show
- iptables-save
- ls -l /dev/disk/by-uuid/
- ls -l /proc/*/exe 2>/dev/null
- ls -l ?path
- ls -lLd ?path
- ls -lZdL ?path
- lsblk -o UUID,MOUNTPOINT
- lspci
- lsusb 2>/dev/null
- lvdisplay 2>/dev/null
- mount
- netstat -vpntua 2>/dev/null
```

```
- networkctl list
- nmcli connection show ?interface_id
- nsenter -t ?container_pid -m /bin/cat /etc/SuSE-release
- nsenter -t ?container_pid -m /bin/cat /etc/centos-release
- nsenter -t ?container_pid -m /bin/cat /etc/debian_version
- nsenter -t ?container_pid -m /bin/cat /etc/enterprise-release
- nsenter -t ?container_pid -m /bin/cat /etc/lsb-release
- nsenter -t ?container_pid -m /bin/cat /etc/oracle-release
- nsenter -t ?container_pid -m /bin/cat /etc/os-release
- nsenter -t ?container_pid -m /bin/cat /etc/redhat-release
- nsenter -t ?container_pid -m rpm -qa '*release*' 2>/dev/null
- openvpn --version
- pargs ?pid
- pgrep -l -x 'dhclient|systemd-network|NetworkManager|dhcpcd|wickedd-dhcp4'
- ps -e -o pid,ppid,tty,user,group,etime,comm
- ps -eo lstart -o ";%p;%P;%U;%G;%y;" -o label -o ";%c;%a"
- pvdisplay 2>/dev/null
- rpm -qa '*release*' 2>/dev/null
- ss -tupan 2>/dev/null
- stat -L ?filepath
- sysctl -a
- systemctl cat openvpn-server@.service
- systemctl cat openvpn@.service
- systemctl get-default
- systemctl list-unit-files -t target --no-pager --no-legend
- systemctl list-units -a --type target --no-pager --no-legend
- systemctl list-units -t service --all --no-pager --no-legend
- systemctl status openvpn*
- test -d ?path; echo $??
- test -e /proc/self/status && cat /proc/self/status
- test -e ?path; echo $??
- test -f ?path; echo $??
- uname
- uname -i
- uname -m
- uname -n
- uname -p
- uname -r
- uname -s
- uname -v
- vgdisplay 2>/dev/null
- who -r
- wicked test dhcp4 ?interface_id
```

Dell iDRAC

При проведении аудита модуль audit выполняет на активе следующие команды:

```
- racadm arp
- racadm get iDRAC.ADGroup
- racadm get iDRAC.ADGroup.?id
- racadm get iDRAC.ActiveDirectory
- racadm get iDRAC.IPMILan
- racadm get iDRAC.IPMISOL
- racadm get iDRAC.IPMISerial
- racadm get iDRAC.IPv4
- racadm get iDRAC.LDAP
- racadm get iDRAC.LDAPRoleGroup.?id
- racadm get iDRAC.NTPConfigGroup
- racadm get iDRAC.Racadm
- racadm get iDRAC.Redfish
- racadm get iDRAC.SNMP
- racadm get iDRAC.SSH
- racadm get iDRAC.Serial
- racadm get iDRAC.Telnet
- racadm get iDRAC.Users.?id
- racadm get iDRAC.VNCServer
- racadm get iDRAC.VirtualConsole
- racadm get iDRAC.WebServer
- racadm get idrac.LDAPRoleGroup
- racadm getsysinfo
- racadm getversion
- racadm hwinventory
- racadm ifconfig
- racadm license view
- racadm netstat
```

Eltex ROS

При проведении аудита модуль audit выполняет на активе следующие команды:

```
- show arp
- show interfaces ?interface_id
- show interfaces description
- show interfaces switchport ?interface_id
- show ip interface
- show ip multicast
- show ip route
- show ipv6 interface
- show lldp configuration
- show mac address-table
- show running-config
```

```
- show system
- show system id
- show version
- show vlan
```

Eltex, маршрутизаторы серии ESR

При проведении аудита модуль audit выполняет на активе следующие команды:

```
- show arp
- show arp vrf ?vrf
- show interfaces status
- show ip route
- show ip route vrf ?vrf
- show ip vrf
- show running-config
- show system
- show vlan
```

FortiNet FortiOS

При проведении аудита модуль audit выполняет на активе следующие команды:

```
- |4
        config global
        get hardware nic ?interface_id
        end
- |4
        config global
        get log memory global-setting
        end
- |4
        config global
        get log syslogd?number filter
        end
- |4
        config global
        get log syslogd?number setting
        end
- |4
        config global
        get system password-policy
        end
- |4
        config global
        show system admin
        end
- |4
```

```
        config global
        show system interface
        end
- |4
        config global
        show system vdom-property
        end
- |4
        config vdom
        edit ?vdom
        diag netlink aggregate name ?interface_id
        end
- |4
        config vdom
        edit ?vdom
        diagnose ip address list
        end
- |4
        config vdom
        edit ?vdom
        get log memory filter
        end
- |4
        config vdom
        edit ?vdom
        get log memory setting
        end
- |4
        config vdom
        edit ?vdom
        get router info routing-table all
        end
- |4
        config vdom
        edit ?vdom
        get router multicast
        end
- |4
        config vdom
        edit ?vdom
        get system arp
        end
- |4
        config vdom
        edit ?vdom
        show user local
```

```
        end
- diag netlink aggregate name ?interface_id
- diagnose ip address list
- get hardware nic ?interface_id
- get log memory filter
- get log memory global-setting
- get log memory setting
- get log syslogd?number filter
- get log syslogd?number setting
- get router info routing-table all
- get router multicast
- get system arp
- get system password-policy
- get system status
- show
- show system admin
- show system interface
- show user local
```

FreeBSD

При проведении аудита модуль audit выполняет на активе следующие команды:

```
- |4
    mount | egrep -o '^/dev/[a-z0-9]+ on / ' | sed 's/ on \/ //g' | xargs dumpfs -l |
sed 's/\/dev\/ufsid\///g'
- |4
    mount | grep ' on / ' | egrep -o '^[a-zA-Z0-9_\-\.]+' | xargs zpool get -H -o
value guid
- /bin/cat /var/run/dmesg.boot | /usr/bin/egrep -i '(vmw|xen|hyper-v|microsoft|vbox|
virtualbox|oracle
    vm|parallels|hitachi|qemu)'
- /bin/kenv
- ?path --version
- ?which_path ?command
- PATH=?path; ?which_path ?command
- arp -an
- dmidecode
- echo $LOGNAME
- env
- file -bL ?path
- file -v
- find -H ?mask
- find /boot -type f -name "kernel" -depth 2
- find ?path -type f -follow
- hostname
- hostname -s
```

```
- ifconfig -a
- ipfstat -ioR
- ls -lLd ?path
- ls /dev/gptid/
- named -v
- netstat -rn
- ntpd --version
- openssl version
- openvpn --version
- pkg info
- pkg_info
- ps -eo lstart -o ";%p;%P;%U;%G;%y;" -o label -o ";%c;%a"
- service -e
- service -r
- service ?service status
- ssh -V
- stat -L ?filepath
- sysctl -n security.jail.jailed
- systemctl cat openvpn-server@.service
- systemctl cat openvpn@.service
- systemctl status openvpn*
- test -d ?path; echo $??
- test -e ?path; echo $??
- uname
- uname -m
- uname -n
- uname -p
- uname -r
- uname -s
- uname -v
```

Generic Linux

При проведении аудита модуль audit выполняет на активе следующие команды:

```
- /etc/init.d/?service_name status 2>/dev/null
- /sbin/blkid ?filesystem
- /sbin/runlevel 2>/dev/null
- /usr/sbin/ifconfig -a
- ?path --version
- ?path -V
- ?which_path ?command
- PATH=?path; ?which_path ?command
- arch
- arp -n
- at -l
- auditctl -l
```

```
- auditctl -v
- chkconfig --list
- df -kP
- df /
- dhcpcd --dumplease ?interface_id
- dhcpcd --version | head -n1
- dmesg
- dmidecode
- dmidecode --string system-uuid
- docker container ls --all --no-trunc --format='{{ .ID}}' | xargs -r docker inspect
- docker image ls --all --no-trunc --format='{{json .ID}}' | uniq | xargs -r docker
    inspect
- docker info --format='{{json .}}'
- docker ps --no-trunc -f "ancestor=?image_id" --format="{{.ID}}" | head -n 1 | xargs
    -r docker inspect --format="{{.State.Pid}}"
- echo $LOGNAME
- env
- fdisk -l
- file -bL ?path
- find -H /etc/rc*.d
- find -H ?mask
- find ?path -type f -follow
- free
- getfacl --skip-base --absolute-names ?path
- |-
    gitlab-rails runner '
    class MemberForExport
      attr_accessor :id
      attr_accessor :type
      attr_accessor :access_level
    end
    class GroupForExport
      attr_accessor :id
      attr_accessor :name
      attr_accessor :full_name
      attr_accessor :full_path
      attr_accessor :visibility
      attr_accessor :parent_id
      attr_accessor :group_members
      def fill_members(group)
        @group_members = []
        group.members.each do |member|
          pm = MemberForExport.new
          pm.id = member.user_id
          pm.access_level = member.access_level
          pm.type = "User"
```

```
          @group_members << pm
        end
        group.shared_with_group_links.each do |group_member|
          pm = MemberForExport.new
          pm.id = group_member.shared_with_group_id
          pm.access_level = group_member.group_access
          pm.type = "Group"
          @group_members << pm
        end
      end
    end
    groups_for_export = []
    Group.all.each do |group|
      gr = GroupForExport.new
      gr.id = group.id
      gr.name = group.name
      gr.full_name = group.full_name
      gr.full_path = group.full_path
      gr.visibility = group.visibility
      gr.parent_id = group.parent.try(:id)
      gr.fill_members(group)
      groups_for_export << gr
    end
    puts groups_for_export.to_json
    '
- "gitlab-rails runner '\nclass
ProjectMemberForExport\n  attr_accessor :id\n  attr_accessor
    :type\n  attr_accessor :access_level\nend\n\nclass
ProjectForExport\n  attr_accessor
    :id\n  attr_accessor :name\n  attr_accessor :full_name\n  attr_accessor :full_pat
h\n
    \
attr_accessor :visibility\n  attr_accessor :owner\n  attr_accessor :project_members\n
\n
    \ def fill_members(project)\n    @owner =
ProjectMemberForExport.new\n    @owner.id
    = project.owner.id\n    @owner.access_level = 50\n    @owner.type =
project.owner.class.name\n
    \   \n    @project_members = [@owner]\n\n    project.members.each do |member|\n
    \     next if @owner.type == \"User\" && member.user_id == @owner.id\n\n      pm
    = ProjectMemberForExport.new\n      pm.id = member.user_id\n      pm.access_level
    = member.access_level\n      pm.type = \"User\"\n\n      @project_members << pm\n
    \   end\n\n    project.project_group_links.each do |group_member|\n      pm =
    ProjectMemberForExport.new\n      pm.id =
group_member.group_id\n      pm.access_level
    = group_member.group_access\n      pm.type = \"Group\"\n\n      @project_members
    << pm\n    end\n  end\nend\n\nproject_for_export = []\n\nProject.all.each do |
project|\n
```

```
    \ pr = ProjectForExport.new\n  pr.id = project.id\n  pr.name = project.name\n
    \ pr.full_name = project.full_name\n  pr.full_path =
project.full_path\n  pr.visibility
    = project.visibility\n\n  pr.fill_members(project)\n\n  project_for_export <<
    pr\nend\n\nputs project_for_export.to_json\n'"
- |-
    gitlab-rails runner '
    class SettingForExport
      attr_accessor :signup_enabled
      attr_accessor :password_authentication_enabled_for_web
      attr_accessor :password_authentication_enabled_for_git
    end
    setting = ApplicationSetting.current
    setting_for_export = SettingForExport.new
    setting_for_export.signup_enabled = setting.signup_enabled
    setting_for_export.password_authentication_enabled_for_web =
      setting.password_authentication_enabled_for_web
    setting_for_export.password_authentication_enabled_for_git =
      setting.password_authentication_enabled_for_git
    puts setting_for_export.to_json
    '
- |-
    gitlab-rails runner '
    class UserForExport
      attr_accessor :id
      attr_accessor :username
      attr_accessor :name
      attr_accessor :admin
      attr_accessor :state
      attr_accessor :otp_required_for_login
      attr_accessor :type
      attr_accessor :identities
      attr_accessor :key_fingerprints
    end
    users_for_export = []
    User.all.each do |user|
      us = UserForExport.new
      us.id = user.id
      us.username = user.username
      us.name = user.name
      us.admin = user.admin
      us.state = user.state
      us.otp_required_for_login = user.otp_required_for_login
      us.type = user.user_type
      us.identities = user.identities
      us.key_fingerprints = user.keys.map { |key| key.fingerprint }
```

```
      users_for_export << us
    end
    puts users_for_export.to_json
    '
- gitlab-rake gitlab:env:info
- host ?host_field
- hostname
- hostname -f 2>/dev/null
- hostname -s
- ifconfig -a
- initctl list
- initctl show-config
- ip -4 route show
- ip -6 route show
- ip addr show
- ip address
- ip neigh show
- iptables-save
- ls -l /dev/disk/by-uuid/
- ls -l /proc/*/exe 2>/dev/null
- ls -l ?path
- ls -lLd ?path
- ls -lZdL ?path
- lsblk -o UUID,MOUNTPOINT
- lspci
- lsusb 2>/dev/null
- lvdisplay 2>/dev/null
- mount
- netstat -vpntua 2>/dev/null
- networkctl list
- nmcli connection show ?interface_id
- nsenter -t ?container_pid -m /bin/cat /etc/SuSE-release
- nsenter -t ?container_pid -m /bin/cat /etc/centos-release
- nsenter -t ?container_pid -m /bin/cat /etc/debian_version
- nsenter -t ?container_pid -m /bin/cat /etc/enterprise-release
- nsenter -t ?container_pid -m /bin/cat /etc/lsb-release
- nsenter -t ?container_pid -m /bin/cat /etc/oracle-release
- nsenter -t ?container_pid -m /bin/cat /etc/os-release
- nsenter -t ?container_pid -m /bin/cat /etc/redhat-release
- nsenter -t ?container_pid -m rpm -qa '*release*' 2>/dev/null
- openvpn --version
- pargs ?pid
- pgrep -l -x 'dhclient|systemd-network|NetworkManager|dhcpcd|wickedd-dhcp4'
- ps -e -o pid,ppid,tty,user,group,etime,comm
- ps -eo lstart -o ";%p;%P;%U;%G;%y;" -o label -o ";%c;%a"
- pvdisplay 2>/dev/null
```

```
- rpm -qa '*release*' 2>/dev/null
- ss -tupan 2>/dev/null
- stat -L ?filepath
- sysctl -a
- systemctl cat openvpn-server@.service
- systemctl cat openvpn@.service
- systemctl get-default
- systemctl list-unit-files -t target --no-pager --no-legend
- systemctl list-units -a --type target --no-pager --no-legend
- systemctl list-units -t service --all --no-pager --no-legend
- systemctl status openvpn*
- test -d ?path; echo $??
- test -e /proc/self/status && cat /proc/self/status
- test -e ?path; echo $??
- test -f ?path; echo $??
- uname
- uname -n
- uname -p
- uname -r
- uname -s
- uname -v
- vgdisplay 2>/dev/null
- who -r
- wicked test dhcp4 ?interface_id
```

HPE Comware Software

При проведении аудита модуль audit выполняет на активе следующие команды:

```
- display arp verbose
- display channel
- display current-configuration
- display info-center
- display interface
- display ip routing-table
- display ip routing-table vpn-instance ?vrf
- display ip vpn-instance
- display ipv6 interface
- display link-aggregation verbose
- display lldp neighbor
- display lldp status
- display mac-address
- display saved-configuration
- display version
- display vlan all
- display vrrp ipv6 verbose
- display vrrp verbose
```

HPE iLO

При проведении аудита модуль audit выполняет на активе следующие команды:

```
- show -a /map1/accounts1
- show -a /map1/enetport1
- show /map1
- show /map1/config1
- show /map1/dnsendpt1
- show /map1/firmware1
- show /map1/gateway1
- show /map1/oemhp_dircfg1
- show /map1/oemhp_sntp1
- show /map1/oemhp_ssocfg1
- show /map1/settings1/StaticIPSettings1
```

HPE UX

При проведении аудита модуль audit выполняет на активе следующие команды:

```
- |4
        export UNIX95= && ps -eo pid= | xargs pfiles 2>/dev/null | awk '
            BEGIN {title = ""; socket_info = "";}
            {
                if ($0 ~ /^[0-9]+:/) title = $0;
                if ($0 ~ /[[:space:]]family=AF_INET/) socket_info = $0;
                if ($1 == "localaddr/port") {
                    print title "\n" socket_info "\n" $0 "\n";
                }
            }'
- /usr/contrib/bin/machinfo -v
- ?which_path ?command
- PATH=?path; ?which_path ?command
- arp -an
- at -l
- date
- diskinfo -v ?device
- echo $LOGNAME
- env
- export UNIX95= && ps -ex -o pid,ppid,tty,user,group,etime,args
- file -bL ?path
- find -H /sbin/rc*.d
- find -H ?mask
- find ?path -type f -follow
- host ?host_field
- hostname
- ifconfig ?interface_name
- ioscan -kC processor
```

```
- ioscan -km dsf
- ipfstat -io
- lanscan
- ls -lLd ?path
- netstat -anf inet
- netstat -in
- netstat -rnv -f inet
- nslookup $(hostname)
- nwmgr
- ps -el
- swapinfo -dftm
- swlist -l bundle 2>/dev/null
- swlist -l file -a file | egrep -v "^#|^  PH(CO|KL|NE|SS)_"
- swlist -l fileset -a revision
- swlist -l product -a name *,c=patch
- test -d ?path; echo $??
- test -e ?path; echo $??
- uname -a
- uname -m
- uname -n
- uname -r
- uname -s
- uname -v
- vgdisplay -v -F
- who -r
```

Huawei VRP

При проведении аудита модуль audit выполняет на активе следующие команды:

```
- display arp
- display bgp ?vpn_af all peer
- display bgp ipv6 peer
- display bgp multicast peer
- display bgp peer
- display channel
- display current-configuration
- display info-center
- display info-center channel
- display interface
- display ip routing-table
- display ip routing-table vpn-instance ?vrf
- display ip vpn-instance
- display ipv6 interface
- display lldp local
- display lldp neighbor
- display mac-address
```

```
- display ospf brief
- display patch-information
- display port vlan
- display rip ?process_id interface verbose
- display saved-configuration
- display snmp-agent community ?type
- display snmp-agent group
- display snmp-agent mib-view
- display snmp-agent sys-info
- display ssh server status
- display ssh user-information
- display user-interface
- display version
- display vlan
- display vlan all
- display vlan brief
- display vrrp
- display vrrp verbose
- display vrrp6
- display vrrp6 verbose
```

IBM AIX

При проведении аудита модуль audit выполняет на активе следующие команды:

```
- ?which_path ?command
- PATH=?path; ?which_path ?command
- arp -an
- at -l
- date
- echo $LOGNAME
- env
- file -bL ?path
- find -H /etc/rc.d/rc*.d
- find -H ?mask
- find ?path -type f -follow
- getconf ?variable_name ?device_name
- host ?address 2>/dev/null
- hostname
- ifconfig -a
- instfix -i 2>/dev/null
- ls -lLd ?path
- lsattr -El ?device_name
- lsdev -C -S a -F"name|||class|||subclass|||location|||physloc|||description"
- lsfilt -v4
- 'lslpp -cL 2>/dev/null | awk -F: ''(NR > 1) {print $2 "~~" $3;}'' | sort | uniq'
- lslpp -cw ?path
```

```
- lslv -L ?lv_name
- lsps -a
- lspv -L ?pv_name
- lssrc -a
- lssrc -ls inetd
- lsuser ALL
- lsvg -L -l ?vg_name
- lsvg -L -p ?vg_name
- lsvg -L | lsvg -L -i
- namerslv -sn
- netstat -Aan -f inet
- netstat -in
- netstat -rn -f inet
- netstat -rn -f inet6
- oslevel -r
- oslevel -s
- prtconf
- ps -AfXo pid,ppid,user,group,tty,etime,comm,args
- ps -Ao pid,ppid,tty,comm
- rmsock ?socket_id tcpcb
- test -d ?path; echo $??
- test -e ?path; echo $??
- uname
- uname -L
- uname -M
- uname -W 2>/dev/null
- uname -f
- uname -m
- uname -n
- uname -p
- uname -r
- uname -s
- uname -u
- who -r
```

Juniper JunOS

При проведении аудита модуль audit выполняет на активе следующие команды:

```
- show arp logical-system ?ls no-resolve
- show arp logical-system ?ls vpn ?ri no-resolve
- show arp no-resolve
- show arp vpn ?ri no-resolve
- show bgp neighbor
- show bgp neighbor logical-system ?ls_name
- show chassis hardware | display xml | no-more
- show configuration ethernet-switching-options secure-access-port | display xml |
```

```
    no-more | display inheritance
- show configuration groups junos-defaults applications | display xml | no-more
- show configuration | display inheritance | no-more
- show configuration | display xml | no-more | display inheritance
- show ethernet-switching table
- show interfaces routing-instance all terse | display xml | no-more
- show interfaces | display xml | no-more
- show lldp neighbors
- show lldp neighbors interface ?port
- show lldp | display xml
- show multicast route
- show ospf overview ?arg
- show route logical-system all | display xml | no-more
- show route | display xml | no-more
- show security flow status
- show security ipsec security-associations
- show services ipsec-vpn ipsec security-associations
- show system connections | no-more
- show version
- show version detail | no-more
- show vlans
- show vrrp detail
```

Microsoft Windows

При проведении аудита модуль audit выполняет на активе следующие команды:

```
- '"?install_path\avp.com" Status'
- '"?oracle_home\OPatch\opatch.bat" lsinventory'
- '"?path\versionInfo.bat"'
- ?system_root\system32\inetsrv\appcmd.exe list site
- ?system_root\syswow64\inetsrv\appcmd.exe list site
- arp.exe -a
- auditpol /backup /file:{output_file}
- chcp 65001 | quser.exe
- chcp 65001 | qwinsta.exe
- dir /b "?oracle_home\database\init*.ora"
- dir /b "?oracle_home\database\spfile*.ora"
- ipconfig /displaydns
- java ru.CryptoPro.JCP.tools.Check
- java ru.CryptoPro.JCP.tools.License
- lsnrctl status
- netsh firewall show currentprofile
- netsh wlan show networks mode=?mode
- netstat -ano
- ping -n 1 -a ?host_field
- reg query "?key"
```

```
- reg query "?key" /s
- reg query "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Component Based
Servicing\Packages"
    /s /v CurrentState
- route print
- sc.exe query lanmanserver
- schtasks /QUERY /V /FO CSV
- secedit /export /cfg {output_file} /areas SECURITYPOLICY
- tasklist /M /FO CSV
- tasklist /V /FO CSV
- tracert -d -h 10 -w 1 ?destination
- type "?filepath"
- winrm enumerate winrm/config/plugin -f:pretty
- winrm get winrm/config
- winrm get winrm/config/client
- winrm get winrm/config/service
- winrm get winrm/config/winrs
```

OpenSUSE

При проведении аудита модуль audit выполняет на активе следующие команды:

```
- /etc/init.d/?service_name status 2>/dev/null
- /sbin/blkid ?filesystem
- /sbin/runlevel 2>/dev/null
- /usr/lib/wicked/bin/wickedd-dhcp4 --test ?interface_id
- /usr/sbin/ifconfig -a
- ?path --version
- ?path -V
- ?which_path ?command
- PATH=?path; ?which_path ?command
- arch
- arp -n
- at -l
- auditctl -l
- auditctl -v
- chkconfig --list
- df -kP
- df /
- dhcpcd --dumplease ?interface_id
- dhcpcd --version | head -n1
- dmesg
- dmidecode
- dmidecode --string system-uuid
- docker container ls --all --no-trunc --format='{{ .ID}}' | xargs -r docker inspect
- docker image ls --all --no-trunc --format='{{json .ID}}' | uniq | xargs -r docker
    inspect
```

```
- docker info --format='{{json .}}'
- docker ps --no-trunc -f "ancestor=?image_id" --format="{{.ID}}" | head -n 1 | xargs
    -r docker inspect --format="{{.State.Pid}}"
- echo $LOGNAME
- env
- fdisk -l
- file -bL ?path
- find -H /etc/rc*.d
- find -H ?mask
- find /var/lib/dhcpcd -type f -name 'dhcpcd-*.info' | while read FILE; do cat $FILE;
    echo; done
- find ?path -type f -follow
- free
- getfacl --skip-base --absolute-names ?path
- |-
    gitlab-rails runner '
    class MemberForExport
      attr_accessor :id
      attr_accessor :type
      attr_accessor :access_level
    end
    class GroupForExport
      attr_accessor :id
      attr_accessor :name
      attr_accessor :full_name
      attr_accessor :full_path
      attr_accessor :visibility
      attr_accessor :parent_id
      attr_accessor :group_members
      def fill_members(group)
        @group_members = []
        group.members.each do |member|
          pm = MemberForExport.new
          pm.id = member.user_id
          pm.access_level = member.access_level
          pm.type = "User"
          @group_members << pm
        end
        group.shared_with_group_links.each do |group_member|
          pm = MemberForExport.new
          pm.id = group_member.shared_with_group_id
          pm.access_level = group_member.group_access
          pm.type = "Group"
          @group_members << pm
        end
      end
```

```
    end
    groups_for_export = []
    Group.all.each do |group|
      gr = GroupForExport.new
      gr.id = group.id
      gr.name = group.name
      gr.full_name = group.full_name
      gr.full_path = group.full_path
      gr.visibility = group.visibility
      gr.parent_id = group.parent.try(:id)
      gr.fill_members(group)
      groups_for_export << gr
    end
    puts groups_for_export.to_json
    '
- "gitlab-rails runner '\nclass
ProjectMemberForExport\n  attr_accessor :id\n  attr_accessor
    :type\n  attr_accessor :access_level\nend\n\nclass
ProjectForExport\n  attr_accessor
    :id\n  attr_accessor :name\n  attr_accessor :full_name\n  attr_accessor :full_pat
h\n
    \
attr_accessor :visibility\n  attr_accessor :owner\n  attr_accessor :project_members\n
\n
    \ def fill_members(project)\n    @owner =
ProjectMemberForExport.new\n    @owner.id
    = project.owner.id\n    @owner.access_level = 50\n    @owner.type =
project.owner.class.name\n
    \   \n    @project_members = [@owner]\n\n    project.members.each do |member|\n
    \     next if @owner.type == \"User\" && member.user_id == @owner.id\n\n      pm
    = ProjectMemberForExport.new\n      pm.id = member.user_id\n      pm.access_level
    = member.access_level\n      pm.type = \"User\"\n\n      @project_members << pm\n
    \   end\n\n    project.project_group_links.each do |group_member|\n      pm =
    ProjectMemberForExport.new\n      pm.id =
group_member.group_id\n      pm.access_level
    = group_member.group_access\n      pm.type = \"Group\"\n\n      @project_members
    << pm\n    end\n  end\nend\n\nproject_for_export = []\n\nProject.all.each do |
project|\n
    \ pr = ProjectForExport.new\n  pr.id = project.id\n  pr.name = project.name\n
    \ pr.full_name = project.full_name\n  pr.full_path =
project.full_path\n  pr.visibility
    = project.visibility\n\n  pr.fill_members(project)\n\n  project_for_export <<
    pr\nend\n\nputs project_for_export.to_json\n'"
- |-
    gitlab-rails runner '
    class SettingForExport
      attr_accessor :signup_enabled
      attr_accessor :password_authentication_enabled_for_web
```

```
      attr_accessor :password_authentication_enabled_for_git
    end
    setting = ApplicationSetting.current
    setting_for_export = SettingForExport.new
    setting_for_export.signup_enabled = setting.signup_enabled
    setting_for_export.password_authentication_enabled_for_web =
      setting.password_authentication_enabled_for_web
    setting_for_export.password_authentication_enabled_for_git =
      setting.password_authentication_enabled_for_git
    puts setting_for_export.to_json
    '
- |-
    gitlab-rails runner '
    class UserForExport
      attr_accessor :id
      attr_accessor :username
      attr_accessor :name
      attr_accessor :admin
      attr_accessor :state
      attr_accessor :otp_required_for_login
      attr_accessor :type
      attr_accessor :identities
      attr_accessor :key_fingerprints
    end
    users_for_export = []
    User.all.each do |user|
      us = UserForExport.new
      us.id = user.id
      us.username = user.username
      us.name = user.name
      us.admin = user.admin
      us.state = user.state
      us.otp_required_for_login = user.otp_required_for_login
      us.type = user.user_type
      us.identities = user.identities
      us.key_fingerprints = user.keys.map { |key| key.fingerprint }
      users_for_export << us
    end
    puts users_for_export.to_json
    '
- gitlab-rake gitlab:env:info
- host ?host_field
- hostname
- hostname -f 2>/dev/null
- hostname -s
- ifconfig -a
```

```
- initctl list
- initctl show-config
- ip -4 route show
- ip -6 route show
- ip addr show
- ip address
- ip neigh show
- iptables-save
- ls -l /dev/disk/by-uuid/
- ls -l /proc/*/exe 2>/dev/null
- ls -l ?path
- ls -lLd ?path
- ls -lZdL ?path
- lsblk -o UUID,MOUNTPOINT
- lspci
- lsusb 2>/dev/null
- lvdisplay 2>/dev/null
- mount
- netstat -vpntua 2>/dev/null
- networkctl list
- nmcli connection show ?interface_id
- nsenter -t ?container_pid -m /bin/cat /etc/SuSE-release
- nsenter -t ?container_pid -m /bin/cat /etc/centos-release
- nsenter -t ?container_pid -m /bin/cat /etc/debian_version
- nsenter -t ?container_pid -m /bin/cat /etc/enterprise-release
- nsenter -t ?container_pid -m /bin/cat /etc/lsb-release
- nsenter -t ?container_pid -m /bin/cat /etc/oracle-release
- nsenter -t ?container_pid -m /bin/cat /etc/os-release
- nsenter -t ?container_pid -m /bin/cat /etc/redhat-release
- nsenter -t ?container_pid -m rpm -qa '*release*' 2>/dev/null
- pargs ?pid
- pgrep -l -x 'dhclient|systemd-network|NetworkManager|dhcpcd|wickedd-dhcp4'
- ps -e -o pid,ppid,tty,user,group,etime,comm
- ps -eo lstart -o ";%p;%P;%U;%G;%y;" -o label -o ";%c;%a"
- pvdisplay 2>/dev/null
- rpm -qa '*release*' 2>/dev/null
- rpm -qa --qf '%{NAME}|%{VERSION}|%{RELEASE}|%{ARCH}\n'
- ss -tupan 2>/dev/null
- sysctl -a
- systemctl get-default
- systemctl list-unit-files -t target --no-pager --no-legend
- systemctl list-units -a --type target --no-pager --no-legend
- systemctl list-units -t service --all --no-pager --no-legend
- test -d ?path; echo $??
- test -e /proc/self/status && cat /proc/self/status
- test -e ?path; echo $??
```

```
- test -f ?path; echo $??
- uname
- uname -m
- uname -p
- uname -s
- vgdisplay 2>/dev/null
- who -r
- wicked test dhcp4 ?interface_id
```

Oracle Linux

При проведении аудита модуль audit выполняет на активе следующие команды:

```
- |4
    ls -1tr /var/lib/{dhcp,dhclient}/dhclient*.lease* 2>/dev/null |
    xargs cat 2>/dev/null | awk '
    BEGIN {block = ""; do_flag = 0; ifname = "";} {
        if ($0 ~ /\}/) {
            do_flag = 0;
            if (ifname) lease_arr[ifname] = block;
        }
        if (do_flag) {
            block = (block "\n" $0);
            if ($0 ~ /^[[:space:]]*interface[[:space:]]+".*";/) {
                ifname = gensub(/^[^"]*"|";.*/, "", "g", $0);
            }
        }
        if ($0 ~ /^lease/) {
            do_flag = 1;
            block = "";
        }
    }
    END {
        for (i in lease_arr) {
            print lease_arr[i];
        }
    }'
- /etc/init.d/?service_name status 2>/dev/null
- /sbin/blkid ?filesystem
- /sbin/runlevel 2>/dev/null
- /usr/sbin/ifconfig -a
- ?path --version
- ?path -V
- ?which_path ?command
- PATH=?path; ?which_path ?command
- arch
- arp -n
```

```
- at -l
- auditctl -l
- auditctl -v
- chkconfig --list
- df -kP
- df /
- dhcpcd --dumplease ?interface_id
- dhcpcd --version | head -n1
- dmesg
- dmidecode
- dmidecode --string system-uuid
- docker container ls --all --no-trunc --format='{{ .ID}}' | xargs -r docker inspect
- docker image ls --all --no-trunc --format='{{json .ID}}' | uniq | xargs -r docker
    inspect
- docker info --format='{{json .}}'
- docker ps --no-trunc -f "ancestor=?image_id" --format="{{.ID}}" | head -n 1 | xargs
    -r docker inspect --format="{{.State.Pid}}"
- echo $LOGNAME
- egrep -i 'ORA_HOME|ORACLE_HOME' /etc/rc*/* /etc/init.d/* /home/*/.oraenv /home/
*/.bash_profile
    -s -l 2>/dev/null
- env
- fdisk -l
- file -bL ?path
- find -H /etc/rc*.d
- find -H ?mask
- find ?oracle_home/dbs -type f \( -iname 'init*.ora' ! -iname 'init.ora' \)
- find ?oracle_home/dbs -type f \( -iname 'spfile*.ora' \)
- find ?path -type f -follow
- free
- getfacl --skip-base --absolute-names ?path
- |-
    gitlab-rails runner '
    class MemberForExport
      attr_accessor :id
      attr_accessor :type
      attr_accessor :access_level
    end
    class GroupForExport
      attr_accessor :id
      attr_accessor :name
      attr_accessor :full_name
      attr_accessor :full_path
      attr_accessor :visibility
      attr_accessor :parent_id
      attr_accessor :group_members
```

```
      def fill_members(group)
        @group_members = []
        group.members.each do |member|
          pm = MemberForExport.new
          pm.id = member.user_id
          pm.access_level = member.access_level
          pm.type = "User"
          @group_members << pm
        end
        group.shared_with_group_links.each do |group_member|
          pm = MemberForExport.new
          pm.id = group_member.shared_with_group_id
          pm.access_level = group_member.group_access
          pm.type = "Group"
          @group_members << pm
        end
      end
    end
    groups_for_export = []
    Group.all.each do |group|
      gr = GroupForExport.new
      gr.id = group.id
      gr.name = group.name
      gr.full_name = group.full_name
      gr.full_path = group.full_path
      gr.visibility = group.visibility
      gr.parent_id = group.parent.try(:id)
      gr.fill_members(group)
      groups_for_export << gr
    end
    puts groups_for_export.to_json
    '
- "gitlab-rails runner '\nclass
ProjectMemberForExport\n  attr_accessor :id\n  attr_accessor
    :type\n  attr_accessor :access_level\nend\n\nclass
ProjectForExport\n  attr_accessor
    :id\n  attr_accessor :name\n  attr_accessor :full_name\n  attr_accessor :full_pat
h\n
    \
attr_accessor :visibility\n  attr_accessor :owner\n  attr_accessor :project_members\n
\n
    \ def fill_members(project)\n    @owner =
ProjectMemberForExport.new\n    @owner.id
    = project.owner.id\n    @owner.access_level = 50\n    @owner.type =
project.owner.class.name\n
    \   \n    @project_members = [@owner]\n\n    project.members.each do |member|\n
    \     next if @owner.type == \"User\" && member.user_id == @owner.id\n\n      pm
    = ProjectMemberForExport.new\n      pm.id = member.user_id\n      pm.access_level
```

```
    = member.access_level\n      pm.type = \"User\"\n\n      @project_members << pm\n
    \   end\n\n    project.project_group_links.each do |group_member|\n      pm =
    ProjectMemberForExport.new\n      pm.id =
group_member.group_id\n      pm.access_level
    = group_member.group_access\n      pm.type = \"Group\"\n\n      @project_members
    << pm\n    end\n  end\nend\n\nproject_for_export = []\n\nProject.all.each do |
project|\n
    \ pr = ProjectForExport.new\n  pr.id = project.id\n  pr.name = project.name\n
    \ pr.full_name = project.full_name\n  pr.full_path =
project.full_path\n  pr.visibility
    = project.visibility\n\n  pr.fill_members(project)\n\n  project_for_export <<
    pr\nend\n\nputs project_for_export.to_json\n'"
- |-
    gitlab-rails runner '
    class SettingForExport
      attr_accessor :signup_enabled
      attr_accessor :password_authentication_enabled_for_web
      attr_accessor :password_authentication_enabled_for_git
    end
    setting = ApplicationSetting.current
    setting_for_export = SettingForExport.new
    setting_for_export.signup_enabled = setting.signup_enabled
    setting_for_export.password_authentication_enabled_for_web =
      setting.password_authentication_enabled_for_web
    setting_for_export.password_authentication_enabled_for_git =
      setting.password_authentication_enabled_for_git
    puts setting_for_export.to_json
    '
- |-
    gitlab-rails runner '
    class UserForExport
      attr_accessor :id
      attr_accessor :username
      attr_accessor :name
      attr_accessor :admin
      attr_accessor :state
      attr_accessor :otp_required_for_login
      attr_accessor :type
      attr_accessor :identities
      attr_accessor :key_fingerprints
    end
    users_for_export = []
    User.all.each do |user|
      us = UserForExport.new
      us.id = user.id
      us.username = user.username
      us.name = user.name
```

```
      us.admin = user.admin
      us.state = user.state
      us.otp_required_for_login = user.otp_required_for_login
      us.type = user.user_type
      us.identities = user.identities
      us.key_fingerprints = user.keys.map { |key| key.fingerprint }
      users_for_export << us
    end
    puts users_for_export.to_json
    '
- gitlab-rake gitlab:env:info
- grubby --info ALL
- host ?host_field
- hostname
- hostname -f 2>/dev/null
- hostname -s
- ifconfig -a
- initctl list
- initctl show-config
- ip -4 route show
- ip -6 route show
- ip addr show
- ip address
- ip neigh show
- iptables-save
- ls -l /dev/disk/by-uuid/
- ls -l /proc/*/exe 2>/dev/null
- ls -l ?path
- ls -lLd ?path
- ls -lZdL ?path
- lsblk -o UUID,MOUNTPOINT
- lsnrctl status
- lspci
- lsusb 2>/dev/null
- lvdisplay 2>/dev/null
- mount
- netstat -vpntua 2>/dev/null
- networkctl list
- nmcli connection show ?interface_id
- nsenter -t ?container_pid -m /bin/cat /etc/SuSE-release
- nsenter -t ?container_pid -m /bin/cat /etc/centos-release
- nsenter -t ?container_pid -m /bin/cat /etc/debian_version
- nsenter -t ?container_pid -m /bin/cat /etc/enterprise-release
- nsenter -t ?container_pid -m /bin/cat /etc/lsb-release
- nsenter -t ?container_pid -m /bin/cat /etc/oracle-release
- nsenter -t ?container_pid -m /bin/cat /etc/os-release
```

```
- nsenter -t ?container_pid -m /bin/cat /etc/redhat-release
- nsenter -t ?container_pid -m rpm -qa '*release*' 2>/dev/null
- openvpn --version
- pargs ?pid
- pgrep -l -x 'dhclient|systemd-network|NetworkManager|dhcpcd|wickedd-dhcp4'
- ps -e -o pid,ppid,tty,user,group,etime,comm
- ps -ef
- ps -eo lstart -o ";%p;%P;%U;%G;%y;" -o label -o ";%c;%a"
- pvdisplay 2>/dev/null
- rpm -qa '*release*' 2>/dev/null
- rpm -qa --qf 'Name=%{NAME}\nEpoch=%{EPOCH}\nVersion=%{VERSION}\nRelease=%{RELEASE}
\n\n'
- rpm -qf --qf '%{NAME}\n' ?path
- ss -tupan 2>/dev/null
- stat -L ?filepath
- sysctl -a
- systemctl cat openvpn-server@.service
- systemctl cat openvpn@.service
- systemctl get-default
- systemctl list-unit-files -t target --no-pager --no-legend
- systemctl list-units -a --type target --no-pager --no-legend
- systemctl list-units -t service --all --no-pager --no-legend
- systemctl status openvpn*
- test -d ?path; echo $??
- test -e /proc/self/status && cat /proc/self/status
- test -e ?path; echo $??
- test -f ?path; echo $??
- uname
- uname -m
- uname -n
- uname -p
- uname -r
- uname -s
- uname -v
- vgdisplay 2>/dev/null
- who -r
- wicked test dhcp4 ?interface_id
```

Oracle Solaris

При проведении аудита модуль audit выполняет на активе следующие команды:

```
- /sbin/dhcpinfo -i ?interface_name 54
- /usr/sbin/check-hostname
- /usr/sbin/ifconfig -a
- ?path --version
- ?which_path ?command
```

```
- PATH=?path; ?which_path ?command
- arp -an
- at -l
- bootadm list-menu
- bootadm set-menu-password -l
- bootadm show-entry -i ?ids
- date +%s 2>/dev/null
- dladm show-link
- echo $LOGNAME
- env
- file -bL ?path
- find -H ?mask
- find ?path -type f -follow
- hostid
- hostname
- ifconfig -a
- iostat -Enr 2>/dev/null
- ip addr show
- ip address
- ipfstat -ioR
- kstat -pm cpu_info
- kstat | egrep -i '(vmw|xen|hyper-v|microsoft|vbox|virtualbox|oracle vm|parallels|
hitachi|qemu)'
- ls -l /proc/?pid/path
- ls -l ?path
- ls -lLd ?path
- netstat -anf inet
- netstat -anf inet6
- netstat -rnv
- nslookup -type=PTR ?host_field
- nslookup ?host_field
- pargs ?pid
- perl -e 'print time."\n"' 2>/dev/null
- pfctl -t ?table -T show
- pfctl -vvsr
- pfiles ?pid
- pkg list
- pkg search -l -H -o pkg.name ?path
- pkgchk -l -p ?path
- pkginfo -x
- prtconf
- prtpicl -v -c cpu
- prtvtoc ?file_name
- ps -e -o pid,ppid,tty,user,group,etime,comm
- ps -eo lstart -o ";%p;%P;%U;%G;%y;" -o label -o ";%c;%a"
- rmformat 2>/dev/null
```

```
- scanpci 2>/dev/null
- showrev -p
- smbios -t SMB_TYPE_BASEBOARD
- smbios -t SMB_TYPE_BIOS
- smbios -t SMB_TYPE_SYSTEM
- svcs -a 2>/dev/null
- svcs -d ?resource_id | uniq
- swap -s
- test -d ?path; echo $??
- test -e ?path; echo $??
- uname
- uname -m
- uname -n
- uname -p
- uname -r
- uname -s
- uname -v
- who -r
- zonename
```

Palo Alto Networks PAN-OS

При проведении аудита модуль audit выполняет на активе следующие команды:

```
- |-
    configure
    show
    exit
- show arp all
- show arp management
- show interface ?name
- show interface hardware
- show interface logical
- show interface management
- show routing route
- show system info
```

Qtech QSW

При проведении аудита модуль audit выполняет на активе следующие команды:

```
- show arp
- show interface
- show ip route
- show ipv6 interface brief
- show mac-address-table
- show running-config
- show startup-config
```

```
- show version
- show vlan
```

Red Hat Enterprise Linux

При проведении аудита модуль audit выполняет на активе следующие команды:

```
- |4
    ls -1tr /var/lib/{dhcp,dhclient}/dhclient*.lease* 2>/dev/null |
    xargs cat 2>/dev/null | awk '
    BEGIN {block = ""; do_flag = 0; ifname = "";} {
        if ($0 ~ /\}/) {
            do_flag = 0;
            if (ifname) lease_arr[ifname] = block;
        }
        if (do_flag) {
            block = (block "\n" $0);
            if ($0 ~ /^[[:space:]]*interface[[:space:]]+".*";/) {
                ifname = gensub(/^[^"]*"|";.*/, "", "g", $0);
            }
        }
        if ($0 ~ /^lease/) {
            do_flag = 1;
            block = "";
        }
    }
    END {
        for (i in lease_arr) {
            print lease_arr[i];
        }
    }'
- /etc/init.d/?service_name status 2>/dev/null
- /sbin/blkid ?filesystem
- /sbin/runlevel 2>/dev/null
- /usr/sbin/ifconfig -a
- ?path --version
- ?path -V
- ?which_path ?command
- PATH=?path; ?which_path ?command
- arch
- arp -n
- at -l
- auditctl -l
- auditctl -v
- chkconfig --list
- df -kP
- df /
```

```
- dhcpcd --dumplease ?interface_id
- dhcpcd --version | head -n1
- dmesg
- dmidecode
- dmidecode --string system-uuid
- docker container ls --all --no-trunc --format='{{ .ID}}' | xargs -r docker inspect
- docker image ls --all --no-trunc --format='{{json .ID}}' | uniq | xargs -r docker
    inspect
- docker info --format='{{json .}}'
- docker ps --no-trunc -f "ancestor=?image_id" --format="{{.ID}}" | head -n 1 | xargs
    -r docker inspect --format="{{.State.Pid}}"
- echo $LOGNAME
- egrep -i 'ORA_HOME|ORACLE_HOME' /etc/rc*/* /etc/init.d/* /home/*/.oraenv /home/
*/.bash_profile
    -s -l 2>/dev/null
- env
- fdisk -l
- file -bL ?path
- find -H /etc/rc*.d
- find -H ?mask
- find ?oracle_home/dbs -type f \( -iname 'init*.ora' ! -iname 'init.ora' \)
- find ?oracle_home/dbs -type f \( -iname 'spfile*.ora' \)
- find ?path -type f -follow
- free
- getfacl --skip-base --absolute-names ?path
- |-
    gitlab-rails runner '
    class MemberForExport
      attr_accessor :id
      attr_accessor :type
      attr_accessor :access_level
    end
    class GroupForExport
      attr_accessor :id
      attr_accessor :name
      attr_accessor :full_name
      attr_accessor :full_path
      attr_accessor :visibility
      attr_accessor :parent_id
      attr_accessor :group_members
      def fill_members(group)
        @group_members = []
        group.members.each do |member|
          pm = MemberForExport.new
          pm.id = member.user_id
          pm.access_level = member.access_level
```

```
          pm.type = "User"
          @group_members << pm
        end
        group.shared_with_group_links.each do |group_member|
          pm = MemberForExport.new
          pm.id = group_member.shared_with_group_id
          pm.access_level = group_member.group_access
          pm.type = "Group"
          @group_members << pm
        end
      end
    end
    groups_for_export = []
    Group.all.each do |group|
      gr = GroupForExport.new
      gr.id = group.id
      gr.name = group.name
      gr.full_name = group.full_name
      gr.full_path = group.full_path
      gr.visibility = group.visibility
      gr.parent_id = group.parent.try(:id)
      gr.fill_members(group)
      groups_for_export << gr
    end
    puts groups_for_export.to_json
    '
- "gitlab-rails runner '\nclass
ProjectMemberForExport\n  attr_accessor :id\n  attr_accessor
    :type\n  attr_accessor :access_level\nend\n\nclass
ProjectForExport\n  attr_accessor
    :id\n  attr_accessor :name\n  attr_accessor :full_name\n  attr_accessor :full_pat
h\n
    \
attr_accessor :visibility\n  attr_accessor :owner\n  attr_accessor :project_members\n
\n
    \ def fill_members(project)\n    @owner =
ProjectMemberForExport.new\n    @owner.id
    = project.owner.id\n    @owner.access_level = 50\n    @owner.type =
project.owner.class.name\n
    \   \n    @project_members = [@owner]\n\n    project.members.each do |member|\n
    \     next if @owner.type == \"User\" && member.user_id == @owner.id\n\n      pm
    = ProjectMemberForExport.new\n      pm.id = member.user_id\n      pm.access_level
    = member.access_level\n      pm.type = \"User\"\n\n      @project_members << pm\n
    \   end\n\n    project.project_group_links.each do |group_member|\n      pm =
    ProjectMemberForExport.new\n      pm.id =
group_member.group_id\n      pm.access_level
    = group_member.group_access\n      pm.type = \"Group\"\n\n      @project_members
```

```
    << pm\n    end\n  end\nend\n\nproject_for_export = []\n\nProject.all.each do |
project|\n
    \ pr = ProjectForExport.new\n  pr.id = project.id\n  pr.name = project.name\n
    \ pr.full_name = project.full_name\n  pr.full_path =
project.full_path\n  pr.visibility
    = project.visibility\n\n  pr.fill_members(project)\n\n  project_for_export <<
    pr\nend\n\nputs project_for_export.to_json\n'"
- |-
    gitlab-rails runner '
    class SettingForExport
      attr_accessor :signup_enabled
      attr_accessor :password_authentication_enabled_for_web
      attr_accessor :password_authentication_enabled_for_git
    end
    setting = ApplicationSetting.current
    setting_for_export = SettingForExport.new
    setting_for_export.signup_enabled = setting.signup_enabled
    setting_for_export.password_authentication_enabled_for_web =
      setting.password_authentication_enabled_for_web
    setting_for_export.password_authentication_enabled_for_git =
      setting.password_authentication_enabled_for_git
    puts setting_for_export.to_json
    '
- |-
    gitlab-rails runner '
    class UserForExport
      attr_accessor :id
      attr_accessor :username
      attr_accessor :name
      attr_accessor :admin
      attr_accessor :state
      attr_accessor :otp_required_for_login
      attr_accessor :type
      attr_accessor :identities
      attr_accessor :key_fingerprints
    end
    users_for_export = []
    User.all.each do |user|
      us = UserForExport.new
      us.id = user.id
      us.username = user.username
      us.name = user.name
      us.admin = user.admin
      us.state = user.state
      us.otp_required_for_login = user.otp_required_for_login
      us.type = user.user_type
      us.identities = user.identities
```

```
      us.key_fingerprints = user.keys.map { |key| key.fingerprint }
      users_for_export << us
    end
    puts users_for_export.to_json
    '
- gitlab-rake gitlab:env:info
- grubby --info ALL
- host ?host_field
- hostname
- hostname -f 2>/dev/null
- hostname -s
- ifconfig -a
- initctl list
- initctl show-config
- ip -4 route show
- ip -6 route show
- ip addr show
- ip address
- ip neigh show
- iptables-save
- ls -l /dev/disk/by-uuid/
- ls -l /proc/*/exe 2>/dev/null
- ls -l ?path
- ls -lLd ?path
- ls -lZdL ?path
- lsblk -o UUID,MOUNTPOINT
- lsnrctl status
- lspci
- lsusb 2>/dev/null
- lvdisplay 2>/dev/null
- mount
- netstat -vpntua 2>/dev/null
- networkctl list
- nmcli connection show ?interface_id
- nsenter -t ?container_pid -m /bin/cat /etc/SuSE-release
- nsenter -t ?container_pid -m /bin/cat /etc/centos-release
- nsenter -t ?container_pid -m /bin/cat /etc/debian_version
- nsenter -t ?container_pid -m /bin/cat /etc/enterprise-release
- nsenter -t ?container_pid -m /bin/cat /etc/lsb-release
- nsenter -t ?container_pid -m /bin/cat /etc/oracle-release
- nsenter -t ?container_pid -m /bin/cat /etc/os-release
- nsenter -t ?container_pid -m /bin/cat /etc/redhat-release
- nsenter -t ?container_pid -m rpm -qa '*release*' 2>/dev/null
- openvpn --version
- pargs ?pid
- pgrep -l -x 'dhclient|systemd-network|NetworkManager|dhcpcd|wickedd-dhcp4'
```

```
- ps -e -o pid,ppid,tty,user,group,etime,comm
- ps -ef
- ps -eo lstart -o ";%p;%P;%U;%G;%y;" -o label -o ";%c;%a"
- pvdisplay 2>/dev/null
- rpm -qa '*release*' 2>/dev/null
- rpm -qa --qf 'Name=%{NAME}\nEpoch=%{EPOCH}\nVersion=%{VERSION}\nRelease=%{RELEASE}
\nSignature=%{SIGGPG:pgpsig}\n\n'
- rpm -qa --qf 'Name=%{NAME}\nEpoch=%{EPOCH}\nVersion=%{VERSION}\nRelease=%{RELEASE}
\nSignature=%{SIGPGP:pgpsig}\n\n'
- rpm -qf --qf '%{NAME}\n' ?path
- ss -tupan 2>/dev/null
- stat -L ?filepath
- sysctl -a
- systemctl cat openvpn-server@.service
- systemctl cat openvpn@.service
- systemctl get-default
- systemctl list-unit-files -t target --no-pager --no-legend
- systemctl list-units -a --type target --no-pager --no-legend
- systemctl list-units -t service --all --no-pager --no-legend
- systemctl status openvpn*
- test -d ?path; echo $??
- test -e /proc/self/status && cat /proc/self/status
- test -e ?path; echo $??
- test -f ?path; echo $??
- uname
- uname -m
- uname -n
- uname -p
- uname -r
- uname -s
- uname -v
- vgdisplay 2>/dev/null
- who -r
- wicked test dhcp4 ?interface_id
```

SUSE Linux Enterprise Server

При проведении аудита модуль audit выполняет на активе следующие команды:

```
- /etc/init.d/?service_name status 2>/dev/null
- /sbin/blkid ?filesystem
- /sbin/runlevel 2>/dev/null
- /usr/lib/wicked/bin/wickedd-dhcp4 --test ?interface_id
- /usr/sbin/ifconfig -a
- ?path --version
- ?path -V
- ?which_path ?command
```

```
- PATH=?path; ?which_path ?command
- arch
- arp -n
- at -l
- auditctl -l
- auditctl -v
- chkconfig --list
- df -kP
- df /
- dhcpcd --dumplease ?interface_id
- dhcpcd --version | head -n1
- dmesg
- dmidecode
- dmidecode --string system-uuid
- docker container ls --all --no-trunc --format='{{ .ID}}' | xargs -r docker inspect
- docker image ls --all --no-trunc --format='{{json .ID}}' | uniq | xargs -r docker
    inspect
- docker info --format='{{json .}}'
- docker ps --no-trunc -f "ancestor=?image_id" --format="{{.ID}}" | head -n 1 | xargs
    -r docker inspect --format="{{.State.Pid}}"
- echo $LOGNAME
- env
- fdisk -l
- file -bL ?path
- find -H /etc/rc*.d
- find -H ?mask
- find /var/lib/dhcpcd -type f -name 'dhcpcd-*.info' | while read FILE; do cat $FILE;
    echo; done
- find ?path -type f -follow
- free
- getfacl --skip-base --absolute-names ?path
- |-
    gitlab-rails runner '
    class MemberForExport
      attr_accessor :id
      attr_accessor :type
      attr_accessor :access_level
    end
    class GroupForExport
      attr_accessor :id
      attr_accessor :name
      attr_accessor :full_name
      attr_accessor :full_path
      attr_accessor :visibility
      attr_accessor :parent_id
      attr_accessor :group_members
```

```
      def fill_members(group)
        @group_members = []
        group.members.each do |member|
          pm = MemberForExport.new
          pm.id = member.user_id
          pm.access_level = member.access_level
          pm.type = "User"
          @group_members << pm
        end
        group.shared_with_group_links.each do |group_member|
          pm = MemberForExport.new
          pm.id = group_member.shared_with_group_id
          pm.access_level = group_member.group_access
          pm.type = "Group"
          @group_members << pm
        end
      end
    end
    groups_for_export = []
    Group.all.each do |group|
      gr = GroupForExport.new
      gr.id = group.id
      gr.name = group.name
      gr.full_name = group.full_name
      gr.full_path = group.full_path
      gr.visibility = group.visibility
      gr.parent_id = group.parent.try(:id)
      gr.fill_members(group)
      groups_for_export << gr
    end
    puts groups_for_export.to_json
    '
- "gitlab-rails runner '\nclass
ProjectMemberForExport\n  attr_accessor :id\n  attr_accessor
    :type\n  attr_accessor :access_level\nend\n\nclass
ProjectForExport\n  attr_accessor
    :id\n  attr_accessor :name\n  attr_accessor :full_name\n  attr_accessor :full_pat
h\n
    \
attr_accessor :visibility\n  attr_accessor :owner\n  attr_accessor :project_members\n
\n
    \ def fill_members(project)\n    @owner =
ProjectMemberForExport.new\n    @owner.id
    = project.owner.id\n    @owner.access_level = 50\n    @owner.type =
project.owner.class.name\n
    \   \n    @project_members = [@owner]\n\n    project.members.each do |member|\n
    \     next if @owner.type == \"User\" && member.user_id == @owner.id\n\n      pm
    = ProjectMemberForExport.new\n      pm.id = member.user_id\n      pm.access_level
```

```
    = member.access_level\n      pm.type = \"User\"\n\n      @project_members << pm\n
    \   end\n\n    project.project_group_links.each do |group_member|\n      pm =
    ProjectMemberForExport.new\n      pm.id =
group_member.group_id\n      pm.access_level
    = group_member.group_access\n      pm.type = \"Group\"\n\n      @project_members
    << pm\n    end\n  end\nend\n\nproject_for_export = []\n\nProject.all.each do |
project|\n
    \ pr = ProjectForExport.new\n  pr.id = project.id\n  pr.name = project.name\n
    \ pr.full_name = project.full_name\n  pr.full_path =
project.full_path\n  pr.visibility
    = project.visibility\n\n  pr.fill_members(project)\n\n  project_for_export <<
    pr\nend\n\nputs project_for_export.to_json\n'"
- |-
    gitlab-rails runner '
    class SettingForExport
      attr_accessor :signup_enabled
      attr_accessor :password_authentication_enabled_for_web
      attr_accessor :password_authentication_enabled_for_git
    end
    setting = ApplicationSetting.current
    setting_for_export = SettingForExport.new
    setting_for_export.signup_enabled = setting.signup_enabled
    setting_for_export.password_authentication_enabled_for_web =
      setting.password_authentication_enabled_for_web
    setting_for_export.password_authentication_enabled_for_git =
      setting.password_authentication_enabled_for_git
    puts setting_for_export.to_json
    '
- |-
    gitlab-rails runner '
    class UserForExport
      attr_accessor :id
      attr_accessor :username
      attr_accessor :name
      attr_accessor :admin
      attr_accessor :state
      attr_accessor :otp_required_for_login
      attr_accessor :type
      attr_accessor :identities
      attr_accessor :key_fingerprints
    end
    users_for_export = []
    User.all.each do |user|
      us = UserForExport.new
      us.id = user.id
      us.username = user.username
      us.name = user.name
```

```
      us.admin = user.admin
      us.state = user.state
      us.otp_required_for_login = user.otp_required_for_login
      us.type = user.user_type
      us.identities = user.identities
      us.key_fingerprints = user.keys.map { |key| key.fingerprint }
      users_for_export << us
    end
    puts users_for_export.to_json
    '
- gitlab-rake gitlab:env:info
- host ?host_field
- hostname
- hostname -f 2>/dev/null
- hostname -s
- ifconfig -a
- initctl list
- initctl show-config
- ip -4 route show
- ip -6 route show
- ip addr show
- ip address
- ip neigh show
- iptables-save
- ls -l /dev/disk/by-uuid/
- ls -l /proc/*/exe 2>/dev/null
- ls -l ?path
- ls -lLd ?path
- ls -lZdL ?path
- lsblk -o UUID,MOUNTPOINT
- lspci
- lsusb 2>/dev/null
- lvdisplay 2>/dev/null
- mount
- netstat -vpntua 2>/dev/null
- networkctl list
- nmcli connection show ?interface_id
- nsenter -t ?container_pid -m /bin/cat /etc/SuSE-release
- nsenter -t ?container_pid -m /bin/cat /etc/centos-release
- nsenter -t ?container_pid -m /bin/cat /etc/debian_version
- nsenter -t ?container_pid -m /bin/cat /etc/enterprise-release
- nsenter -t ?container_pid -m /bin/cat /etc/lsb-release
- nsenter -t ?container_pid -m /bin/cat /etc/oracle-release
- nsenter -t ?container_pid -m /bin/cat /etc/os-release
- nsenter -t ?container_pid -m /bin/cat /etc/redhat-release
- nsenter -t ?container_pid -m rpm -qa '*release*' 2>/dev/null
```

```
- pargs ?pid
- pgrep -l -x 'dhclient|systemd-network|NetworkManager|dhcpcd|wickedd-dhcp4'
- ps -e -o pid,ppid,tty,user,group,etime,comm
- ps -eo lstart -o ";%p;%P;%U;%G;%y;" -o label -o ";%c;%a"
- pvdisplay 2>/dev/null
- rpm -qa '*release*' 2>/dev/null
- rpm -qa --qf '%{NAME}|%{VERSION}|%{RELEASE}|%{ARCH}\n'
- ss -tupan 2>/dev/null
- sysctl -a
- systemctl get-default
- systemctl list-unit-files -t target --no-pager --no-legend
- systemctl list-units -a --type target --no-pager --no-legend
- systemctl list-units -t service --all --no-pager --no-legend
- test -d ?path; echo $??
- test -e /proc/self/status && cat /proc/self/status
- test -e ?path; echo $??
- test -f ?path; echo $??
- uname
- uname -m
- uname -p
- uname -s
- vgdisplay 2>/dev/null
- who -r
- wicked test dhcp4 ?interface_id
```

VMware vSphere Hypervisor (ESXi)

При проведении аудита модуль audit выполняет на активе следующие команды:

```
- esxcfg-info --hardware --format xml
- esxcfg-nics -l
- esxcli hardware cpu global get
- esxcli hardware memory get
- esxcli network firewall get
- esxcli network firewall ruleset allowedip list
- esxcli network firewall ruleset list
- esxcli network firewall ruleset rule list
- esxcli network ip interface ipv4 get
- esxcli network ip interface list
- esxcli network ip neighbor list
- esxcli network nic list
- esxcli system hostname get
- esxcli system uuid get
- esxcli system version get
- find ?path -type f -follow
- hostname
- uname -a
```

```
- vmkvsitools lspci
- vsish -e get /hardware/bios/biosInfo
- vsish -e get /hardware/cpu/cpuModelName
```

Предметный указатель

I

J

M

N

O

P

Q

R

S

U

V

W

Б

Р

positive technologies

Positive Technologies — лидер рынка результативной кибербезопасности. Компания является ведущим разработчиком продуктов, решений и сервисов, позволяющих выявлять и предотвращать кибератаки до того, как они причинят неприемлемый ущерб бизнесу и целым отраслям экономики. Наши технологии используют более 3300 организаций по всему миру, в том числе 80% компаний из рейтинга «Эксперт-400». Positive Technologies — первая и единственная компания из сферы кибербезопасности на Московской бирже (MOEX: POSI), у нее более 170 тысяч акционеров.