MaxPatrol VM версия 2.8

Настройка источников

Дата редакции документа: 10.06.2025

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 и обновлению 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. Антивирусное программное обеспечение

Раздел содержит инструкции для настройки аудита поддерживаемого в MaxPatrol VM антивирусного программного обеспечения.

В этом разделе

2.1. Kaspersky Security Center 13—14.2: настройка актива

Настройку актива нужно выполнять в Kaspersky Security Center Web Console от имени учетной записи с ролью «Главный администратор».

Инструкции по настройке и установке Kaspersky Security Center Web Console см. на сайте kaspersky.ru.

Для аудита актива нужно:

1. Создать учетную запись для доступа MP 10 Collector к активу через веб-API.
2. Создать и настроить роль для учетной записи.
3. Назначить созданную роль учетной записи.

► Чтобы создать и настроить учетную запись для доступа к активу:

1. Запустите Kaspersky Security Center Web Console.
2. Войдите на сервер администрирования от имени учетной записи с ролью «Главный администратор».
3. На главной странице выберите **Пользователи и роли** → **Пользователи**.
4. Нажмите **Добавить**.
5. Выберите тип учетной записи **Пользователь**.
6. Введите логин учетной записи.
7. Введите пароль учетной записи.
8. Нажмите **ОК**.
9. На главной странице выберите **Пользователи и роли** → **Роли**.
10. Нажмите **Добавить**.
11. Введите название роли.
12. Нажмите **ОК**.
13. Выберите вкладку **Права доступа**.

14. В иерархическом списке выберите **Сервер администрирования** → **Общий функционал** → **Базовая функциональность**.
15. Установите флажок **Чтение**.
16. Нажмите **Сохранить**.
17. На главной странице выберите **Пользователи и роли** → **Пользователи и группы**.
18. Выберите вкладку **Пользователи**.
19. Выберите учетную запись для доступа к активу.
20. Нажмите **Назначить роль**.
21. Выберите созданную ранее роль.
22. Нажмите **Далее**.
23. Выберите область действия роли.
24. Нажмите **Назначить роль**.

2.2. Kaspersky Security Center 13—14.2: настройка MaxPatrol VM

Для аудита актива в MaxPatrol VM нужно добавить учетную запись для доступа к активу, создать и запустить задачу на аудит.

В этом разделе

Добавление учетной записи для доступа к активу через веб-API (см. раздел 2.2.1)

Создание задачи на аудит актива через веб-API (см. раздел 2.2.2)

2.2.1. Добавление учетной записи для доступа к активу через веб-API

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

1. В главном меню выберите **Сбор данных** → **Учетные записи**.
2. Нажмите **Добавить учетную запись** → **Логин — пароль**.
3. Введите название учетной записи.
4. В раскрывающемся списке **Метки** установите флажок **Web_API**.
5. Введите логин учетной записи.
6. Введите пароль и подтвердите его.
7. Нажмите **Создать**.

2.2.2. Создание задачи на аудит актива через веб-API

- Чтобы создать и запустить задачу на аудит актива:

  1. В главном меню выберите **Сбор данных** → **Задачи**.
  2. Нажмите **Создать задачу** → **Сбор данных**.
  3. Введите название задачи.
  4. В раскрывающемся списке **Профиль** выберите **Web API Audit**.
  5. В иерархическом списке выберите **Сканирование систем** → **Через веб-API**.
  6. В раскрывающемся списке **Тип аутентификации** выберите **Учетные данные**.
  7. Выберите учетную запись для доступа к активу.
  8. Если требуется, выберите коллекторы для сбора данных.
  9. 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.

  10. Нажмите **Сохранить и запустить** → **Запустить сбор данных**.

3. Межсетевые экраны

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

В этом разделе

3.1. 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. Пройдите аутентификацию 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.

3.2. 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

3.2.1. Добавление учетной записи для доступа по SSH

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

  1. В главном меню выберите **Сбор данных** → **Учетные записи**.

Откроется страница **Учетные записи**.

2. Нажмите **Добавить учетную запись** → **Логин — пароль**.

   Откроется страница **Добавление учетной записи**.

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

Учетная запись добавлена.

3.2.2. Добавление пароля для повышения привилегий для аудита по SSH

- Чтобы добавить в MaxPatrol VM пароль для повышения привилегий:

  1. В главном меню выберите **Сбор данных** → **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. Введите название учетной записи.
  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.

3.2.3. Создание задачи на аудит актива по SSH

- Чтобы создать задачу на проведение аудита актива:

  1. В главном меню выберите **Сбор данных** → **Задачи**.

     Откроется страница **Задачи по сбору данных**.

  2. Нажмите **Создать задачу** → **Сбор данных**.

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

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

4. 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.

5. В иерархическом списке выберите пункт **Сканирование систем** → **Через терминал: SSH и Telnet**.
6. В раскрывающемся списке **Учетная запись** выберите учетную запись для доступа к активу.
7. В раскрывающемся списке **Учетная запись для повышения привилегий** выберите учетную запись для повышения привилегий на активе.
8. Если требуется, в раскрывающемся списке **Коллекторы** выберите коллекторы для сбора данных.
9. 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.

10. Нажмите кнопку **Сохранить**.

Задача на проведение аудита актива создана.

3.3. Cisco FTD 6.6: настройка актива

Настройку актива нужно выполнять от имени учетной записи администратора устройства.

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

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

► Чтобы создать учетную запись для доступа к активу:

1. На узле, с которого производится настройка, запустите терминальный клиент, поддерживающий протокол SSH.
2. Пройдите аутентификацию на активе.
3. Создайте учетную запись для доступа к активу:

   ```
   configure user add <Логин> basic
   ```

4. Установите пароль учетной записи и подтвердите его.

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

3.4. Cisco FTD 6.6: настройка MaxPatrol VM

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

В этом разделе

3.4.1. Добавление учетной записи для доступа к активу по SSH

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

  1. В главном меню выберите **Сбор данных** → **Учетные записи**.
  2. Нажмите **Добавить учетную запись** → **Логин — пароль**.
  3. Введите название учетной записи.
  4. В раскрывающемся списке **Метки** установите флажок **Terminal**.
  5. Введите логин учетной записи.
  6. Введите пароль и подтвердите его.
  7. Нажмите **Создать**.

3.4.2. Создание и запуск задачи на аудит актива по SSH

- Чтобы создать и запустить задачу на аудит актива:

  1. В главном меню выберите **Сбор данных** → **Задачи**.
  2. Нажмите **Создать задачу** → **Сбор данных**.
  3. Введите название задачи.
  4. В раскрывающемся списке **Профиль** выберите **SSH Network Device Audit**.
  5. В иерархическом списке выберите **Сканирование систем** → **Через терминал: SSH**.
  6. Выберите учетную запись для доступа к активу.
  7. Если требуется, выберите коллекторы для сбора данных.
  8. В панели **Цели сбора данных** на вкладке **Включить** выполните одно из следующих действий:

     - Если для сканируемой цели ранее был добавлен актив, в поле **Активы** введите IP-адрес или доменное имя (в формате FQDN) узла актива.

- Если для сканируемой цели актив ранее не был добавлен, в поле **Сетевые адреса** введите ее IP-адрес или доменное имя (в формате FQDN).

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

9. Нажмите **Сохранить и запустить** → **Запустить сбор данных**.

3.5. Fortinet FortiGate 5.4.2—7.4.4: 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.

Для проведения аудита нужно создать на активе учетную запись с правом на чтение для доступа MP 10 Collector по протоколу SSH версии 2.

В этом разделе

Настройка актива для устройств с отключенной технологией виртуальных доменов VDOM (см. раздел 3.5.1)

Настройка актива для устройств с включенной технологией виртуальных доменов VDOM (см. раздел 3.5.2)

3.5.1. Настройка актива для устройств с отключенной технологией виртуальных доменов VDOM

► 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. Пройдите аутентификацию на активе.
3. Перейдите в режим конфигурирования:
   ```
   config system admin
   ```
4. Создайте учетную запись для доступа к активу:
   ```
   edit "<Логин>"
   set accprofile "super_admin_readonly"
   set vdom "root"
   set password "<Пароль>"
   ```
5. Выйдите из режима конфигурирования:
   ```
   end
   ```

3.5.2. Настройка актива для устройств с включенной технологией виртуальных доменов VDOM

- 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. Пройдите аутентификацию на активе.
3. Перейдите в режим глобального конфигурирования:
   ```
   config global
   ```
4. Перейдите в режим конфигурирования системных профилей:
   ```
   config system accprofile
   ```
5. Создайте профиль с правом на чтение:
   ```
   edit "<Название профиля>"
   set scope vdom
   set secfabgrp read
   set ftviewgrp read
   set authgrp read
   set sysgrp read
   set netgrp read
   set loggrp read
   set fwgrp read
   set vpngrp read
   set utmgrp read
   set wifi read
   ```
6. Выйдите из режима конфигурирования глобальных профилей:
   ```
   end
   ```
7. Перейдите в режим конфигурирования:
   ```
   config system admin
   ```
8. Создайте для каждого виртуального домена учетную запись для доступа к активу:
   ```
   edit "<Логин>"
   set accprofile "<Название профиля>"
   set vdom "<Имя виртуального домена>"
   set password "<Пароль>"
   ```
   Например:
   ```
   edit "username1_example"
   set accprofile "RO_Profile_example"
   set vdom "vdom1_example"
   set password "password1_example"
   next
   edit "username2_example"
   set accprofile "RO_Profile_example"
   ```

```
set vdom "vdom2_example"
set password "password2_example"
```

9. Выйдите из режима конфигурирования:
   ```
   end
   ```
10. Выйдите из режима глобального конфигурирования:
    ```
    end
    ```

3.6. Fortinet FortiGate 5.4.2—7.4.4: настройка MaxPatrol VM

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

Для устройств с включенной технологией виртуальных доменов VDOM в MaxPatrol VM нужно добавить учетную запись для доступа к активу, создать и запустить задачу на проведение аудита для каждого виртуального домена.

В этом разделе

Добавление учетной записи для доступа по SSH (см. раздел 3.6.1)

Создание задачи на аудит актива по SSH (см. раздел 3.6.2)

3.6.1. Добавление учетной записи для доступа по SSH

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

  1. В главном меню выберите **Сбор данных** → **Учетные записи**.

     Откроется страница **Учетные записи**.
  2. Нажмите **Добавить учетную запись** → **Логин — пароль**.

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

  Учетная запись добавлена.

3.6.2. Создание задачи на аудит актива по SSH

- Чтобы создать задачу на проведение аудита актива:

  1. В главном меню выберите **Сбор данных** → **Задачи**.

Откроется страница **Задачи по сбору данных**.

2. Нажмите **Создать задачу** → **Сбор данных**.

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

3. В поле **Название** введите название задачи.
4. В раскрывающемся списке **Профиль** выберите **SSH Network Device Audit**.
5. В иерархическом списке выберите пункт **Сканирование систем** → **Через терминал: SSH**.
6. В раскрывающемся списке **Учетная запись** выберите учетную запись для доступа к активу.
7. Если требуется, в раскрывающемся списке **Коллекторы** выберите коллекторы для сбора данных.
8. В панели **Цели сбора данных** на вкладке **Включить** выполните одно из следующих действий:
   - Если для сканируемой цели ранее был добавлен актив, в поле **Активы** введите IP-адрес или доменное имя (в формате FQDN) узла актива.
   - Если для сканируемой цели актив ранее не был добавлен, в поле **Сетевые адреса** введите ее IP-адрес или доменное имя (в формате FQDN).

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

Задача на проведение аудита актива создана.

3.7. UserGate UTM 6: настройка актива

Настройку актива нужно выполнять от имени учетной записи администратора.

Для проведения аудита на активе нужно создать профиль администратора с правом чтения настроек по API и учетную запись администратора для доступа MaxPatrol VM по протоколу XML-RPC API.

В этом разделе

Создание профиля администратора с правом чтения настроек по API (см. раздел 3.7.1)

Создание учетной записи администратора (см. раздел 3.7.2)

3.7.1. Создание профиля администратора с правом чтения настроек по API

- Чтобы создать профиль администратора с правом чтения настроек по API:

  1. Откройте браузер и в адресной строке введите IP-адрес веб-интерфейса UserGate.
  2. Войдите в UserGate под учетной записью с правами администратора.
  3. В главном меню перейдите по ссылке **Настройки**.
  4. Выберите **UserGate** → **Администраторы**.
  5. В панели **Профили администраторов** нажмите **Добавить**.
  6. На вкладке **Общее** введите название нового профиля.
  7. Выберите вкладку **Разрешения для API**.

     Отроется таблица, содержащая перечень объектов, доступных для делегирования доступа при работе через программный интерфейс (API).
  8. Для всех объектов в столбце **Разрешения** выберите вариант **Чтение**.

     Примечание. На вкладках **Разрешения доступа** и **Разрешения для CLI** для всех объектов в столбце **Разрешения** должен быть выбран вариант **Нет доступа**.
  9. Нажмите **Сохранить**.

3.7.2. Создание учетной записи администратора

- Чтобы создать учетную запись администратора:

  1. Откройте браузер и в адресной строке введите IP-адрес веб-интерфейса UserGate.
  2. Войдите в UserGate под учетной записью с правами администратора.
  3. В главном меню перейдите по ссылке **Настройки**.
  4. Выберите **UserGate** → **Администраторы**.
  5. В панели **Администраторы** нажмите **Добавить** → **Добавить локального администратора**.
  6. Введите логин учетной записи администратора актива.
  7. В поле **Профиль администратора** → **Выберите профиль администратора** выберите профиль с правом чтения настроек по API, созданный ранее.
  8. Введите пароль и подтвердите его.
  9. Нажмите **Сохранить**.

3.8. UserGate UTM 6: настройка MaxPatrol VM

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

В этом разделе

3.8.1. Добавление учетной записи для доступа по XML-RPC API

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

  1. В главном меню выберите **Сбор данных** → **Учетные записи**.
  2. Нажмите **Добавить учетную запись** → **Логин — пароль**.
  3. Введите название учетной записи.
  4. В раскрывающемся списке **Метки** установите флажок **Web_API**.
  5. Введите логин учетной записи администратора актива с правом чтения настроек по API.
  6. Введите пароль учетной записи администратора актива с правом чтения настроек по API и подтвердите его.
  7. Нажмите **Сохранить**.

3.8.2. Создание задачи на аудит актива по XML-RPC API

- Чтобы создать задачу на проведение аудита актива:

  1. В главном меню выберите **Сбор данных** → **Задачи**.
  2. Нажмите **Создать задачу** → **Сбор данных**.
  3. Введите название задачи.
  4. В панели **Параметры сбора данных** выберите **Профиль** → **Web API Audit**.
  5. Выберите пункт **Сканирование систем** → **Через веб-API**.
  6. В раскрывающемся списке **Учетная запись** выберите учетную запись для доступа к активу.
  7. 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.

8. Нажмите **Сохранить**.

4. Операционные системы

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

В этом разделе

4.1. Microsoft Windows XP—11; Windows Server 2003—2022: 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 TCP-порты 135, 139, 445, динамические TCP-порты 1025—5000. В Windows версии от Vista и выше, а также Windows Server версии от 2008 и выше используются TCP-порты 135, 139, 445, динамические TCP-порты 49152—65535 и UDP-порты 135, 137, 138, 445.

Для проведения аудита на активе нужно создать учетную запись для доступа MP 10 Collector к активу. Перечень типов учетных записей, которые можно использовать для аудита, а также необходимые параметры представлены в разделе «Использование различных учетных записей для сбора данных из Windows (см. раздел 17.4)».

Для использования учетной записи, не включенной в группу локальных администраторов, необходимо вручную назначить соответствующие права. Вы можете настроить учетную запись по инструкциям из разделов:

- «Настройка учетной записи, не включенной в группу локальных администраторов (см. раздел 17.4.3)»;
- «Настройка контроля локальных учетных записей (UAC) (см. раздел 17.4.2)»;
- «Отключение контроля учетных записей (UAC) (см. раздел 17.4.1)»;
- «Настройка подключения к службе WMI (см. раздел 17.5)».

4.2. Microsoft Windows XP—11; Windows Server 2003—2022: 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

4.2.1. Добавление учетной записи ОС

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

  1. В главном меню выберите **Сбор данных** → **Учетные записи**.

     Откроется страница **Учетные записи**.
  2. Нажмите **Добавить учетную запись** → **Логин — пароль**.

     Откроется страница **Добавление учетной записи**.
  3. Введите название учетной записи.
  4. В раскрывающемся списке **Метки** установите флажок **WindowsAudit**.
  5. 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, введите имя домена.
  8. Нажмите кнопку **Сохранить**.

  Учетная запись добавлена.

4.2.2. Создание и запуск задачи на аудит актива

- Чтобы создать и запустить задачу на аудит актива:

  1. В главном меню выберите **Сбор данных** → **Задачи**.

     Откроется страница **Задачи по сбору данных**.
  2. Нажмите **Создать задачу** → **Сбор данных**.

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

4. В раскрывающемся списке **Профиль** выберите **Windows Audit**.
5. В иерархическом списке выберите пункт **Сканирование систем** → **Windows**.
6. Выберите учетную запись пользователя ОС.
7. Если требуется, в раскрывающемся списке **Коллекторы** выберите коллекторы для сбора данных.
8. 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.
9. Нажмите кнопку **Сохранить и запустить**.

Задача на проведение аудита актива создана и запущена.

4.3. Unix-подобные ОС: 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.

Поддерживается настройка аудита следующих ОС семейства Unix:

- «Альт» 9, 10;
- «РЕД ОС» 7.1—7.3;
- Astra Linux Common Edition 2.12;
- Astra Linux Special Edition 1.6, 1.7;
- Canonical Ubuntu 16.04, 18.04, 20.04, 22.04;
- CentOS 7, 8;
- Debian 10, 11;
- FreeBSD 12;
- HPE HP-UX 11.31;
- IBM AIX 7.3;
- Oracle Linux 7—9;
- Oracle Solaris 11;
- Red Hat Enterprise Linux 7—9;
- SUSE Linux Enterprise Server 15.

В этом разделе

4.3.1. Аудит с помощью учетной записи root

Внимание! Аудит с использованием учетной записи root считается небезопасным, поскольку эта учетная запись предоставляет полный доступ к системе.

Настройка актива

- Чтобы настроить актив:

  1. Откройте файл конфигурации `/etc/ssh/sshd_config`.

     Примечание. В операционной системе «Альт» файл находится по пути `/etc/openssh/sshd_config`.

  2. Добавьте в файл строку:
     ```
     PermitRootLogin yes
     ```
  3. Сохраните изменения и закройте файл.

  Примечание. Для используемой учетной записи root в операционной системе Astra Linux Special Edition нужно дополнительно настроить уровень целостности (см. раздел 17.2.6).

4.3.2. Аудит с помощью повышения привилегий учетной записи через команду su

Команда `su` позволяет временно изменить учетную запись, под которой вы работаете на другую, например root.

Способы использования команды:

1. `su` — переключение на другую учетную запись с сохранением текущего окружения (например, рабочий каталог);
2. `su -` — переключение на другую учетную запись с применением окружения выбранной учетной записи.

Сценарии повышения привилегий:

1. Вход по протоколу SSH с помощью непривилегированной учетной записи и повышение привилегий до учетной записи root.
2. Вход по протоколу SSH с помощью непривилегированной учетной записи и повышение привилегий до учетной записи с настроенными sudo-обертками.

   Примечание. Второй вариант повышения привилегий возможен только с использованием команды `su -`.

   Примечание. При использовании доменной учетной записи, нужно указать доменное имя учетной записи. Если в конфигурации Winbind (`/etc/samba/smb.conf`) установлен параметр `winbind use default domain = yes`, нужно указать логин учетной записи. Если параметр не установлен, нужно использовать доменное имя учетной записи.

Настройка актива

- Чтобы настроить актив:

  1. Если требуется, создайте учетную запись для доступа к активу (см. раздел 17.2.1).
  2. Выполните дальнейшую настройку в зависимости от операционной системы.

     Примечание. Для операционной системы Oracle Solaris дальнейшая настройка не требуется.

Linux

Использование команды `su` по умолчанию разрешено для всех учетных записей. Для аудита рекомендуется разрешить использование команды `su` только учетным записям из группы `wheel`, группы с идентификатором `0` или другой группы, используя параметр `group`.

- Чтобы настроить актив:

  1. Откройте файл `/etc/pam.d/su`.
  2. Выполните одно из следующих действий:
     - Если строка `auth required pam_wheel.so` (также может иметь вид `auth required pam_wheel.so group=<Название группы>`) закомментирована в файле, раскомментируйте ее.
     - Если строка отсутствует, добавьте ее в файл.
  3. Добавьте учетную запись в группу:
     ```
     usermod -aG <Название группы> <Логин учетной записи>
     ```
  4. Сохраните изменения и закройте файл.

  Примечание. Для команды su в операционной системе «Альт» нужно дополнительно настроить политику control (см. раздел 17.2.5).

IBM AIX

- Чтобы настроить актив,

  выполните команду:

  ```
  chuser su=true sugroups=ALL <Логин учетной записи>
  ```

HPE HP-UX

Для настройки вам понадобится название группы, которое указано в файле `/etc/default/security` в параметре `SU_ROOT_GROUP`.

- Чтобы настроить актив,

  добавьте учетную запись в группу:

  ```
  usermod -G <Название группы> <Логин учетной записи>
  ```

  Примечание. Учетная запись получит как привилегии указанной группы, так и возможность использовать команду `su`.

FreeBSD

Использование команды `su` по умолчанию разрешено для всех учетных записей. Для аудита рекомендуется разрешить использование команды `su` только учетным записям из группы `wheel`, группы с идентификатором `0` или другой группы, используя параметр `group`.

- Чтобы настроить актив:

  1. Откройте файл `/etc/pam.d/su`.
  2. Выполните одно из следующих действий:
     - Если строка `auth required pam_group.so_warn group=<Название группы> root_only fail_safe ruser` закомментирована в файле, раскомментируйте ее.
     - Если строка отсутствует, добавьте ее в файл.
  3. Добавьте учетную запись в группу:
     ```
     pw usermod <Логин учетной записи> -G <Название группы>
     ```
  4. Сохраните изменения и закройте файл.

4.3.3. Аудит с помощью учетной записи с sudo-привилегиями

Внимание! На активе должна быть установлена программа sudo.

Примечание. При использовании доменной учетной записи нужно указать доменное имя учетной записи. Если в конфигурации Winbind (`/etc/samba/smb.conf`) установлен параметр `winbind use default domain = yes`, нужно указать логин учетной записи. Если параметр не установлен, нужно использовать доменное имя учетной записи.

Настройка актива

- Чтобы настроить актив:

  1. Если требуется, создайте учетную запись для доступа к активу (см. раздел 17.2.1).
  2. Выполните команду:
     ```
     visudo
     ```
  3. Добавьте в конфигурационный файл строку:
     ```
     <Логин учетной записи> ALL=(ALL) ALL
     ```
  4. Сохраните изменения и закройте файл.

  Примечание. Для используемой учетной записи в операционной системе Astra Linux Special Edition нужно дополнительно настроить уровень целостности (см. раздел 17.2.6).

  Примечание. Для команды sudo в операционной системе «Альт» нужно дополнительно настроить политику control (см. раздел 17.2.5).

4.3.4. Аудит с помощью учетной записи с sudo-обертками

В этом разделе описывается настройка учетной записи с ограничениями на выполнение команд от имени суперпользователя (root). Повышенные привилегии выдаются только командам, которые при сборе данных с актива используют MP 10 Collector.

Внимание! На активе должна быть установлена программа sudo.

Примечание. В комплект поставки MaxPatrol VM входит архив `audit_sudo_wrappers.zip`, который содержит TAR-архивы с необходимыми файлами для различных сценариев настройки. Для настройки конкретного актива достаточно выбрать один из этих сценариев. При использовании сценария настройки на языке Python или роли Ansible описанные ниже шаги выполняются автоматически.

Таблица 1. Способы настройки sudo-оберток

Способ настройки	Область применения	Автоматизация
Вручную	Один актив	Нет
С помощью роли Ansible	Один или несколько активов	Да
С помощью сценария на языке Python	Один актив	Да

Для аудита актива нужно:

1. Создать учетную запись ОС (см. раздел 17.2.1) для доступа MP 10 Collector к активу.

   Если вы планируете использовать уже существующую учетную запись, приведенную ниже настройку нужно выполнять для нее.

2. В домашний каталог учетной записи поместить каталог `bin` со сценариями sudo-оберток.

   Каталог `bin` содержит исполняемые файлы, написанные на языке shell. При их запуске выполняется одноименная утилита с использованием команды sudo. В этой инструкции под sudo-обертками подразумеваются именно эти файлы. Разрешения для выполнения утилит с использованием команды sudo настраиваются на шаге 4.

3. В домашний каталог учетной записи поместить файл `.bash_profile` с параметрами переменной окружения `$PATH`.

   Переменная `$PATH` указывает, в каких каталогах искать утилиты для выполнения команд. В поставляемом файле `.bash_profile` переменная настраивается так, чтобы приоритет был у исполняемых файлов из каталога `bin`, добавленного ранее. Настройка будет действовать только для настраиваемой учетной записи.

4. Настроить команду sudo для предоставления учетной записи права на выполнение команд для сбора данных.

   Настройка команды sudo заключается в перечислении конкретных команд, которые разрешено выполнять учетной записи с повышенными привилегиями. Разрешения выдаются только для утилит с sudo-обертками. Для одной утилиты может быть указано несколько команд, а все команды сгруппированы в тематические `Cmnd_Alias`.

В этом разделе

4.3.4.1. Автоматическая настройка sudo-оберток с помощью роли Ansible

Для этого сценария настройки нужно использовать архив `sudo_wrappers_ansible_role.tar` из архива `audit-sudo-wrappers.zip`, входящего в комплект поставки MaxPatrol 10.

На узле, с которого будет выполняться централизованная настройка, должны быть выполнены следующие условия:

— установлена система управления конфигурациями Ansible версии 2.9 или выше;

— установлена Python-библиотека passlib;

— при настройке активов от имени учетной записи, использующей связку «логин — пароль», установлен пакет `sshpass`.

На активах, которые будут настраиваться, должны быть выполнены следующие условия:

— установлен Python 2 (версия 2.6 или выше) или Python 3 (версия 3.5 или выше);

— создана учетная запись с общими данными для всех настраиваемых активов (связка «логин — пароль» или SSH-ключ);

— для команды sudo в дистрибутивах операционной системы «Альт» политика control настроена в режиме public (см. раздел Настройка политики control для команд su и sudo в операционной системе «Альт» (см. раздел 17.2.5)).

При применении роли к активу выполняются следующие действия:

— проверяется наличие необходимых утилит для сканирования;

— создается учетная запись для сканирования;

— в домашнем каталоге учетной записи создаются файлы-обертки для утилит с возможностью их запуска через программу sudo;

— изменяются правила в конфигурационном файле `/etc/sudoers.d/<Логин учетной записи>` для предоставления учетной записи прав на запуск утилит сканирования с повышенными привилегиями.

Примечание. В качестве учетных данных может использоваться как связка «логин — пароль», так и SSH-ключ.

► Чтобы запустить роль Ansible:

1. Скопируйте архив `sudo_wrappers_ansible_role.tar` на настраиваемый актив.
2. Распакуйте архив:
   ```
   tar -xvf sudo_wrappers_ansible_role.tar
   ```
3. Перейдите в каталог с файлами роли:
   ```
   cd sudo_wrappers_ansible_role
   ```
4. Откройте на редактирование инвентарный файл `hosts`.
5. В параметре `ansible_user` укажите логин учетной записи для настройки актива.

   Примечание. Если какой-то из активов использует нестандартный порт для SSH, необходимо указать этот порт в параметре `ansible_port`. Например, `ansible_port=2222`.

6. После блока параметров `targets` построчно перечислите адреса активов, на которых будет настраиваться команда sudo.

   Примечание. Если какой-то из активов использует нестандартный порт для SSH, необходимо указать этот порт рядом с IP-адресом в параметре `ansible_port`. Например, `10.10.10.10 ansible_port=2222`.

7. Сохраните изменения и закройте файл.
8. Задайте необходимые значения переменных (см. таблицу ниже) в файле `sudo-wrappers-config/defaults/main.yml`.
9. Если планируется использовать вариант конфигурации с SSH-ключом, вставьте содержимое ключа создаваемой учетной записи в файл `sudo-wrappers-config/files/mp_ssh_key.pub`.
10. Выполните команду для запуска роли на всех активах, указанных в инвентарном файле:
    ```
    ansible-playbook -i hosts --ask-become-pass sudo-wrappers-config.yml
    ```

    Примечание. При настройке активов от имени учетной записи, использующей связку «логин — пароль», необходимо добавить к команде запуска параметр `--ask-pass`. При использовании этого параметра в начале выполнения роли будет запрошен пароль, указанный в параметре `ansible_user`.

11. Введите пароль учетной записи, от имени которой производится настройка актива.
12. Введите логин учетной записи для доступа к активу (по умолчанию — `mpuser`).
13. Введите пароль учетной записи для доступа к активу и подтвердите его.

Примечание. Если доступ к активам осуществляется по логину и паролю, Ansible запросит пароль.

Таблица 2. Переменные в файле sudo-wrappers-config/defaults/main.yml

Переменная	Описание
`mp_user_name`	Логин учетной записи MaxPatrol 10 для аудита актива (по умолчанию — `mpuser`)
`mp_user_set_passwd`	Указывает, будет ли учетная запись MaxPatrol 10 использовать пароль для входа в систему. Принимает значения `true` или `false` (по умолчанию — `true`)
`mp_user_set_ssh_key`	Указывает, будет ли учетная запись MaxPatrol 10 использовать SSH-ключ для входа в систему. Принимает значения `true` или `false` (по умолчанию — `false`)

Для удобства модификации и добавления пользовательских параметров переменные, отвечающие за обработку специфики каждого дистрибутива, вынесены в файл `sudo-wrappers-config/vars/main.yml`.

Примечание. При запуске роль Ansible осуществляет проверку переменных, которая останавливается, если в обеих переменных `mp_user_set_passwd` и `mp_user_set_ssh_key` указано значение `false`.

4.3.4.2. Автоматическая настройка sudo-оберток с помощью сценария на языке Python

Для этого сценария настройки нужно использовать архив `sudo_wrappers_python_script.tar` из архива `audit-sudo-wrappers.zip`, входящего в комплект поставки MaxPatrol 10.

Внимание! Для выполнения сценария на активе должен быть установлен интерпретатор языка Python версии 3.7 или выше.

При запуске сценария на активе выполняются следующие действия:

- проверяется наличие необходимых утилит для сканирования;
- создается учетная запись для сканирования;
- в домашнем каталоге учетной записи создаются файлы-обертки для утилит с возможностью их запуска через программу sudo;
- изменяются правила в конфигурационном файле `/etc/sudoers.d/<Логин учетной записи>` для предоставления учетной записи прав на запуск утилит сканирования с повышенными привилегиями.

  Примечание. Способ настройки, приведенный в этом разделе, не предназначен для операционных систем IBM AIX, HP-UX, FreeBSD, Oracle Solaris.

► Чтобы запустить сценарий:

1. Скопируйте архив `sudo_wrappers_python_script.tar` на настраиваемый актив.
2. Распакуйте архив:
   ```
   tar -xvf sudo_wrappers_python_script.tar
   ```
3. Перейдите в каталог с файлами сценария:
   ```
   cd sudo_wrappers_python_script
   ```
4. Сделайте файл `configure_am_host.py` исполняемым:
   ```
   chmod +x configure_am_host.py
   ```
5. Выполните одно из следующих действий:
   - Если на активе нужно настроить sudo-обертки для существующей учетной записи, выполните команду:
     ```
     ./configure_am_host.py --username=<Логин учетной записи> --confirm --verbose
     ```
   - Если на активе нужно создать учетную запись для аудита и настроить для нее sudo-обертки, выполните команду:
     ```
     ./configure_am_host.py --new-user --username=<Логин учетной записи> --confirm --verbose
     ```

Внимание! Если вы создали учетную запись для аудита, нужно вручную установить для нее пароль после выполнения сценария.

Запуск необходимо производить из каталога с файлами сценария. Дополнительные параметры команды запуска указаны в таблице ниже. Справку вы можете вывести на экран с помощью команды `./configure_am_host.py --help`.

Таблица 3. Параметры запуска сценария

Параметр	Описание
`--username=USERNAME`	Логин учетной записи, для которой будет выполняться настройка команды sudo
`--new-user`	Создание учетной записи
`--install-all`	Настройка команды sudo для всех утилит, используемых во время аудита. Применяется в случаях, когда утилита еще не установлена на активе
`--confirm`	Запрос подтверждения на изменение файлов `sudoers` при выполнении сценария
`--verbose`	Вывод информации о пошаговом выполнении сценария

4.3.4.3. Настройка sudo-оберток вручную

Для этого сценария настройки нужно использовать архив `sudo_wrappers_static.tar` из архива `audit-sudo-wrappers.zip`, входящего в комплект поставки MaxPatrol 10.

Для настройки sudo-оберток вручную необходимо создать учетную запись, настроить пользовательские сценарии и команду sudo. Для отдельных дистрибутивов необходимо настроить специфичные для них параметры.

Примечание. При использовании доменной учетной записи, нужно указать доменное имя учетной записи. Если в конфигурации Winbind (`/etc/samba/smb.conf`) установлен параметр `winbind use default domain = yes`, нужно указать логин учетной записи. Если параметр не установлен, нужно использовать доменное имя учетной записи.

Создание учетной записи

Если требуется, создайте учетную запись для доступа к активу (см. раздел 17.2.1).

Примечание. Для используемой учетной записи в операционной системе Astra Linux Special Edition нужно дополнительно настроить уровень целостности (см. раздел 17.2.6).

Примечание. Для команды sudo в операционной системе «Альт» нужно дополнительно настроить политику control (см. раздел 17.2.5).

Подготовка сценариев для аудита

- Чтобы настроить пользовательские сценарии:

  1. Из архива `sudo_wrappers_static.tar` в каталоге соответствующей ОС перенесите содержимое каталога `bin` в домашний каталог учетной записи.
  2. Перейдите в домашний каталог:
     - на Oracle Solaris:
       ```
       cd /export/home/<Логин учетной записи>
       ```
     - на другой ОС:
       ```
       cd /home/<Логин учетной записи>
       ```
  3. Настройте права доступа к каталогу:
     ```
     chmod -R 700 ~/bin
     chown -R <Логин учетной записи> ~/bin
     ```
  4. Перенесите файл `.bash_profile` (или `.profile`, в зависимости от используемой командной оболочки в операционной системе) в домашний каталог учетной записи.
  5. Настройте права доступа к файлу:
     ```
     chmod 600 .bash_profile
     chown <Логин учетной записи> .bash_profile
     ```

  Примечание. Вы можете просмотреть список каталогов в переменной окружения $PATH, выполнив вход под настроенной учетной записью, затем команду `echo $PATH`. Название каталога `/home/<Логин учетной записи>/bin` отображается первым в списке.

Настройка программы sudo

Примечание. В операционной системе FreeBSD файл конфигурации sudo находится по пути `/usr/local/etc`.

- Чтобы настроить программу sudo:

  1. Выполните одно из следующих действий:
     - Если вы используете файл `/etc/sudoers` без добавления каталогов и дополнительных файлов, откройте его на редактирование, выполнив команду `visudo`.
     - Если вы импортируете в файл `/etc/sudoers` дополнительный каталог (по умолчанию `#includedir /etc/sudoers.d` или `@includedir /etc/sudoers.d`), создайте в этом каталоге новый файл и откройте его для редактирования, выполнив команду `visudo -f /etc/sudoers.d/<Логин учетной записи>`.
  2. Из архива `sudo_wrappers_static.tar` в каталоге настраиваемой ОС скопируйте содержимое файла `mpuser` в редактируемый файл.

3. В скопированном содержимом файла замените параметр `mpuser` на логин учетной записи, созданной для сканирования актива.
4. Сохраните изменения и закройте файл.

4.3.5. Аудит с использованием доменной учетной записи

Внимание! На узле актива должна быть установлена программа sudo.

Для этого сценария настройки необходимо использовать архив `sudo_wrappers_static.tar` из архива `audit-sudo-wrappers.zip`, входящего в комплект поставки MaxPatrol 10.

В этом разделе

Настройка SSSD (см. раздел 4.3.5.1)

Настройка Winbind (см. раздел 4.3.5.2)

4.3.5.1. Настройка SSSD

Для настройки актива в SSSD необходимо настроить домашний каталог, командную оболочку, пользовательские сценарии и файл конфигурации `sudoers`.

> **Примечание.** Для указания доменного имени учетной записи следует использовать формат user principal name. Например, `example@domain.ru`.

Настройка домашнего каталога

Для настройки домашнего каталога нужно:

1. Задать путь к каталогу, если он нигде не задан, одним из способов:
   - через атрибут `unixHomeDirectory` в Active Directory (AD) (см. раздел 4.3.5.1);
   - через параметр `fallback_homedir` или `override_homedir` в файле `/etc/sssd/sssd.conf` на активе (см. раздел 4.3.5.1).
2. Создать каталог на активе по заданному пути, если его не существует (см. раздел 4.3.5.1).

Настройка пути к каталогу в Active Directory

Примечание. Если используемый контроллер домена отличается от Active Directory, вы можете воспользоваться документацией вендора, чтобы правильно настроить домашний каталог. Вы также можете вручную задать значения `fallback_homedir` или `override_homedir` в файле `/etc/sssd/sssd.conf` на каждом активе.

► Чтобы задать путь к домашнему каталогу:

1. Войдите в интерфейс Active Directory.
2. Нажмите **Пользователи и компьютеры**.

3. Нажмите **Вид** → **Дополнительные компоненты**.
4. В левой части окна выберите **<Имя домена>** → **Users**.
5. В контекстном меню выберите **Свойства**.
6. Выберите вкладку **Редактор атрибутов**.
7. В блоке параметров **Атрибуты** выберите **unixHomeDirectory**.
8. В параметре задайте путь к домашнему каталогу.
9. Нажмите **OK**.
10. Нажмите **Применить**.

    Если в дальнейшем потребуется получить значение параметра `unixHomeDirectory`, вы можете выполнить команду `Get-ADUser -Identity <Логин учетной записи> -Properties "unixHomeDirectory"`.

Далее создайте домашний каталог (см. раздел 4.3.5.1).

Настройка пути к каталогу на активе

На активе путь к каталогу можно задать с помощью параметров `fallback_homedir` и `override_homedir`.

Параметр `fallback_homedir` следует использовать, если нужно задать каталог по умолчанию, который будет применяться только в случае отсутствия пути из поставщика данных (например, если атрибут `unixHomeDirectory` в Active Directory не задан). Параметр `override_homedir` следует использовать, если нужно задать путь, который будет применяться всегда, игнорируя значение `unixHomeDirectory`.

При указании пути к каталогу вы можете использовать следующие переменные:

— `%u` — логин учетной записи;

— `%U` — числовой идентификатор учетной записи;

— `%d` — имя домена;

— `%f` — доменное имя учетной записи (например, `example@domain.ru`);

— `%l` — первая буква логина учетной записи;

— `%o` — домашний каталог, полученный от поставщика данных идентификации (например, значение параметра `unixHomeDirectory`);

— `%h` — домашний каталог, полученный от поставщика данных идентификации, в нижнем регистре;

— `%H` — значение атрибута `homedir_substring` из файла `/etc/sssd/sssd.conf`;

— `%%` — символ «%».

► Чтобы задать путь к домашнему каталогу:

1. Откройте на редактирование файл `/etc/sssd/sssd.conf`.
2. Выполните одно из следующих действий:
   - Если нужно задать путь к каталогу для всех доменов, в секции `[nss]` добавьте параметр `fallback_homedir` или `override_homedir`.

     Например:
     ```
     [nss]
     fallback_homedir = /home/%u@%d
     ```
   - Если нужно задать путь к каталогу для конкретного домена, в секции `[domain/<Имя домена>]` добавьте параметр `fallback_homedir` или `override_homedir.`
3. Сохраните изменения и закройте файл.

Далее создайте домашний каталог (см. раздел 4.3.5.1).

Создание домашнего каталога

► Чтобы создать домашний каталог:

1. Выполните одно из следующих действий:
   - Если вы задали путь к домашнему каталогу с помощью параметра `fallback_homedir` или `override_homedir` в файле конфигурации `/etc/sssd/sssd.conf`, создайте каталог по указанному пути, учитывая указанные ранее переменные при необходимости.

     Например, если в параметре `fallback_homedir` указано значение `/home/%u`, нужно выполнить команду `mkdir /home/<Логин учетной записи>`.
   - Если вы задали путь с помощью параметра `unixHomeDirectory`, создайте каталог, выполнив команду `mkdir <Значение unixHomeDirectory>`.
2. Задайте владельца домашнего каталога, выполнив команду `chown <Доменное имя учетной записи>:<Название группы> <Путь к домашнему каталогу>`.

Настройка командной оболочки

Настроить командную оболочку можно одним из способов:

— через атрибут `loginShell` в Active Directory (см. раздел 4.3.5.1);

— через параметр `shell_fallback`, `override_shell` или `default_shell` в файле `/etc/sssd/sssd.conf` на активе (см. раздел 4.3.5.1).

Настройка пути к командной оболочке в Active Directory

Примечание. Если используемый контроллер домена отличается от Active Directory, используйте документацию вендора, чтобы правильно настроить домашний каталог. Вы также можете вручную задать значения `shell_fallback`, `override_shell` или `default_shell` в файле `/etc/sssd/sssd.conf` на каждом активе.

- Чтобы задать путь к командной оболочке:

  1. Войдите в интерфейс Active Directory.
  2. Нажмите **Пользователи и компьютеры**.
  3. Нажмите **Вид** → **Дополнительные компоненты**.
  4. В левой части окна выберите **<Имя домена>** → **Users**.
  5. В контекстном меню пользователя выберите **Свойства**.
  6. Выберите вкладку **Редактор атрибутов**.
  7. В блоке параметров **Атрибуты** выберите **loginShell**.
  8. В параметре укажите путь к командной оболочке для пользователя.
  9. Нажмите **ОК**.
  10. Нажмите **Применить**.

  Если в дальнейшем потребуется получить значение параметра `loginShell`, вы можете выполнить команду `Get-ADUser -Identity <Логин учетной записи> -Properties "loginShell"`.

Настройка пути к командной оболочке на активе

- Чтобы задать путь к командной оболочке на активе:

  1. Откройте на редактирование файл `/etc/sssd/sssd.conf`.
  2. Выполните одно из следующих действий:

     - Если нужно задать путь к командной оболочке для всех доменов, в секции `[nss]` добавьте параметр добавьте параметр `shell_fallback`, `override_shell` или `default_shell`.
     - Если нужно задать путь к командной оболочке для конкретного домена, в секции `[domain/<Имя домена>]` добавьте параметр `shell_fallback`, `override_shell` или `default_shell`.

  3. Сохраните изменения и закройте файл.

Подготовка сценариев для аудита

Вы можете настроить пользовательские сценарии по инструкции из раздела «Настройка sudo-оберток вручную (см. раздел 4.3.4.3)».

Настройка программы sudo

Вы можете настроить программу sudo по инструкции из раздела «Настройка sudo-оберток вручную (см. раздел 4.3.4.3)».

4.3.5.2. Настройка Winbind

Для настройки актива в Winbind необходимо настроить домашний каталог, командную оболочку, пользовательские сценарии и файл конфигурации `sudoers`.

> **Примечание.** Для указания доменного имени учетной записи следует использовать формат Down-Level Logon Name. Например, `DOMAIN\example`. Обратная косая черта при этом должна экранироваться — `DOMAIN\\example`.

Настройка домашнего каталога

- Чтобы настроить домашний каталог:

1. Откройте файл конфигурации `/etc/samba/smb.conf`.
2. Выполните одно из следующих действий:
   - Если в параметре `template homedir` указан путь, создайте каталог по указанному пути.

     Например, если в параметре указано значение `/home/%U`, то нужно создать каталог, выполнив следующие команды:

     ```
     mkdir /home/<Логин учетной записи>
     chown <Доменное имя учетной записи>:<Название группы> /home/<Логин учетной записи>
     ```

   - Если параметр не задан, для создания каталога используйте значение `/home/%D/%U`, выполнив следующие команды:

     ```
     mkdir /home/<NetBIOS-домен>/<Логин учетной записи>
     chown <Доменное имя учетной записи>:<Название группы> /home/<NetBIOS-домен>/<Логин учетной записи>
     ```

3. Сохраните изменения и закройте файл.

Настройка командной оболочки

- Чтобы настроить командную оболочку:

  1. Откройте файл конфигурации `/etc/samba/smb.conf`.
  2. Добавьте строку:
     ```
     template shell = /bin/bash
     ```
  3. Сохраните изменения и закройте файл.

Подготовка сценариев для аудита

Вы можете настроить пользовательские сценарии по инструкции из раздела «Настройка sudo-оберток вручную (см. раздел 4.3.4.3)».

Настройка программы sudo

Вы можете настроить программу sudo по инструкции из раздела «Настройка sudo-оберток вручную (см. раздел 4.3.4.3)».

4.4. Unix-подобные ОС: 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 SSH Audit.

В этом разделе

4.4.1. Добавление учетной записи

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

  1. В главном меню выберите **Сбор данных** → **Учетные записи**.
  2. Нажмите **Добавить учетную запись** → **Логин — пароль**.
  3. Введите название учетной записи.
  4. Введите логин учетной записи.
  5. Введите пароль и подтвердите его.
  6. Нажмите **Сохранить**.

4.4.2. Создание и запуск задачи на аудит актива

► Чтобы создать и запустить задачу на аудит актива:

1. В главном меню выберите **Сбор данных** → **Задачи**.
2. Нажмите **Создать задачу** → **Сбор данных**.
3. Введите название задачи.
4. В раскрывающемся списке **Профиль** выберите **Unix SSH Audit**.
5. В иерархическом списке выберите **Сканирование систем** → **Через терминал: SSH**.
6. Выберите учетную запись для доступа к активу.
7. Если используется аудит с помощью su или sudo-привилегий, выберите способ повышения привилегий:
   - для аудита с помощью su — **su** или **su_minus**;
   - для аудита с помощью sudo-привилегий — **sudo**.
8. Если требуется, в раскрывающемся списке **Коллекторы** выберите коллекторы для сбора данных.
9. 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.
10. Нажмите **Сохранить и запустить**.

5. Прокси-серверы

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

В этом разделе

5.1. 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 4).

5.2. 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 4).

6. Сетевые устройства

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

Для аудита сетевых устройств с целью выявления уязвимостей нужно использовать протокол SSH. Для сбора информации об адресе, модели и версии устройства вы можете использовать протокол SNMP.

В этом разделе

6.1. 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 — порты UDP 161 и 162.

Внимание! Использование сетевого протокола SSH-1 небезопасно из-за выявленных в нем уязвимостей. Передача данных осуществляется по протоколу SSH-2, утвержденному в 2006 году в качестве стандарта. Для настройки SSH-2 обратитесь к документации вендора.

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

6.1.1. 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. Пройдите аутентификацию на активе.
  3. Создайте учетную запись для доступа к активу:

     ```
     user <Логин> password <Пароль>
     ```
  4. Сохраните изменения:

     ```
     configuration snapshot all
     ```

  Учетная запись создана.

6.1.2. 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. Пройдите аутентификацию 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.

6.2. 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

6.2.1. Добавление учетной записи для доступа по SSH

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

  1. В главном меню выберите **Сбор данных** → **Учетные записи**.

     Откроется страница **Учетные записи**.
  2. Нажмите **Добавить учетную запись** → **Логин — пароль**.

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

  Учетная запись добавлена.

6.2.2. Создание задачи на аудит актива по SSH

- Чтобы создать задачу на проведение аудита актива:

  1. В главном меню выберите **Сбор данных** → **Задачи**.

     Откроется страница **Задачи по сбору данных**.
  2. Нажмите **Создать задачу** → **Сбор данных**.

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

3. В поле **Название** введите название задачи.
4. В раскрывающемся списке **Профиль** выберите **SSH Network Device Audit**.
5. В иерархическом списке выберите пункт **Сканирование систем** → **Через терминал: SSH**.
6. В раскрывающемся списке **Учетная запись** выберите учетную запись для доступа к активу.
7. Если требуется, в раскрывающемся списке **Коллекторы** выберите коллекторы для сбора данных.
8. В панели **Цели сбора данных** на вкладке **Включить** выполните одно из следующих действий:
   - Если для сканируемой цели ранее был добавлен актив, в поле **Активы** введите IP-адрес или доменное имя (в формате FQDN) узла актива.
   - Если для сканируемой цели актив ранее не был добавлен, в поле **Сетевые адреса** введите ее IP-адрес или доменное имя (в формате FQDN).

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

Задача на проведение аудита актива создана.

6.2.3. Добавление пароля для доступа по SNMP

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

1. В главном меню выберите **Сбор данных** → **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. Введите название учетной записи.
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.

6.2.4. Создание задачи на аудит актива по SNMP

- Чтобы создать задачу на проведение аудита актива:

  1. В главном меню выберите **Сбор данных** → **Задачи**.
  2. Нажмите **Создать задачу** → **Сбор данных**.
  3. Введите название задачи.
  4. Выберите профиль **SNMP Network Device Audit**.
  5. В иерархическом списке выберите **Сканирование систем** → **По протоколу SNMP**.
  6. Выберите **Версия 3**.
  7. В раскрывающемся списке **Учетная запись** выберите учетную запись с ключом аутентификации для доступа к активу.
  8. Включите аутентификацию.
  9. Выберите алгоритм аутентификации, указанный при настройке актива.
  10. Включите шифрование.
  11. Выберите алгоритм шифрования, указанный при настройке актива.
  12. В раскрывающемся списке **Учетная запись типа «пароль»** выберите учетную запись с ключом шифрования для доступа к активу.
  13. Если требуется, выберите MP 10 Collector для сбора событий.
  14. 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.

  15. Нажмите **Сохранить**.

6.3. Arista EOS: настройка актива

Настройку актива нужно выполнять от имени учетной записи администратора устройства.

Для проведения аудита на активе нужно создать учетную запись для доступа MP 10 Collector по протоколу SSH и предоставить ей права на чтение файлов конфигурации с помощью роли.

Перед настройкой актива необходимо убедиться, что администраторам сетевого устройства назначена роль `network-admin`. Если роль не назначена, то после включения ролевой модели управления доступом их права будут ограничены в соответствии с текущей ролью. Вы можете выполнить команду `show running-config` и проверить, что в результате ее выполнения отображаются параметры текущей конфигурации устройства.

Инструкция, приведенная ниже, применима, если на сетевом устройстве используется локальная аутентификация пользователей.

- Чтобы создать учетную запись для доступа к активу:

  1. На узле, с которого производится настройка, запустите терминальный клиент, поддерживающий протокол SSH.
  2. Пройдите аутентификацию на активе.
  3. Перейдите в режим конфигурирования:
     ```
     configure
     ```
  4. Создайте метод локальной аутентификации:
     ```
     aaa authentication login <Название метода> local
     ```
  5. Создайте метод локальной авторизации с возможностью перехода в привилегированный режим EXEC:
     ```
     aaa authorization exec default local
     ```
  6. Создайте роль с правом на чтение файлов конфигурации:
     ```
     role <Название роли>-role
     10 deny mode exec command configure|bash|python-shell|\|
     20 permit mode exec command .*
     ```
  7. Создайте учетную запись для доступа к активу:
     ```
     username <Логин> privilege 2 role <Название роли>-role secret <Пароль>
     ```
  8. Включите ролевую модель управления доступом:
     ```
     aaa authorization commands all default local
     ```
  9. Выйдите из режима конфигурирования:
     ```
     exit
     ```
  10. Сохраните изменения:
      ```
      write
      ```

  Примечание. Если на сетевом устройстве используется централизованная аутентификация пользователей (например, определен метод аутентификации `aaa authentication login <Название метода> <Имя сервера> local`), то необходимо создать учетную запись на указанном сервере с правом выполнения команд для чтения файлов конфигурации устройства в привилегированном режиме.

6.4. Arista EOS: настройка MaxPatrol VM

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

В этом разделе

Добавление учетной записи для доступа к активу по SSH (см. раздел 6.4.1)

Создание и запуск задачи на аудит актива по SSH (см. раздел 6.4.2)

6.4.1. Добавление учетной записи для доступа к активу по SSH

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

  1. В главном меню выберите **Сбор данных** → **Учетные записи**.
  2. Нажмите **Добавить учетную запись** → **Логин — пароль**.
  3. Введите название учетной записи.
  4. В раскрывающемся списке **Метки** установите флажок **Terminal**.
  5. Введите логин учетной записи.
  6. Введите пароль и подтвердите его.
  7. Нажмите **Создать**.

6.4.2. Создание и запуск задачи на аудит актива по SSH

- Чтобы создать и запустить задачу на аудит актива:

  1. В главном меню выберите **Сбор данных** → **Задачи**.
  2. Нажмите **Создать задачу** → **Сбор данных**.
  3. Введите название задачи.
  4. В раскрывающемся списке **Профиль** выберите **SSH Network Device Audit**.
  5. В иерархическом списке выберите **Сканирование систем** → **Через терминал: SSH**.
  6. Выберите учетную запись для доступа к активу.
  7. Если требуется, выберите коллекторы для сбора данных.
  8. В панели **Цели сбора данных** на вкладке **Включить** выполните одно из следующих действий:
     - Если для сканируемой цели ранее был добавлен актив, в поле **Активы** введите IP-адрес или доменное имя (в формате FQDN) узла актива.
     - Если для сканируемой цели актив ранее не был добавлен, в поле **Сетевые адреса** введите ее IP-адрес или доменное имя (в формате FQDN).

     Примечание. В панели **Расписание** вы можете включить и настроить автоматический запуск задачи.
  9. Нажмите **Сохранить и запустить** → **Запустить сбор данных**.

6.5. 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 — порты UDP 161 и 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.

6.6. 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

6.6.1. Добавление учетной записи для доступа по SSH

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

  1. В главном меню выберите **Сбор данных** → **Учетные записи**.

     Откроется страница **Учетные записи**.

  2. Нажмите **Добавить учетную запись** → **Логин — пароль**.

     Откроется страница **Добавление учетной записи**.

  3. Введите название учетной записи.

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

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

Учетная запись добавлена.

6.6.2. Создание задачи на аудит актива по SSH

► Чтобы создать задачу на проведение аудита актива:

1. В главном меню выберите **Сбор данных** → **Задачи**.

   Откроется страница **Задачи по сбору данных**.
2. Нажмите **Создать задачу** → **Сбор данных**.

   Откроется страница **Создание задачи на сбор данных**.
3. В поле **Название** введите название задачи.
4. В раскрывающемся списке **Профиль** выберите **SSH Network Device Audit**.
5. В иерархическом списке выберите пункт **Сканирование систем** → **Через терминал: SSH**.
6. В раскрывающемся списке **Учетная запись** выберите учетную запись для доступа к активу.
7. Если требуется, в раскрывающемся списке **Коллекторы** выберите коллекторы для сбора данных.
8. В панели **Цели сбора данных** на вкладке **Включить** выполните одно из следующих действий:
   - Если для сканируемой цели ранее был добавлен актив, в поле **Активы** введите IP-адрес или доменное имя (в формате FQDN) узла актива.
   - Если для сканируемой цели актив ранее не был добавлен, в поле **Сетевые адреса** введите ее IP-адрес или доменное имя (в формате FQDN).

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

Задача на проведение аудита актива создана.

6.6.3. Добавление пароля для доступа по SNMP

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

1. В главном меню выберите **Сбор данных** → **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. Введите название учетной записи.
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.

6.6.4. Создание задачи на аудит актива по SNMP

- Чтобы создать задачу на проведение аудита актива:

1. В главном меню выберите **Сбор данных** → **Задачи**.
2. Нажмите **Создать задачу** → **Сбор данных**.
3. Введите название задачи.
4. Выберите профиль **SNMP Network Device Audit**.
5. В иерархическом списке выберите **Сканирование систем** → **По протоколу SNMP**.
6. Выберите **Версия 3**.
7. В раскрывающемся списке **Учетная запись** выберите учетную запись с ключом аутентификации для доступа к активу.
8. Включите аутентификацию.
9. Выберите алгоритм аутентификации, указанный при настройке актива.
10. Включите шифрование.
11. Выберите алгоритм шифрования, указанный при настройке актива.
12. В раскрывающемся списке **Учетная запись типа «пароль»** выберите учетную запись с ключом шифрования для доступа к активу.
13. Если требуется, выберите MP 10 Collector для сбора событий.
14. 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.

15. Нажмите **Сохранить**.

6.7. B4Tech: настройка актива

Настройку актива нужно выполнять от имени учетной записи администратора устройства.

> **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 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, запустите терминальный клиент, поддерживающий протокол SSH.
2. Пройдите аутентификацию на активе.
3. Перейдите в режим конфигурирования:
   ```
   configure terminal
   ```
4. Создайте учетную запись для доступа к активу:
   ```
   username <Логин> privilege 4 algorithm-type sha256 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:
   ```
   wtite memory
   ```

6.8. B4Tech: настройка MaxPatrol VM

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

В этом разделе

6.8.1. Добавление учетной записи для доступа к активу по SSH

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

  1. В главном меню выберите **Сбор данных** → **Учетные записи**.
  2. Нажмите **Добавить учетную запись** → **Логин — пароль**.
  3. Введите название учетной записи.
  4. Введите логин учетной записи.
  5. Введите пароль и подтвердите его.
  6. Нажмите **Создать**.

6.8.2. Создание и запуск задачи на аудит актива по SSH

- Чтобы создать и запустить задачу на аудит актива:

  1. В главном меню выберите **Сбор данных** → **Задачи**.
  2. Нажмите **Создать задачу** → **Сбор данных**.
  3. Введите название задачи.
  4. В раскрывающемся списке **Профиль** выберите **SSH Network Device Audit**.
  5. В иерархическом списке выберите **Сканирование систем** → **Через терминал: SSH**.
  6. Выберите учетную запись для доступа к активу.
  7. Если требуется, выберите коллекторы для сбора данных.
  8. В панели **Цели сбора данных** на вкладке **Включить** выполните одно из следующих действий:

     - Если для сканируемой цели ранее был добавлен актив, в поле **Активы** введите IP-адрес или доменное имя (в формате FQDN) узла актива.
     - Если для сканируемой цели актив ранее не был добавлен, в поле **Сетевые адреса** введите ее IP-адрес или доменное имя (в формате FQDN).

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

  9. Нажмите **Сохранить и запустить** → **Запустить сбор данных**.

6.9. Bcom: настройка актива

Настройку актива нужно выполнять от имени учетной записи администратора устройства.

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

Для проведения аудита на активе нужно создать учетную запись с ролью network-operator для доступа MP 10 Collector по протоколу SSH.

► Чтобы создать учетную запись для доступа к активу:

1. На узле, с которого производится настройка, запустите терминальный клиент, поддерживающий протокол SSH.
2. Пройдите аутентификацию на активе.
3. Перейдите в режим конфигурирования:
   ```
   configure terminal
   ```
4. Настройте локальный список аутентификации в зависимости от используемой сети:
   - Если для доступа к активу используется основная сеть (VRF по умолчанию), выполните команду:
     ```
     aaa authentication login default local
     ```
   - Если для доступа к активу используется специальная сеть (управленческая VRF), выполните команду:
     ```
     aaa authentication login default vrf management local
     ```
5. Настройте локальный список авторизации в зависимости от используемой сети:
   - Если для доступа к активу используется основная сеть (VRF по умолчанию), выполните команду:
     ```
     aaa authorization default local
     ```
   - Если для доступа к активу используется специальная сеть (управленческая VRF), выполните команду:
     ```
     aaa authorization default vrf management local
     ```
6. Перейдите в режим конфигурирования линий VTY:
   ```
   line vty 0 871
   ```
7. Установите уровень привилегий учетной записи:
   ```
   privilege level 15
   ```
8. Создайте учетную запись для доступа к активу:
   ```
   username <Логин> role network-operator password <Пароль>
   ```
9. Примените внесенные изменения:
   ```
   commit
   ```
10. Выйдите из режима конфигурирования:
    ```
    end
    ```
11. Сохраните изменения:
    ```
    wtite memory
    ```

6.10. Bcom: настройка MaxPatrol VM

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

В этом разделе

6.10.1. Добавление учетной записи для доступа к активу по SSH

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

  1. В главном меню выберите **Сбор данных** → **Учетные записи**.
  2. Нажмите **Добавить учетную запись** → **Логин — пароль**.
  3. Введите название учетной записи.
  4. В раскрывающемся списке **Метки** установите флажок **Terminal**.
  5. Введите логин учетной записи.
  6. Введите пароль и подтвердите его.
  7. Нажмите **Создать**.

6.10.2. Создание и запуск задачи на аудит актива по SSH

- Чтобы создать и запустить задачу на аудит актива:

  1. В главном меню выберите **Сбор данных** → **Задачи**.
  2. Нажмите **Создать задачу** → **Сбор данных**.
  3. Введите название задачи.
  4. В раскрывающемся списке **Профиль** выберите **SSH Network Device Audit**.
  5. В иерархическом списке выберите **Сканирование систем** → **Через терминал: SSH**.
  6. Выберите учетную запись для доступа к активу.
  7. Если требуется, выберите коллекторы для сбора данных.
  8. В панели **Цели сбора данных** на вкладке **Включить** выполните одно из следующих действий:

     - Если для сканируемой цели ранее был добавлен актив, в поле **Активы** введите IP-адрес или доменное имя (в формате FQDN) узла актива.

- Если для сканируемой цели актив ранее не был добавлен, в поле **Сетевые адреса** введите ее IP-адрес или доменное имя (в формате FQDN).

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

9. Нажмите **Сохранить и запустить** → **Запустить сбор данных**.

6.11. Brocade VDX, версия NOS 6.0.1: настройка актива

Настройку актива нужно выполнять от имени учетной записи администратора устройства.

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

Внимание! Инструкция предназначена для создания учетной записи на сетевом устройстве, где используется локальная аутентификация пользователей.

► Чтобы создать учетную запись для доступа к активу:

1. На узле, с которого производится настройка, запустите терминальный клиент, поддерживающий протокол SSH.
2. Пройдите аутентификацию на активе.
3. Перейдите в режим конфигурирования:
   ```
   configure terminal
   ```
4. Создайте учетную запись для доступа к активу:
   ```
   username <Логин> password <Пароль> role user encryption-level 7 enable true
   ```
   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:
   ```
   exit
   ```
6. Сохраните изменения:
   ```
   write
   ```

6.12. Brocade VDX, версия NOS 6.0.1: настройка MaxPatrol VM

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

В этом разделе

Добавление учетной записи для доступа к активу по SSH (см. раздел 6.12.1)

Создание и запуск задачи на аудит актива по SSH (см. раздел 6.12.2)

6.12.1. Добавление учетной записи для доступа к активу по SSH

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

  1. В главном меню выберите **Сбор данных** → **Учетные записи**.
  2. Нажмите **Добавить учетную запись** → **Логин — пароль**.
  3. Введите название учетной записи.
  4. Введите логин учетной записи.
  5. Введите пароль и подтвердите его.
  6. Нажмите **Создать**.

6.12.2. Создание и запуск задачи на аудит актива по SSH

- Чтобы создать и запустить задачу на аудит актива:

  1. В главном меню выберите **Сбор данных** → **Задачи**.
  2. Нажмите **Создать задачу** → **Сбор данных**.
  3. Введите название задачи.
  4. В раскрывающемся списке **Профиль** выберите **SSH Network Device Audit**.
  5. В иерархическом списке выберите **Сканирование систем** → **Через терминал: SSH**.
  6. Выберите учетную запись для доступа к активу.
  7. Если требуется, выберите коллекторы для сбора данных.
  8. В панели **Цели сбора данных** на вкладке **Включить** выполните одно из следующих действий:

     - Если для сканируемой цели ранее был добавлен актив, в поле **Активы** введите IP-адрес или доменное имя (в формате FQDN) узла актива.
     - Если для сканируемой цели актив ранее не был добавлен, в поле **Сетевые адреса** введите ее IP-адрес или доменное имя (в формате FQDN).

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

  9. Нажмите **Сохранить и запустить** → **Запустить сбор данных**.

6.13. 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

6.13.1. 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.

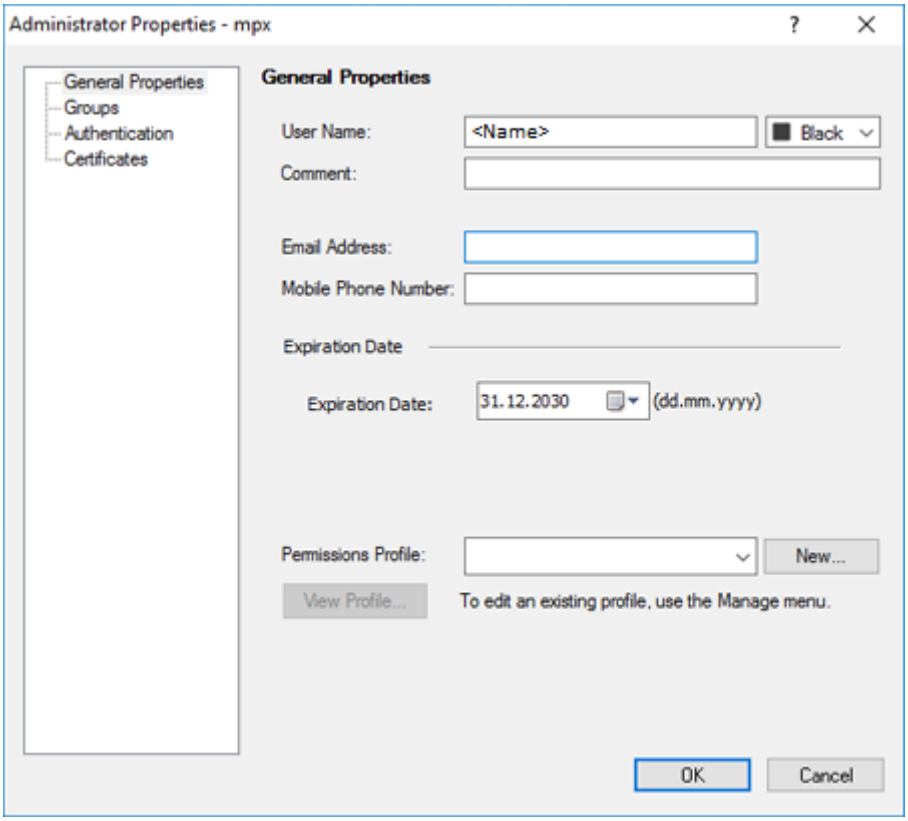

Рисунок 1. Настройка учетной записи

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

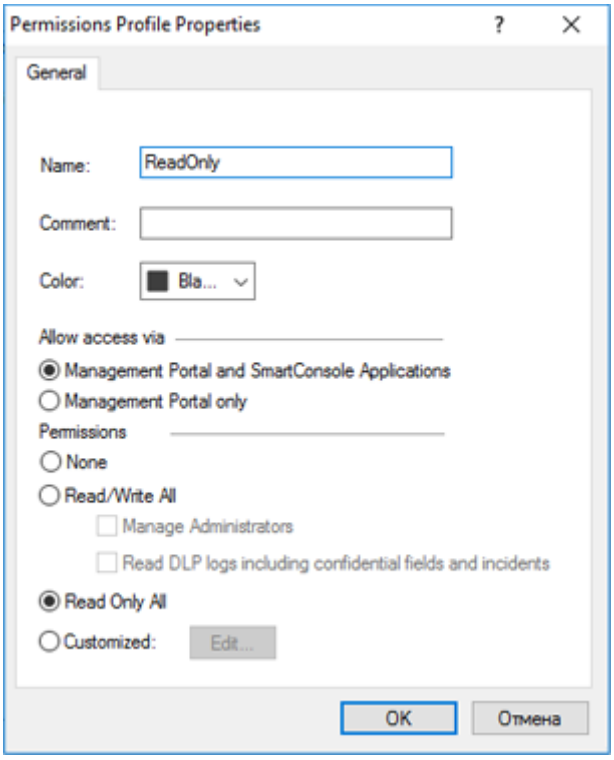

Рисунок 2. Настройка профиля учетной записи

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.

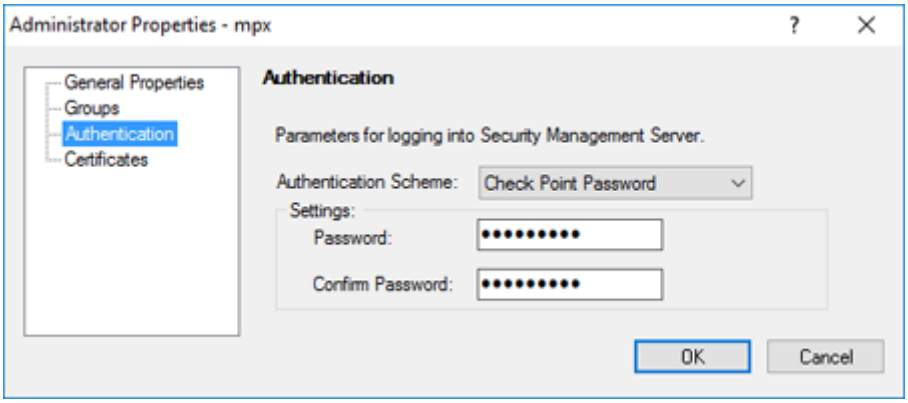

Рисунок 3. Настройка способа проверки учетной записи

11. Нажмите кнопку **OK**.

Учетная запись администратора создана.

6.13.2. 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**.

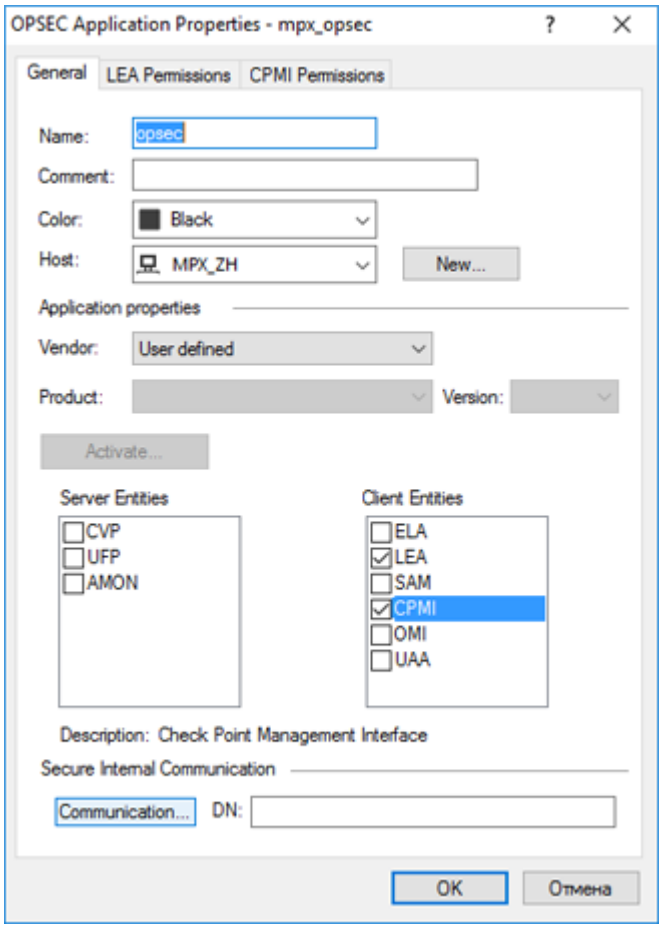

Рисунок 4. Настройка параметров приложения

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

   Примечание. Название приложения OPSEC вам понадобится при экспорте сертификата.

6. Нажмите **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**.

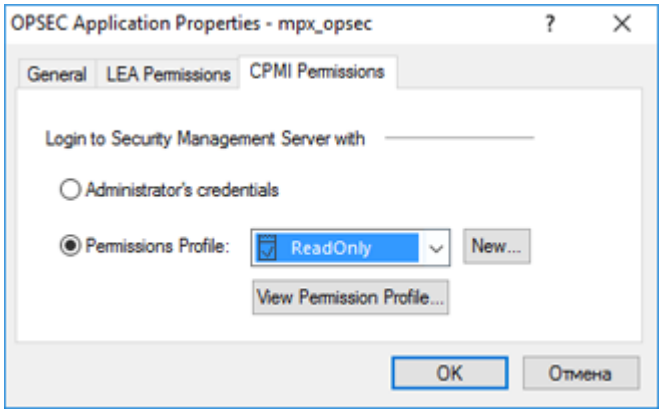

Рисунок 5. Настройка прав доступа приложения

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

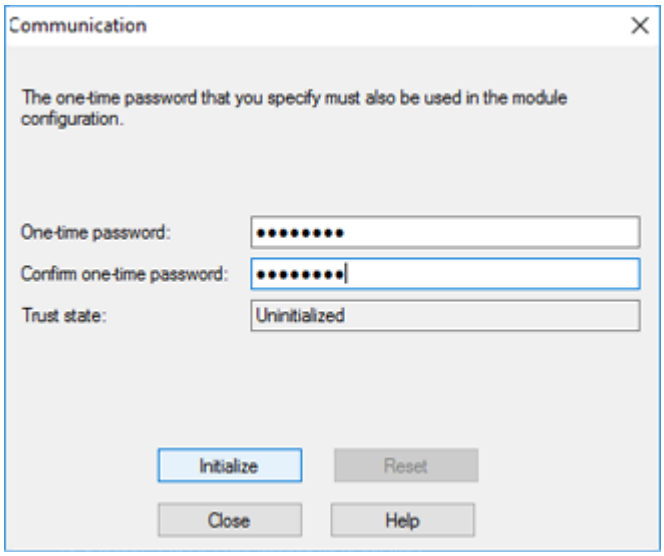

Рисунок 6. Создание пароля доступа

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.

6.13.3. 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.

6.13.4. 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. Пройдите аутентификацию на активе.
  3. Создайте учетную запись для доступа к активу:

     ```
     add user <Логин> uid 0 homedir /home/<Логин>
     ```

  4. Установите пароль учетной записи:

     ```
     set user <Логин> password
     ```

  5. Введите пароль.

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

Учетная запись создана.

6.14. Check Point GAiA OS 80.10—81.20: 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 в MaxPatrol VM.
3. На базе этой же учетной записи создать учетную запись администратора сервера управления Check Point GAiA.

В этом разделе

6.14.1. 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. Пройдите аутентификацию 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.

6.14.2. 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. Пройдите аутентификацию на активе.
3. Создайте учетную запись для доступа к активу:
   ```
   add user <Логин> uid 0 homedir /home/<Логин>
   ```
4. Установите пароль учетной записи:
   ```
   set user <Логин> password
   ```
5. Введите пароль.
6. Назначьте учетной записи роль администратора:
   ```
   add rba user <Логин> roles adminRole
   ```
7. Сохраните изменения:
   ```
   save config
   ```

Учетная запись создана.

6.14.3. 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.

6.15. Check Point GAiA OS 76—81.20: настройка MaxPatrol VM

Check Point GAiA OS состоит из следующих активов:

— Security Management Server — определяет политики безопасности и осуществляет журналирование событий;

— Security Gateway — отвечает за контроль доступа и предотвращение угроз;

— Standalone Security Gateway — выполняет функции Security Management Server и Security Gateway одновременно.

Для аудита активов в MaxPatrol VM используются следующие профили:

— SSH Network Device Audit — для сбора информации обо всех активах Check Point GAiA OS 76—81.20 по протоколу SSH. Позволяет собирать информацию об основных параметрах ОС, в том числе данные о конфигурации и статусе интерфейсов и сервисов, таблицы маршрутов и ARP-записей.

— Checkpoint OPSEC Audit — для сбора информации об активах Security Management Server версий 76—77.30 через API OPSEC. Позволяет собирать информацию о политиках безопасности, сведения о NAT, VPN и другие данные.

Примечание. Для сканирования активов с профилем Checkpoint OPSEC Audit необходим MP 10 Collector, установленный на Windows.

— Web API Audit — для сбора информации об активах Security Management Server версий 80—81.20 через веб-API. Позволяет собирать информацию о политиках безопасности, сведения о NAT, VPN и другие данные.

Аудит активов необходимо выполнять в следующем порядке:

1. Для всех активов Check Point GAiA OS — сканирование по протоколу SSH. Для этого в MaxPatrol VM нужно добавить учетную запись для доступа по протоколу SSH, создать и запустить задачу на проведение аудита.
2. Если требуется собирать дополнительную информацию (информацию о политиках безопасности, сведения о NAT, VPN и другие данные) об активах Security Management Server версий 76—77.30 — сканирование через API OPSEC. Для этого в MaxPatrol VM нужно добавить учетную запись и сертификат сервера управления, создать задачу на проведение аудита.

   Если требуется собирать дополнительную информацию (информацию о политиках безопасности, сведения о NAT, VPN и другие данные) об активах Security Management Server версий 80—81.20 — сканирование через веб-API. Для этого в MaxPatrol VM нужно добавить учетную запись для доступа через веб-API, создать и запустить задачу на проведение аудита.

В этом разделе

6.15.1. Добавление учетной записи для доступа по SSH

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

1. В главном меню выберите **Сбор данных** → **Учетные записи**.

   Откроется страница **Учетные записи**.
2. Нажмите **Добавить учетную запись** → **Логин — пароль**.

   Откроется страница **Добавление учетной записи**.
3. Введите название учетной записи.

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

Учетная запись добавлена.

6.15.2. Создание задачи на аудит актива по SSH

► Чтобы создать задачу на проведение аудита актива:

1. В главном меню выберите **Сбор данных** → **Задачи**.

   Откроется страница **Задачи по сбору данных**.
2. Нажмите **Создать задачу** → **Сбор данных**.

   Откроется страница **Создание задачи на сбор данных**.
3. В поле **Название** введите название задачи.
4. В раскрывающемся списке **Профиль** выберите **SSH Network Device Audit**.
5. В иерархическом списке выберите пункт **Сканирование систем** → **Через терминал: SSH**.
6. В раскрывающемся списке **Учетная запись** выберите учетную запись для доступа к активу.
7. Если требуется, в раскрывающемся списке **Коллекторы** выберите коллекторы для сбора данных.
8. В панели **Цели сбора данных** на вкладке **Включить** выполните одно из следующих действий:
   - Если для сканируемой цели ранее был добавлен актив, в поле **Активы** введите IP-адрес или доменное имя (в формате FQDN) узла актива.
   - Если для сканируемой цели актив ранее не был добавлен, в поле **Сетевые адреса** введите ее IP-адрес или доменное имя (в формате FQDN).

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

Задача на проведение аудита актива создана.

6.15.3. Добавление учетной записи для доступа через OPSEC

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

  1. В главном меню выберите **Сбор данных** → **Учетные записи**.

     Откроется страница **Учетные записи**.

  2. Нажмите **Добавить учетную запись** → **Логин — пароль**.

     Откроется страница **Добавление учетной записи**.

  3. Введите название учетной записи.
  4. В раскрывающемся списке **Метки** установите флажок **OPSEC_Audit**.
  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.

6.15.4. Добавление сертификата для доступа к активу через OPSEC

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

  1. В главном меню выберите **Сбор данных** → **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.
  4. В раскрывающемся списке **Метки** установите флажок **OPSEC_Audit**.
  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.

6.15.5. Создание задачи на аудит актива через OPSEC

- Чтобы создать задачу на проведение аудита актива:

  1. В главном меню выберите **Сбор данных** → **Задачи**.

     Откроется страница **Задачи по сбору данных**.

  2. Нажмите **Создать задачу** → **Сбор данных**.

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

  3. В поле **Название** введите название задачи.
  4. В раскрывающемся списке **Профиль** выберите **Checkpoint OPSEC Audit**.
  5. В иерархическом списке выберите пункт **Сканирование систем** → **Check Point через OPSEC**.
  6. В раскрывающемся списке **Учетная запись** выберите сертификат для доступа к активу.
  7. В раскрывающемся списке **Учетная запись CPMI** выберите учетную запись для доступа к активу.
  8. В панели **Цели сбора данных** на вкладке **Включить** выполните одно из следующих действий:

     - Если для сканируемой цели ранее был добавлен актив, в поле **Активы** введите IP-адрес или доменное имя (в формате FQDN) узла актива.
     - Если для сканируемой цели актив ранее не был добавлен, в поле **Сетевые адреса** введите ее IP-адрес или доменное имя (в формате FQDN).

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

  9. Нажмите кнопку **Сохранить**.

  Задача на проведение аудита актива создана.

6.15.6. Добавление учетной записи для доступа через веб-API

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

  1. В главном меню выберите **Сбор данных** → **Учетные записи**.

     Откроется страница **Учетные записи**.

  2. Нажмите **Добавить учетную запись** → **Логин — пароль**.

     Откроется страница **Добавление учетной записи**.

  3. Введите название учетной записи.

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

Учетная запись добавлена.

6.15.7. Создание задачи на аудит актива через веб-API

- Чтобы создать задачу на проведение аудита актива:

1. В главном меню выберите **Сбор данных** → **Задачи**.

   Откроется страница **Задачи по сбору данных**.
2. Нажмите **Создать задачу** → **Сбор данных**.

   Откроется страница **Создание задачи на сбор данных**.
3. В поле **Название** введите название задачи.
4. В раскрывающемся списке **Профиль** выберите **Web API Audit**.
5. В иерархическом списке выберите пункт **Сканирование систем** → **Через веб-API**.
6. В раскрывающемся списке **Учетная запись** выберите учетную запись для доступа к активу.
7. В панели **Параметры профиля** установите флажок **Показывать дополнительные параметры**.
8. Если актив содержит более 500 правил политики безопасности, в иерархическом списке выберите пункт **Сканирование систем** → **Особенности сканирования систем** и в поле **Количество элементов на странице ответа** введите количество элементов для отображения на странице ответа на запрос.

   Примечание. Количество элементов, отображаемых на одной странице по умолчанию, — 200.
9. В панели **Цели сбора данных** на вкладке **Включить** выполните одно из следующих действий:

   - Если для сканируемой цели ранее был добавлен актив, в поле **Активы** введите IP-адрес или доменное имя (в формате FQDN) узла актива.
   - Если для сканируемой цели актив ранее не был добавлен, в поле **Сетевые адреса** введите ее IP-адрес или доменное имя (в формате FQDN).

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

10. Нажмите кнопку **Сохранить**.

Задача на проведение аудита актива создана.

6.16. 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 — порты UDP 161 и 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 6.16.1)

Создание пароля для доступа к активу по SNMP (см. раздел 6.16.2)

6.16.1. 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. Пройдите аутентификацию 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.

6.16.2. 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. Пройдите аутентификацию 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.

6.17. 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

6.17.1. Добавление учетной записи для доступа по SSH

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

  1. В главном меню выберите **Сбор данных** → **Учетные записи**.

     Откроется страница **Учетные записи**.
  2. Нажмите **Добавить учетную запись** → **Логин — пароль**.

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

  Учетная запись добавлена.

6.17.2. Добавление пароля для повышения привилегий для аудита по SSH

- Чтобы добавить в MaxPatrol VM пароль для повышения привилегий:

  1. В главном меню выберите **Сбор данных** → **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. Введите название учетной записи.
  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.

6.17.3. Создание задачи на аудит актива по SSH

- Чтобы создать задачу на проведение аудита актива:

  1. В главном меню выберите **Сбор данных** → **Задачи**.

     Откроется страница **Задачи по сбору данных**.

  2. Нажмите **Создать задачу** → **Сбор данных**.

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

  3. В поле **Название** введите название задачи.
  4. 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.

  5. В иерархическом списке выберите пункт **Сканирование систем** → **Через терминал: SSH и Telnet**.
  6. В раскрывающемся списке **Учетная запись** выберите учетную запись для доступа к активу.
  7. 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 *).*$`.

8. Если требуется, в раскрывающемся списке **Коллекторы** выберите коллекторы для сбора данных.
9. 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.
10. Нажмите кнопку **Сохранить**.

Задача на проведение аудита актива создана.

6.17.4. Добавление пароля для доступа по SNMP

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

1. В главном меню выберите **Сбор данных** → **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. Введите название учетной записи.
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.

6.17.5. Создание задачи на аудит актива по SNMP

- Чтобы создать задачу на проведение аудита актива:

1. В главном меню выберите **Сбор данных** → **Задачи**.
2. Нажмите **Создать задачу** → **Сбор данных**.
3. Введите название задачи.
4. Выберите профиль **SNMP Network Device Audit**.
5. В иерархическом списке выберите **Сканирование систем** → **По протоколу SNMP**.
6. Выберите **Версия 3**.

7. В раскрывающемся списке **Учетная запись** выберите учетную запись с ключом аутентификации для доступа к активу.
8. Включите аутентификацию.
9. Выберите алгоритм аутентификации, указанный при настройке актива.
10. Включите шифрование.
11. Выберите алгоритм шифрования, указанный при настройке актива.
12. В раскрывающемся списке **Учетная запись типа «пароль»** выберите учетную запись с ключом шифрования для доступа к активу.
13. Если требуется, выберите MP 10 Collector для сбора событий.
14. 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.
15. Нажмите **Сохранить**.

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

Настройка актива для проведения аудита выполняется аналогично Cisco IOS 12, 15, 16 (см. раздел 6.16).

6.19. 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 6.17).

6.20. 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. Пройдите аутентификацию 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.

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

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

В этом разделе

Добавление учетной записи для доступа по SSH (см. раздел 6.21.1)

Создание задачи на аудит актива по SSH (см. раздел 6.21.2)

6.21.1. Добавление учетной записи для доступа по SSH

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

  1. В главном меню выберите **Сбор данных** → **Учетные записи**.

     Откроется страница **Учетные записи**.
  2. Нажмите **Добавить учетную запись** → **Логин — пароль**.

     Откроется страница **Добавление учетной записи**.
  3. Введите название учетной записи.
  4. В раскрывающемся списке **Метки** установите флажок **Terminal**.
  5. Введите логин учетной записи.

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

Учетная запись добавлена.

6.21.2. Создание задачи на аудит актива по SSH

► Чтобы создать задачу на проведение аудита актива:

1. В главном меню выберите **Сбор данных** → **Задачи**.

   Откроется страница **Задачи по сбору данных**.
2. Нажмите **Создать задачу** → **Сбор данных**.

   Откроется страница **Создание задачи на сбор данных**.
3. В поле **Название** введите название задачи.
4. В раскрывающемся списке **Профиль** выберите **SSH Network Device Audit**.
5. В иерархическом списке выберите пункт **Сканирование систем** → **Через терминал: SSH**.
6. В раскрывающемся списке **Учетная запись** выберите учетную запись для доступа к активу.
7. Если требуется, в раскрывающемся списке **Коллекторы** выберите коллекторы для сбора данных.
8. В панели **Цели сбора данных** на вкладке **Включить** выполните одно из следующих действий:
   - Если для сканируемой цели ранее был добавлен актив, в поле **Активы** введите IP-адрес или доменное имя (в формате FQDN) узла актива.
   - Если для сканируемой цели актив ранее не был добавлен, в поле **Сетевые адреса** введите ее IP-адрес или доменное имя (в формате FQDN).

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

Задача на проведение аудита актива создана.

6.22. 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 — порты UDP 161 и 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 6.22.1)

Создание пароля для доступа к активу по SNMP (см. раздел 6.22.2)

6.22.1. 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. Пройдите аутентификацию 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.

6.22.2. 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. Пройдите аутентификацию 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.

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

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

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

6.23.1. Добавление учетной записи для доступа по SSH

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

  1. В главном меню выберите **Сбор данных** → **Учетные записи**.

     Откроется страница **Учетные записи**.
  2. Нажмите **Добавить учетную запись** → **Логин — пароль**.

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

  Учетная запись добавлена.

6.23.2. Создание задачи на аудит актива по SSH

- Чтобы создать задачу на проведение аудита актива:

  1. В главном меню выберите **Сбор данных** → **Задачи**.

     Откроется страница **Задачи по сбору данных**.
  2. Нажмите **Создать задачу** → **Сбор данных**.

     Откроется страница **Создание задачи на сбор данных**.
  3. В поле **Название** введите название задачи.
  4. В раскрывающемся списке **Профиль** выберите **SSH Network Device Audit**.
  5. В иерархическом списке выберите пункт **Сканирование систем** → **Через терминал: SSH**.
  6. В раскрывающемся списке **Учетная запись** выберите учетную запись для доступа к активу.

7. Если требуется, в раскрывающемся списке **Коллекторы** выберите коллекторы для сбора данных.
8. В панели **Цели сбора данных** на вкладке **Включить** выполните одно из следующих действий:
   - Если для сканируемой цели ранее был добавлен актив, в поле **Активы** введите IP-адрес или доменное имя (в формате FQDN) узла актива.
   - Если для сканируемой цели актив ранее не был добавлен, в поле **Сетевые адреса** введите ее IP-адрес или доменное имя (в формате FQDN).

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

Задача на проведение аудита актива создана.

6.23.3. Добавление пароля для доступа по SNMP

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

1. В главном меню выберите **Сбор данных** → **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. Введите название учетной записи.
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.

6.23.4. Создание задачи на аудит актива по SNMP

► Чтобы создать задачу на проведение аудита актива:

1. В главном меню выберите **Сбор данных** → **Задачи**.
2. Нажмите **Создать задачу** → **Сбор данных**.
3. Введите название задачи.
4. Выберите профиль **SNMP Network Device Audit**.
5. В иерархическом списке выберите **Сканирование систем** → **По протоколу SNMP**.

6. Выберите **Версия 3**.
7. В раскрывающемся списке **Учетная запись** выберите учетную запись с ключом аутентификации для доступа к активу.
8. Включите аутентификацию.
9. Выберите алгоритм аутентификации, указанный при настройке актива.
10. Включите шифрование.
11. Выберите алгоритм шифрования, указанный при настройке актива.
12. В раскрывающемся списке **Учетная запись типа «пароль»** выберите учетную запись с ключом шифрования для доступа к активу.
13. Если требуется, выберите MP 10 Collector для сбора событий.
14. 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.
15. Нажмите **Сохранить**.

6.24. Eltex, модель MES 5448: настройка актива

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 версии 2.

► 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. Перейдите в режим конфигурирования:
   ```
   configure
   ```
3. Создайте локальный список аутентификации:
   ```
   aaa authentication login default local
   ```

4. Создайте локальный список аутентификации с возможностью перехода в привилегированный режим EXEC:
   ```
   aaa authorization exec default local
   ```
5. Создайте группу задач на просмотр данных:
   ```
   taskgroup maxpatrol
   ```
6. Добавьте в группу задачи с правом на просмотр данных:
   ```
   task read aaa
   task read bgp
   task read ospf
   exit
   ```
7. Создайте группу пользователей:
   ```
   usergroup maxpatrol
   ```
8. Добавьте в группу пользователей созданную ранее группу задач:
   ```
   taskgroup maxpatrol
   exit
   ```
9. Создайте учетную запись для доступа к активу:
   ```
   username <Логин> password <Пароль> level 15
   ```
10. Добавьте учетную запись в группу пользователей:
    ```
    username maxpatrol usergroup maxpatrol
    ```
11. Выйдите из режима конфигурирования:
    ```
    exit
    ```
12. Сохраните изменения:
    ```
    write memory confirm
    ```

Учетная запись создана.

6.25. Eltex, модель MES 5448: настройка MaxPatrol VM

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

В этом разделе

6.25.1. Добавление учетной записи для доступа по SSH

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

  1. В главном меню выберите **Сбор данных** → **Учетные записи**.

Откроется страница **Учетные записи**.

2. Нажмите **Добавить учетную запись** → **Логин — пароль**.

   Откроется страница **Добавление учетной записи**.

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

Учетная запись добавлена.

6.25.2. Создание задачи на аудит актива по SSH

► Чтобы создать задачу на проведение аудита актива:

1. В главном меню выберите **Сбор данных** → **Задачи**.

   Откроется страница **Задачи по сбору данных**.

2. Нажмите **Создать задачу** → **Сбор данных**.

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

3. В поле **Название** введите название задачи.
4. В раскрывающемся списке **Профиль** выберите **SSH Network Device Audit**.
5. В иерархическом списке выберите пункт **Сканирование систем** → **Через терминал: SSH**.
6. В раскрывающемся списке **Учетная запись** выберите учетную запись для доступа к активу.
7. Если требуется, в раскрывающемся списке **Коллекторы** выберите коллекторы для сбора данных.
8. В панели **Цели сбора данных** на вкладке **Включить** выполните одно из следующих действий:

   - Если для сканируемой цели ранее был добавлен актив, в поле **Активы** введите IP-адрес или доменное имя (в формате FQDN) узла актива.
   - Если для сканируемой цели актив ранее не был добавлен, в поле **Сетевые адреса** введите ее IP-адрес или доменное имя (в формате FQDN).

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

9. Нажмите кнопку **Сохранить**.

Задача на проведение аудита актива создана.

6.26. Eltex, серия ESR: 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, запустите терминальный клиент, поддерживающий протокол SSH.
2. Пройдите аутентификацию на активе.
3. Перейдите в режим конфигурирования:
   ```
   configure
   ```
4. Создайте метод локальной аутентификации:
   ```
   aaa authentication login <Название метода> local
   ```
5. Добавьте метод локальной аутентификации к линии протокола SSH:
   ```
   line ssh
   login authentication <Название метода>
   ```
6. Создайте учетную запись для доступа к активу:
   ```
   username <Логин>
   password <Пароль>
   privilege 15
   ```
7. Выйдите из режима конфигурирования:
   ```
   exit
   ```
8. Примените внесенные изменения:
   ```
   commit
   ```
9. Подтвердите изменение конфигурации:
   ```
   confirm
   ```

6.27. Eltex, серия ESR: настройка MaxPatrol VM

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

В этом разделе

6.27.1. Добавление учетной записи для доступа по SSH

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

  1. В главном меню выберите **Сбор данных** → **Учетные записи**.

     Откроется страница **Учетные записи**.
  2. Нажмите **Добавить учетную запись** → **Логин — пароль**.

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

  Учетная запись добавлена.

6.27.2. Создание задачи на аудит актива по SSH

- Чтобы создать задачу на проведение аудита актива:

  1. В главном меню выберите **Сбор данных** → **Задачи**.

     Откроется страница **Задачи по сбору данных**.
  2. Нажмите **Создать задачу** → **Сбор данных**.

     Откроется страница **Создание задачи на сбор данных**.
  3. В поле **Название** введите название задачи.
  4. В раскрывающемся списке **Профиль** выберите **SSH Network Device Audit**.
  5. В иерархическом списке выберите пункт **Сканирование систем** → **Через терминал: SSH**.

6. В раскрывающемся списке **Учетная запись** выберите учетную запись для доступа к активу.
7. Если требуется, в раскрывающемся списке **Коллекторы** выберите коллекторы для сбора данных.
8. В панели **Цели сбора данных** на вкладке **Включить** выполните одно из следующих действий:
   - Если для сканируемой цели ранее был добавлен актив, в поле **Активы** введите IP-адрес или доменное имя (в формате FQDN) узла актива.
   - Если для сканируемой цели актив ранее не был добавлен, в поле **Сетевые адреса** введите ее IP-адрес или доменное имя (в формате FQDN).

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

Задача на проведение аудита актива создана.

6.28. Eltex ROS, модели MES 1000, 2000, 23xx, 33xx, 35xx, 53xx, 5400-xx, 5500-32: 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. Пройдите аутентификацию 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.

6.29. Eltex ROS, модели MES 1000, 2000, 23xx, 33xx, 35xx, 53xx, 5400-xx, 5500-32: настройка MaxPatrol VM

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

В этом разделе

Добавление учетной записи для доступа по SSH (см. раздел 6.29.1)

Создание задачи на аудит актива по SSH (см. раздел 6.29.2)

6.29.1. Добавление учетной записи для доступа по SSH

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

1. В главном меню выберите **Сбор данных** → **Учетные записи**.

   Откроется страница **Учетные записи**.
2. Нажмите **Добавить учетную запись** → **Логин — пароль**.

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

Учетная запись добавлена.

6.29.2. Создание задачи на аудит актива по SSH

- Чтобы создать задачу на проведение аудита актива:

1. В главном меню выберите **Сбор данных** → **Задачи**.

Откроется страница **Задачи по сбору данных**.

2. Нажмите **Создать задачу** → **Сбор данных**.

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

3. В поле **Название** введите название задачи.
4. В раскрывающемся списке **Профиль** выберите **SSH Network Device Audit**.
5. В иерархическом списке выберите пункт **Сканирование систем** → **Через терминал: SSH**.
6. В раскрывающемся списке **Учетная запись** выберите учетную запись для доступа к активу.
7. Если требуется, в раскрывающемся списке **Коллекторы** выберите коллекторы для сбора данных.
8. В панели **Цели сбора данных** на вкладке **Включить** выполните одно из следующих действий:
   - Если для сканируемой цели ранее был добавлен актив, в поле **Активы** введите IP-адрес или доменное имя (в формате FQDN) узла актива.
   - Если для сканируемой цели актив ранее не был добавлен, в поле **Сетевые адреса** введите ее IP-адрес или доменное имя (в формате FQDN).

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

Задача на проведение аудита актива создана.

6.30. 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. Пройдите аутентификацию 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.

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

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

В этом разделе

Добавление учетной записи для доступа по SSH (см. раздел 6.31.1)

Создание задачи на аудит актива по SSH (см. раздел 6.31.2)

6.31.1. Добавление учетной записи для доступа по SSH

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

  1. В главном меню выберите **Сбор данных** → **Учетные записи**.

     Откроется страница **Учетные записи**.
  2. Нажмите **Добавить учетную запись** → **Логин — пароль**.

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

  Учетная запись добавлена.

6.31.2. Создание задачи на аудит актива по SSH

► Чтобы создать задачу на проведение аудита актива:

1. В главном меню выберите **Сбор данных** → **Задачи**.

   Откроется страница **Задачи по сбору данных**.

2. Нажмите **Создать задачу** → **Сбор данных**.

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

3. В поле **Название** введите название задачи.
4. В раскрывающемся списке **Профиль** выберите **SSH Network Device Audit**.
5. В иерархическом списке выберите пункт **Сканирование систем** → **Через терминал: SSH**.
6. В раскрывающемся списке **Учетная запись** выберите учетную запись для доступа к активу.
7. Если требуется, в раскрывающемся списке **Коллекторы** выберите коллекторы для сбора данных.
8. В панели **Цели сбора данных** на вкладке **Включить** выполните одно из следующих действий:
   - Если для сканируемой цели ранее был добавлен актив, в поле **Активы** введите IP-адрес или доменное имя (в формате FQDN) узла актива.
   - Если для сканируемой цели актив ранее не был добавлен, в поле **Сетевые адреса** введите ее IP-адрес или доменное имя (в формате FQDN).

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

Задача на проведение аудита актива создана.

6.32. Huawei VRP: 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 — порты UDP 161 и 162.

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

В этом разделе

6.32.1. Создание учетной записи для доступа к активу по SSH

- Чтобы создать учетную запись для доступа к активу:

  1. На узле, с которого производится настройка источника, запустите терминальный клиент, поддерживающий SSH.
  2. Пройдите аутентификацию на активе.
  3. Перейдите в режим конфигурирования:
     ```
     system-view
     ```
  4. Создайте учетную запись для доступа к активу:
     - Если установлена версия VRP 8, используйте команду:
       ```
       aaa
       local-user <Логин> password irreversible-cipher <Пароль>
       local-user <Логин> level 3
       local-user <Логин> service-type ssh
       ```
     - Если установлена версия VRP 5, используйте команду:
       ```
       aaa
       local-user <Логин> password irreversible-cipher <Пароль> privilege level 15
       local-user <Логин> service-type ssh
       ```
     - Если установлена версия ниже VRP 5, используйте команду:
       ```
       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
     ```

6.32.2. Создание ключей для доступа к активу по SNMP

- Чтобы создать ключи:

1. На узле, с которого производится настройка актива, запустите терминальный клиент, поддерживающий сетевые протоколы SSH и Telnet.
2. Пройдите аутентификацию на активе.

   ```
   system-view
   ```
3. Если необходимо ограничить доступ по протоколу SNMP, создайте список доступа 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
   ```
4. Включите поддержку версии протокола SNMPv3:

   ```
   snmp-agent sys-info version v3
   ```
5. Создайте группу с уровнем безопасности AuthPriv:

   ```
   snmp-agent group v3 <Имя группы> privacy
   ```
6. Добавьте пользователя в группу и укажите алгоритмы аутентификации и шифрования, значения ключей:

   ```
   snmp-agent usm-user v3 <Имя пользователя> <Имя группы> authentication-mode sha <Значение ключа аутентификации> privacy-mode aes128 <Значение ключа шифрования>
   ```

   Примечание. Рекомендуется использовать стойкие алгоритмы аутентификации (SHA и выше) и шифрования (AES-128 и выше).
7. Примените конфигурацию:

   ```
   commit
   ```

6.33. Huawei VRP: настройка MaxPatrol VM

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

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

В этом разделе

6.33.1. Добавление учетной записи для доступа по SSH

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

  1. В главном меню выберите **Сбор данных** → **Учетные записи**.

     Откроется страница **Учетные записи**.

  2. Нажмите **Добавить учетную запись** → **Логин — пароль**.

     Откроется страница **Добавление учетной записи**.

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

  Учетная запись добавлена.

6.33.2. Создание задачи на аудит актива по SSH

- Чтобы создать задачу на проведение аудита актива:

  1. В главном меню выберите **Сбор данных** → **Задачи**.

     Откроется страница **Задачи по сбору данных**.

  2. Нажмите **Создать задачу** → **Сбор данных**.

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

  3. В поле **Название** введите название задачи.
  4. В раскрывающемся списке **Профиль** выберите **SSH Network Device Audit**.
  5. В иерархическом списке выберите пункт **Сканирование систем** → **Через терминал: SSH**.
  6. В раскрывающемся списке **Учетная запись** выберите учетную запись для доступа к активу.
  7. Если требуется, в раскрывающемся списке **Коллекторы** выберите коллекторы для сбора данных.
  8. В панели **Цели сбора данных** на вкладке **Включить** выполните одно из следующих действий:

     - Если для сканируемой цели ранее был добавлен актив, в поле **Активы** введите IP-адрес или доменное имя (в формате FQDN) узла актива.

- Если для сканируемой цели актив ранее не был добавлен, в поле **Сетевые адреса** введите ее IP-адрес или доменное имя (в формате FQDN).

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

9. Нажмите кнопку **Сохранить**.

Задача на проведение аудита актива создана.

6.33.3. Добавление ключей для доступа по SNMP

Для добавление ключей в MaxPatrol VM необходимо создать для каждого из них отдельную учетную запись.

Добавление ключа аутентификации

► Чтобы добавить в MaxPatrol VM ключ аутентификации:

1. В главном меню выберите **Сбор данных** → **Учетные записи**.
2. Нажмите **Добавить учетную запись** → **Логин — пароль**.
3. Введите название учетной записи.
4. В раскрывающемся списке **Метки** установите флажок **SNMP**.
5. Введите логин учетной записи.
6. В полях **Пароль** и **Подтверждение пароля** введите значение ключа аутентификации, указанное при создании учетной записи.
7. Нажмите **Сохранить**.

Добавление ключа шифрования

► Чтобы добавить в MaxPatrol VM ключ шифрования:

1. В главном меню выберите **Сбор данных** → **Учетные записи**.
2. Нажмите **Добавить учетную запись** → **Пароль**.
3. Введите название учетной записи.
4. В раскрывающемся списке **Метки** установите флажок **SNMP**.
5. В полях **Пароль** и **Подтверждение пароля** введите значение ключа шифрования, указанное при создании учетной записи.
6. Нажмите **Сохранить**.

6.33.4. Создание задачи на аудит актива по SNMP

- Чтобы создать задачу на проведение аудита актива:

  1. В главном меню выберите **Сбор данных** → **Задачи**.
  2. Нажмите **Создать задачу** → **Сбор данных**.
  3. Введите название задачи.
  4. Выберите профиль **SNMP Network Device Audit**.
  5. В иерархическом списке выберите **Сканирование систем** → **По протоколу SNMP**.
  6. Выберите **Версия 3**.
  7. В раскрывающемся списке **Учетная запись** выберите учетную запись с ключом аутентификации для доступа к активу.
  8. Включите аутентификацию.
  9. Выберите алгоритм аутентификации, указанный при настройке актива.
  10. Включите шифрование.
  11. Выберите алгоритм шифрования, указанный при настройке актива.
  12. В раскрывающемся списке **Учетная запись типа «пароль»** выберите учетную запись с ключом шифрования для доступа к активу.
  13. Если требуется, выберите MP 10 Collector для сбора событий.
  14. 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.

  15. Нажмите **Сохранить**.

6.34. Huawei YunShan 1.22.1: настройка актива

Настройку актива нужно выполнять от имени учетной записи администратора устройства.

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

Внимание! Инструкция предназначена для создания учетной записи на сетевом устройстве, где используется локальная аутентификация пользователей.

- Чтобы создать учетную запись для доступа к активу:

  1. На узле, с которого производится настройка, запустите терминальный клиент, поддерживающий протокол SSH.
  2. Пройдите аутентификацию на активе.

3. Перейдите в режим конфигурирования:
   ```
   system-view
   ```
4. Создайте учетную запись для доступа к активу:
   ```
   aaa
   local-user <Логин> password irreversible-cipher <Пароль>
   local-user <Логин> privilege level 3
   local-user <Логин> service-type ssh
   ```
5. Выйдите из режима конфигурирования:
   ```
   quit
   ```
6. Сохраните изменения:
   ```
   save
   ```

6.35. Huawei YunShan 1.22.1: настройка MaxPatrol VM

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

В этом разделе

Добавление учетной записи для доступа к активу по SSH (см. раздел 6.35.1)

Создание и запуск задачи на аудит актива по SSH (см. раздел 6.35.2)

6.35.1. Добавление учетной записи для доступа к активу по SSH

- Чтобы добавить в MaxPatrol VM учетную запись для доступа к активу:
  1. В главном меню выберите **Сбор данных** → **Учетные записи**.
  2. Нажмите **Добавить учетную запись** → **Логин — пароль**.
  3. Введите название учетной записи.
  4. Введите логин учетной записи.
  5. Введите пароль и подтвердите его.
  6. Нажмите **Создать**.

6.35.2. Создание и запуск задачи на аудит актива по SSH

- Чтобы создать и запустить задачу на аудит актива:
  1. В главном меню выберите **Сбор данных** → **Задачи**.
  2. Нажмите **Создать задачу** → **Сбор данных**.

3. Введите название задачи.
4. В раскрывающемся списке **Профиль** выберите **SSH Network Device Audit**.
5. В иерархическом списке выберите **Сканирование систем** → **Через терминал: SSH**.
6. Выберите учетную запись для доступа к активу.
7. Если требуется, выберите коллекторы для сбора данных.
8. В панели **Цели сбора данных** на вкладке **Включить** выполните одно из следующих действий:
   - Если для сканируемой цели ранее был добавлен актив, в поле **Активы** введите IP-адрес или доменное имя (в формате FQDN) узла актива.
   - Если для сканируемой цели актив ранее не был добавлен, в поле **Сетевые адреса** введите ее IP-адрес или доменное имя (в формате FQDN).

     Примечание. В панели **Расписание** вы можете включить и настроить автоматический запуск задачи.
9. Нажмите **Сохранить и запустить** → **Запустить сбор данных**.

6.36. 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 — порты UDP 161 и 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 6.36.1)

Создание пароля для доступа к активу по SNMP (см. раздел 6.36.2)

6.36.1. 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. Пройдите аутентификацию 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.

6.36.2. 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. Пройдите аутентификацию на активе.
  3. Перейдите в режим конфигурирования:
     ```
     configure
     ```
  4. Создайте пароль для доступа к активу:
     ```
     edit snmp community <Пароль>
     ```
  5. Настройте доступ с IP-адреса узла MP 10 Collector с правом на чтение:
     ```
     set clients <IP-адрес MP 10 Collector>/32
     set authorization read-only
     ```
  6. Примените изменения и выйдите из режима конфигурирования:
     ```
     end
     ```

  Пароль создан.

6.37. Juniper JunOS 11—19: настройка MaxPatrol VM

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

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

6.37.1. Добавление учетной записи для доступа по SSH

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

  1. В главном меню выберите **Сбор данных** → **Учетные записи**.

     Откроется страница **Учетные записи**.
  2. Нажмите **Добавить учетную запись** → **Логин — пароль**.

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

  Учетная запись добавлена.

6.37.2. Создание задачи на аудит актива по SSH

- Чтобы создать задачу на проведение аудита актива:

  1. В главном меню выберите **Сбор данных** → **Задачи**.

     Откроется страница **Задачи по сбору данных**.
  2. Нажмите **Создать задачу** → **Сбор данных**.

     Откроется страница **Создание задачи на сбор данных**.
  3. В поле **Название** введите название задачи.
  4. В раскрывающемся списке **Профиль** выберите **SSH Network Device Audit**.
  5. В иерархическом списке выберите пункт **Сканирование систем** → **Через терминал: SSH**.

6. В раскрывающемся списке **Учетная запись** выберите учетную запись для доступа к активу.
7. Если требуется, в раскрывающемся списке **Коллекторы** выберите коллекторы для сбора данных.
8. В панели **Цели сбора данных** на вкладке **Включить** выполните одно из следующих действий:
   - Если для сканируемой цели ранее был добавлен актив, в поле **Активы** введите IP-адрес или доменное имя (в формате FQDN) узла актива.
   - Если для сканируемой цели актив ранее не был добавлен, в поле **Сетевые адреса** введите ее IP-адрес или доменное имя (в формате FQDN).

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

Задача на проведение аудита актива создана.

6.37.3. Добавление пароля для доступа по SNMP

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

1. В главном меню выберите **Сбор данных** → **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. Введите название учетной записи.
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.

6.37.4. Создание задачи на аудит актива по SNMP

► Чтобы создать задачу на проведение аудита актива:

1. В главном меню выберите **Сбор данных** → **Задачи**.
2. Нажмите **Создать задачу** → **Сбор данных**.
3. Введите название задачи.

4. Выберите профиль **SNMP Network Device Audit**.
5. В иерархическом списке выберите **Сканирование систем** → **По протоколу SNMP**.
6. Выберите **Версия 3**.
7. В раскрывающемся списке **Учетная запись** выберите учетную запись с ключом аутентификации для доступа к активу.
8. Включите аутентификацию.
9. Выберите алгоритм аутентификации, указанный при настройке актива.
10. Включите шифрование.
11. Выберите алгоритм шифрования, указанный при настройке актива.
12. В раскрывающемся списке **Учетная запись типа «пароль»** выберите учетную запись с ключом шифрования для доступа к активу.
13. Если требуется, выберите MP 10 Collector для сбора событий.
14. 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.
15. Нажмите **Сохранить**.

6.38. Lenovo ENOS 8.4: настройка актива

Настройку актива нужно выполнять от имени учетной записи администратора устройства.

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

Внимание! Инструкция предназначена для создания учетной записи на сетевом устройстве, где используется локальная аутентификация пользователей.

► Чтобы создать учетную запись для доступа к активу:

1. На узле, с которого производится настройка, запустите терминальный клиент, поддерживающий протокол SSH.
2. Пройдите аутентификацию на активе.
3. Перейдите в режим конфигурирования:
   ```
   configure terminal
   ```
4. Создайте учетную запись для доступа к активу:
   ```
   access user <Идентификатор учетной записи> name <Логин>
   ```
5. Установите пароль учетной записи:
   ```
   access user <Идентификатор учетной записи> password
   ```
6. Введите пароль.

7. Установите учетной записи уровень доступа:
   ```
   access user <Идентификатор учетной записи> level user
   ```
8. Активируйте учетную запись:
   ```
   access user <Идентификатор учетной записи> enable
   ```
9. Сохраните изменения:
   ```
   write
   ```

6.39. Lenovo ENOS 8.4: настройка MaxPatrol VM

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

В этом разделе

Добавление учетной записи для доступа к активу по SSH (см. раздел 6.39.1)

Создание и запуск задачи на аудит актива по SSH (см. раздел 6.39.2)

6.39.1. Добавление учетной записи для доступа к активу по SSH

- Чтобы добавить в MaxPatrol VM учетную запись для доступа к активу:
  1. В главном меню выберите **Сбор данных** → **Учетные записи**.
  2. Нажмите **Добавить учетную запись** → **Логин — пароль**.
  3. Введите название учетной записи.
  4. Введите логин учетной записи.
  5. Введите пароль и подтвердите его.
  6. Нажмите **Создать**.

6.39.2. Создание и запуск задачи на аудит актива по SSH

- Чтобы создать и запустить задачу на аудит актива:
  1. В главном меню выберите **Сбор данных** → **Задачи**.
  2. Нажмите **Создать задачу** → **Сбор данных**.
  3. Введите название задачи.
  4. В раскрывающемся списке **Профиль** выберите **SSH Network Device Audit**.
  5. В иерархическом списке выберите **Сканирование систем** → **Через терминал: SSH**.
  6. Выберите учетную запись для доступа к активу.

7. Если требуется, выберите коллекторы для сбора данных.
8. В панели **Цели сбора данных** на вкладке **Включить** выполните одно из следующих действий:
   - Если для сканируемой цели ранее был добавлен актив, в поле **Активы** введите IP-адрес или доменное имя (в формате FQDN) узла актива.
   - Если для сканируемой цели актив ранее не был добавлен, в поле **Сетевые адреса** введите ее IP-адрес или доменное имя (в формате FQDN).

     Примечание. В панели **Расписание** вы можете включить и настроить автоматический запуск задачи.
9. Нажмите **Сохранить и запустить** → **Запустить сбор данных**.

6.40. MikroTik RouterOS 6, 7: настройка актива

Настройку актива нужно выполнять от имени учетной записи администратора устройства.

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

► Чтобы создать учетную запись для доступа к активу:

1. На узле, с которого производится настройка, запустите терминальный клиент, поддерживающий протокол SSH.
2. Пройдите аутентификацию на активе.
3. Создайте учетную запись для доступа к активу:
   ```
   user add name=<Логин> group=read password=<Пароль>
   ```
4. Разрешите подключение по протоколу SSH с IP-адреса сервера MP 10 Collector:
   ```
   ip service set ssh address=<IP-адрес MP 10 Collector>
   ```

6.41. MikroTik RouterOS 6, 7: настройка MaxPatrol VM

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

В этом разделе

6.41.1. Добавление учетной записи для доступа к активу по SSH

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

  1. В главном меню выберите **Сбор данных** → **Учетные записи**.
  2. Нажмите **Добавить учетную запись** → **Логин — пароль**.
  3. Введите название учетной записи.
  4. Укажите логин учетной записи в формате `<Логин>+c`.

     Например:
     `administrator+c`
  5. Введите пароль и подтвердите его.
  6. Нажмите **Создать**.

6.41.2. Создание и запуск задачи на аудит актива по SSH

- Чтобы создать и запустить задачу на аудит актива:

  1. В главном меню выберите **Сбор данных** → **Задачи**.
  2. Нажмите **Создать задачу** → **Сбор данных**.
  3. Введите название задачи.
  4. В раскрывающемся списке **Профиль** выберите **SSH Network Device Audit**.
  5. В иерархическом списке выберите **Сканирование систем** → **Через терминал: SSH**.
  6. Выберите учетную запись для доступа к активу.
  7. Включите **Показывать дополнительные параметры**.
  8. В поле **Параметры SSH** → **Разделитель команд** укажите значение `\r\n`.
  9. Если требуется, выберите коллекторы для сбора данных.
  10. В панели **Цели сбора данных** на вкладке **Включить** выполните одно из следующих действий:

      - Если для сканируемой цели ранее был добавлен актив, в поле **Активы** введите IP-адрес или доменное имя (в формате FQDN) узла актива.
      - Если для сканируемой цели актив ранее не был добавлен, в поле **Сетевые адреса** введите ее IP-адрес или доменное имя (в формате FQDN).

      Примечание. В панели **Расписание** вы можете включить и настроить автоматический запуск задачи.
  11. Нажмите **Сохранить и запустить** → **Запустить сбор данных**.

6.42. 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. Пройдите аутентификацию 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.

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

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

В этом разделе

6.43.1. Добавление учетной записи для доступа по SSH

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

  1. В главном меню выберите **Сбор данных** → **Учетные записи**.

     Откроется страница **Учетные записи**.
  2. Нажмите **Добавить учетную запись** → **Логин — пароль**.

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

  Учетная запись добавлена.

6.43.2. Создание задачи на аудит актива по SSH

- Чтобы создать задачу на проведение аудита актива:

  1. В главном меню выберите **Сбор данных** → **Задачи**.

     Откроется страница **Задачи по сбору данных**.
  2. Нажмите **Создать задачу** → **Сбор данных**.

     Откроется страница **Создание задачи на сбор данных**.
  3. В поле **Название** введите название задачи.
  4. В раскрывающемся списке **Профиль** выберите **SSH Network Device Audit**.

5. В иерархическом списке выберите пункт **Сканирование систем** → **Через терминал: SSH**.
6. В раскрывающемся списке **Учетная запись** выберите учетную запись для доступа к активу.
7. Если требуется, в раскрывающемся списке **Коллекторы** выберите коллекторы для сбора данных.
8. В панели **Цели сбора данных** на вкладке **Включить** выполните одно из следующих действий:
   - Если для сканируемой цели ранее был добавлен актив, в поле **Активы** введите IP-адрес или доменное имя (в формате FQDN) узла актива.
   - Если для сканируемой цели актив ранее не был добавлен, в поле **Сетевые адреса** введите ее IP-адрес или доменное имя (в формате FQDN).

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

Задача на проведение аудита актива создана.

6.44. ViPNet Coordinator 4 и выше: настройка актива

Настройку актива нужно выполнять от имени учетной записи администратора защищенной сети ViPNet.

Для аудита на активе нужно создать учетную запись с помощью программного обеспечения «ViPNet Центр управления сетью» или ViPNet Prime для доступа MP 10 Collector к активу по протоколу SSH.

Внимание! Максимальная длина имени объекта в правилах фильтрации — 51 символ.

Для подключения MP 10 Collector к активу по протоколу SSH необходимо добавить правило доступа в локальный фильтр firewall.

► Чтобы добавить правило доступа в локальный фильтр firewall,

выполните команду:

```
firewall local add <Номер правила доступа> rule "<Название правила доступа>" src <IP-адрес MP 10 Collector> dst @local tcp dport 22 pass
```

6.45. ViPNet Coordinator 4 и выше: настройка MaxPatrol VM

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

В этом разделе

6.45.1. Добавление учетной записи для доступа к активу по SSH

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

  1. В главном меню выберите **Сбор данных** → **Учетные записи**.
  2. Нажмите **Добавить учетную запись** → **Логин — пароль**.
  3. Введите название учетной записи.
  4. Введите логин учетной записи.
  5. Введите пароль и подтвердите его.
  6. Нажмите **Создать**.

6.45.2. Создание и запуск задачи на аудит актива

- Чтобы создать и запустить задачу на аудит актива:

  1. В главном меню выберите **Сбор данных** → **Задачи**.
  2. Нажмите **Создать задачу** → **Сбор данных**.
  3. Введите название задачи.
  4. В раскрывающемся списке **Профиль** выберите **SSH Network Device Audit**.
  5. В иерархическом списке выберите **Сканирование систем** → **Через терминал: SSH**.
  6. Выберите учетную запись для доступа к активу.
  7. Если требуется, выберите коллекторы для сбора данных.
  8. В панели **Цели сбора данных** на вкладке **Включить** выполните одно из следующих действий:

     - Если для сканируемой цели ранее был добавлен актив, в поле **Активы** введите IP-адрес или доменное имя (в формате FQDN) узла актива.
     - Если для сканируемой цели актив ранее не был добавлен, в поле **Сетевые адреса** введите ее IP-адрес или доменное имя (в формате FQDN).

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

  9. Нажмите **Сохранить и запустить** → **Запустить сбор данных**.

7. Системы аутентификации, авторизации и учета

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

В этом разделе

7.1. Cisco ACS 5: настройка актива

Настройка актива выполняется аналогично Cisco ADE-OS (см. раздел 7.3).

7.2. Cisco ACS 5: настройка MaxPatrol VM

Настройка MaxPatrol VM для аудита актива выполняется аналогично Cisco ADE-OS (см. раздел 7.4).

7.3. 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 — порты UDP 161 и 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

7.3.1. 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. Пройдите аутентификацию 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.

7.3.2. 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. Пройдите аутентификацию 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.

7.4. 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

7.4.1. Добавление учетной записи для доступа по SSH

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

  1. В главном меню выберите **Сбор данных** → **Учетные записи**.

     Откроется страница **Учетные записи**.
  2. Нажмите **Добавить учетную запись** → **Логин — пароль**.

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

  Учетная запись добавлена.

7.4.2. Создание задачи на аудит актива по SSH

- Чтобы создать задачу на проведение аудита актива:

  1. В главном меню выберите **Сбор данных** → **Задачи**.

     Откроется страница **Задачи по сбору данных**.
  2. Нажмите **Создать задачу** → **Сбор данных**.

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

3. В поле **Название** введите название задачи.
4. В раскрывающемся списке **Профиль** выберите **SSH Network Device Audit**.
5. В иерархическом списке выберите пункт **Сканирование систем** → **Через терминал: SSH**.
6. В раскрывающемся списке **Учетная запись** выберите учетную запись для доступа к активу.
7. Если требуется, в раскрывающемся списке **Коллекторы** выберите коллекторы для сбора данных.
8. В панели **Цели сбора данных** на вкладке **Включить** выполните одно из следующих действий:
   - Если для сканируемой цели ранее был добавлен актив, в поле **Активы** введите IP-адрес или доменное имя (в формате FQDN) узла актива.
   - Если для сканируемой цели актив ранее не был добавлен, в поле **Сетевые адреса** введите ее IP-адрес или доменное имя (в формате FQDN).

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

Задача на проведение аудита актива создана.

7.4.3. Добавление пароля для доступа по SNMP

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

1. В главном меню выберите **Сбор данных** → **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. Введите название учетной записи.
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.

7.4.4. Создание задачи на аудит актива по SNMP

- Чтобы создать задачу на проведение аудита актива:

  1. В главном меню выберите **Сбор данных** → **Задачи**.
  2. Нажмите **Создать задачу** → **Сбор данных**.
  3. Введите название задачи.
  4. Выберите профиль **SNMP Network Device Audit**.
  5. В иерархическом списке выберите **Сканирование систем** → **По протоколу SNMP**.
  6. Выберите **Версия 3**.
  7. В раскрывающемся списке **Учетная запись** выберите учетную запись с ключом аутентификации для доступа к активу.
  8. Включите аутентификацию.
  9. Выберите алгоритм аутентификации, указанный при настройке актива.
  10. Включите шифрование.
  11. Выберите алгоритм шифрования, указанный при настройке актива.
  12. В раскрывающемся списке **Учетная запись типа «пароль»** выберите учетную запись с ключом шифрования для доступа к активу.
  13. Если требуется, выберите MP 10 Collector для сбора событий.
  14. 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.

  15. Нажмите **Сохранить**.

7.5. 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 7.3).

7.6. Cisco Identity Services Engine (ISE) 2.3: настройка MaxPatrol VM

Настройка MaxPatrol VM для аудита актива выполняется аналогично Cisco ADE-OS (см. раздел 7.4).

8. Системы виртуализации

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

В этом разделе

8.1. oVirt Engine 4.4—4.5: настройка актива

Настройку актива нужно выполнять от имени учетной записи администратора устройства.

Для аудита актива нужно:

1. Средствами ОС создать учетную запись для доступа MP 10 Collector к активу через веб-API.
2. Создать и настроить роль для созданной учетной записи.
3. Назначить созданную роль учетной записи.
4. Создать учетную запись для доступа MP 10 Collector к активу по протоколу SSH в операционной системе, где установлен актив. Настройку нужно выполнять по инструкциям раздела «Unix-подобные ОС: настройка актива (см. раздел 4.3)».

В этом разделе

8.1.1. Создание учетной записи для доступа к активу через веб-API

- Чтобы создать учетную запись для доступа к активу:

  1. На узле, с которого производится настройка, запустите терминальный клиент, поддерживающий протокол SSH.
  2. Пройдите аутентификацию на активе.
  3. Создайте учетную запись для доступа к активу:

     ```
     ovirt-aaa-jdbc-tool user add <Логин>
     ```

  4. Установите пароль учетной записи и срок его действия:

     ```
     ovirt-aaa-jdbc-tool user password-reset <Логин> --password-valid-to=<Дата и время окончания действия пароля>
     ```

     Например:

     ```
     ovirt-aaa-jdbc-tool user password-reset <Логин> --password-valid-to="2025-08-01 12:00:00+0000"
     ```

8.1.2. Создание и настройка роли

- Чтобы создать и настроить роль:

  1. Войдите в веб-интерфейс актива от имени учетной записи с правами администратора.
  2. Нажмите **Administration Portal.**
  3. Нажмите **Administration** → **Configure**.
  4. Нажмите **New**.
  5. В поле **Name** введите название роли.
  6. Выберите тип учетной записи **Admin**.
  7. В иерархическом списке выберите **System** → **Configure System**.
  8. Установите флажок **Login Permissions**.
  9. Нажмите **OK**.

8.1.3. Назначение роли учетной записи

- Чтобы назначить роль учетной записи:

  1. Войдите в веб-интерфейс актива от имени учетной записи с правами администратора.
  2. Нажмите **Administration Portal.**
  3. Нажмите **Administration** → **Users**.

4. Нажмите **Add**.
5. В поле поиска введите учетную запись для доступа к активу и нажмите **GO**.
6. В появившемся списке результатов поиска выберите учетную запись для доступа к активу и нажмите **Add and Close**.

   На странице **Users** в списке учетных записей отобразится учетная запись для доступа к активу.
7. В столбце **User Name** выберите логин учетной записи для доступа к активу.

   Откроется страница с параметрами учетной записи.
8. Выберите вкладку **Permissions**.
9. Нажмите **Add System Permissions**.
10. В раскрывающемся списке **Role to Assign** выберите созданную ранее роль.
11. Нажмите **OK**.

8.2. oVirt Engine 4.4—4.5: настройка MaxPatrol VM

Для аудита актива в MaxPatrol VM нужно добавить две учетные записи: одну для доступа к активу через веб-API и другую для доступа по протоколу SSH, а также создать и запустить задачу на аудит.

В этом разделе

Добавление учетной записи для доступа к активу через веб-API (см. раздел 8.2.1)

Добавление учетной записи для доступа к активу по SSH (см. раздел 8.2.2)

Создание и запуск задачи на аудит актива (см. раздел 8.2.3)

8.2.1. Добавление учетной записи для доступа к активу через веб-API

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

  1. В главном меню выберите **Сбор данных** → **Учетные записи**.
  2. Нажмите **Добавить учетную запись** → **Логин — пароль**.
  3. Введите название учетной записи.
  4. В раскрывающемся списке **Метки** установите флажок **Web_API**.
  5. Укажите логин учетной записи в формате `<Логин>@<Домен учетной записи>`.
  6. Введите пароль и подтвердите его.
  7. Нажмите **Создать**.

8.2.2. Добавление учетной записи для доступа к активу по SSH

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

  1. В главном меню выберите **Сбор данных** → **Учетные записи**.
  2. Нажмите **Добавить учетную запись** → **Логин — пароль**.
  3. Введите название учетной записи.
  4. В раскрывающемся списке **Метки** установите флажок **Terminal**.
  5. Введите логин учетной записи.
  6. Введите пароль и подтвердите его.
  7. Нажмите **Создать**.

8.2.3. Создание и запуск задачи на аудит актива

- Чтобы создать и запустить задачу на аудит актива:

  1. В главном меню выберите **Сбор данных** → **Задачи**.
  2. Нажмите **Создать задачу** → **Сбор данных**.
  3. Введите название задачи.
  4. В раскрывающемся списке **Профиль** выберите **Unix SSH and Web API Audit**.
  5. В иерархическом списке выберите **Сканирование систем** → **Через терминал: SSH**.
  6. Выберите учетную запись для доступа к активу по SSH.
  7. В иерархическом списке выберите **Сканирование систем** → **Через веб-API**.
  8. Выберите тип аутентификации **Учетные данные**.
  9. Выберите учетную запись для доступа к активу через веб-API.
  10. Включите **Показывать дополнительные параметры**.
  11. Укажите номер порта.
  12. Если требуется, выберите коллекторы для сбора данных.
  13. 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.

  14. Нажмите **Сохранить и запустить** → **Запустить сбор данных**.

8.3. VMware vCenter Server 5.5—8.0: настройка актива

Настройку VMware vCenter Server for Windows 5.5—6.5 нужно выполнять от имени учетной записи, имеющей права администратора ОС и права администратора VMware vCenter Server for Windows.

Настройку VMware vCenter Server Appliance 6.7—8.0 нужно выполнять от имени учетной записи, имеющей права администратора VMware vCenter Server Appliance.

> **Внимание!** При использовании межсетевого экрана требуется настроить в нем правила, разрешающие внешние подключения к используемым портам TCP/IP. Для доступа к VMware vCenter Server 5.5—8.0 по умолчанию используется порт 443/TCP.

Для аудита VMware vCenter Server for Windows 5.5—6.5 через vSphere API нужно:

1. Средствами ОС создать учетную запись (см. раздел 17.1.2) для доступа MP 10 Collector.
2. Добавить учетную запись в локальную (групповую) политику безопасности (см. раздел 17.1.3) «Доступ к компьютеру из сети» (Access this computer from the network).
3. Добавить учетную запись в VMware vCenter Server for Windows и назначить ей права с помощью роли. Настройку нужно выполнять по инструкциям из разделов:
   - «Добавление учетной записи и назначение роли в VMware vCenter Server for Windows 5.5, 6.0 (см. раздел 17.7.1)»;
   - «Добавление учетной записи и назначение роли в VMware vCenter Server for Windows 6.5 (см. раздел 17.7.2)».

Для аудита VMware vCenter Server Appliance 6.7—8.0 через vSphere API нужно:

1. Создать учетную запись (см. раздел 17.7.3) для VMware vCenter Server Appliance.
2. Назначить права учетной записи с помощью роли (см. раздел 17.7.4).

См. также

Создание учетной записи для VMware vCenter Server Appliance 6.7—8.0 (см. раздел 17.7.3)

8.4. VMware vCenter Server 5.5—8.0: настройка MaxPatrol VM

Для аудита актива в MaxPatrol VM нужно добавить учетную запись для доступа к активу, создать и запустить задачу на аудит.

> **Примечание.** Для доступа на сервер VMware vCenter Server 5.5—8.0 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

8.4.1. Добавление учетной записи для доступа к активу

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

  1. В главном меню выберите **Сбор данных** → **Учетные записи**.
  2. Нажмите **Добавить учетную запись** → **Логин — пароль**.
  3. Введите название учетной записи.
  4. В раскрывающемся списке **Метки** установите флажок **vSphere_API**.
  5. Введите логин учетной записи.
  6. Введите пароль и подтвердите его.
  7. Если для доступа к источнику используется доменная учетная запись, введите имя домена.
  8. Нажмите **Создать**.

8.4.2. Создание и запуск задачи на аудит актива

- Чтобы создать и запустить задачу на аудит актива:

  1. В главном меню выберите **Сбор данных** → **Задачи**.
  2. Нажмите **Создать задачу** → **Сбор данных**.
  3. Введите название задачи.
  4. В раскрывающемся списке **Профиль** выберите **vSphere Audit**.
  5. В иерархическом списке выберите **Сканирование систем** → **VMware vSphere**.
  6. Выберите учетную запись для доступа к активу.
  7. Если требуется, выберите коллекторы для сбора данных.
  8. 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.
  9. Нажмите **Сохранить и запустить** → **Запустить сбор данных**.

8.5. VMware vSphere Hypervisor (ESXi) 6.5—7.0: настройка актива

Настройку нужно выполнять от имени учетной записи, имеющей права администратора VMware vSphere Hypervisor (ESXi).

Для VMware vSphere Hypervisor (ESXi) поддерживается сбор данных через vSphere API и по протоколу SSH. Достаточно настроить один из способов.

> **Внимание!** При использовании межсетевого экрана требуется настроить в нем правила, разрешающие внешние подключения к используемым портам TCP/IP. Для доступа к активу через vSphere API по умолчанию используется порт 443/TCP, для доступа к активу по протоколу SSH — порт 22/TCP.

Для аудита актива нужно:

1. Создать учетную запись для доступа MP 10 Collector к активу.

   Внимание! Для сбора информации об учетных записях VMware vSphere Hypervisor (ESXi) в режиме Lockdown mode, требуется привилегия Global.Settings. Для сбора других данных достаточно привилегий из группы System.

2. Создать и настроить роль для учетной записи.
3. Назначить созданную роль учетной записи.
4. Добавить учетную запись в список исключений режима Lockdown mode.
5. Настроить IP-адрес и FQDN на активе.

Для доступа по протоколу SSH нужно включить доступ по SSH в веб-интерфейсе актива, затем настроить доступ по SSH для созданной учетной записи.

В этом разделе

8.5.1. Создание учетной записи для доступа к активу

- Чтобы создать учетную запись для доступа к активу:
  1. Войдите в веб-интерфейс актива от имени учетной записи с правами администратора.
  2. Нажмите **Host** → **Manage**.
  3. Выберите вкладку **Security & users**.
  4. В левой части страницы выберите **Users**.
  5. Нажмите **Add user**.
  6. В поле **User name** введите логин учетной записи.
  7. В поле **Password** укажите пароль учетной записи и подтвердите его в поле **Confirm password**.
  8. Нажмите **Add**.

8.5.2. Создание и настройка роли

- Чтобы создать и настроить роль:
  1. Войдите в веб-интерфейс актива от имени учетной записи с правами администратора.
  2. Нажмите **Host** → **Manage**.
  3. Выберите вкладку **Security & users**.
  4. В левой части страницы выберите **Roles**.
  5. Нажмите **Add role**.
  6. В поле **Role name** введите название роли.
  7. Установите флажок **System**.
  8. Нажмите **Global** и установите флажок **Settings**.
  9. Нажмите **Add**.

8.5.3. Назначение роли учетной записи

- Чтобы назначить роль учетной записи:
  1. Войдите в веб-интерфейс актива от имени учетной записи с правами администратора.
  2. Нажмите **Host** → **Permissions**.
  3. Нажмите **Add user**.
  4. В раскрывающемся списке слева выберите учетную запись для доступа к активу.

5. В раскрывающемся списке справа выберите роль, созданную ранее.
6. Нажмите кнопку **Add user**.

   Выбранная учетная запись добавится в список пользователей в окне **Manage permissions**.

8.5.4. Добавление учетной записи в список исключений режима Lockdown mode

► Чтобы добавить учетную запись в список исключений режима Lockdown mode:

1. Войдите в веб-интерфейс актива от имени учетной записи с правами администратора.
2. Нажмите **Host** → **Manage**.
3. Выберите вкладку **Security & users**.
4. В левой части страницы выберите **Lockdown mode**.
5. Нажмите **Add user exception**.
6. В поле **User name** укажите название учетной записи для доступа к активу.
7. Нажмите **Add exception**.

8.5.5. Настройка IP-адреса и FQDN на активе

Внимание! Если VMware vSphere Hypervisor (ESXi) уже входит в кластер, изменение его FQDN может привести к проблемам в работе кластера.

► Чтобы настроить IP-адрес и FQDN на активе:

1. На узле, с которого производится настройка, запустите терминальный клиент, поддерживающий протокол SSH.
2. Пройдите аутентификацию на активе.
3. Откройте файл `/etc/hosts`.
4. Добавьте в файл строки:

   ```
   <IP-адрес сервера VMware vSphere Hypervisor (ESXi)> <FQDN сервера VMware vSphere Hypervisor (ESXi)>
   127.0.0.1 <FQDN сервера VMware vSphere Hypervisor (ESXi)>
   ::1 <FQDN сервера VMware vSphere Hypervisor (ESXi)>
   ```
5. Сохраните файл.
6. Перезагрузите актив.

8.5.6. Включение и настройка доступа к активу по протоколу SSH

- Чтобы включить и настроить доступ к активу по протоколу SSH:

  1. Войдите в веб-интерфейс актива от имени учетной записи с правами администратора.
  2. Нажмите **Host** → **Services** → **Enable Secure Shell (SSH)**.
  3. На узле, с которого производится настройка, запустите терминальный клиент, поддерживающий протокол SSH.
  4. Пройдите аутентификацию на активе.
  5. Откройте на редактирование файл `/etc/security/access.conf`.
  6. В строке `-:<Логин учетной записи для доступа к активу>:ALL` замените `-` на `+`.

8.6. VMware vSphere Hypervisor (ESXi) 6.5—7.0: настройка MaxPatrol VM

Для аудита актива в MaxPatrol VM нужно добавить учетную запись для доступа к активу, создать и запустить задачу на аудит.

В этом разделе

8.6.1. Добавление учетной записи для доступа к активу по SSH

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

  1. В главном меню выберите **Сбор данных** → **Учетные записи**.
  2. Нажмите **Добавить учетную запись** → **Логин — пароль**.
  3. Введите название учетной записи.
  4. Введите логин учетной записи.
  5. Введите пароль и подтвердите его.
  6. Нажмите **Создать**.

8.6.2. Добавление учетной записи для доступа к активу через vSphere API

- Чтобы добавить в MaxPatrol VM учетную запись для доступа к активу:
  1. В главном меню выберите **Сбор данных** → **Учетные записи**.
  2. Нажмите **Добавить учетную запись** → **Логин — пароль**.
  3. Введите название учетной записи.
  4. В раскрывающемся списке **Метки** установите флажок **vSphere_API**.
  5. Введите логин учетной записи.
  6. Введите пароль и подтвердите его.
  7. Нажмите **Создать**.

8.6.3. Создание и запуск задачи на аудит актива по SSH

- Чтобы создать и запустить задачу на аудит актива:
  1. В главном меню выберите **Сбор данных** → **Задачи**.
  2. Нажмите **Создать задачу** → **Сбор данных**.
  3. Введите название задачи.
  4. В раскрывающемся списке **Профиль** выберите **Unix SSH Audit**.
  5. В иерархическом списке выберите **Сканирование систем** → **Через терминал: SSH**.
  6. Выберите учетную запись для доступа к активу.
  7. Если требуется, выберите коллекторы для сбора данных.
  8. В поле **Активы** введите IP-адрес или доменное имя (в формате FQDN) узла актива.
  9. Нажмите **Сохранить и запустить** → **Запустить сбор данных**.

8.6.4. Создание и запуск задачи на аудит актива через vSphere API

- Чтобы создать и запустить задачу на аудит актива:
  1. В главном меню выберите **Сбор данных** → **Задачи**.
  2. Нажмите **Создать задачу** → **Сбор данных**.
  3. Введите название задачи.
  4. В раскрывающемся списке **Профиль** выберите **vSphere Audit**.

5. В иерархическом списке выберите **Сканирование систем** → **VMware vSphere**.
6. Выберите учетную запись для доступа к активу.
7. Если требуется, выберите коллекторы для сбора данных.
8. 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.
9. Нажмите **Сохранить и запустить** → **Запустить сбор данных**.

8.7. zVirt Engine 4.4—4.5: настройка актива

Настройку актива нужно выполнять от имени учетной записи администратора устройства.

Для аудита актива нужно:

1. Средствами ОС создать учетную запись для доступа MP 10 Collector к активу через веб-API.
2. Создать и настроить роль для созданной учетной записи.
3. Назначить созданную роль учетной записи.
4. Снять ограничения на сессии для созданной учетной записи.
5. Создать учетную запись для доступа MP 10 Collector к активу по протоколу SSH в операционной системе, где установлен актив. Настройку нужно выполнять по инструкциям раздела «Unix-подобные ОС: настройка актива (см. раздел 4.3)».

В этом разделе

8.7.1. Создание учетной записи для доступа к активу через веб-API

- Чтобы создать учетную запись для доступа к активу:

  1. На узле, с которого производится настройка, запустите терминальный клиент, поддерживающий протокол SSH.
  2. Пройдите аутентификацию на активе.

3. Создайте учетную запись для доступа к активу:

   ```
   ovirt-aaa-jdbc-tool user add <Логин>
   ```

4. Установите пароль учетной записи и срок его действия:

   ```
   ovirt-aaa-jdbc-tool user password-reset <Логин> --password-valid-to=<Дата и время окончания действия пароля>
   ```

   Например:

   ```
   ovirt-aaa-jdbc-tool user password-reset <Логин> --password-valid-to="2025-08-01 12:00:00+0000"
   ```

8.7.2. Создание и настройка роли

- Чтобы создать и настроить роль:

1. Войдите в веб-интерфейс актива от имени учетной записи с правами администратора.
2. Нажмите **Портал администрирования**.
3. Нажмите **Управление** → **Настройка**.
4. Нажмите **Новая**.
5. В поле **Имя** введите название роли.
6. Выберите тип учетной записи **Администратор**.
7. В иерархическом списке выберите **Система** → **Настроить систему**.
8. Установите флажок **Разрешения входа**.
9. Нажмите **ОК**.

8.7.3. Назначение роли учетной записи

- Чтобы назначить роль учетной записи:

1. Войдите в веб-интерфейс актива от имени учетной записи с правами администратора.
2. Нажмите **Портал администрирования**.
3. Нажмите **Управление** → **Пользователи**.
4. Нажмите **Добавить**.
5. В поле поиска введите учетную запись для доступа к активу и нажмите **Поиск**.
6. В появившемся списке результатов поиска выберите учетную запись для доступа к активу и нажмите **Добавить и закрыть**.

   На странице **Пользователи** в списке учетных записей отобразится учетная запись для доступа к активу.
7. В столбце **Имя пользователя** выберите логин учетной записи для доступа к активу.

Откроется страница с параметрами учетной записи.

8. Выберите вкладку **Разрешения**.
9. Нажмите **Добавление системных разрешений**.
10. В раскрывающемся списке **Роль для связи** выберите созданную ранее роль.
11. Нажмите **ОК**.

8.7.4. Снятие ограничений на сессии для учетной записи

- Чтобы снять ограничения на сессии для учетной записи:

1. Войдите в веб-интерфейс актива от имени учетной записи с правами администратора.
2. Нажмите **Портал администрирования**.
3. Нажмите **Управление** → **Пользователи**.

   Откроется страница **Пользователи** со списком учетных записей.
4. В столбце **Имя пользователя** выберите логин учетной записи для доступа к активу.

   Откроется страница с параметрами учетной записи.
5. Нажмите **Управление ограничениями**.
6. В полях **Количество сессий** и **Время сессий (минуты)** укажите `0`.
7. Нажмите **Сохранить**.

8.8. zVirt Engine 4.4—4.5: настройка MaxPatrol VM

Для аудита актива в MaxPatrol VM нужно добавить две учетные записи: одну для доступа к активу через веб-API и другую для доступа по протоколу SSH, а также создать и запустить задачу на аудит.

В этом разделе

Добавление учетной записи для доступа к активу через веб-API (см. раздел 8.8.1)

Добавление учетной записи для доступа к активу по SSH (см. раздел 8.8.2)

Создание и запуск задачи на аудит актива (см. раздел 8.8.3)

8.8.1. Добавление учетной записи для доступа к активу через веб-API

- Чтобы добавить в MaxPatrol VM учетную запись для доступа к активу:
  1. В главном меню выберите **Сбор данных** → **Учетные записи**.
  2. Нажмите **Добавить учетную запись** → **Логин — пароль**.
  3. Введите название учетной записи.
  4. В раскрывающемся списке **Метки** установите флажок **Web_API**.
  5. Укажите логин учетной записи в формате `<Логин>@<Домен учетной записи>`.
  6. Введите пароль и подтвердите его.
  7. Нажмите **Создать**.

8.8.2. Добавление учетной записи для доступа к активу по SSH

- Чтобы добавить в MaxPatrol VM учетную запись для доступа к активу:
  1. В главном меню выберите **Сбор данных** → **Учетные записи**.
  2. Нажмите **Добавить учетную запись** → **Логин — пароль**.
  3. Введите название учетной записи.
  4. В раскрывающемся списке **Метки** установите флажок **Terminal**.
  5. Введите логин учетной записи.
  6. Введите пароль и подтвердите его.
  7. Нажмите **Создать**.

8.8.3. Создание и запуск задачи на аудит актива

- Чтобы создать и запустить задачу на аудит актива:
  1. В главном меню выберите **Сбор данных** → **Задачи**.
  2. Нажмите **Создать задачу** → **Сбор данных**.
  3. Введите название задачи.
  4. В раскрывающемся списке **Профиль** выберите **Unix SSH and Web API Audit**.
  5. В иерархическом списке выберите **Сканирование систем** → **Через терминал: SSH**.
  6. Выберите учетную запись для доступа к активу по SSH.

7. В иерархическом списке выберите **Сканирование систем** → **Через веб-API**.
8. Выберите тип аутентификации **Учетные данные**.
9. Выберите учетную запись для доступа к активу через веб-API.
10. Включите **Показывать дополнительные параметры**.
11. Укажите номер порта.
12. Если требуется, выберите коллекторы для сбора данных.
13. 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.
14. Нажмите **Сохранить и запустить** → **Запустить сбор данных**.

9. Системы защиты сети

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

В этом разделе

9.1. 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. Пройдите аутентификацию 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.

9.2. Palo Alto Networks PAN-OS 6.1—8.1: настройка MaxPatrol VM

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

В этом разделе

9.2.1. Добавление учетной записи для доступа по SSH

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

  1. В главном меню выберите **Сбор данных** → **Учетные записи**.

     Откроется страница **Учетные записи**.
  2. Нажмите **Добавить учетную запись** → **Логин — пароль**.

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

  Учетная запись добавлена.

9.2.2. Создание задачи на аудит актива по SSH

- Чтобы создать задачу на проведение аудита актива:

  1. В главном меню выберите **Сбор данных** → **Задачи**.

     Откроется страница **Задачи по сбору данных**.
  2. Нажмите **Создать задачу** → **Сбор данных**.

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

3. В поле **Название** введите название задачи.
4. В раскрывающемся списке **Профиль** выберите **SSH Network Device Audit**.
5. В иерархическом списке выберите пункт **Сканирование систем** → **Через терминал: SSH**.
6. В раскрывающемся списке **Учетная запись** выберите учетную запись для доступа к активу.
7. Если требуется, в раскрывающемся списке **Коллекторы** выберите коллекторы для сбора данных.
8. В панели **Цели сбора данных** на вкладке **Включить** выполните одно из следующих действий:
   - Если для сканируемой цели ранее был добавлен актив, в поле **Активы** введите IP-адрес или доменное имя (в формате FQDN) узла актива.
   - Если для сканируемой цели актив ранее не был добавлен, в поле **Сетевые адреса** введите ее IP-адрес или доменное имя (в формате FQDN).

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

Задача на проведение аудита актива создана.

9.3. 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 17.1.1) «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 17.1.2) 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 17.1.3) «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

9.3.1. 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. 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 **ОК**.

Учетная запись добавлена.

9.3.2. 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 **ОК**.

Пользовательский профиль создан.

9.3.3. 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. В списке **Узлы** по ссылке **Добавить профиль** добавьте строку.
  7. В колонке **Профиль и переопределения** в раскрывающемся списке выберите профиль сканирования.
  8. В колонке **Узлы** введите через запятую IP-адреса узлов для сканирования.
  9. Нажмите кнопку **ОК**.
  10. В панели **Задачи** нажмите .

      В панели **Активные сканы** появится строка статуса сканирования.

  Задача на сканирование создана и запущена.

9.3.4. 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 **ОК**.

  Доставка отчетов настроена.

9.3.5. 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. Укажите 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.

9.3.6. 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.

9.4. 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

9.4.1. Добавление учетной записи

- Чтобы добавить в MaxPatrol VM учетную запись для доступа на узел MP8:

  1. В главном меню выберите **Сбор данных** → **Учетные записи**.

     Откроется страница **Учетные записи**.
  2. Нажмите **Добавить учетную запись** → **Логин — пароль**.

     Откроется страница **Добавление учетной записи**.
  3. Введите название учетной записи.
  4. В раскрывающемся списке **Метки** установите флажок **SMB**.
  5. 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.

9.4.2. Создание и запуск задачи на импорт отчета

- Чтобы создать и запустить задачу на импорт отчета:

  1. В главном меню выберите **Сбор данных** → **Задачи**.

     Откроется страница **Задачи по сбору данных**.
  2. Нажмите **Создать задачу** → **Сбор данных**.

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

3. В поле **Название** введите название задачи.
4. В раскрывающемся списке **Профиль** выберите **MP8ScanImporter**.
5. В раскрывающемся списке **Учетная запись** выберите учетную запись пользователя ОС.
6. В поле **Путь к общей папке** введите путь к папке с отчетами.
7. Если требуется, выберите MP 10 Collector для сбора событий.
8. 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.
9. Нажмите кнопку **Сохранить и запустить**.

Задача на импорт отчета создана и запущена.

10. Системы мониторинга сети

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

В этом разделе

10.1. 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 17.1.2) или доменную (см. раздел 17.6.3) учетную запись пользователя Windows.

   Примечание. Данные этой учетной записи нужно указать при добавлении учетной записи в MaxPatrol VM. Для коллекторов, установленных на Linux, необходимо использовать только доменную учетную запись с аутентификацией по протоколу Kerberos.

   Примечание. Вместо учетной записи пользователя Windows вы можете использовать учетную запись SQL Server Authentication.

2. Настроить локальную (см. раздел 17.6.2) или групповую (см. раздел 17.6.4) политику безопасности для удаленного доступа учетной записи.

3. Настроить локальную или групповую (см. раздел 17.3.6) 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 17.6.6).
6. Настроить автоматический запуск SQL Server Browser (см. раздел 17.6.7).

   Примечание. Если используется дополнительная аутентификация через Kerberos, необходимо зарегистрировать в службе каталогов Active Directory имя участника-службы (SPN) узла с установленным Microsoft SQL Server. Для корректной аутентификации имя SPN должно содержать полное доменное имя сервера (FQDN). Подробную инструкцию см. на сайте learn.microsoft.com в разделе «Регистрация имени субъекта-службы для подключений Kerberos» для соответствующей версии Microsoft SQL Server.

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 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 **Grant** 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 **Grant** 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;
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.

10.2. Microsoft System Center Configuration Manager (SCCM) 2012—2019: настройка MaxPatrol VM

Примечание. Для доступа в СУБД Microsoft SQL Server на узле MP 10 Collector необходимо установить Microsoft ODBC Driver for SQL Server. Вы можете скачать его с сайта microsoft.com. Для Windows нужно установить 32-разрядную версию, для ОС семейства Linux — 64-разрядную (см. раздел 17.2.4).

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

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 выберите **Сбор данных** → **Учетные записи**.

Откроется страница **Учетные записи**.

2. Нажмите **Добавить учетную запись** → **Логин — пароль**.

   Откроется страница **Добавление учетной записи**.

3. Введите название учетной записи.
4. В раскрывающемся списке **Метки** установите флажки **DB_MSSQL** и **WindowsAudit**.
5. 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, 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 аудит актива:

1. В главном меню выберите **Сбор данных** → **Задачи**.

   Откроется страница **Задачи по сбору данных**.

2. Нажмите **Создать задачу** → **Сбор данных**.

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

3. В поле **Название** введите название задачи.
4. В раскрывающемся списке **Профиль** выберите **MSSQL Audit**.
5. В иерархическом списке выберите пункт **Сканирование систем** → **Windows**.
6. Выберите учетную запись пользователя ОС.
7. В иерархическом списке выберите пункт **Сканирование систем** → **Microsoft SQL Server**.
8. Выберите учетную запись пользователя ОС.
9. В поле **Имя экземпляра СУБД** введите имя экземпляра.
10. Если требуется, в раскрывающемся списке **Коллекторы** выберите коллекторы для сбора данных.
11. 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.

12. Нажмите кнопку **Сохранить и запустить**.

Задача на проведение аудита актива создана и запущена.

10.3. Microsoft Endpoint Configuration Manager (MECM) 2303: 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 Endpoint Configuration Manager, сохраняются в БД 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 17.6.1) или доменную (см. раздел 17.6.3) учетную запись пользователя Windows.

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

2. Настроить локальную (см. раздел 17.6.2) или групповую (см. раздел 17.6.4) политику безопасности для удаленного доступа учетной записи.
3. Настроить локальную или групповую (см. раздел 17.3.6) политику безопасности для доступа учетной записи к разделам реестра.
4. Предоставить учетной записи полномочия роли db_datareader.
5. Настроить порты TCP/IP для подключения к СУБД (см. раздел 17.6.6).
6. Включить правило межсетевого экрана Windows (см. раздел 17.1.1), разрешающее подключение к порту базы данных.

См. также

Создание учетной записи Microsoft SQL Server (см. раздел 10.1.1)

Создание учетной записи Microsoft SQL Server с помощью запроса (см. раздел 10.1.2)

10.4. Microsoft Endpoint Configuration Manager (MECM) 2303: настройка MaxPatrol VM

Примечание. Для доступа в СУБД Microsoft SQL Server на узле MP 10 Collector необходимо установить Microsoft ODBC Driver for SQL Server. Вы можете скачать его с сайта microsoft.com. Для Windows нужно установить 32-разрядную версию, для ОС семейства Linux — 64-разрядную (см. раздел 17.2.4).

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

10.4.1. Добавление учетной записи для СУБД Microsoft SQL Server

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

  1. В главном меню выберите **Сбор данных** → **Учетные записи**.

     Откроется страница **Учетные записи**.
  2. Нажмите **Добавить учетную запись** → **Логин — пароль**.

     Откроется страница **Добавление учетной записи**.
  3. Введите название учетной записи.
  4. В раскрывающемся списке **Метки** установите флажки **DB_MSSQL** и **WindowsAudit**.
  5. 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, введите имя домена.
  8. Нажмите кнопку **Сохранить**.

  Учетная запись добавлена.

10.4.2. Создание и запуск задачи на аудит актива

► Чтобы создать и запустить задачу на аудит актива:

1. В главном меню выберите **Сбор данных** → **Задачи**.

   Откроется страница **Задачи по сбору данных**.

2. Нажмите **Создать задачу** → **Сбор данных**.

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

3. В поле **Название** введите название задачи.
4. В раскрывающемся списке **Профиль** выберите **MSSQL Audit**.
5. В иерархическом списке выберите пункт **Сканирование систем** → **Windows**.
6. Выберите учетную запись пользователя ОС.
7. В иерархическом списке выберите пункт **Сканирование систем** → **Microsoft SQL Server**.
8. Выберите учетную запись пользователя ОС.
9. В поле **Имя экземпляра СУБД** введите имя экземпляра.
10. Если требуется, в раскрывающемся списке **Коллекторы** выберите коллекторы для сбора данных.
11. 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.

12. Нажмите кнопку **Сохранить и запустить**.

Задача на проведение аудита актива создана и запущена.

11. Системы управления базами данных

Раздел содержит инструкции для настройки аудита поддерживаемых в MaxPatrol VM систем управления базами данных.

В этом разделе

11.1. MariaDB 10.0 и выше: настройка актива

Для проведения аудита на активе нужно создать учетную запись ОС, настроить удаленный доступ к БД, создать учетную запись MariaDB и выдать ей права на просмотр таблиц БД.

Настройка в Windows

Настройку источника нужно выполнять от имени учетной записи, имеющей права локального администратора Windows.

Для проведения аудита на активе нужно:

1. Средствами ОС создать учетную запись локального пользователя ОС (см. раздел 17.1.2) для доступа MP 10 Collector.

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

2. Настроить локальную (см. раздел 17.6.2) или групповую (см. раздел 17.6.4) политику безопасности для удаленного доступа учетной записи.
3. Настроить удаленный доступ к СУБД (см. раздел 11.1.1).
4. Создать учетную запись СУБД (см. раздел 11.1.2) и выдать ей права на просмотр таблиц БД с данными для аудита.

Настройка в ОС семейства Unix

Настройку источника нужно выполнять от имени суперпользователя (root).

Для проведения аудита на активе нужно:

1. Создать учетную запись пользователя ОС семейства Unix (см. раздел 17.2.1) для доступа MP 10 Collector.

   Примечание. Данные этой учетной записи нужно указать при добавлении учетной записи в MaxPatrol VM.
2. Создать учетную запись СУБД (см. раздел 11.1.2) и выдать ей права на просмотр таблиц БД с данными для аудита.
3. Создать учетную запись СУБД (см. раздел 11.1.2) и выдать ей права на просмотр таблиц БД с данными для аудита.

В этом разделе

11.1.1. Настройка удаленного доступа в MariaDB

- Чтобы настроить удаленный доступ в СУБД:

  1. Откройте конфигурационный файл `my.cnf`.

     Примечание. Вы можете узнать расположение файла, выполнив команду `mysqld --help --verbose | grep my.cnf`.
  2. В секцию `[mysqld]` добавьте строки:

     ```
     port = 3306
     bind_address = <IP-адрес СУБД источника>
     ```

3. Сохраните конфигурационный файл.
4. Перезапустите СУБД:
   ```
   systemctl restart mysqld
   ```

Удаленный доступ в СУБД настроен.

11.1.2. Создание учетной записи MariaDB

- Чтобы создать учетную запись пользователя СУБД:

1. Откройте интерфейс командной строки актива.
2. Создайте учетную запись для доступа к активу:
   ```
   CREATE USER '<Логин>'@'<Имя актива>' IDENTIFIED BY '<Пароль>';
   ```
3. Предоставьте учетной записи права на чтение БД:
   ```
   GRANT SELECT ON mysql.* TO '<Логин>'@'<Имя актива>';
   GRANT SHOW DATABASES ON *.* TO '<Логин>'@'<Имя актива>';
   GRANT SHOW VIEW ON *.* TO '<Логин>'@'<Имя актива>';
   FLUSH PRIVIlEGES;
   ```

Учетная запись СУБД создана.

11.2. MariaDB 10.0 и выше: настройка MaxPatrol VM

Примечание. Для доступа в СУБД MariaDB на узле MP 10 Collector требуется установить драйвер ODBC, версию для 32-разрядной архитектуры. Драйвер вы можете скачать с сайта mariadb.com.

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

В этом разделе

Добавление учетной записи для СУБД MariaDB (см. раздел 11.2.1)

Создание и запуск задачи на аудит актива (см. раздел 11.2.2)

11.2.1. Добавление учетной записи для СУБД MariaDB

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

1. В главном меню выберите **Сбор данных** → **Учетные записи**.

   Откроется страница **Учетные записи**.
2. Нажмите **Добавить учетную запись** → **Логин — пароль**.

   Откроется страница **Добавление учетной записи**.

3. Введите название учетной записи.
4. В раскрывающемся списке **Метки** установите флажок **DB_MySQL**.
5. 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, введите имя домена.
8. Нажмите кнопку **Сохранить**.

Учетная запись добавлена.

11.2.2. Создание и запуск задачи на аудит актива

► Чтобы создать и запустить задачу на аудит актива:

1. В главном меню выберите **Сбор данных** → **Задачи**.

   Откроется страница **Задачи по сбору данных**.
2. Нажмите **Создать задачу** → **Сбор данных**.

   Откроется страница **Создание задачи на сбор данных**.
3. В поле **Название** введите название задачи.
4. В раскрывающемся списке **Профиль** выберите **MySQL Audit**.
5. Если на активе используется Windows, в иерархическом списке выберите пункт **Сканирование систем** → **Windows**.
6. Если на активе используется ОС семейства Unix, в иерархическом списке выберите **Сканирование систем** → **Через терминал**.
7. Выберите учетную запись пользователя ОС.
8. В иерархическом списке выберите пункт **Сканирование систем** → **Oracle MySQL**.
9. В раскрывающемся списке **Учетная запись** выберите добавленную ранее учетную запись пользователя СУБД MariaDB.
10. 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.
11. Нажмите кнопку **Сохранить и запустить**.

Задача на проведение аудита актива создана и запущена.

11.3. 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 17.1.2) или доменную (см. раздел 17.6.3) учетную запись пользователя Windows.

   Примечание. Данные этой учетной записи нужно указать при добавлении учетной записи в MaxPatrol VM. Для коллекторов, установленных на Linux, необходимо использовать только доменную учетную запись с аутентификацией по протоколу Kerberos.

   Примечание. Вместо учетной записи пользователя Windows вы можете использовать учетную запись SQL Server Authentication.

2. Настроить локальную (см. раздел 17.6.2) или групповую (см. раздел 17.6.4) политику безопасности для удаленного доступа учетной записи.
3. Настроить локальную или групповую (см. раздел 17.3.6) 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 11.3.1) или с помощью запроса (см. раздел 11.3.2).
5. Настроить порты TCP/IP для подключения к СУБД (см. раздел 17.6.6).
6. Настроить автоматический запуск SQL Server Browser (см. раздел 17.6.7).

   Примечание. Если используется дополнительная аутентификация через Kerberos, необходимо зарегистрировать в службе каталогов Active Directory имя участника-службы (SPN) узла с установленным Microsoft SQL Server. Для корректной аутентификации имя SPN должно содержать полное доменное имя сервера (FQDN). Подробную инструкцию см. на сайте learn.microsoft.com в разделе «Регистрация имени субъекта-службы для подключений Kerberos» для соответствующей версии Microsoft SQL Server.

В этом разделе

11.3.1. 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 **Grant** 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 **Grant** установите флажок в строке **View definition**.
9. Нажмите кнопку **OK**.

Право на просмотр определений объектов БД выдано учетной записи.

11.3.2. 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.

11.4. Microsoft SQL Server 2008—2019: настройка MaxPatrol VM

Примечание. Для доступа в СУБД Microsoft SQL Server на узле MP 10 Collector необходимо установить Microsoft ODBC Driver for SQL Server. Вы можете скачать его с сайта microsoft.com. Для Windows нужно установить 32-разрядную версию, для ОС семейства Linux — 64-разрядную (см. раздел 17.2.4).

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

11.4.1. Добавление учетной записи для СУБД Microsoft SQL Server

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

1. В главном меню выберите **Сбор данных** → **Учетные записи**.

   Откроется страница **Учетные записи**.

2. Нажмите **Добавить учетную запись** → **Логин — пароль**.

   Откроется страница **Добавление учетной записи**.

3. Введите название учетной записи.
4. В раскрывающемся списке **Метки** установите флажки **DB_MSSQL** и **WindowsAudit**.
5. 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, введите имя домена.
8. Нажмите кнопку **Сохранить**.

Учетная запись добавлена.

11.4.2. Создание и запуск задачи на аудит актива

- Чтобы создать и запустить задачу на аудит актива:

1. В главном меню выберите **Сбор данных** → **Задачи**.

   Откроется страница **Задачи по сбору данных**.
2. Нажмите **Создать задачу** → **Сбор данных**.

   Откроется страница **Создание задачи на сбор данных**.
3. В поле **Название** введите название задачи.
4. В раскрывающемся списке **Профиль** выберите **MSSQL Audit**.
5. В иерархическом списке выберите пункт **Сканирование систем** → **Windows**.
6. Выберите учетную запись пользователя ОС.
7. В иерархическом списке выберите пункт **Сканирование систем** → **Microsoft SQL Server**.
8. Выберите учетную запись пользователя ОС.
9. В поле **Имя экземпляра СУБД** введите имя экземпляра.
10. Если требуется, в раскрывающемся списке **Коллекторы** выберите коллекторы для сбора данных.
11. 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.
12. Нажмите кнопку **Сохранить и запустить**.

Задача на проведение аудита актива создана и запущена.

11.5. MongoDB 3.6 и выше: настройка актива

При сканировании СУБД MongoDB используется протокол подключения MongoDB Wire Protocol и TCP-порт. Номер порта вы можете узнать в строке с параметром `port` в конфигурационном файле (значение порта по умолчанию — 27017).

В этом разделе

11.5.1. Создание ограниченной учетной записи

- Чтобы создать учетную запись СУБД MongoDB с набором привилегий auditor с помощью роли auditrole:

  1. Откройте конфигурационный файл СУБД MongoDB.

     Примечание. По умолчанию путь к конфигурационному файлу MongoDB — `/etc/mongod.conf`.

  2. Добавьте в файл строки:

     ```
     use admin


     db.createRole({
     role: "auditrole",
     privileges: [{
     resource: { anyResource: true },
     actions: [ "viewUser", "viewRole" ]
     }],
     roles: [ { role: "clusterMonitor", db: "admin" } ]
     })


     db.createUser({
     user: "<Логин>",
     pwd: "<Пароль>",
     roles: [ { role: "auditrole", db: "admin" } ]
     })
     ```

  3. Сохраните изменения и закройте файл.

  Учетная запись создана.

11.5.2. Операции MongoDB

Для успешного сканирования необходимо предоставить учетной записи привилегии на выполнение операций, указанных в таблице ниже.

Таблица 4. Операции MongoDB

Операция	Необходимые привилегии	Описание
buildInfo	—	Получение информации о версии MongoDB

Операция	Необходимые привилегии	Описание
getCmdLineOpts	clusterMonitor	Получение информации о пути установки MongoDB, файле конфигурации `mongod.cfg`, журнале аудита и событиях входа пользователей в систему
getParameter	clusterMonitor	Получение информации о параметрах enableLocalhostAuthBypass и tlsMode
getDBNames	clusterMonitor	Получение информации о базах MongoDB
getUsers	viewUser	Получение информации о пользователях MongoDB
getRoles	viewRole	Получение информации о ролях MongoDB

11.6. MongoDB 3.6 и выше: настройка MaxPatrol VM

Для проведения аудита актива по протоколу MongoDB Wire Protocol необходимо добавить учетную запись для доступа к активу и создать задачу на проведение аудита.

В этом разделе

Добавление учетной записи (см. раздел 11.6.1)

Создание задачи на аудит актива (см. раздел 11.6.2)

11.6.1. Добавление учетной записи

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

  1. В главном меню выберите **Сбор данных** → **Учетные записи**.

     Откроется страница **Учетные записи**.
  2. Нажмите **Добавить учетную запись** → **Логин — пароль**.

     Откроется страница **Добавление учетной записи**.
  3. Введите название учетной записи.
  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 изменения**.

Учетная запись добавлена.

11.6.2. Создание задачи на аудит актива

► Чтобы создать задачу на проведение аудита актива:

1. В главном меню выберите **Сбор данных** → **Задачи**.

   Откроется страница **Задачи по сбору данных**.
2. Нажмите **Создать задачу** → **Сбор данных**.

   Откроется страница **Создание задачи на сбор данных**.
3. В поле **Название** введите название задачи.
4. В раскрывающемся списке **Профиль** выберите **MongoDB Audit**.
5. В раскрывающемся списке **Учетная запись** выберите сертификат для доступа к активу.
6. В панели **Цели сбора данных** на вкладке **Включить** в поле **Активы** введите IP-адрес или FQDN сервера управления.

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

Задача на проведение аудита актива создана.

11.7. Oracle Database 11, 12, 18, 19, 21, 23: настройка актива

Для проведения аудита на активе нужно создать учетную запись ОС, настроить удаленный доступ к БД, создать учетную запись Oracle Database и выдать ей права на просмотр представлений БД и следующих системных таблиц:

- SYS.AUD$;
- SYS.DEFROLE$;
- SYS.FGA_LOG$;
- SYS.JOB$;
- SYS.LIBRARY$;
- SYS.LINK$;
- SYS.OBJ$;
- SYS.OBJAUTH$;

- SYS.SCHEDULER$_JOB;
- SYS.SOURCE$;
- SYS.SYSAUTH$;
- SYS.USER$;
- SYS.AUDIT_UNIFIED_POLICIES (только для версии 12);
- SYS.AUDIT_UNIFIED_ENABLED_POLICIES (только для версии 12).

Настройка в Windows

Настройку источника нужно выполнять от имени учетной записи, имеющей права локального администратора Windows.

Для проведения аудита на активе нужно:

1. Средствами ОС создать учетную запись локального пользователя ОС (см. раздел 17.1.2) для доступа MP 10 Collector.

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

2. Настроить локальную (см. раздел 17.6.2) или групповую (см. раздел 17.6.4) политику безопасности для удаленного доступа учетной записи.
3. Настроить удаленный доступ к СУБД.
4. Создать учетную запись СУБД и выдать ей права на просмотр таблиц БД с данными для аудита.

Настройка в ОС семейства Unix

Настройку источника нужно выполнять от имени суперпользователя (root).

Для проведения аудита на активе нужно:

1. Создать учетную запись пользователя ОС семейства Unix (см. раздел 17.2.1) для доступа MP 10 Collector.

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

2. Настроить удаленный доступ к СУБД.
3. Создать учетную запись СУБД и выдать ей права на просмотр таблиц БД с данными для аудита.

В этом разделе

Настройка удаленного доступа в Oracle Database Express Edition (см. раздел 11.7.1)

Создание учетной записи Oracle Database (см. раздел 11.7.2)

11.7.1. Настройка удаленного доступа в Oracle Database Express Edition

- Чтобы настроить удаленный доступ в СУБД:

  1. Остановите службу `Oracle<Имя сервера СУБД>TNSListener`.
  2. В файле `sqlnet.ora` укажите для параметра `SQLNET.AUTHENTICATION_SERVICES` значение `(NONE)`.

     Примечание. Параметр `SQLNET.AUTHENTICATION_SERVICES=(NONE)` отключает аутентификацию на основе операционной системы.
  3. В файле `listener.ora` укажите для параметра `HOST` значение `$GLOBAL_HOST_NAME`:
     ```
     (ADDRESS = (PROTOCOL = TCP)(HOST = $GLOBAL_HOST_NAME)(PORT = 1521))
     ```
  4. Запустите службу СУБД.

  Удаленный доступ в СУБД настроен.

11.7.2. Создание учетной записи Oracle Database

- Чтобы создать учетную запись пользователя СУБД:

  1. Откройте интерфейс командной строки актива.
  2. Создайте учетную запись для доступа к активу:
     ```
     create user auditor identified by "<Пароль>" default tablespace system quota 0 on system;
     create role auditrole;
     grant connect, auditrole to auditor;
     ```
  3. Предоставьте учетной записи права на просмотр таблиц, в которых хранятся данные об активе:
     ```
     grant select on SYS.AUD$ to auditrole;
     grant select on SYS.DEFROLE$ to auditrole;
     grant select on SYS.FGA_LOG$ to auditrole;
     grant select on SYS.JOB$ to auditrole;
     grant select on SYS.LIBRARY$ to auditrole;
     grant select on SYS.LINK$ to auditrole;
     grant select on SYS.OBJ$ to auditrole;
     grant select on SYS.OBJAUTH$ to auditrole;
     grant select on SYS.SCHEDULER$_JOB to auditrole;
     grant select on SYS.SOURCE$ to auditrole;
     grant select on SYS.SYSAUTH$ to auditrole;
     grant select on SYS.USER$ to auditrole;
     ```
  4. Если используется Oracle Database версии 12, предоставьте учетной записи права на чтение таблиц AUDIT_UNIFIED_POLICIES и AUDIT_UNIFIED_ENABLED_POLICIES:
     ```
     grant select on SYS.AUDIT_UNIFIED_POLICIES to auditrole;
     grant select on SYS.AUDIT_UNIFIED_ENABLED_POLICIES to auditrole;
     ```

5. Предоставьте учетной записи права на просмотр представлений БД:

```
grant select on sys.all_def_audit_opts to auditrole;
grant select on sys.all_objects to auditrole;
grant select on sys.all_source to auditrole;
grant select on sys.all_tab_privs to auditrole;
grant select on sys.all_tab_privs_made to auditrole;
grant select on sys.all_tables to auditrole;
grant select on sys.audit_actions to auditrole;
grant select on sys.database_properties to auditrole;
grant select on sys.dba_audit_policies to auditrole;
grant select on sys.dba_audit_trail to auditrole;
grant select on sys.dba_data_files to auditrole;
grant select on sys.dba_db_links to auditrole;
grant select on sys.dba_feature_usage_statistics to auditrole;
grant select on sys.dba_fga_audit_trail to auditrole;
grant select on sys.dba_free_space to auditrole;
grant select on sys.dba_jobs to auditrole;
grant select on sys.dba_hist_active_sess_history to auditrole;
grant select on sys.dba_libraries to auditrole;
grant select on sys.dba_obj_audit_opts to auditrole;
grant select on sys.dba_objects to auditrole;
grant select on sys.dba_priv_audit_opts to auditrole;
grant select on sys.dba_profiles to auditrole;
grant select on sys.dba_proxies to auditrole;
grant select on sys.dba_registry to auditrole;
grant select on sys.dba_role_privs to auditrole;
grant select on sys.dba_roles to auditrole;
grant select on sys.dba_scheduler_jobs to auditrole;
grant select on sys.dba_segments to auditrole;
grant select on sys.dba_source to auditrole;
grant select on sys.dba_stmt_audit_opts to auditrole;
grant select on sys.dba_sys_privs to auditrole;
grant select on sys.dba_tab_privs to auditrole;
grant select on sys.dba_tablespaces to auditrole;
grant select on sys.dba_temp_files to auditrole;
grant select on sys.dba_ts_quotas to auditrole;
grant select on sys.dba_users to auditrole;
grant select on sys.dba_users_with_defpwd to auditrole;
grant select on sys.dba_views to auditrole;
grant select on sys.product_component_version to auditrole;
grant select on sys.system_privilege_map to auditrole;
grant select on sys.user_astatus_map to auditrole;
grant select on sys.v_$database to auditrole;
grant select on sys.v_$datafile to auditrole;
grant select on sys.v_$datafile_header to auditrole;
grant select on sys.v_$instance to auditrole;
grant select on sys.v_$license to auditrole;
grant select on sys.v_$logfile to auditrole;
grant select on sys.v_$option to auditrole;
```

```
grant select on sys.v_$parameter to auditrole;
grant select on sys.v_$pwfile_users to auditrole;
grant select on sys.v_$session to auditrole;
grant select on sys.v_$sesstat to auditrole;
grant select on sys.v_$spparameter to auditrole;
grant select on sys.v_$statname to auditrole;
grant select on sys.v_$tablespace to auditrole;
grant select on sys.v_$temp_space_header to auditrole;
grant select on sys.v_$tempfile to auditrole;
grant select on sys.v_$version to auditrole;
grant select on sys.wrh$_active_session_history to auditrole;
```

6. Предоставьте учетной записи право на подсчет хеш-сумм:
   ```
   grant execute on sys.dbms_utility to auditrole;
   ```
7. Предоставьте учетной записи право на определение пути к домашнему каталогу Oracle:
   ```
   grant execute on sys.dbms_system to auditrole;
   ```
8. Предоставьте учетной записи право на создание таблиц в БД:
   ```
   grant create table to auditrole;
   ```

Учетная запись СУБД создана.

11.8. Oracle Database 11, 12, 18, 19, 21, 23: настройка MaxPatrol VM

Примечание. Для доступа в СУБД Oracle Database на узле MP 10 Collector необходимо установить ODBC-драйвер. Вы можете скачать его с сайта oracle.com. Для Windows нужно установить 32-разрядную версию, для ОС семейства Linux — 64-разрядную (см. раздел 17.2.4).

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

В этом разделе

11.8.1. Добавление учетной записи для СУБД Oracle Database

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

  1. В главном меню выберите **Сбор данных** → **Учетные записи**.

     Откроется страница **Учетные записи**.
  2. Нажмите **Добавить учетную запись** → **Логин — пароль**.

Откроется страница **Добавление учетной записи**.

3. Введите название учетной записи.
4. В раскрывающемся списке **Метки** установите флажок **DB_Oracle**.
5. 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, введите имя домена.
8. Нажмите кнопку **Сохранить**.

Учетная запись добавлена.

11.8.2. Создание и запуск задачи на аудит актива

► Чтобы создать и запустить задачу на аудит актива:

1. В главном меню выберите **Сбор данных** → **Задачи**.

   Откроется страница **Задачи по сбору данных**.
2. Нажмите **Создать задачу** → **Сбор данных**.

   Откроется страница **Создание задачи на сбор данных**.
3. В поле **Название** введите название задачи.
4. В раскрывающемся списке **Профиль** выберите **Oracle Audit**.
5. Если на активе используется Windows, в иерархическом списке выберите пункт **Сканирование систем** → **Windows**.
6. Если на активе используется ОС семейства Unix, в иерархическом списке выберите **Сканирование систем** → **Через терминал**.
7. Выберите учетную запись пользователя ОС.
8. В иерархическом списке выберите пункт **Сканирование систем** → **Oracle Database**.
9. В раскрывающемся списке **Тип имени экземпляра СУБД** выберите тип.
10. В поле **Имя экземпляра СУБД** введите имя экземпляра.
11. В раскрывающемся списке **Учетная запись** выберите добавленную ранее учетную запись пользователя СУБД Oracle Database.
12. 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.

13. Нажмите кнопку **Сохранить и запустить**.

Задача на проведение аудита актива создана и запущена.

11.9. Oracle MySQL 5.7 и выше: настройка актива

Для проведения аудита на активе нужно создать учетную запись ОС, настроить удаленный доступ к БД, создать учетную запись Oracle MySQL и выдать ей права на просмотр таблиц БД.

Настройка в Windows

Настройку источника нужно выполнять от имени учетной записи, имеющей права локального администратора Windows.

Для проведения аудита на активе нужно:

1. Средствами ОС создать учетную запись локального пользователя ОС (см. раздел 17.1.2) для доступа MP 10 Collector.

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

2. Настроить локальную (см. раздел 17.6.2) или групповую (см. раздел 17.6.4) политику безопасности для удаленного доступа учетной записи.
3. Настроить удаленный доступ к СУБД (см. раздел 11.9.1).
4. Создать учетную запись СУБД (см. раздел 11.9.2) и выдать ей права на просмотр таблиц БД с данными для аудита.

Настройка в ОС семейства Unix

Настройку источника нужно выполнять от имени суперпользователя (root).

Для проведения аудита на активе нужно:

1. Создать учетную запись пользователя ОС семейства Unix (см. раздел 17.2.1) для доступа MP 10 Collector.

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

2. Настроить удаленный доступ к СУБД (см. раздел 11.9.1).
3. Создать учетную запись СУБД (см. раздел 11.9.2) и выдать ей права на просмотр таблиц БД с данными для аудита.

В этом разделе

11.9.1. Настройка удаленного доступа в MySQL

- Чтобы настроить удаленный доступ в СУБД:

  1. Откройте конфигурационный файл `my.cnf`.

     Примечание. Вы можете узнать расположение файла, выполнив команду `mysqld --help --verbose | grep my.cnf`.

  2. В секцию `[mysqld]` добавьте строки:

     ```
     port = 3306
     bind_address = <IP-адрес СУБД источника>
     ```

  3. Сохраните конфигурационный файл.

  4. Перезапустите СУБД:

     ```
     systemctl restart mysqld
     ```

11.9.2. Создание учетной записи Oracle MySQL

- Чтобы создать учетную запись пользователя СУБД:

  1. Откройте интерфейс командной строки актива.

  2. Создайте учетную запись для доступа к активу:

     ```
     CREATE USER '<Логин>'@'<Имя актива>' IDENTIFIED BY '<Пароль>';
     ```

  3. Предоставьте учетной записи права на чтение БД:

     ```
     GRANT SELECT ON performance_schema.global_variables TO '<Логин>'@'<Имя актива>';
     GRANT SELECT ON mysql.* TO '<Логин>'@'<Имя актива>';
     GRANT SHOW DATABASES ON *.* TO '<Логин>'@'<Имя актива>';
     GRANT SHOW VIEW ON *.* TO '<Логин>'@'<Имя актива>';
     FLUSH PRIVIlEGES;
     ```

  4. Если используется Oracle MySQL версии 8.0.21 и выше, предоставьте учетной записи права на чтение таблицы tls_channel_status:

     ```
     GRANT SELECT ON performance_schema.tls_channel_status TO '<Логин>'@'<Имя актива>';
     ```

  Учетная запись СУБД создана.

11.10. Oracle MySQL 5.7 и выше: настройка MaxPatrol VM

Примечание. Для доступа в СУБД Oracle MySQL на узле MP 10 Collector требуется установить драйвер ODBC, версию для 32-разрядной архитектуры. Драйвер вы можете скачать с сайта mysql.com.

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

В этом разделе

11.10.1. Добавление учетной записи для СУБД Oracle MySQL

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

  1. В главном меню выберите **Сбор данных** → **Учетные записи**.

     Откроется страница **Учетные записи**.
  2. Нажмите **Добавить учетную запись** → **Логин — пароль**.

     Откроется страница **Добавление учетной записи**.
  3. Введите название учетной записи.
  4. В раскрывающемся списке **Метки** установите флажок **DB_MySQL**.
  5. 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, введите имя домена.
  8. Нажмите кнопку **Сохранить**.

  Учетная запись добавлена.

11.10.2. Создание и запуск задачи на аудит актива

- Чтобы создать и запустить задачу на аудит актива:

  1. В главном меню выберите **Сбор данных** → **Задачи**.

Откроется страница **Задачи по сбору данных**.

2. Нажмите **Создать задачу** → **Сбор данных**.

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

3. В поле **Название** введите название задачи.
4. В раскрывающемся списке **Профиль** выберите **MySQL Audit**.
5. Если на активе используется Windows, в иерархическом списке выберите пункт **Сканирование систем** → **Windows**.
6. Если на активе используется ОС семейства Unix, в иерархическом списке выберите **Сканирование систем** → **Через терминал**.
7. Выберите учетную запись пользователя ОС.
8. В иерархическом списке выберите пункт **Сканирование систем** → **Oracle MySQL**.
9. В раскрывающемся списке **Учетная запись** выберите добавленную ранее учетную запись пользователя СУБД Oracle MySQL.
10. 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.

11. Нажмите кнопку **Сохранить и запустить**.

Задача на проведение аудита актива создана и запущена.

11.11. PostgreSQL 9—15: настройка актива

Для проведения аудита на активе нужно создать учетную запись ОС, настроить удаленный доступ к БД, создать учетную запись PostgreSQL и выдать ей права на просмотр следующих таблиц БД:

- information_schema.table_privileges;
- pg_catalog.pg_database;
- pg_catalog.pg_authid;
- pg_catalog.pg_tablespace;
- pg_catalog.pg_namespace;
- pg_catalog.pg_roles;
- pg_catalog.pg_auth_members;
- pg_catalog.pg_settings;
- pg_catalog.pg_ident_file_mappings;
- pg_catalog.pg_hba_file_rules;

— pg_catalog.pg_extension;

— pg_catalog.pg_policies.

Настройка в Windows

Настройку источника нужно выполнять от имени учетной записи, имеющей права локального администратора Windows.

Для проведения аудита на активе нужно:

1. Средствами ОС создать учетную запись локального пользователя ОС (см. раздел 17.1.2) для доступа MP 10 Collector.

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

2. Настроить локальную (см. раздел 17.6.2) или групповую (см. раздел 17.6.4) политику безопасности для удаленного доступа учетной записи.

3. Настроить удаленный доступ к СУБД (см. раздел 11.11.1).

4. Создать учетную запись СУБД (см. раздел 11.11.2) и выдать ей права на просмотр таблиц БД с данными для аудита.

Настройка в ОС семейства Unix

Настройку источника нужно выполнять от имени суперпользователя (root).

Для проведения аудита на активе нужно:

1. Создать учетную запись пользователя ОС семейства Unix (см. раздел 17.2.1) для доступа MP 10 Collector.

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

2. Настроить удаленный доступ к СУБД (см. раздел 11.11.1).

3. Создать учетную запись СУБД (см. раздел 11.11.2) и выдать ей права на просмотр таблиц БД с данными для аудита.

В этом разделе

11.11.1. Настройка удаленного доступа

Вы можете настроить удаленный доступ изменив файл `pg_hba.conf` вручную или с помощью утилиты pgAdmin III.

Настройка вручную

- Чтобы настроить удаленный доступ к БД источника для учетной записи MP 10 Collector:

  1. Откройте файл `pg_hba.conf`.

     Файл расположен в папке установки СУБД, например: `C:\Program Files\PostgreSQL\<Версия СУБД>\data\`.

  2. Добавьте в конец файла строку:

     - если используется PostgreSQL версии 10 и выше:
       `host all auditor <IP-адрес MP 10 Collector>/32 scram-sha-256`
     - если недоступно использование метода аутентификации scram-sha-256 или используется PostgreSQL версии 9:
       `host all auditor <IP-адрес MP 10 Collector>/32 md5`

  3. Сохраните изменения и закройте файл.

  4. Перезапустите службу `postgresql`.

  Удаленный доступ в СУБД настроен.

Настройка с помощью утилиты pgAdmin III

- Чтобы настроить удаленный доступ к БД источника для учетной записи MP 10 Collector:

  1. Запустите pgAdmin III от имени учетной записи локального администратора ОС.

  2. В открывшемся окне в главном меню выберите **Файл** → **Открыть pg_hba.conf**.

  3. В открывшемся окне укажите расположение файла `pg_hba.conf` и нажмите кнопку **Открыть**.

     Файл расположен в папке установки СУБД, например: `C:\Program Files\PostgreSQL\<Версия СУБД>\data\`.

  4. В окне **Редактор конфигурации доступа к серверу** двойным щелчком в пустой строке откройте окно **Настройка доступа клиента**.

  5. Установите флажок **Включен**.

  6. В раскрывающемся списке **Тип** выберите **host**.

  7. В раскрывающемся списке **База данных** выберите имя БД источника.

  8. В раскрывающемся списке **Пользователь** выберите логин учетной записи MP 10 Collector.

  9. В поле **IP Адреса** введите IP-адрес и маску подсети узла MP 10 Collector.

  10. В раскрывающемся списке **Метод** выберите **md5**:

      - если используется PostgreSQL версии 10 и выше — **scram-sha-256**;

- если недоступно использование метода аутентификации scram-sha-256 или используется PostgreSQL версии 9 — **md5**.

11. Нажмите кнопку **OK**.
12. Закройте окно **Редактор конфигурации доступа к серверу**.
13. В панели **Браузер объектов** в контекстном меню узла **Группы серверов** → **Серверы** → **<Имя экземпляра СУБД>** выберите пункт **Перечитать конфигурацию**.

Удаленный доступ в СУБД настроен.

11.11.2. Создание учетной записи PostgreSQL

► Чтобы создать учетную запись пользователя СУБД:

1. Откройте интерфейс командной строки актива.
2. Создайте учетную запись для доступа к активу:
   ```
   CREATE USER auditor WITH LOGIN PASSWORD '<Пароль>';
   ```
3. Предоставьте учетной записи права на просмотр таблиц, в которых хранятся данные об активе:
   ```
   GRANT SELECT ON information_schema.table_privileges TO auditor;
   GRANT SELECT ON pg_catalog.pg_authid TO auditor;
   GRANT SELECT ON pg_catalog.pg_tablespace TO auditor;
   GRANT SELECT ON pg_catalog.pg_namespace TO auditor;
   GRANT SELECT ON pg_catalog.pg_roles TO auditor;
   GRANT SELECT ON pg_catalog.pg_auth_members TO auditor;
   GRANT SELECT ON pg_catalog.pg_settings TO auditor;
   GRANT SELECT ON pg_catalog.pg_ident_file_mappings TO auditor;
   GRANT SELECT ON pg_catalog.pg_hba_file_rules TO auditor;
   GRANT SELECT ON pg_catalog.pg_extension TO auditor;
   GRANT SELECT ON pg_catalog.pg_policies TO auditor;
   GRANT pg_read_all_settings TO auditor;
   ```

11.12. PostgreSQL 9—15: настройка MaxPatrol VM

Примечание. Для доступа в СУБД PostgreSQL на узле MP 10 Collector требуется установить ODBC-драйвер, версию для 32-разрядной архитектуры. Драйвер вы можете скачать с сайта postgresql.org.

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

В этом разделе

11.12.1. Добавление учетной записи для СУБД PostgreSQL

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

  1. В главном меню выберите **Сбор данных** → **Учетные записи**.

     Откроется страница **Учетные записи**.

  2. Нажмите **Добавить учетную запись** → **Логин — пароль**.

     Откроется страница **Добавление учетной записи**.

  3. Введите название учетной записи.
  4. В раскрывающемся списке **Метки** установите флажок **DB_PostgreSQL**.
  5. 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, введите имя домена.
  8. Нажмите кнопку **Сохранить**.

  Учетная запись добавлена.

11.12.2. Создание и запуск задачи на аудит актива

- Чтобы создать и запустить задачу на аудит актива:

  1. В главном меню выберите **Сбор данных** → **Задачи**.

     Откроется страница **Задачи по сбору данных**.

  2. Нажмите **Создать задачу** → **Сбор данных**.

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

  3. В поле **Название** введите название задачи.
  4. В раскрывающемся списке **Профиль** выберите **PostgreSQL Audit**.
  5. Если на активе используется Windows, в иерархическом списке выберите пункт **Сканирование систем** → **Windows**.
  6. Если на активе используется ОС семейства Unix, в иерархическом списке выберите **Сканирование систем** → **Через терминал**.
  7. Выберите учетную запись пользователя ОС.
  8. В иерархическом списке выберите пункт **Сканирование систем** → **PostgreSQL**.
  9. В поле **Имя экземпляра СУБД** введите имя экземпляра.

10. В раскрывающемся списке **Учетная запись** выберите добавленную ранее учетную запись пользователя СУБД PostgreSQL.
11. 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.
12. Нажмите кнопку **Сохранить и запустить**.

Задача на проведение аудита актива создана и запущена.

11.13. Redis 6.2 и выше: настройка актива

Настройку актива нужно выполнять от имени учетной записи администратора устройства.

Для аудита актива нужно:

1. Добавить IP-адрес сервера MP 10 Collector в главный конфигурационный файл `/etc/redis/redis.conf/`.
2. Создать внешний файл для управления доступом.
3. Создать учетную запись для доступа MP 10 Collector к активу по протоколу SSH и предоставить ей разрешение на выполнение следующих команд: `CONFIG`, `GET`, `ACL USERS`, `INFO`, `ACL GETUSER`, `SELECT` и `PING`.
4. Если включен режим защиты protected mode, установить пароль для пользователя default.
5. Если требуется, настроить защищенное соединение по протоколу SSL.

В этом разделе

11.13.1. Добавление IP-адреса MP 10 Collector в главный конфигурационный файл

- Чтобы добавить IP-адрес MP 10 Collector в главный конфигурационный файл:

  1. Откройте главный конфигурационный файл:
     ```
     sudo nano /etc/redis/redis.conf
     ```
  2. В секции `NETWORK` в параметре `bind` укажите IP-адрес MP 10 Collector.

3. Сохраните изменения.
4. Перезапустите актив:
   ```
   sudo systemctl restart redis-server
   ```

11.13.2. Создание внешнего файла для управления доступом

Перед созданием внешнего файла необходимо проверить, содержатся ли в главном конфигурационном файле `/etc/redis/redis.conf/` данные об учетных записях.

> **Примечание.** Строки, содержащие данные об учетных записях, начинаются с параметра `user`. Например, `user example on nopass sanitize-payload ~* &* +@all`.

Создание внешнего файла при отсутствии данных об учетных записях в `redis.conf`

- Чтобы создать внешний файл для управления доступом:

1. Выполните команду:
   ```
   sudo touch /etc/redis/users.acl
   ```
2. Откройте главный конфигурационный файл `/etc/redis/redis.conf`.
3. Раскомментируйте строку:
   ```
   aclfile /etc/redis/users.acl
   ```
4. Сохраните изменения.
5. Перезапустите актив:
   ```
   sudo systemctl restart redis-server
   ```

Создание внешнего файла при наличии данных об учетных записях в `redis.conf`

- Чтобы создать внешний файл для управления доступом:

1. Выполните команду:
   ```
   sudo touch /etc/redis/users.acl
   ```
2. Перенесите данные об учетных записях из главного конфигурационного файла `/etc/redis/redis.conf/` во внешний файл `/etc/redis/users.acl`.

   Внимание! В главном конфигурационном файле `/etc/redis/redis.conf/` не должно остаться данных об учетных записях.
3. В файле `/etc/redis/redis.conf` раскомментируйте строку:
   ```
   aclfile /etc/redis/users.acl
   ```

4. Сохраните изменения.
5. Перезапустите актив:
   ```
   sudo systemctl restart redis-server
   ```

11.13.3. Создание учетной записи для доступа к активу по SSH

- Чтобы создать учетную запись для доступа к активу:

1. Подключитесь к Redis от имени учетной записи с правами администратора.
2. Выполните команду:
   ```
   ACL SETUSER <Логин> on ><Пароль> -@all +config|get +acl|users +info +acl|getuser +select +ping
   ```
3. Сохраните изменения:
   ```
   ACL SAVE
   ```

11.13.4. Установка пароля для пользователя default

- Чтобы установить пароль для пользователя default:

1. Подключитесь к Redis от имени учетной записи с правами администратора.
2. Выполните команду:
   ```
   ACL SETUSER default ><Пароль>
   ```
3. Сохраните изменения:
   ```
   ACL SAVE
   ```

11.13.5. Настройка защищенного соединения по протоколу SSL

Вы можете настроить защищенное соединение по протоколу SSL, чтобы обеспечить безопасность передаваемых данных.

Для настройки вам понадобятся следующие файлы в формате PEM: сертификат, закрытый ключ и пакет сертификатов центра сертификации (CA).

- Чтобы настроить защищенное соединение по протоколу SSL:

1. Откройте главный конфигурационный файл:
   ```
   sudo nano /etc/redis/redis.conf
   ```
2. Раскомментируйте строки:
   ```
   port 0
   tls-port 6379
   ```

3. В строке `tls-cert-file` укажите путь к файлу сертификата.

   Например:
   ```
   tls-cert-file /etc/ssl/certs/redis.crt
   ```

4. В строке `tls-key-file` укажите путь к файлу закрытого ключа.

   Например:
   ```
   tls-key-file /etc/ssl/certs/redis.key
   ```

5. В строке `tls-ca-cert-file` укажите путь к файлу пакета сертификатов центра сертификации (CA).

   Например:
   ```
   tls-ca-cert-file /etc/ssl/certs/ca.crt
   ```

6. Отключите проверку сертификатов по протоколу SSL, указав в строке `tls-auth-clients` значение `no`:
   ```
   tls-auth-clients no
   ```

7. Перезапустите актив:
   ```
   sudo systemctl restart redis-server
   ```

11.14. Redis 6.2 и выше: настройка MaxPatrol VM

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

В этом разделе

11.14.1. Добавление учетной записи для доступа к активу по SSH

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

  1. В главном меню выберите **Сбор данных** → **Учетные записи**.
  2. Нажмите **Добавить учетную запись** → **Логин — пароль**.
  3. Введите название учетной записи.
  4. В раскрывающемся списке **Метки** установите флажок **DB_Redis**.
  5. Введите логин учетной записи.
  6. Введите пароль и подтвердите его.
  7. Нажмите **Создать**.

11.14.2. Создание и запуск задачи на аудит актива по SSH

► Чтобы создать и запустить задачу на аудит актива:

1. В главном меню выберите **Сбор данных** → **Задачи**.
2. Нажмите **Создать задачу** → **Сбор данных**.
3. Введите название задачи.
4. В раскрывающемся списке **Профиль** выберите **Redis Audit**.
5. В иерархическом списке выберите **Сканирование систем** → **Redis**.
6. Выберите учетную запись для доступа к активу.
7. Введите название БД источника.
8. Если требуется, включите **Использовать протокол SSL**.
9. Если требуется, выберите коллекторы для сбора данных.
10. В панели **Цели сбора данных** на вкладке **Включить** выполните одно из следующих действий:
    - Если для сканируемой цели ранее был добавлен актив, в поле **Активы** введите IP-адрес или доменное имя (в формате FQDN) узла актива.
    - Если для сканируемой цели актив ранее не был добавлен, в поле **Сетевые адреса** введите ее IP-адрес или доменное имя (в формате FQDN).

    Примечание. В панели **Расписание** вы можете включить и настроить автоматический запуск задачи.
11. Нажмите **Сохранить и запустить** → **Запустить сбор данных**.

12. Системы управления серверами

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

В этом разделе

12.1. 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

12.1.1. 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**.

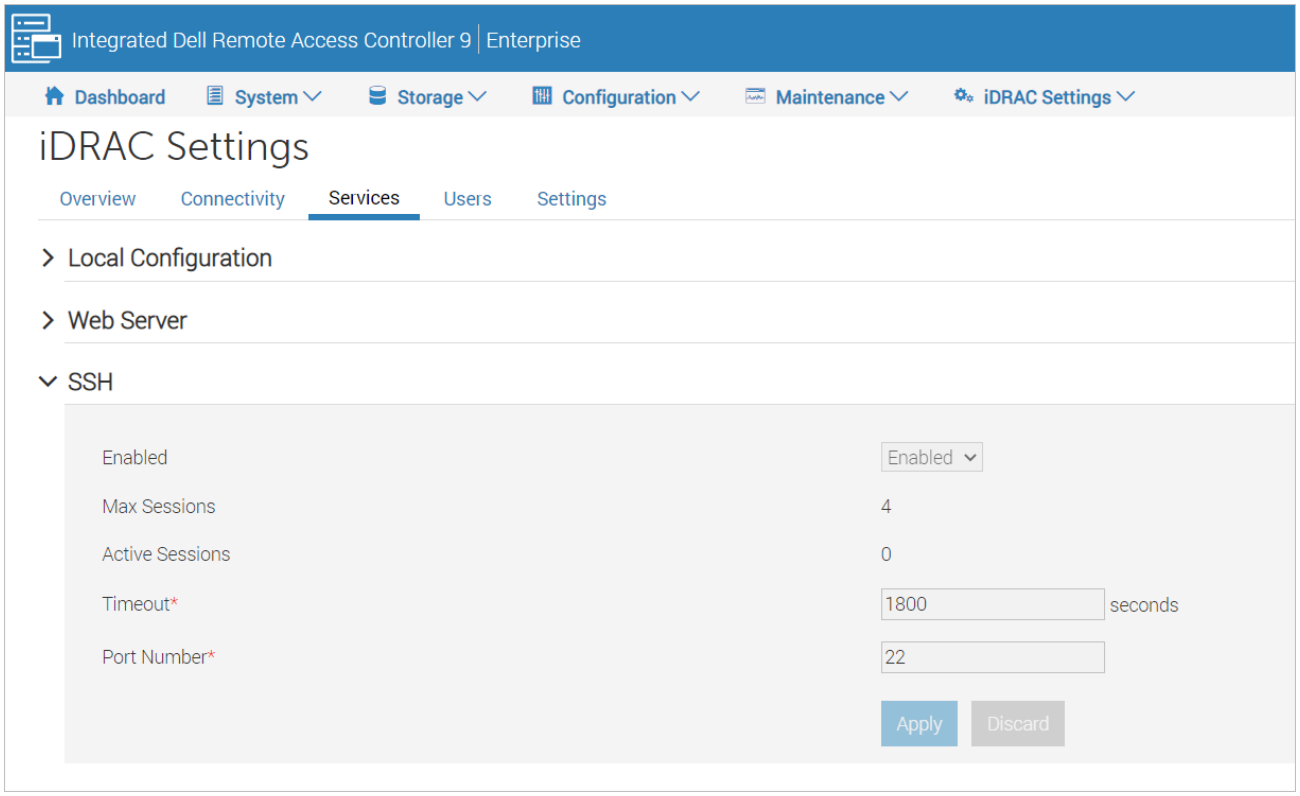

Рисунок 7. Включение доступа к активу по протоколу SSH

3. В раскрывающемся блоке **SSH** в раскрывающемся списке **Enabled** выберите значение **Enabled**.
4. Нажмите кнопку **Apply**.

Доступ к активу по протоколу SSH включен.

12.1.2. 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.

12.2. Dell iDRAC 7—9: настройка MaxPatrol VM

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

12.3. 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

Включение доступа к активу по протоколу SSH (см. раздел 12.3.1)

Создание учетной записи для доступа к активу (см. раздел 12.3.2)

12.3.1. 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**.

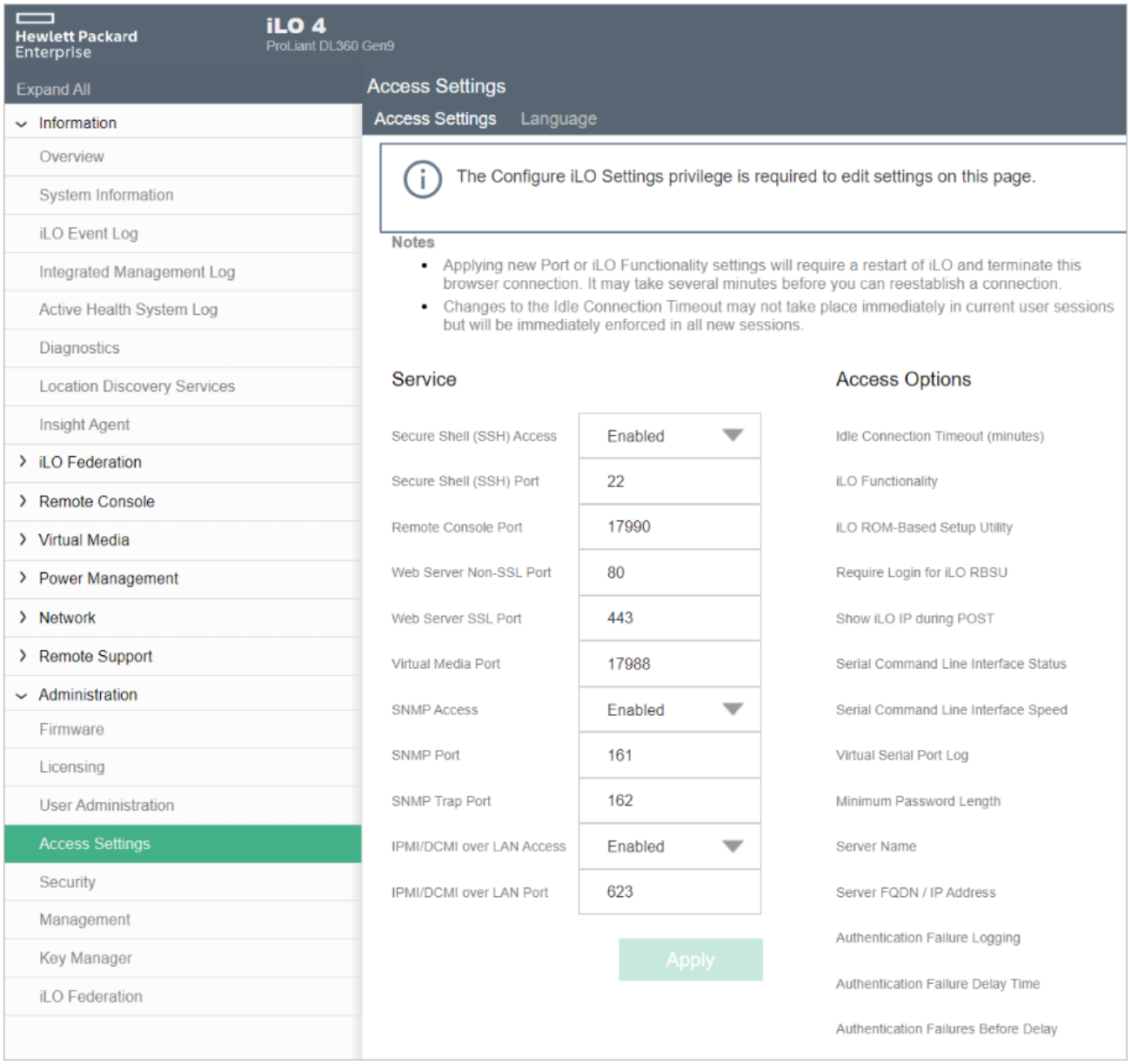

Рисунок 8. Включение доступа к активу по протоколу SSH

3. В раскрывающемся списке **Secure Shell (SSH) Access** выберите значение **Enabled**.
4. Нажмите кнопку **Apply**.

Доступ к активу по протоколу SSH включен.

12.3.2. 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.

12.4. HPE iLO 3—5: настройка MaxPatrol VM

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

13. Системы электронной почты

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

В этом разделе

13.1. Почта VK WorkSpace 1.20 и выше: настройка актива

Поддерживается только русскоязычная версия актива.

Настройку актива нужно выполнять от имени учетной записи администратора устройства.

Для аудита на активе нужно:

1. Создать учетную запись для доступа MP 10 Collector к активу через веб-API и назначить ей права.
2. Настроить доступ для IP-адреса MP 10 Collector к поддоменам biz.* и o2.*.
3. Настроить доступ к API.

В этом разделе

13.1.1. Создание учетной записи и назначение прав

- Чтобы создать учетную запись и назначить ей права:

  1. Войдите в веб-интерфейс актива от имени учетной записи с правами администратора.
  2. Выберите **Пользователи**.
  3. Нажмите **Создать**.
  4. Введите логин учетной записи.
  5. Установите пароль учетной записи.
  6. Нажмите **Создать**.
  7. Выберите **Администраторы**.
  8. Нажмите **Добавить**.

9. Введите адрес электронной почты учетной записи в формате `<Логин>@<Почтовый домен>`.
10. В раскрывающемся списке **Тип прав** выберите **Администратор**.
11. Нажмите **Выслать приглашение**.

На указанный адрес электронной почты придет письмо со ссылкой для подтверждения и получения прав администратора.

13.1.2. Настройка доступа для IP-адреса MP 10 Collector к поддоменам biz.* и o2.*

В процессе сканирования MP 10 Collector может обращаться к поддоменам biz.* и o2.* для сбора данных. Вам необходимо настроить доступ для IP-адреса MP 10 Collector к этим поддоменам.

- Чтобы настроить доступ для IP-адреса MP 10 Collector к поддоменам biz.* и o2.*:

1. Войдите в веб-интерфейс актива от имени учетной записи с правами администратора.
2. В главном меню нажмите **Настройки**.
3. Выберите вкладку **Настройки компонентов**.
4. В левой части страницы нажмите **Ограничение доступа к доменам**.
5. Выберите поддомен biz.* и настройте доступ:
   - Если включен параметр **Ограничить доступ к домену** и отключен параметр **Режим запрета**, добавьте IP-адрес MP 10 Collector в список разрешенных IP-адресов.
   - Если включен параметр **Ограничить доступ к домену** и включен параметр **Режим запрета**, исключите IP-адрес MP 10 Collector из списка запрещенных IP-адресов.
6. Повторите шаг 6 для настройки доступа IP-адреса MP 10 Collector к поддомену o2.*.

13.1.3. Настройка доступа к API

Необходимо предоставить MP 10 Collector доступ к API с использованием идентификатора (client_id). MP 10 Collector будет использовать этот идентификатор для авторизации по протоколу OAuth2.

Инструкцию необходимо выполнять от имени учетной записи операционной системы, где установлен актив, с правами sudo.

Внимание! Если узлы объединены в кластер, настройку нужно выполнять на главном узле.

Внимание! Настраивать доступ к API необходимо после каждого перезапуска контейнеров.

- Чтобы настроить доступ к API:

  1. На узле, с которого производится настройка, запустите терминальный клиент, поддерживающий протокол SSH.
  2. Пройдите аутентификацию на активе.
  3. Выполните команду:

     ```
     docker exec -i swadb1 mysql <<< "use oauth; update client set
     scope=concat(scope,',mail.biz') where name='mail-ios';"
     ```

  4. Перезапустите сервисы swa* и cube*:

     ```
     systemctl restart onpremise-container-cube1
     systemctl restart onpremise-container-swa1
     ```

13.2. Почта VK WorkSpace 1.20 и выше: настройка MaxPatrol VM

Для аудита актива в MaxPatrol VM нужно добавить две ученые записи: одну типа «логин — пароль» и другую типа «пароль», а также создать и запустить задачу на аудит.

В этом разделе

13.2.1. Добавление учетной записи типа «логин — пароль»

- Чтобы добавить в MaxPatrol VM учетную запись типа «логин — пароль»:

  1. В главном меню выберите **Сбор данных** → **Учетные записи**.
  2. Нажмите **Добавить учетную запись** → **Логин — пароль**.
  3. Введите название учетной записи.
  4. В раскрывающемся списке **Метки** установите флажок **Web_API**.
  5. Укажите логин учетной записи в формате `<Логин>@<Домен учетной записи>`.
  6. Введите пароль и подтвердите его.
  7. Нажмите **Создать**.

13.2.2. Добавление учетной записи типа «пароль»

- Чтобы добавить в MaxPatrol VM учетную запись типа «пароль»:

  1. В главном меню выберите **Сбор данных** → **Учетные записи**.
  2. Нажмите **Добавить учетную запись** → **Пароль**.
  3. Введите название учетной записи.
  4. В раскрывающемся списке **Метки** установите флажок **Web_API**.
  5. Введите идентификатор приложения (client_id) и подтвердите его.
  6. Нажмите **Создать**.

13.2.3. Создание и запуск задачи на аудит актива

- Чтобы создать и запустить задачу на аудит актива:

  1. В главном меню выберите **Сбор данных** → **Задачи**.
  2. Нажмите **Создать задачу** → **Сбор данных**.
  3. Введите название задачи.
  4. В раскрывающемся списке **Профиль** выберите **Web API Audit**.
  5. В иерархическом списке выберите **Сканирование систем** → **Через веб-API**.
  6. В раскрывающемся списке **Тип аутентификации** выберите **По протоколу OAuth**.
  7. В раскрывающемся списке **Учетная запись** выберите учетную запись типа «логин — пароль».
  8. В раскрывающемся списке **Идентификатор приложения (client_id)** выберите учетную запись типа «пароль».
  9. Если требуется, включите **Использовать протокол SSL** и **Проверять сертификат SSL**.
  10. Если требуется, выберите коллекторы для сбора данных.
  11. В поле **Сетевые адреса** введите доменное имя (в формате FQDN) узла актива.

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

  12. Нажмите **Сохранить и запустить** → **Запустить сбор данных**.

14. Службы каталогов

Раздел содержит инструкции для настройки аудита поддерживаемых в MaxPatrol VM служб каталогов.

В этом разделе

14.1. Microsoft Active Directory в Windows Server 2003—2022: настройка актива

Для проведения аудита Active Directory нужно создать учетную запись, имеющую права на чтение домена Active Directory. Данные этой учетной записи нужно указать при добавлении учетной записи в MaxPatrol VM.

> **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. При подключении по протоколу LDAP используется TCP-порт 389 и UDP-порт 389, при подключении по протоколу LDAPS (если контроллер домена является глобальным каталогом) — TCP-порт 636 и UDP-порт 636 или TCP-порт 3269 и UDP-порт 3269. Для подключения по протоколу LDAPS необходима предварительная настройка (инструкцию см. на сайте learn.microsoft.com в разделе «Включение протокола LDAP через протокол SSL с использованием стороннего центра сертификации»).
>
> **Примечание.** Если с момента последнего входа учетной записи компьютера в домен Active Directory прошло более 90 суток, то для этого компьютера не будет добавлен актив. Для определения даты последнего входа в домен используется атрибут `LastLogonTimestamp`.
>
> **Примечание.** Вы можете детально настроить учетную запись, предоставив ей права на выполнение команд для проведения аудита (см. приложение).

14.2. Microsoft Active Directory в Windows Server 2003—2022: 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.

Для просмотра данных, полученных в результате сканирования с профилями Microsoft Active Directory Audit или Windows DC Audit, необходимо создать динамическую группу активов с фильтром, содержащим условие `ActiveDirectory`.

При большом количестве активов их сканирование может занимать значительное время. Чтобы уменьшить время сканирования, вы можете ограничить количество сканируемых активов. Для ограничения количества активов необходимо:

1. Создать профиль для сбора данных Computers.
2. Создать профиль для сбора данных Users.
3. Создать профиль для сбора данных Groups.
4. Создать и запустить задачу на проведение аудита с профилем Computers.
5. Создать и запустить задачу на проведение аудита с профилем Users.
6. Создать и запустить задачу на проведение аудита с профилем Groups.

Рекомендуется запускать задачи последовательно с интервалом в 10 минут и увеличивать его, если на узлах активов обнаружена повышенная нагрузка.

В этом разделе

Добавление учетной записи ОС (см. раздел 14.2.1)

Создание и запуск задачи на аудит актива (см. раздел 14.2.2)

Создание профиля для сбора данных Computers (см. раздел 14.2.3)

Создание профиля для сбора данных Users (см. раздел 14.2.4)

Создание профиля для сбора данных Groups (см. раздел 14.2.5)

14.2.1. Добавление учетной записи ОС

- Чтобы добавить в MaxPatrol VM учетную запись для доступа к активу:
  1. В главном меню выберите **Сбор данных** → **Учетные записи**.
  2. Нажмите **Добавить учетную запись** → **Логин — пароль**.
  3. Введите название учетной записи.
  4. В раскрывающемся списке **Метки** установите флажок **LDAP**.
  5. Введите логин учетной записи.

     Внимание! Для сканирования коллекторами, установленными на Windows, можно использовать локальную или доменную учетную запись. Для сканирования коллекторами, установленными на Linux, можно использовать только доменную учетную запись.
  6. Введите пароль и подтвердите его.
  7. Если для доступа к активу используется доменная учетная запись, введите имя домена.

Например:

```
example.com
```

8. Нажмите **Создать**.

14.2.2. Создание и запуск задачи на аудит актива

► Чтобы создать и запустить задачу на аудит актива:

1. В главном меню выберите **Сбор данных** → **Задачи**.
2. Нажмите **Создать задачу** → **Сбор данных**.
3. Введите название задачи.
4. В раскрывающемся списке **Профиль** выберите **Microsoft Active Directory Audit**.
5. В иерархическом списке выберите **Сканирование систем** → **По протоколу LDAP**.
6. Выберите учетную запись для доступа к активу.
7. Если требуется, выберите коллекторы для сбора данных.
8. Укажите цели сбора данных:
   - Если коллекторы установлены на Windows и для сканируемой цели ранее был создан актив, введите IP-адрес или доменное имя (в формате FQDN) узла актива в поле **Активы**.
   - Если коллекторы установлены на Windows и для сканируемой цели ранее не был создан актив, введите IP-адрес или доменное имя (в формате FQDN) узла актива в поле **Сетевые адреса**.
   - Если коллекторы установлены на Linux и для сканируемой цели ранее был создан актив, введите доменное имя (в формате FQDN) узла актива в поле **Активы**.
   - Если коллекторы установлены на Linux и для сканируемой цели ранее не был создан актив, введите доменное имя (в формате FQDN) узла актива в поле **Сетевые адреса**.

     Примечание. При использовании FQDN в качестве адресов на узлах необходимо настроить DNS для корректного разрешения имен узлов в IP-адреса.

     Примечание. В панели **Расписание** вы можете включить и настроить автоматический запуск задачи.
9. Нажмите **Сохранить и запустить** → **Запустить сбор данных**.

14.2.3. Создание профиля для сбора данных Computers

► Чтобы создать в MaxPatrol VM профиль для сбора данных Computers:

1. В главном меню выберите **Сбор данных** → **Профили**.

Откроется страница **Профили**.

2. Выберите профиль **Microsoft Active Directory Audi**t.
3. Нажмите **Создать** → **На базе выбранного профиля**.

   Откроется страница **Новый профиль**.
4. В поле **Название** введите `Computers`.
5. В панели **Параметры профиля** установите флажок **Показывать дополнительные параметры**.
6. На вкладке **Область сбора данных** в раскрывающемся списке **Частичный сбор данных** выберите **По классам модели активов**.
7. В поле **Имена заполняемых классов** введите имена классов, которые будут заполняться для создаваемого профиля:

   ```
   DirectoryService.ForestTrust;DirectoryService.DomainTrust;DirectoryService.ActiveDirectory
   ;DirectoryService.Domain;DirectoryService.Computer
   ```
8. Нажмите кнопку **Сохранить**.

Профиль для сбора данных Computers создан.

14.2.4. Создание профиля для сбора данных Users

- Чтобы создать в MaxPatrol VM профиль для сбора данных Users:

1. В главном меню выберите **Сбор данных** → **Профили**.

   Откроется страница **Профили**.
2. Выберите профиль **Microsoft Active Directory Audi**t.
3. Нажмите **Создать** → **На базе выбранного профиля**.

   Откроется страница **Новый профиль**.
4. В поле **Название** введите `Users`.
5. В панели **Параметры профиля** установите флажок **Показывать дополнительные параметры**.
6. На вкладке **Область сбора данных** в раскрывающемся списке **Частичный сбор данных** выберите **По классам модели активов**.
7. В поле **Имена заполняемых классов** введите имена классов, которые будут заполняться для создаваемого профиля:

   ```
   DirectoryService.ForestTrust;DirectoryService.DomainTrust;DirectoryService.ActiveDirectory
   ;DirectoryService.Domain;DirectoryService.ServicePrincipalName;DirectoryService.User
   ```
8. Нажмите кнопку **Сохранить**.

Профиль для сбора данных Users создан.

14.2.5. Создание профиля для сбора данных Groups

- Чтобы создать в MaxPatrol VM профиль для сбора данных Groups:

  1. В главном меню выберите **Сбор данных** → **Профили**.

     Откроется страница **Профили**.

  2. Выберите профиль **Microsoft Active Directory Audi**t.

  3. Нажмите **Создать** → **На базе выбранного профиля**.

     Откроется страница **Новый профиль**.

  4. В поле **Название** введите `Groups`.

  5. В панели **Параметры профиля** установите флажок **Показывать дополнительные параметры**.

  6. На вкладке **Область сбора данных** в раскрывающемся списке **Частичный сбор данных** выберите **По классам модели активов**.

  7. В поле **Имена заполняемых классов** введите имена классов, которые будут заполняться для создаваемого профиля:

     ```
     DirectoryService.ForestTrust;DirectoryService.DomainTrust;DirectoryService.ActiveDirectory
     ;DirectoryService.Domain;DirectoryService.Group
     ```

  8. Нажмите кнопку **Сохранить**.

  Профиль для сбора данных Groups создан.

15. Устройства беспроводной сети

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

В этом разделе

15.1. 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. Пройдите аутентификацию 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.

15.2. Cisco AireOS Wireless Controller 7.4, 7.6: настройка MaxPatrol VM

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

В этом разделе

15.2.1. Добавление учетной записи для доступа по SSH

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

  1. В главном меню выберите **Сбор данных** → **Учетные записи**.

     Откроется страница **Учетные записи**.
  2. Нажмите **Добавить учетную запись** → **Логин — пароль**.

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

  Учетная запись добавлена.

15.2.2. Создание задачи на аудит актива по SSH

- Чтобы создать задачу на проведение аудита актива:

  1. В главном меню выберите **Сбор данных** → **Задачи**.

     Откроется страница **Задачи по сбору данных**.
  2. Нажмите **Создать задачу** → **Сбор данных**.

     Откроется страница **Создание задачи на сбор данных**.
  3. В поле **Название** введите название задачи.
  4. В раскрывающемся списке **Профиль** выберите **SSH Network Device Audit**.
  5. В иерархическом списке выберите пункт **Сканирование систем** → **Через терминал: SSH**.
  6. В раскрывающемся списке **Учетная запись** выберите учетную запись для доступа к активу.
  7. Если требуется, в раскрывающемся списке **Коллекторы** выберите коллекторы для сбора данных.

8. В панели **Цели сбора данных** на вкладке **Включить** выполните одно из следующих действий:
   - Если для сканируемой цели ранее был добавлен актив, в поле **Активы** введите IP-адрес или доменное имя (в формате FQDN) узла актива.
   - Если для сканируемой цели актив ранее не был добавлен, в поле **Сетевые адреса** введите ее IP-адрес или доменное имя (в формате FQDN).

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

Задача на проведение аудита актива создана.

16. Другие активы

Раздел содержит инструкции для настройки аудита других активов, поддерживаемых в MaxPatrol VM.

В этом разделе

16.1. Продукты Siemens: настройка активов

Настройку актива нужно выполнять от имени учетной записи администратора устройства.

Поддерживается аудит следующих продуктов и компонентов компании Siemens AG:

- Automation License Manager версий 3—7;
- SIMATIC Logon версий 6—18;
- SIMATIC NET PC Software версий 6—18;
- SIMATIC PCS 7 версий 4.0—9.1;

— SIMATIC STEP 7 версий 4.0—5.6;

— SIMATIC WinCC версий 5.0—7.5;

— SIMATIC WinCC Runtime версий 5.0—7.5;

— TIA Portal версий 12—17.

Для проведения аудита на активе нужно создать учетную запись локального пользователя ОС (см. раздел 17.1.2) для доступа MP 10 Collector к активу. Данные этой учетной записи нужно указать при добавлении учетной записи в MaxPatrol VM.

16.2. Продукты Siemens: 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

16.2.1. Добавление учетной записи

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

1. В главном меню выберите **Сбор данных** → **Учетные записи**.

   Откроется страница **Учетные записи**.

2. Нажмите **Добавить учетную запись** → **Логин — пароль**.

   Откроется страница **Добавление учетной записи**.

3. Введите название учетной записи.

4. Введите логин учетной записи.

5. Если требуется, в поле **Пароль** введите пароль и подтвердите его в поле **Подтверждение пароля**.

6. Нажмите кнопку **Сохранить**.

Учетная запись добавлена.

16.2.2. Создание и запуск задачи на аудит актива

► Чтобы создать и запустить задачу на аудит актива:

1. В главном меню выберите **Сбор данных** → **Задачи**.

Откроется страница **Задачи по сбору данных**.

2. Нажмите **Создать задачу** → **Сбор данных**.

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

3. В поле **Название** введите название задачи.
4. В раскрывающемся списке **Профиль** выберите **Windows Audit**.
5. В иерархическом списке выберите пункт **Сканирование систем** → **Windows**.
6. Выберите учетную запись пользователя ОС.
7. Если требуется, в раскрывающемся списке **Коллекторы** выберите коллекторы для сбора данных.
8. 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.

9. Нажмите кнопку **Сохранить и запустить**.

Задача на проведение аудита актива создана и запущена.

16.3. «1С-Битрикс: Управление сайтом» 20.0.0 и выше: 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 используются TCP-порты 22 и 3306.

Для проведения аудита на активе нужно:

1. Создать учетную запись пользователя в ОС семейства Linux для доступа MP 10 Collector к активу. Настройку нужно выполнять по инструкциям раздела «Unix-подобные ОС: настройка актива (см. раздел 4.3)».
2. Настроить удаленный доступ к СУБД MySQL.
3. Создать учетную запись СУБД с правом на чтение базы данных актива.

В этом разделе

16.3.1. Настройка удаленного доступа в MySQL

- Чтобы настроить удаленный доступ в СУБД:

  1. Откройте конфигурационный файл `my.cnf`.

     Примечание. Вы можете узнать расположение файла, выполнив команду `mysqld --help --verbose | grep my.cnf`.

  2. В секцию `[mysqld]` добавьте строки:

     ```
     port = 3306
     bind_address = <IP-адрес СУБД источника>
     ```

  3. Сохраните конфигурационный файл.

  4. Перезапустите СУБД:

     ```
     systemctl restart mysqld
     ```

16.3.2. Настройка СУБД MySQL

Данные актива сохраняются в базу данных (по умолчанию sitemanager) под управлением СУБД MySQL.

- Чтобы настроить СУБД MySQL для аудита актива:

  1. Настройте удаленный доступ к СУБД (см. раздел 16.3.1).

  2. В интерфейсе терминала запустите консоль MySQL с правами суперпользователя (root):

     ```
     mysql -u root -p
     ```

  3. Переключитесь на базу данных sitemanager:

     ```
     USE sitemanager;
     ```

  4. Создайте учетную запись пользователя с правами удаленного доступа к базе данных:

     ```
     CREATE USER 'mpuser'@'%' 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 базы данных:

     ```
     GRANT SELECT ON sitemanager.* TO 'mpuser'@'%';
     ```

  6. Примените внесенные изменения:

     ```
     FLUSH PRIVILEGES;
     ```

  7. Завершите сеанс работы с консолью MySQL:

     ```
     EXIT;
     ```

16.4. «1С-Битрикс: Управление сайтом» 20.0.0 и выше: настройка MaxPatrol VM

Примечание. Для доступа в СУБД Oracle MySQL на узле MP 10 Collector необходимо установить ODBC-драйвер. Вы можете скачать его с сайта mysql.com. Для Windows нужно установить 32-разрядную версию, для ОС семейства Linux — 64-разрядную (см. раздел 17.2.4).

Для аудита актива в MaxPatrol VM нужно:

1. Добавить учетную запись для доступа к активу.
2. Добавить учетную запись для доступа MP 10 Collector к БД с данными актива.
3. Создать и запустить задачу на сбор данных с профилем 1C-Bitrix Audit.

В этом разделе

16.4.1. Добавление учетной записи пользователя ОС

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

1. В главном меню выберите **Сбор данных** → **Учетные записи**.

   Откроется страница **Учетные записи**.
2. Нажмите **Добавить учетную запись** → **Логин — пароль**.

   Откроется страница **Добавление учетной записи**.
3. Введите название учетной записи.
4. Введите логин учетной записи.
5. Если требуется, в поле **Пароль** введите пароль и подтвердите его в поле **Подтверждение пароля**.
6. Нажмите кнопку **Сохранить**.

Учетная запись добавлена.

16.4.2. Добавление учетной записи СУБД MySQL

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

1. В главном меню выберите **Сбор данных** → **Учетные записи**.

Откроется страница **Учетные записи**.

2. Нажмите **Добавить учетную запись** → **Логин — пароль**.

   Откроется страница **Добавление учетной записи**.

3. Введите название учетной записи.
4. В раскрывающемся списке **Метки** установите флажок **DB_MySQL**.
5. 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, введите имя домена.
8. Нажмите кнопку **Сохранить**.

Учетная запись добавлена.

16.4.3. Создание и запуск задачи на аудит актива

► Чтобы создать и запустить задачу на аудит актива:

1. В главном меню выберите **Сбор данных** → **Задачи**.

   Откроется страница **Задачи по сбору данных**.

2. Нажмите **Создать задачу** → **Сбор данных**.

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

3. В поле **Название** введите название задачи.
4. В раскрывающемся списке **Профиль** выберите **1C-Bitrix Audit**.
5. В иерархическом списке выберите **Сканирование систем** → **Через терминал: SSH**.
6. В раскрывающемся списке **Учетная запись** выберите учетную запись для доступа к активу.
7. В иерархическом списке выберите пункт **Сканирование систем** → **Oracle MySQL**.
8. В раскрывающемся списке **Учетная запись** выберите добавленную ранее учетную запись СУБД MySQL.
9. Если требуется, в раскрывающемся списке **Коллекторы** выберите коллекторы для сбора данных.
10. 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.

11. Нажмите кнопку **Сохранить и запустить**.

Задача на проведение аудита актива создана и запущена.

16.5. 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 (см. раздел 16.3.1).
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.

16.6. 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

Добавление учетной записи СУБД MySQL (см. раздел 16.6.1)

Создание профиля для сканирования (см. раздел 16.6.2)

Создание и запуск задачи на аудит актива (см. раздел 16.6.3)

16.6.1. Добавление учетной записи СУБД MySQL

- Чтобы добавить в MaxPatrol VM учетную запись для доступа к БД с данными актива:
  1. В главном меню выберите **Сбор данных** → **Учетные записи**.

     Откроется страница **Учетные записи**.
  2. Нажмите **Добавить учетную запись** → **Логин — пароль**.

     Откроется страница **Добавление учетной записи**.
  3. Введите название учетной записи.
  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.

16.6.2. Создание профиля для сканирования

- Чтобы создать в MaxPatrol VM профиль для сканирования актива:

1. В главном меню выберите **Сбор данных** → **Профили**.

   Откроется страница **Профили**.
2. В рабочей области выберите профиль **Unix SSH Audit**.
3. Нажмите **Создать** → **На базе выбранного профиля**.

   Откроется страница **Новый профиль**.
4. Введите название профиля.
5. В панели **Параметры профиля** в раскрывающемся списке **Сканирование систем** выберите пункт **Oracle MySQL**.
6. Нажмите кнопку **Сохранить**.

Профиль для сканирования актива создан.

16.6.3. Создание и запуск задачи на аудит актива

- Чтобы создать задачу на проведение аудита актива:

1. В главном меню выберите **Сбор данных** → **Задачи**.

   Откроется страница **Задачи по сбору данных**.
2. Нажмите **Создать задачу** → **Сбор данных**.

   Откроется страница **Создание задачи на сбор данных**.
3. В поле **Название** введите название задачи.
4. В панели **Параметры сбора данных** в раскрывающемся списке **Профиль** выберите профиль, созданный ранее.
5. В иерархическом списке выберите пункт **Сканирование систем** → **Oracle MySQL**.
6. В раскрывающемся списке **Учетная запись** выберите созданную ранее учетную запись для доступа к СУБД MySQL.
7. В иерархическом списке выберите **Сканирование систем** → **Через терминал: SSH**.
8. Настройте сканирование ОС актива (см. раздел 4).

9. Если требуется, в раскрывающемся списке **Коллекторы** выберите коллекторы для сбора данных.
10. Если в системе заведено больше одной инфраструктуры, в раскрывающемся списке **Инфраструктура** выберите инфраструктуру.
11. 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.
12. Нажмите кнопку **Сохранить**.

Задача на проведение аудита актива создана.

16.7. AVEVA (Wonderware) Historian, Insight, InTouch, System Platform: настройка активов

Поддерживается аудит следующих продуктов и компонентов компании AVEVA:

- AVEVA (Wonderware) Application Server 3.5—20;
- AVEVA (Wonderware) ArchestrA 1—5.5;
- AVEVA (Wonderware) Auto-Build Core 5.5—20;
- AVEVA (Wonderware) FactorySuite Gateway 5.5—20;
- AVEVA (Wonderware) Historian 10—20;
- AVEVA (Wonderware) Historian Client 10—20;
- AVEVA (Wonderware) Historian Search 10—20;
- AVEVA (Wonderware) Information Model 2012—2020;
- AVEVA (Wonderware) Information Server 04.05—5.6;
- AVEVA (Wonderware) Insight 10—20;
- AVEVA (Wonderware) Insight Publisher 5.5—20;
- AVEVA (Wonderware) InTouch 5.5—20;
- AVEVA (Wonderware) InTouch Access Anywhere 10—20;
- AVEVA (Wonderware) InTouch Access Anywhere Server 10—20;
- AVEVA (Wonderware) InTouch OMI 5.5—20;
- AVEVA (Wonderware) License Server 3.5.0—20;
- AVEVA (Wonderware) Logger 5.5—20;
- AVEVA (Wonderware) System Platform 2012—2020.

Для проведения аудита на активе нужно создать учетную запись локального пользователя ОС (см. раздел 17.1.2) для доступа MP 10 Collector к активу. Данные этой учетной записи нужно указать при добавлении учетной записи в MaxPatrol VM.

16.8. AVEVA (Wonderware) Historian, Insight, InTouch, System Platform: 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

16.8.1. Добавление учетной записи

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

  1. В главном меню выберите **Сбор данных** → **Учетные записи**.

     Откроется страница **Учетные записи**.
  2. Нажмите **Добавить учетную запись** → **Логин — пароль**.

     Откроется страница **Добавление учетной записи**.
  3. Введите название учетной записи.
  4. Введите логин учетной записи.
  5. Если требуется, в поле **Пароль** введите пароль и подтвердите его в поле **Подтверждение пароля**.
  6. Нажмите кнопку **Сохранить**.

  Учетная запись добавлена.

16.8.2. Создание и запуск задачи на аудит актива

- Чтобы создать и запустить задачу на аудит актива:

  1. В главном меню выберите **Сбор данных** → **Задачи**.

     Откроется страница **Задачи по сбору данных**.
  2. Нажмите **Создать задачу** → **Сбор данных**.

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

3. В поле **Название** введите название задачи.
4. В раскрывающемся списке **Профиль** выберите **Windows Audit**.
5. В иерархическом списке выберите пункт **Сканирование систем** → **Windows**.
6. Выберите учетную запись пользователя ОС.
7. Если требуется, в раскрывающемся списке **Коллекторы** выберите коллекторы для сбора данных.
8. 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.
9. Нажмите кнопку **Сохранить и запустить**.

Задача на проведение аудита актива создана и запущена.

16.9. JetBrains Hub 2018.1—2022: настройка актива

Настройку актива нужно выполнять от имени учетной записи администратора устройства.

Для проведения аудита на активе нужно:

1. Создать роль с правами, необходимыми для аудита JetBrains Hub.
2. Создать учетную запись с созданной ролью.
3. Выпустить для созданной учетной записи токен доступа.

В этом разделе

16.9.1. Создание и настройка роли

- Чтобы создать и настроить роль:

  1. Войдите в веб-интерфейс JetBrains Hub под учетной записью с правами администратора.
  2. Перейдите на страницу **Administration** → **Access Management** → **Roles**.
  3. Нажмите кнопку **New role**.
  4. В поле **Name** укажите название роли и нажмите кнопку **Create**.

     Откроется окно с параметрами роли.

5. Выберите вкладку **Permissions**.
6. В столбце **Hub** установите следующие флажки:
   - **Low-level Admin Read**;
   - **Read Group**;
   - **Read Organization**;
   - **Read User Full**;
   - **Read Project Basic**;
   - **Read Project Full**;
   - **Read Role**.

   Примечание. Параметры роли сохраняются автоматически.

Роль создана и настроена.

16.9.2. Создание и настройка учетной записи для доступа к активу

► Чтобы создать учетную запись для доступа к активу:

1. Войдите в веб-интерфейс JetBrains Hub под учетной записью с правами администратора.
2. Перейдите на страницу **Administration** → **Access Management** → **Users**.
3. Нажмите кнопку **Create**.

   Откроется окно **New User**.
4. Выберите вкладку **Create user**.
5. В поле **Full name** введите имя учетной записи.
6. В поле **Password** введите пароль учетной записи и повторите его в поле **Confirm**.
7. Нажмите кнопку **Create**.

   Откроется страница с параметрами учетной записи.
8. Выберите вкладку **Roles**.
9. Нажмите кнопку **Grant role**.

   Откроется окно **Grant Role**.
10. В раскрывающемся списке **Role** выберите созданную роль (см. раздел 16.9.1).

11. В раскрывающемся списке **Scope** выберите проект **Global**.
12. Нажмите кнопку **Grant**.

Учетная запись создана.

16.9.3. Выпуск токена для учетной записи

Токен необходим для получения доступа к информации о событиях на активе с помощью REST API.

- Чтобы выпустить токен для учетной записи:

1. Войдите в веб-интерфейс JetBrains Hub под учетной записью с правами администратора.
2. Перейдите на страницу **Administration** → **Access Management** → **Users**.
3. Выберите учетную запись, для которой необходимо выпустить токен.

   Откроется страница с параметрами учетной записи.
4. Выберите вкладку **Account Security**.
5. Нажмите кнопку **New token**.

   Откроется окно **New Permanent Token**.
6. В поле **Name** введите название токена.
7. В поле **Scope** выберите **Hub**.
8. Нажмите кнопку **Create**.
9. В открывшемся окне нажмите кнопку **Copy token**.
10. Сохраните токен из буфера обмена в текстовый файл.

Токен для учетной записи выпущен.

16.10. JetBrains Hub 2018.1—2022: настройка MaxPatrol VM

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

В этом разделе

Добавление учетной записи (см. раздел 16.10.1)

Создание и запуск задачи на аудит актива (см. раздел 16.10.2)

16.10.1. Добавление учетной записи

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

  1. В главном меню выберите **Сбор данных** → **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. Введите название учетной записи.
  4. В раскрывающемся списке **Метки** выберите **Web_API**.
  5. В поле **Пароль** введите значение токена и подтвердите его в поле **Подтверждение пароля**.
  6. Нажмите кнопку **Создать**.

  Учетная запись добавлена.

16.10.2. Создание и запуск задачи на аудит актива

- Чтобы создать задачу на проведение аудита актива:

  1. В главном меню выберите **Сбор данных** → **Задачи**.

     Откроется страница **Задачи по сбору данных**.

  2. Нажмите **Создать задачу** → **Сбор данных**.

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

  3. В поле **Название** введите название задачи.
  4. В панели **Параметры сбора данных** в раскрывающемся списке **Профиль** выберите **Web API Audit**.
  5. В иерархическом списке выберите пункт **Сканирование систем** → **Через веб-API**.
  6. В раскрывающемся списке **Тип аутентификации** выберите **Токен доступа Bearer**.
  7. В раскрывающемся списке **Учетная запись** выберите учетную запись для доступа к активу.
  8. В поле **Порт** укажите номер порта для подключения к веб-серверу JetBrains Hub.
  9. 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.

10. Нажмите кнопку **Сохранить**.

Задача на проведение аудита актива создана.

16.11. JetBrains YouTrack 2019: настройка актива

Настройку актива нужно выполнять от имени учетной записи администратора системы.

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 HTTP/REST API используются порты TCP 80 и 443.

Для проведения аудита на активе нужно:

1. Создать роль с правами, необходимыми для аудита JetBrains YouTrack.
2. Создать учетную запись.
3. Создать токен доступа для учетной записи.

В этом разделе

Добавление новой роли (см. раздел 16.11.1)

Создание учетной записи (см. раздел 16.11.2)

Создание токена (см. раздел 16.11.3)

16.11.1. Добавление новой роли

- Чтобы добавить новую роль:

  1. Войдите в веб-интерфейс JetBrains YouTrack под учетной записью с правами администратора.
  2. Перейдите на страницу **Administration** → **Access Management** → **Roles**.
  3. Нажмите кнопку **New role**.
  4. В поле **Name** введите название роли.
  5. Нажмите кнопку **Create**.

     Откроется окно с параметрами роли.

6. Выберите вкладку **Permissions**.
7. В столбце **YouTrack** установите следующие флажки:
   - **Low-level Admin Read**;
   - **Read Group**;
   - **Read Work Item**;
   - **Read Organization**;
   - **Read Project Basic**;
   - **Read Project Full**;
   - **Read Role**;
   - **Read User Basic**;
   - **Read User Full**;
   - **Update Self**.

   Примечание. Параметры роли сохраняются автоматически.

Роль создана и настроена.

16.11.2. Создание учетной записи

► Чтобы создать учетную запись:

1. Войдите в веб-интерфейс JetBrains YouTrack под учетной записью с правами администратора.
2. Перейдите на страницу **Administration** → **Access Management** → **Users**.
3. Нажмите кнопку **Create**.

   Откроется окно **New User**.
4. В поле **Full name** введите имя учетной записи.
5. В поле **Password** введите пароль учетной записи и повторите его в поле **Confirm**.

   Откроется страница с параметрами учетной записи.
6. Выберите вкладку **Roles**.
7. В раскрывающемся списке **Role** выберите созданную ранее роль.
8. В раскрывающемся списке **Scope** выберите **Global**.
9. Нажмите кнопку **Grant**.

Учетная запись создана.

16.11.3. Создание токена

- Чтобы создать токен для учетной записи:

  1. Войдите в веб-интерфейс JetBrains Hub под учетной записью с правами администратора.
  2. Перейдите на страницу **Administration** → **Access Management** → **Users**.
  3. Выберите вкладку **Account Security**.
  4. Нажмите кнопку **New token**.

     Откроется окно **New Permanent Token**.
  5. В поле **Name** введите название токена.
  6. В поле **Scope** выберите **YouTrack** и **YouTrack Administration**.
  7. Нажмите кнопку **Create**.

  Токен создан.

16.12. JetBrains YouTrack 2019: настройка MaxPatrol VM

Для аудита актива MaxPatrol VM нужно добавить учетную запись для доступа к активу и создать задачу на проведение аудита с профилем Web API Audit.

В этом разделе

Добавление учетной записи (см. раздел 16.12.1)

Создание и запуск задачи на аудит актива (см. раздел 16.12.2)

16.12.1. Добавление учетной записи

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

  1. В главном меню выберите **Сбор данных** → **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. Введите название учетной записи.
  4. В раскрывающемся списке **Метки** выберите **Web_API**.

5. В поле **Пароль** введите значение токена и подтвердите его в поле **Подтверждение пароля**.
6. Нажмите кнопку **Создать**.

Учетная запись добавлена.

16.12.2. Создание и запуск задачи на аудит актива

- Чтобы создать задачу на проведение аудита актива:

1. В главном меню выберите **Сбор данных** → **Задачи**.

   Откроется страница **Задачи по сбору данных**.
2. Нажмите **Создать задачу** → **Сбор данных**.

   Откроется страница **Создание задачи на сбор данных**.
3. В поле **Название** введите название задачи.
4. В панели **Параметры сбора данных** в раскрывающемся списке **Профиль** выберите **Web API Audit**.
5. В иерархическом списке выберите пункт **Сканирование систем** → **Через веб-API**.
6. В раскрывающемся списке **Тип аутентификации** выберите **Токен доступа Bearer**.
7. В раскрывающемся списке **Учетная запись** выберите учетную запись для доступа к активу.
8. В поле **Порт** укажите номер порта для подключения к веб-серверу YouTrack.
9. 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.
10. Нажмите кнопку **Сохранить**.

Задача на проведение аудита актива создана.

16.13. JFrog Artifactory 6—6.23: настройка актива

Настройку актива нужно выполнять от имени учетной записи администратора устройства.

Для аудита на активе нужно:

1. Создать учетную запись для доступа MP 10 Collector к активу через веб-API.
2. Создать группу с привилегиями администратора и добавить в нее учетную запись.
3. Выпустить токен доступа для учетной записи.

В этом разделе

16.13.1. Создание учетной записи для доступа к активу через веб-API

- Чтобы создать учетную запись для доступа к активу:
  1. Войдите в веб-интерфейс актива от имени учетной записи с правами администратора.
  2. Нажмите **Admin** → **Security** → **User**.
  3. Нажмите **New**.
  4. Введите логин учетной записи.
  5. Введите адрес электронной почты учетной записи.
  6. Установите флажки **Disable UI Access** и **Disable Internal Password**.
  7. Нажмите **Save**.

16.13.2. Создание группы и добавление учетной записи в группу

- Чтобы создать группу и добавить в нее учетную запись:
  1. Войдите в веб-интерфейс актива от имени учетной записи с правами администратора.
  2. Нажмите **Admin** → **Security** → **Groups**.
  3. Нажмите **New**.
  4. Введите название группы.
  5. Установите флажок **Admin Privileges**.
  6. Добавьте в группу созданную ранее учетную запись.

16.13.3. Выпуск токена доступа для учетной записи

Внимание! На узле актива должна быть установлена программа cURL.

- Чтобы выпустить токен доступа:

  1. На узле, с которого производится настройка, запустите терминальный клиент, поддерживающий протокол SSH.
  2. Пройдите аутентификацию на активе.
  3. Выполните команду:

     ```
     curl -u <Логин учетной записи администратора>:<Пароль учетной записи администратора>
     -XPOST "http://localhost:8081/artifactory/api/security/token" -d "username=<Логин учетной
     записи для доступа к активу>" -d "expires_in=<Срок действия токена доступа>"
     ```

     Например:

     ```
     curl -u admin_login:admin_password -XPOST "http://localhost:8081/artifactory/api/security/
     token" -d "username=user_login" -d "expires_in=0"
     ```
  4. Скопируйте токен доступа и сохраните в текстовый файл.

Токен доступа понадобится при добавлении учетной записи в MaxPatrol VM.

16.14. JFrog Artifactory 7 и выше: настройка актива

Для доступа MP 10 Collector к активу используется токен доступа.

- Чтобы выпустить токен доступа:

  1. Войдите в веб-интерфейс актива от имени учетной записи с правами администратора.
  2. Нажмите **Administration** → **User Management** → **Access Tokens**.
  3. Нажмите **Generate Token**.
  4. В раскрывающемся списке **Token scope** выберите **Admin**.
  5. В поле **User name** введите имя пользователя, которое будет использоваться для MP 10 Collector.
  6. В раскрывающемся списке **Expiration time** выберите срок действия токена доступа.
  7. Нажмите **Generate**.
  8. Скопируйте токен доступа и сохраните в текстовый файл.

Токен доступа понадобится при добавлении учетной записи в MaxPatrol VM.

16.15. JFrog Artifactory 6 и выше: настройка MaxPatrol VM

Для аудита актива в MaxPatrol VM нужно добавить учетную запись для доступа к активу, создать и запустить задачу на аудит.

В этом разделе

16.15.1. Добавление учетной записи для доступа к активу

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

  1. В главном меню выберите **Сбор данных** → **Учетные записи**.
  2. Нажмите **Добавить учетную запись** → **Пароль**.
  3. Введите название учетной записи.
  4. В раскрывающемся списке **Метки** установите флажок **Web_API**.
  5. В поле **Пароль** введите значение токена, полученное при настройке актива, и подтвердите его в поле **Подтверждение пароля**.
  6. Нажмите **Создать**.

16.15.2. Создание и запуск задачи на аудит актива

- Чтобы создать и запустить задачу на аудит актива:

  1. В главном меню выберите **Сбор данных** → **Задачи**.
  2. Нажмите **Создать задачу** → **Сбор данных**.
  3. Введите название задачи.
  4. В раскрывающемся списке **Профиль** выберите **Web API Audit**.
  5. В иерархическом списке выберите **Сканирование систем** → **Через веб-API**.
  6. В раскрывающемся списке **Тип аутентификации** выберите **Токен доступа Bearer**.
  7. Выберите учетную запись для доступа к активу.
  8. Включите **Показывать дополнительные параметры**.
  9. Укажите номер порта.
  10. Если требуется, включите **Использовать протокол SSL** и **Проверять сертификат SSL**.
  11. Если требуется, выберите коллекторы для сбора данных.
  12. 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.

  13. Нажмите **Сохранить и запустить** → **Запустить сбор данных**.

16.16. Yokogawa CENTUM VP R4—R6 и ProSafe-RS R2—R4: настройка активов

Настройку актива нужно выполнять от имени учетной записи администратора устройства.

Для проведения аудита на активе нужно создать учетную запись локального пользователя ОС (см. раздел 17.1.2) для доступа MP 10 Collector к активу. Данные этой учетной записи нужно указать при добавлении учетной записи в MaxPatrol VM.

16.17. Yokogawa CENTUM VP R4—R6 и ProSafe-RS R2—R4: 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

16.17.1. Добавление учетной записи

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

  1. В главном меню выберите **Сбор данных** → **Учетные записи**.

     Откроется страница **Учетные записи**.

  2. Нажмите **Добавить учетную запись** → **Логин — пароль**.

     Откроется страница **Добавление учетной записи**.

  3. Введите название учетной записи.

  4. Введите логин учетной записи.

  5. Если требуется, в поле **Пароль** введите пароль и подтвердите его в поле **Подтверждение пароля**.

  6. Нажмите кнопку **Сохранить**.

  Учетная запись добавлена.

16.17.2. Создание и запуск задачи на аудит актива

- Чтобы создать и запустить задачу на аудит актива:

  1. В главном меню выберите **Сбор данных** → **Задачи**.

     Откроется страница **Задачи по сбору данных**.

  2. Нажмите **Создать задачу** → **Сбор данных**.

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

  3. В поле **Название** введите название задачи.
  4. В раскрывающемся списке **Профиль** выберите **Windows Audit**.
  5. В иерархическом списке выберите пункт **Сканирование систем** → **Windows**.
  6. Выберите учетную запись пользователя ОС.
  7. Если требуется, в раскрывающемся списке **Коллекторы** выберите коллекторы для сбора данных.
  8. 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.

  9. Нажмите кнопку **Сохранить и запустить**.

  Задача на проведение аудита актива создана и запущена.

17. Стандартные операции для настройки активов

Раздел содержит инструкции для стандартных операций, выполняемых при настройке аудита активов.

В этом разделе

17.1. Стандартные операции в Windows

Раздел содержит инструкции для стандартных операций, выполняемых в Windows.

В этом разделе

17.1.1. 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.
  5. В главном меню выберите **Действия** → **Включить правило**.

  Правило включено.

17.1.2. Создание учетной записи ОС

Внимание! Инструкция подходит только для сканирования коллекторами, установленными на Windows.

- 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**.
  4. В главном меню выберите **Действие** → **Новый пользователь**.
  5. В поле **Пользователь** введите логин учетной записи.
  6. Установите флажок **Запретить смену пароля пользователем**.
  7. Установите флажок **Срок действия пароля не ограничен**.
  8. Введите пароль и подтвердите его.
  9. Нажмите **Создать**.

17.1.3. 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.
  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 **ОК**.

10. В поле **Введите имена выбираемых объектов** введите логин учетной записи и нажмите кнопку **ОК**.
11. В окне **Свойства <Имя политики>** нажмите кнопку **ОК**.

Учетная запись добавлена в локальную политику безопасности.

17.1.4. 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.
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 **ОК**.
10. В поле **Введите имена выбираемых объектов** введите логин учетной записи и нажмите кнопку **ОК**.
11. В окне **Свойства <Имя группы>** нажмите кнопку **ОК**.

Учетная запись добавлена в группу.

17.1.5. Настройка общего доступа к папке

► Чтобы настроить общий доступ к папке:

1. В контекстном меню папки выберите пункт **Свойства**.
2. В открывшемся окне выберите вкладку **Доступ**.
3. Нажмите кнопку **Расширенная настройка**.
4. В окне **Расширенная настройка общего доступа** установите флажок **Открыть общий доступ к этой папке**.

5. Нажмите кнопку **Разрешения** и в открывшемся окне выберите пользователей, которые будут иметь доступ к папке, а также укажите права доступа для них.
6. Нажмите кнопку **OK**.
7. Нажмите кнопку **OK**.

Общий доступ к папке настроен.

17.2. Стандартные операции в ОС семейства Unix

Раздел содержит инструкции для стандартных операций, выполняемых в ОС семейства Unix.

В этом разделе

17.2.1. Создание учетной записи в ОС семейства Unix

Внимание! Процедуру создания учетной записи нужно выполнять от имени учетной записи root.

- Чтобы создать и настроить учетную запись:

1. Создайте учетную запись для нового пользователя, выполнив следующие команды (в зависимости от дистрибутива):
   - FreeBSD:

     ```
     adduser
     ```

     После выполнения команды нужно указать данные нового пользователя:

     ```
     Login: <Логин>
     Shell: sh
     Password: empty - no, random - no
     <Пароль>
     ```

   - Oracle Solaris:

     ```
     useradd -m <Логин>
     passwd <Логин>
     ```

После выполнения команд нужно указать пароль для нового пользователя.

- IBM AIX:

```
useradd -m -s /bin/sh <Логин>
echo '<Логин>:<Пароль>' | chpasswd
pwdadm -c <Логин>
```

- HPE HP-UX:

```
useradd -m -g users -s /bin/sh <Логин>
passwd <Логин>
```

После выполнения команд нужно указать пароль для нового пользователя.

- Другая ОС:

```
useradd -m -g users -s /bin/bash <Логин>
passwd <Логин>
```

После выполнения команд нужно указать пароль для нового пользователя.

2. Настройте права доступа к домашнему каталогу:

- Oracle Solaris:

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

- Другая ОС:

```
chmod 700 /home/<Логин>
```

3. Войдите в систему от имени созданной учетной записи, чтобы проверить корректность выполненной настройки:

```
su - <Логин>
<Пароль>
```

17.2.2. Определение используемой службы журналирования

► Чтобы определить используемую на источнике службу журналирования,

выполните команду:

- если установлена операционная система «Альт»:

```
rpm -qa | grep syslog
```

- если Astra Linux, Debian или Ubuntu:

```
dpkg --list | grep syslog
```

- если CentOS, Oracle Linux, Red Hat Enterprise Linux или «РЕД ОС»:

```
rpm -qa *syslog*
```

- если SUSE Linux Enterprise Server:

```
zypper search *syslog* --installed-only | grep 'i |'
```

На экране появится название используемой службы.

17.2.3. 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.

17.2.4. Установка ODBC-драйвера

Для подключения к СУБД на узле MP 10 Collector нужно установить ODBC-драйвер. Для узлов с ОС семейства Linux необходимо использовать 64-разрядную версию.

Внимание! Инструкции разработаны для установки ODBC-драйвера на узел с Debian 10. В других ОС команды и пути к файлам могут отличаться.

Подготовка к установке

- Чтобы подготовить узел к установке ODBC-драйвера:

  1. Если в домашней папке пользователя, от имени которого запускается MP 10 Collector, есть файл `/.config/pip/pip.conf`, удалите в файле адрес `pypi-proxy.ptsecurity.ru`.
  2. Откройте файл `/etc/apt/sources.list`.
  3. Замените все строки в файле на следующие:
     ```
     deb http://deb.debian.org/debian/ buster main
     deb-src http://deb.debian.org/debian/ buster main
     deb http://security.debian.org/debian-security buster/updates main
     deb-src http://security.debian.org/debian-security buster/updates main
     deb http://deb.debian.org/debian/ buster-updates main
     deb-src http://deb.debian.org/debian/ buster-updates main
     ```
  4. Сохраните изменения и закройте файл.

Для СУБД Firebird

- Чтобы установить ODBC-драйвер:

  1. Скачайте с сайта firebirdsql.org, распакуйте и установите ODBC-драйвер.

     Например:

     ```
     wget https://sourceforge.net/projects/firebird/files/firebird-ODBC-driver/2.0.5-Release/OdbcFb-LIB-2.0.5.156.amd64.gz/download -O - | tar –xz
     ```

  2. Переместите файл `libOdbcFb.so` в каталог для библиотек:

     ```
     mv libOdbcFb.so /usr/lib64/libOdbcFb.so
     ```

  3. Запустите установку библиотеки libfbclient2:

     ```
     apt install libfbclient2
     ```

  4. Создайте символическую ссылку для библиотеки libfbclient:

     ```
     ln -s /usr/lib/x86_64-linux-gnu/firebird/3.0/lib/libfbclient.so.2 /usr/lib/x86_64-linux-gnu/libgds.so
     ```

  5. Откройте файл `/etc/odbcinst.ini`.

  6. Добавьте в файл строки:

     ```
     [Firebird]
     Description=InterBase/Firebird ODBC Driver
     Driver=/usr/lib64/libOdbcFb.so
     Setup=/usr/lib64/libOdbcFb.so
     Threading=1
     FileUsage=1
     CPTimeout=
     CPReuse=
     ```

  7. Сохраните изменения и закройте файл.

  8. Если требуется, проверьте подключение к СУБД:

     ```
     isql -k -v "Driver={Firebird};Uid=<Логин>;Pwd=<Пароль>;Dbname=<IP-адрес>/<Порт>:<Путь к файлу БД>;"
     ```

     Например:

     ```
     isql -k -v "Driver={Firebird};Uid=SIEM_user;Pwd=P@ssw0rd;Dbname=10.10.10.10/3050:C:\Bastion\Data\BPROT.GDB;"
     ```

     При успешном подключении появится сообщение `Connected`.

Для СУБД Microsoft SQL Server

- Чтобы установить ODBC-драйвер:

  1. Добавьте репозиторий для Debian 10:

     ```
     curl https://packages.microsoft.com/keys/microsoft.asc | apt-key add -
     curl https://packages.microsoft.com/config/debian/10/prod.list > /etc/apt/sources.list.d/mssql-release.list
     ```

Примечание. При установке в Astra Linux вы также можете использовать репозиторий для Debian версии 10 или выше.

2. Установите ODBC-драйвер:
```
apt-get update
ACCEPT_EULA=Y apt-get install -y msodbcsql17
```
3. Установите инструменты командной строки bcp и sqlcmd:
```
ACCEPT_EULA=Y apt-get install -y mssql-tools
echo 'export PATH="$PATH:/opt/mssql-tools/bin"' >> ~/.bashrc
source ~/.bashrc
```
4. Установите дополнительные компоненты:
```
apt-get install -y unixodbc-dev
apt-get install -y libgssapi-krb5-2
```
5. Если требуется, проверьте подключение к СУБД:
```
isql -vv -k "Driver={ODBC Driver 17 for SQL Server};Server=<IP-адрес>;Database=<Название БД>;Uid=<Логин>;Pwd=<Пароль>;"
```
При успешном подключении появится сообщение `Connected`.

Для СУБД MySQL

- Чтобы установить ODBC-драйвер:

1. Скачайте с сайта mysql.com, распакуйте и установите ODBC-драйвер, например:
```
wget https://dev.mysql.com/get/Downloads/Connector-ODBC/5.3/mysql-connector-odbc-5.3.14-linux-glibc2.12-x86-64bit.tar.gz -O - | tar -xz
```
2. Откройте файл `/etc/odbcinst.ini`.
3. Добавьте в файл строки, указав в параметре `Driver` пути к файлам ODBC-драйвера.

   Например:
```
[MySQL ODBC 5.3 Unicode Driver]
Driver=/root/mysql-connector-odbc-5.3.14-linux-glibc2.12-x86-64bit/lib/libmyodbc5w.so
UsageCount=1
[MySQL ODBC 5.3 ANSI Driver]
Driver=/root/mysql-connector-odbc-5.3.14-linux-glibc2.12-x86-64bit/lib/libmyodbc5a.so
UsageCount=1
```
4. Сохраните изменения и закройте файл.
5. Если требуется, проверьте подключение к СУБД:
```
isql -v -k "Driver={MySQL ODBC 5.3 ANSI Driver};Server=<IP-адрес>;Port=<Порт>;User=<Логин>;Password=<Пароль>;Charset=utf8;Option=3;"
```
   Например:
```
isql -v -k "Driver={MySQL ODBC 5.3 ANSI Driver};Server=10.0.10.10;Port=3306;User=SIEM_user;Password=P@ssw0rd;Charset=utf8;Option=3;"
```
   При успешном подключении появится сообщение `Connected`.

Для СУБД Oracle Database

- Чтобы установить ODBC-драйвер:

  1. Скачайте с сайта oracle.com, распакуйте и установите набор инструментов разработчика Oracle Instant Client:

     ```
     mkdir oracle
     wget https://download.oracle.com/otn_software/linux/instantclient/217000/instantclient-basiclite-linux.x64-21.7.0.0.0dbru.zip
     unzip instantclient-basiclite-linux.x64-21.7.0.0.0dbru.zip -d oracle
     ```

  2. Скачайте с сайта oracle.com, распакуйте и установите ODBC-драйвер:

     ```
     wget https://download.oracle.com/otn_software/linux/instantclient/217000/instantclient-odbc-linux.x64-21.7.0.0.0dbru.zip
     unzip instantclient-odbc-linux.x64-21.7.0.0.0dbru.zip -d oracle
     ```

  3. Настройте ODBC-драйвер:

     ```
     cd oracle/instantclient_21_7/
     ./odbc_update_ini.sh /
     ```

     Примечание. Вы можете не обращать внимания на предупреждение `ODBCINI environment variable not set, defaulting it to HOME directory.`

     ```
     echo "/root/oracle/instantclient_21_7" >> /etc/ld.so.conf.d/oracle_odbc.conf
     ldconfig
     cd ~
     ```

  4. Если требуется, проверьте подключение к СУБД:

     ```
     isql -v -k "Driver={Oracle 21 ODBC driver};Dbq=<IP-адрес>:<Порт>/<Идентификатор системы>;Uid=<Логин>;Pwd=<Пароль>"
     ```

     Например:

     ```
     isql -v -k "Driver={Oracle 21 ODBC driver};Dbq=10.10.10.10:1521/ORCL;Uid=SIEM_user;Pwd=Passw0rd"
     ```

     При успешном подключении появится сообщение `Connected`.

Для СУБД PostgreSQL

- Чтобы установить ODBC-драйвер:

  1. Скачайте с сайта postgresql.org и установите ODBC-драйвер:

     ```
     apt install odbc-postgresql
     ```

  2. Откройте файл `/etc/odbcinst.ini`.

  3. Укажите в соответствующих секциях в параметрах `Driver` пути к файлам ODBC-драйвера, например:

     ```
     [PostgreSQL Unicode]
     Driver=/usr/lib/x86_64-linux-gnu/odbc/psqlodbcw.so
     [PostgreSQL ANSI]
     Driver=/usr/lib/x86_64-linux-gnu/odbc/psqlodbca.so
     ```

4. Сохраните изменения и закройте файл.
5. Если требуется, проверьте подключение к СУБД:

   ```
   isql -v -k "Driver={PostgreSQL Unicode};Server=<IP-
   адрес>;Port=<Порт>;Uid=<Логин>;Pwd=<Пароль>;Database=<Название
   БД>;sslmode=prefer;pqopt={keepalives=1 keepalives_idle=5 keepalives_count=1
   keepalives_interval=1};"
   ```

   Например:

   ```
   isql -v -k "Driver={PostgreSQL
   Unicode};Server=10.10.10.10;Port=5432;Uid=SIEM_user;Pwd=P@ssw0rd;Database=drwcs;sslmode=pr
   efer;pqopt={keepalives=1 keepalives_idle=5 keepalives_count=1 keepalives_interval=1};"
   ```

   При успешном подключении появится сообщение `Connected`.

Для СУБД ClickHouse

- Чтобы установить ODBC-драйвер:

1. Скачайте с сайта github.com архив `clickhouse-odbc-1.1.10-linux.tar.gz` с ODBC-драйвером версии 1.1.10.20210822.
2. Распакуйте полученный архив:

   ```
   tar -xf clickhouse-odbc-1.1.10-Linux.tar.gz
   ```

3. Перенесите файлы `libclickhouseodbc.so` и `libclickhouseodbcw.so` из полученного каталога `/clickhouse-odbc-1.1.10-Linux/lib64/` в каталог для установки, например `/var/lib/clickhouse-odbc/`:

   ```
   sudo mv clickhouse-odbc-1.1.10-Linux/lib64/* /var/lib/clickhouse-odbc/
   ```

4. Перенесите файлы `clickhouse-odbc.tdc.sample`, `odbc.ini.sample` и `odbcinst.ini.sample` из полученного каталога `/clickhouse-odbc-1.1.10-Linux/share/doc/clickhouse-odbc/config/` в каталог для установки, например `/var/lib/clickhouse-odbc/doc/`:

   ```
   sudo mv clickhouse-odbc-1.1.10-Linux/share/doc/clickhouse-odbc/config/* /var/lib/
   clickhouse-odbc/doc/
   ```

5. Откройте на редактирование файл `/var/lib/clickhouse-odbc/doc/odbcinst.ini.sample`.
6. Добавьте в файл строки:

   ```
   [ClickHouse ODBC Driver (ANSI)]
      Driver = /var/lib/clickhouse-odbc/libclickhouseodbc.so
      Setup = /var/lib/clickhouse-odbc/libclickhouseodbc.so
   [ClickHouse ODBC Driver (Unicode)]
      Driver = /var/lib/clickhouse-odbc/libclickhouseodbcw.so
      Setup = /var/lib/clickhouse-odbc/libclickhouseodbcw.so
   ```

7. Сохраните изменения и закройте файл.
8. Выполните команду:

   ```
   sudo apt install openssl unixodbc
   ```

9. Зарегистрируйте драйвер:
   ```
   sudo odbcinst -i -d -f /var/lib/clickhouse-odbc/doc/odbcinst.ini.sample
   sudo odbcinst -i -s -l -f /var/lib/clickhouse-odbc/doc/odbc.ini.sample
   ```
10. В конфигурационном файле `core-agent.conf` укажите путь к каталогу с библиотеками:
    ```
    sudo echo /usr/local/lib > /etc/ld.so.conf.d/core-agent.conf && ldconfig
    ```
11. Если драйвер устанавливается на Astra Linux, установите пакет execstack и отключите запрет на использование исполняемого стека для драйвера:
    ```
    sudo apt install execstack
    sudo execstack -c /usr/local/lib64/libclickhouseodbc.so
    ```

17.2.5. Настройка политики control для команд su и sudo в операционной системе «Альт»

Внимание! Настройку политики нужно выполнять от имени учетной записи root.

Настройка политики для команды su

- Чтобы настроить политику control для команды `su` в операционной системе «Альт»:

1. Получите текущее значение политики:
   ```
   control su status
   ```
2. В зависимости от полученного значения выполните команды:
   - Если отобразилось значение `restricted`, выполните одну из следующих команд:

     – если вы хотите, чтобы все пользователи могли использовать команду `su`, выполните команду `control su public`;

     – если вы хотите, чтобы только пользователи группы wheel могли использовать команду `su`, выполните команду `control su wheelonly`, а затем `usermod -aG wheel <Логин>`;

     – если вы хотите, чтобы все пользователи могли использовать команду `su`, но только пользователи группы wheel могли переключаться на суперпользователя, выполните команду `control su wheel`, а затем `usermod -aG wheel <Логин>`.
   - Если отобразилось значение `wheelonly` или `wheel`:
     ```
     usermod -aG wheel <Логин>
     ```
   - Если отобразилось значение `public`, дополнительных действий не требуется.

Настройка политики для команды sudo

- Чтобы настроить политику control для команды `sudo` в операционной системе «Альт»:

  1. Получите текущее значение политики:
     `control sudo status`
  2. В зависимости от полученного значения выполните команды:
     - Если отобразилось значение `restricted`, выполните одну из следующих команд:

       – если вы хотите, чтобы все пользователи могли использовать команду `sudo`, выполните команду `control sudo public`;

       – если вы хотите, чтобы только пользователи группы wheel могли использовать команду `sudo`, выполните команду `control sudo wheelonly`, а затем `usermod -aG wheel <Логин>`.
     - Если отобразилось значение `wheelonly`:
       `usermod -aG wheel <Логин>`
     - Если отобразилось значение `public`, дополнительных действий не требуется.

17.2.6. Настройка уровня целостности для учетной записи в Astra Linux Special Edition

Внимание! Настройку нужно выполнять от имени учетной записи root.

- Чтобы настроить уровень целостности в Astra Linux Special Edition:

  1. Получите значение максимального уровня целостности:
     `cat /sys/module/parsec/parameters/max_ilev`
  2. Задайте полученное значение для требуемого пользователя:
     `pdpl-user -i <Значение> <Логин>`

17.3. 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

17.3.1. 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 группы.
6. Нажмите кнопку **ОК**.

Доменная группа пользователей создана.

17.3.2. 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**.
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.
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**.
11. Нажмите кнопку **Далее**.
12. Нажмите кнопку **Готово**.

Доменная учетная запись создана.

17.3.3. 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.
9. Нажмите кнопку **ОК**.
10. В списке **Член групп** выберите добавленную группу и нажмите кнопку **Задать основную группу**.
11. В списке **Член групп** выберите группу Domain Users и нажмите кнопку **Удалить**.
12. В окне **Свойства: <Логин>** нажмите кнопку **ОК**.

Учетная запись добавлена в доменную группу пользователей.

17.3.4. 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**.
4. В главном меню выберите **Действие** → **Создать**.

   Откроется окно **Новый объект групповой политики**.

5. В поле **Имя** введите имя групповой политики.
6. Нажмите кнопку **ОК**.

Групповая политика создана.

17.3.5. 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**.
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.

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.

17.3.6. 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**.
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.
13. Нажмите кнопку **ОК**.
14. В раскрывающемся списке **Применяется к** выберите **Этот объект**.
15. Нажмите ссылку **Отображение дополнительных разрешений**.
16. Установите флажки **Уведомление**, **Чтение разрешений**.
17. Нажмите кнопку **ОК**.
18. В окне **Дополнительные параметры безопасности для "MACHINE"** нажмите кнопку **ОК**.
19. В окне **Безопасность базы данных для MACHINE** нажмите кнопку **ОК**.
20. В окне **Добавление объекта** нажмите кнопку **ОК**.

Групповая политика для раздела реестра настроена.

17.3.7. 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 данные.
4. В главном меню выберите **Действие** → **Связать существующий объект групповой политики**.

   Откроется окно **Выбор объекта групповой политики**.
5. В списке **Объекты групповой политики** выберите созданную для объекта политику.
6. Нажмите кнопку **ОК**.

Групповая политика назначена.

17.4. Использование различных учетных записей для сбора данных из Windows

Внимание! До начала сканирования требуется включить или отключить функцию DCOM Hardening на сканирующем и сканируемом узлах. Подробности см. на сайтах support.microsoft.com и msrc.microsoft.com. Также рекомендуется установить все обновления ОС на всех узлах, участвующих в сканировании.

Для сбора данных на активах могут использоваться следующие учетные записи:

— встроенная локальная учетная запись администратора;

— локальная учетная запись, включенная в группу локальных администраторов;

— локальная учетная запись, не включенная в группу локальных администраторов;

— доменная учетная запись, включенная в группу локальных администраторов;

— доменная учетная запись, не включенная в группу локальных администраторов.

Уровень привилегий учетной записи влияет на результаты сбора данных. Например, учетная запись администратора имеет доступ к административным сетевым папкам (например, C$ или Admin$) и пользовательским подразделам в HKEY_USERS в реестре Windows, тогда как у учетной записи обычного пользователя такого доступа нет.

Сбор данных через WMI может выполняться с узлов, которые находятся в домене или в рабочей группе.

Для сбора данных с узла, который находится в рабочей группе, нужно использовать локальную учетную запись этого узла. При этом результаты сбора могут быть неполными из-за влияния функции UAC (контроль учетных записей пользователей). Допустимые значения параметров UAC при сборе данных различными учетными записями приведены в таблице ниже.

Таблица 5. Значения параметров UAC для учетных записей

Учетная запись	EnableLUA	FilterAdministratorToken	LocalAccountTokenFilterPolicy
Встроенная локальная учетная запись администратора	1	0; параметр отсутствует	0; параметр отсутствует
Локальная учетная запись, включенная в группу локальных администраторов	1	0; параметр отсутствует	1

Учетная запись	EnableLUA	FilterAdministratorToken	LocalAccountTokenFilterPolicy
Локальная учетная запись, не включенная в группу локальных администраторов	1	0; параметр отсутствует	1
Доменная учетная запись, включенная в группу локальных администраторов	1	0; параметр отсутствует	Любое; 0 или параметр отсутствует — при сборе данных с контроллера домена
Доменная учетная запись, не включенная в группу локальных администраторов	Любое	Любое	Любое

UAC не влияет на сбор данных при использовании встроенной локальной учетной записи администратора на контроллере домена.

Если сбор данных выполняется не от имени доменной учетной записи, включенной в группу локальных администраторов, следует отключить сетевые ограничения UAC (см. раздел 17.4.1).

Если UAC невозможно отключить из-за политики безопасности компании, необходимо выполнить следующие действия:

1. Настроить контроль учетных записей (см. раздел 17.4.2) (в параметре LocalAccountTokenFilterPolicy указать значение 0);
2. Выдать учетной записи разрешения на удаленный запуск и удаленную активацию (см. раздел 17.5.1) COM-приложений.
3. Выдать учетной записи разрешения (см. раздел 17.5.3) на удаленный запуск и удаленную активацию службы WMI.
4. Добавить следующие разрешения для учетной записи в пространство Root и все его дочерние пространства: «Выполнение методов», «Включить учетную запись» и «Включить удаленно».

В этом разделе

Отключение контроля учетных записей (UAC) (см. раздел 17.4.1)

Настройка контроля локальных учетных записей (UAC) (см. раздел 17.4.2)

Настройка учетной записи, не включенной в группу локальных администраторов (см. раздел 17.4.3)

См. также

Использование доменной учетной записи для доступа к реестру Windows (см. раздел 17.3)

17.4.1. Отключение контроля учетных записей (UAC)

Если сбор данных выполняется не от доменной учетной записи, включенной в группу локальных администраторов, необходимо отключить сетевые ограничения UAC.

> **Примечание.** Если UAC невозможно отключить из-за политики компании, необходимо выполнить дополнительные действия (см. раздел 17.4) при настройке учетной записи. Результаты сбора данных при этом будут неполными.

- Чтобы отключить контроль учетных записей:

1. Нажмите **Пуск** → **Выполнить**.
2. В поле **Открыть** введите `regedit` и нажмите **OK**.

   Откроется окно **Редактор реестра**.
3. В иерархическом списке выберите **Компьютер** → **HKEY_LOCAL_MACHINE** → **SOFTWARE** → **Microsoft** → **Windows** → **CurrentVersion** → **Policies** → **System**.
4. В главном меню в разделе **Правка** выберите пункт **Создать** → **Параметр DWORD (32 бита)** и введите имя параметра `LocalAccountTokenFilterPolicy`.
5. В главном меню выберите **Правка** → **Изменить**.

   Откроется окно **Изменение параметра DWORD (32 бита)**.
6. В блоке параметров **Система исчисления** выберите вариант **Десятичная**.
7. В поле **Значение** введите `1` и нажмите кнопку **OK**.

Контроль учетных записей отключен.

17.4.2. Настройка контроля локальных учетных записей (UAC)

Настройка выполняется для следующих учетных записей:

— встроенная локальная учетная запись администратора;

— локальная учетная запись, включенная в группу локальных администраторов;

— локальная учетная запись, не включенная в группу локальных администраторов.

- Чтобы настроить контроль локальных учетных записей:

1. Нажмите **Пуск** → **Выполнить**.
2. В поле **Открыть** введите `regedit` и нажмите **OK**.

Откроется окно **Редактор реестра**.

3. В иерархическом списке выберите **Компьютер** → **HKEY_LOCAL_MACHINE** → **SOFTWARE** → **Microsoft** → **Windows** → **CurrentVersion** → **Policies** → **System**.
4. В контекстом меню объекта **EnableLUA** выберите пункт **Изменить**.

   Откроется окно **Изменение параметра DWORD (32 бита)**.
5. В поле **Значение** введите `1` и нажмите кнопку **OK**.
6. В контекстом меню объекта **FilterAdministratorToken** выберите пункт **Изменить**.

   Откроется окно **Изменение параметра DWORD (32 бита)**.
7. В поле **Значение** укажите `0` и нажмите кнопку **OK**.
8. В контекстом меню объекта **LocalAccountTokenFilterPolicy** выберите пункт **Изменить**.

   Откроется окно **Изменение параметра DWORD (32 бита)**.
9. Если используется локальная учетная запись без повышенных привилегий, независимо от того, включена ли она в локальную группу администраторов, то в поле **Значение** укажите `1`.

   Внимание! Для локальной учетной записи, не включенной в группу локальных администраторов, результаты сбора данных будут неполными. Для этой УЗ необходимо выполнить дополнительную настройку (см. раздел 17.4.3).
10. Если используется локальная учетная запись администратора, то в поле **Значение** укажите `0`.
11. Нажмите кнопку **OK**.
12. Перезагрузите узел.

Контроль локальных учетных записей настроен.

17.4.3. Настройка учетной записи, не включенной в группу локальных администраторов

Внимание! При использовании учетной записи, не включенной в группу локальных администраторов, результаты сбора данных будут неполными.

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. Используются TCP-порты 135 и 445 и динамические TCP-порты 49152—65535.

До начала сканирования рекомендуется установить все обновления ОС на всех узлах, участвующих в сканировании.

Для сканирования с использованием локальной или доменной учетной записи, не включенной в группу локальных администраторов, нужно:

1. Настроить контроль локальных учетных записей (см. раздел 17.4.2) (для доменной учетной записи настройка не требуется).
2. Настроить для группы пользователей «Анонимный вход» разрешения на локальный и удаленный доступ к COM-приложениям (см. раздел 17.5.2).
3. Настроить для учетной записи разрешения на удаленный запуск и удаленную активацию COM-приложений (см. раздел 17.5.2).
4. Настроить для учетной записи разрешения на удаленный запуск и удаленную активацию (см. раздел 17.5.3) службы WMI.
5. Добавить разрешения для учетной записи во все пространства имен WMI.
6. Выдать права доступа на чтение содержимого и запись в папку `%systemroot%\Temp` (например, `c:\windows\temp`).
7. Настроить диспетчер управления службами (см. раздел 17.4.3.1) (Service Control Manager, SCM).
8. Выдать учетной записи разрешение на чтение следующих разделов реестра:

   HKEY_CURRENT_USER\Environment;

   HKEY_CURRENT_USER\SOFTWARE;

   HKEY_LOCAL_MACHINE\SOFTWARE;

   HKEY_LOCAL_MACHINE\SOFTWARE\Classes\AppID;

   HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node;

   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet.
9. Настроить полный доступ (см. раздел 17.4.3.2) к реестру службы установки модулей ОС (TrustedInstaller).
10. Выдать учетной записи разрешения (см. раздел 17.4.3.3) к службе установки модулей ОС.
11. Добавить учетную запись в локальную группу пользователей «Операторы архива» (см. раздел 17.1.4).
12. Добавить учетную запись или группу, в которой она состоит, в локальную политику безопасности «Доступ к компьютеру из сети» (см. раздел 17.1.3).
13. Удалить учетную запись из локальной политики безопасности «Запретить вход в систему через службу удаленных рабочих столов», если она состоит в ней.
14. Выполнить команду `net share` и убедиться, что общие административные ресурсы Admin$, C$ и IPC$ активны.

15. Запустить службу «Удаленный реестр».
16. Включить компонент «Общий доступ к файлам и принтерам для сетей Microsoft» для сетевого адаптера.

В этом разделе

Настройка диспетчера управления службами (SCM) (см. раздел 17.4.3.1)

Настройка доступа к реестру службы установки модулей ОС (TrustedInstaller) (см. раздел 17.4.3.2)

Добавление разрешений к службе установки модулей ОС (см. раздел 17.4.3.3)

17.4.3.1. Настройка диспетчера управления службами (SCM)

- Чтобы настроить диспетчер управления службами:

  1. Нажмите **Пуск** → **Выполнить**.
  2. В поле **Открыть** введите `cmd` и нажмите **ОК**.

     Откроется интерфейс командной строки.
  3. Получите текущий дескриптор безопасности (SDDL) диспетчера управления службами:
     ```
     sc sdshow scmanager > c:\1.txt
     ```
  4. Выполните команду:
     ```
     wmic useraccount get name,sid
     ```
     Откроется список идентификаторов безопасности (SID) учетных записей.
  5. Сохраните идентификатор учетной записи для доступа MP 10 Collector.
  6. Откройте файл `1.txt`.
  7. Перед группой параметров `S:(<Значения>)` добавьте значение:
     ```
     (A;;CCLCRPRC;;;<Идентификатор безопасности (SID) учетной записи>)
     ```
  8. Сохраните и закройте файл.
  9. Выполните команду:
     ```
     sc sdset scmanager "<Все строки из файла 1.txt>"
     ```

  Диспетчер управления службами настроен.

17.4.3.2. Настройка доступа к реестру службы установки модулей ОС (TrustedInstaller)

- Чтобы настроить доступ к реестру:

  1. Нажмите **Пуск** → **Выполнить**.
  2. В поле **Открыть** введите `regedit` и нажмите **ОК**.

     Откроется окно **Редактор реестра**.
  3. В иерархическом списке выберите **Компьютер** → **HKEY_LOCAL_MACHINE** → **SOFTWARE** → **Classes** → **AppID** → **{752073A2-23F2-4396-85F0-8FDB879ED0ED}**.
  4. В главном меню в разделе **Правка** выберите пункт **Разрешения**.

     Откроется окно **Разрешения для группы {752073A2-23F2-4396-85F0-8FDB879ED0ED}**.
  5. Выберите пользователя, от имени которого выполняются текущие действия, и в столбце **Разрешения** установите флажок **Полный доступ**.
  6. Нажмите кнопку **Применить**.
  7. В иерархическом списке выберите **Компьютер** → **HKEY_LOCAL_MACHINE** → **SYSTEM** → **CurrentControlSet** → **Control** → **SecurePipeServers** → **winreg**.
  8. В главном меню в разделе **Правка** выберите пункт **Разрешения**.

     Откроется окно **Разрешения для группы winreg**.
  9. Выберите группу **Local Service** и в столбце **Разрешения** установите флажок **Чтение**.
  10. Нажмите кнопку **ОК**.

17.4.3.3. Добавление разрешений к службе установки модулей ОС

- Чтобы добавить разрешения к службе установки модулей ОС:

  1. Нажмите **Пуск** → **Выполнить**.
  2. В поле **Открыть** введите `dcomcnfg` и нажмите кнопку **ОК**.

     Откроется окно **Службы компонентов**.
  3. Выберите узел **Корень консоли** → **Службы компонентов** → **Компьютеры** → **Мой компьютер** → **Настройка DCOM** → **Trusted Installer service**.
  4. В главном меню выберите **Действие** → **Свойства**.

     Откроется окно **Свойства: Trusted Installer service**.

5. Выберите вкладку **Безопасность**.
6. В блоке параметров **Разрешения на запуск и активацию** нажмите **Изменить**.

   Откроется окно **Разрешение на запуск и активацию**.
7. Выберите учетную запись и в столбце **Разрешить** установите все флажки.
8. Нажмите кнопку **ОК**.
9. В блоке параметров **Разрешения на доступ** нажмите **Изменить**.

   Откроется окно **Разрешение на доступ**.
10. Выберите учетную запись и в столбце **Разрешить** установите все флажки.
11. Нажмите кнопку **ОК**.

17.5. Настройка подключения к службе WMI

В этом разделе приводятся инструкции для настройки учетных записей Windows, используемых для сбора данных через службу Windows Management Instrumentation (WMI).

В этом разделе

17.5.1. Настройка службы DCOM

- Чтобы настроить службу DCOM:

  1. Нажмите **Пуск** → **Выполнить**.
  2. В поле **Открыть** введите `dcomcnfg` и нажмите кнопку **ОК**.

     Откроется окно **Службы компонентов**.
  3. Выберите узел **Службы компонентов** → **Компьютеры** → **Мой компьютер**.
  4. В главном меню выберите **Действие** → **Свойства**.

     Откроется окно **Свойства: Мой компьютер**.
  5. Выберите вкладку **Свойства по умолчанию**.

6. Установите флажок **Разрешить использование DCOM на этом компьютере**.
7. В раскрывающемся списке **Уровень проверки подлинности по умолчанию** выберите **Подключиться**.
8. В раскрывающемся списке **Уровень олицетворения по умолчанию** выберите **Определить**.
9. Выберите вкладку **Набор протоколов** и в блоке параметров **Протоколы DCOM** нажмите **Добавить**.

   Откроется окно **Выбор протокола DCOM**.
10. В раскрывающемся списке **Последовательность протоколов** выберите **TCP/IP с ориентацией на подключения**.
11. Нажмите кнопку **OK**.
12. Выберите вкладку **MSDTC** и установите флажок **Использовать локальный координатор**.
13. Нажмите кнопку **OK**.

Служба DCOM настроена.

17.5.2. Настройка разрешений для COM-приложений

► Чтобы настроить разрешения для COM-приложений:

1. Нажмите **Пуск** → **Выполнить**.
2. В поле **Открыть** введите `dcomcnfg` и нажмите кнопку **OK**.

   Откроется окно **Службы компонентов**.
3. Выберите узел **Службы компонентов** → **Компьютеры** → **Мой компьютер**.
4. В главном меню выберите **Действие** → **Свойства**.

   Откроется окно **Свойства: Мой компьютер**.
5. Выберите вкладку **Безопасность COM**.
6. В блоке параметров **Права доступа** нажмите кнопку **Изменить ограничения**.

   Откроется окно **Разрешение на доступ**.
7. Выберите группу пользователей **Все** и в столбце **Разрешить** установите флажки **Локальный доступ** и **Удаленный доступ**.
8. Выберите группу **Все пакеты приложений** и в столбце **Разрешить** установите флажок **Локальный доступ**.
9. Выберите группу **Пользователи журналов производительности** и в столбце **Разрешить** установите флажки **Локальный доступ** и **Удаленный доступ**.

10. Выберите группу **Пользователи DCOM** и в столбце **Разрешить** установите флажки **Локальный доступ** и **Удаленный доступ**.
11. Выберите группу **Анонимный вход** и в столбце **Разрешить** установите флажки **Локальный доступ** и **Удаленный доступ**.
12. Нажмите кнопку **OK**.
13. В области **Разрешения на запуск и активацию** нажмите кнопку **Изменить ограничения**.

    Откроется окно **Разрешение на запуск и активацию**.
14. Выберите группу пользователей **Все** и в столбце **Разрешить** установите флажки **Локальный запуск** и **Локальная активация**.
15. Выберите группу **Все пакеты приложений** и в столбце **Разрешить** установите флажки **Локальный запуск** и **Локальная активация**.
16. Выберите группу **Администраторы** и в столбце **Разрешить** установите все флажки.
17. Выберите группу **Пользователи журналов производительности** и в столбце **Разрешить** установите все флажки.
18. Выберите группу **Пользователи DCOM** и в столбце **Разрешить** установите все флажки.
19. Нажмите кнопку **OK**.
20. В окне **Свойства: Мой компьютер** нажмите кнопку **OK**.

Разрешения для COM-приложений настроены.

17.5.3. Настройка разрешений для службы WMI

► Чтобы настроить разрешения для службы WMI:

1. Нажмите **Пуск** → **Выполнить**.
2. В поле **Открыть** введите `dcomcnfg` и нажмите кнопку **OK**.

   Откроется окно **Службы компонентов**.
3. Выберите узел **Службы компонентов** → **Компьютеры** → **Мой компьютер** → **Настройка DCOM** → **Windows Management and Instrumentation**.
4. В главном меню выберите **Действие** → **Свойства**.

   Откроется окно **Свойства: Windows Management and Instrumentation**.
5. В раскрывающемся списке **Уровень проверки подлинности** выберите **По умолчанию**.
6. Выберите вкладку **Размещение** и установите флажок **Запустить приложение на данном компьютере**.
7. Выберите вкладку **Безопасность**.

8. В блоке параметров **Разрешения на запуск и активацию** выберите вариант **Настроить** и нажмите кнопку **Изменить**.

   Откроется окно **Разрешение на запуск и активацию**.

9. Выберите группу пользователей **Прошедшие проверку** и в столбце **Разрешить** установите флажки **Локальный запуск**, **Локальная активация** и **Удаленная активация**.
10. Выберите группу **Администраторы** и в столбце **Разрешить** установите все флажки.
11. Нажмите кнопку **ОК**.
12. В блоке параметров **Разрешения на изменение настроек** выберите **Настроить** и нажмите кнопку **Изменить**.

    Откроется окно **Разрешение на изменение настройки**.

13. Выберите группу пользователей **Все пакеты приложений** и в столбце **Разрешить** установите флажок **Чтение**.
14. Выберите группу **Создатель-владелец** и в столбце **Разрешить** установите флажки **Полный доступ** и **Чтение**.
15. Выберите группу **Система** и в столбце **Разрешить** установите флажки **Полный доступ** и **Чтение**.
16. Выберите группу **Администраторы** и в столбце **Разрешить** установите флажки **Полный доступ** и **Чтение**.
17. Выберите группу **Пользователи** и в столбце **Разрешить** установите флажок **Чтение**.
18. Нажмите кнопку **ОК**.
19. Выберите вкладку **Конечные узлы**.
20. В блоке параметров **Протоколы и конечные узлы DCOM** удалите все строки, кроме **Системные протоколы по умолчанию**.
21. Нажмите кнопку **Применить**.
22. Выберите вкладку **Удостоверение** и выберите вариант **Системная учетная запись (только службы)**.
23. Нажмите кнопку **ОК**.

Разрешения для службы WMI настроены.

17.5.4. Настройка разрешений в пространстве имен WMI

► Чтобы настроить разрешения в пространстве имен WMI:

1. Нажмите **Пуск** → **Выполнить**.
2. В поле **Открыть** введите `mmc`.

3. Нажмите **ОК**.

   Откроется окно **Консоль1**.

4. В главном меню выберите **Файл** → **Добавить или удалить оснастку**.
5. В списке доступных оснасток выберите **Управление компьютером**.
6. Нажмите **Добавить**.
7. Выберите **локальным компьютером** и нажмите **Готово**.
8. Нажмите **ОК**.
9. Выберите узел **Корень консоли** → **Управление компьютером** → **Службы и приложения** → **Управляющий элемент WMI**.
10. В главном меню выберите **Действие** → **Свойства**.
11. Выберите вкладку **Безопасность**.
12. Выберите пространство имен **Root**.
13. Нажмите **Безопасность**.
14. Выполните одно из следующих действий:

- Если учетная запись включена в группу локальных администраторов, установите следующие флажки:

  Выполнение методов;

  Полная запись;

  Частичная запись;

  Запись поставщика;

  Включить учетную запись;

  Включить удаленно;

  Прочесть безопасность;

  Изменение правил безопасности.

- Если учетная запись не включена в группу локальных администраторов, нажмите **Дополнительно** → **Добавить** и выберите учетную запись или группу, установите тип **Разрешить**, примените его к данному пространству и подпространству имен, затем установите следующие флажки:

  Выполнение методов;

  Включить учетную запись;

  Включить удаленно;

Прочесть безопасность.

15. Нажмите **OK**.

Для пространств имен AccessLogging, InventoryLogging, PEH, RSOP и ServiceModel по умолчанию отключено наследование прав доступа. Для них необходимо выдать разрешения учетной записи или группе, аналогично настройке пространства имен Root.

Если на узле появляются новые пространства имен WMI (например, при обновлении системы или установке новой программы), необходимо убедиться, что у используемой для сбора данных учетной записи есть разрешения на новое пространство.

17.5.5. Настройка служб для сбора данных

- Чтобы настроить службы для сбора данных:

1. Нажмите **Пуск** → **Выполнить**.
2. В поле **Открыть** введите `services.msc` и нажмите кнопку **OK**.

   Откроется консоль управления службами.
3. Выберите службу **Инструментарий управления Windows**.
4. В главном меню выберите **Действие** → **Свойства**.

   Откроется окно **Свойства: Инструментарий управления Windows**.
5. В раскрывающемся списке **Тип запуска** выберите **Автоматически**.
6. Если служба находится в состоянии, отличном от **Выполняется**, нажмите кнопку **Запустить**.
7. Нажмите кнопку **Применить**.
8. Выберите вкладку **Вход в систему** и выберите вариант **С системной учетной записью**.
9. Нажмите кнопку **OK**.
10. Выберите службу **Модуль запуска процессов DCOM-сервера**.
11. В главном меню выберите **Действие** → **Свойства**.

    Откроется окно **Свойства: Модуль запуска процессов DCOM-сервера**.
12. В раскрывающемся списке **Тип запуска** выберите **Автоматически**.
13. Если служба находится в состоянии, отличном от **Выполняется**, нажмите кнопку **Запустить**.
14. Нажмите кнопку **OK**.
15. Выберите службу **Сопоставитель конечных точек RPC**.
16. В главном меню выберите **Действие** → **Свойства**.

Откроется окно **Свойства: Сопоставитель конечных точек RPC**.

17. В раскрывающемся списке **Тип запуска** выберите **Автоматически**.
18. Если служба находится в состоянии, отличном от **Выполняется**, нажмите кнопку **Запустить**.
19. Нажмите кнопку **OK**.

Службы для сбора данных настроены.

17.5.6. Настройка межсетевого экрана Windows

При использовании в IT-инфраструктуре организации межсетевого экрана Windows требуется настроить правило для удаленного взаимодействия со службой WMI.

Для процесса загрузки служб ОС (svchost.exe) необходимо разрешить исходящий трафик WMI с любого локального порта TCP на любой удаленный порт TCP.

Примечание. В операционных системах Windows Starter, Windows Home Basic и Windows Home Premium сетевое подключение недоступно.

► Чтобы настроить правило для входящего подключения WMI:

1. Нажмите **Пуск** → **Выполнить**.
2. В поле **Открыть** введите `firewall.cpl` и нажмите кнопку **OK**.

   Откроется окно **Брандмауэр Защитника Windows**.
3. Перейдите по ссылке **Дополнительные параметры**.

   Откроется окно **Монитор брандмауэра Защитника Windows в режиме повышенной безопасности**.
4. В иерархическом списке выберите **Монитор брандмауэра Защитника Windows в режиме повышенной безопасности включен Локальный компьютер** → **Правила для входящих подключений**.
5. В панели **Действия** нажмите кнопку **Создать правило**.

   Откроется окно **Мастер создания правила для нового входящего подключения**.
6. Выберите вариант **Предопределенные** и в раскрывающемся списке выберите **Инструментарий управления Windows (WMI)**.
7. Нажмите кнопку **Далее**.
8. В блоке параметров **Правила** установите все флажки.
9. Нажмите кнопку **Далее**.
10. Нажмите кнопку **Готово**.

Правило для входящего подключения WMI настроено.

17.5.7. Настройка фиксированного порта для WMI

Вы можете настроить службу WMI для запуска в качестве единственного процесса на узле с фиксированным портом.

Примечание. При необходимости вы можете проверить, какой порт использует WMI, с помощью команд `tasklist /svc /fi "services eq winmgmt"` и `netstat -ano | find "<Идентификатор процесса (PID)>"`.

- Чтобы настроить WMI с фиксированным портом:

  1. Нажмите **Пуск** → **Выполнить**.
  2. В поле **Открыть** введите `cmd` и нажмите **ОК**.

     Откроется интерфейс командной строки.
  3. Выполните команду:

     ```
     winmgmt -standalonehost
     ```

     Появится уведомление об успешном изменении конфигурации службы.
  4. Выполните команду:

     ```
     net stop winmgmt
     ```
  5. Выполните команду:

     ```
     net start winmgmt
     ```

     По умолчанию WMI будет использовать фиксированный порт — 24158.

  Примечание. Для отмены изменений вы можете выполнить команду `winmgmt /sharedhost`, а затем остановить и запустить службу WMI (winmgmt).

Смена фиксированного порта

Внимание! При использовании в IT-инфраструктуре организации межсетевого экрана Windows требуется настроить правило, разрешающее внешние подключения к указанному порту TCP.

- Чтобы сменить фиксированный порт для службы WMI:

  1. Нажмите **Пуск** → **Выполнить**.
  2. В поле **Открыть** введите `dcomcnfg` и нажмите кнопку **ОК**.

     Откроется окно **Службы компонентов**.
  3. Выберите узел **Службы компонентов** → **Компьютеры** → **Мой компьютер** → **Настройка DCOM** → **Windows Management and Instrumentation**.
  4. В главном меню выберите **Действие** → **Свойства**.

     Откроется окно **Свойства: Windows Management and Instrumentation**.

5. Выберите вкладку **Конечные узлы**.
6. Нажмите кнопку **Добавить**.

   Откроется окно **Выберите протокол DCOM и конечный узел**.
7. Выберите вариант **Использовать статический узел** и введите номер свободного порта.
8. Нажмите кнопку **OK**.
9. Откройте интерфейс командной строки и выполните команду:
   ```
   net stop winmgmt
   ```
10. Выполните команду:
    ```
    net start winmgmt
    ```

Фиксированный порт для службы WMI сменен.

17.6. Настройка доступа в СУБД Microsoft SQL Server

Внимание! При использовании на узле источника межсетевого экрана требуется настроить в нем правила, разрешающие внешние подключения к TCP-портам, используемым экземплярами Microsoft SQL Server. Для сканирования по имени экземпляра необходимо также настроить UDP-порт 1434.

Для настройки доступа MP 10 Collector к БД под управлением СУБД Microsoft SQL Server нужно:

1. Создать локальную (см. раздел 17.6.1) или доменную (см. раздел 17.6.3) учетную запись пользователя Windows.

   Примечание. Данные этой учетной записи нужно указать при добавлении учетной записи в MaxPatrol VM. Для коллекторов, установленных на Linux, необходимо использовать только доменную учетную запись с аутентификацией по протоколу Kerberos.

   Примечание. Вместо учетной записи пользователя Windows вы можете использовать учетную запись SQL Server Authentication.
2. Настроить локальную (см. раздел 17.6.2) или групповую (см. раздел 17.6.4) 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 17.6.5).
4. Настроить порты TCP/IP для подключения к СУБД (см. раздел 17.6.6).
5. Настроить автоматический запуск SQL Server Browser (см. раздел 17.6.7).

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

17.6.1. Создание учетной записи ОС

Внимание! Инструкция подходит только для сканирования коллекторами, установленными на Windows.

- 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**.
  4. В главном меню выберите **Действие** → **Новый пользователь**.
  5. В поле **Пользователь** введите логин учетной записи.
  6. Установите флажок **Запретить смену пароля пользователем**.
  7. Установите флажок **Срок действия пароля не ограничен**.
  8. Введите пароль и подтвердите его.
  9. Нажмите **Создать**.

17.6.2. 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**.
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 **ОК**.
10. В поле **Введите имена выбираемых объектов** введите имя учетной записи и нажмите кнопку **Проверить имена**.
11. Нажмите кнопку **ОК**.
12. В окне **Свойства: Доступ к компьютеру из сети** нажмите кнопку **ОК**.

Локальная политика безопасности настроена.

17.6.3. 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**.
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.
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**.

11. Нажмите кнопку **Далее**.
12. Нажмите кнопку **Готово**.

Доменная учетная запись создана.

17.6.4. 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**.
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.
10. Нажмите кнопку **ОК**.
11. В окне **Добавление пользователя или группы** нажмите кнопку **ОК**.
12. В окне **Свойства: Доступ к компьютеру из сети** нажмите кнопку **ОК**.

Групповая политика для удаленного доступа настроена.

17.6.5. 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**.

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**.

5. Выберите **Windows authentication** и нажмите кнопку **Search**.

   Откроется окно **Select User or Group**.

6. Нажмите **Locations**.

7. В открывшемся окне выберите:

   - если используется локальная учетная запись — имя узла;
   - если используется доменная учетная запись — имя домена.

8. Нажмите **OK**.

9. В поле **Enter the object name to select** введите логин созданной ранее учетной записи Windows и нажмите кнопку **Check Names**.

10. Нажмите **OK**.

11. В окне **Login — New** в раскрывающемся списке **Default database** выберите название БД источника.

    Примечание. Если вы планируете использовать для аутентификации учетную запись SQL Server, нужно выбрать **SQL Server authentication**, ввести и подтвердить пароль, а также снять флажки **Enforce password expiration** и **User must change password at next login**.

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**.

15. Нажмите **OK**.

17.6.6. 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**.
4. В контекстном меню протоколов передачи данных TCP/IP выберите пункт **Свойства**.
5. В открывшемся окне **Свойства: TCP/IP** выберите вкладку **IP Addresses**.
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.

17.6.7. 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**.
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**.
6. Выберите вкладку **Log On**.
7. Нажмите кнопку **Start** для запуска службы SQL Server Browser.
8. Нажмите кнопку **OK**.
9. Перезапустите СУБД.

Автоматический запуск службы SQL Server Browser настроен.

17.7. Стандартные операции в системах виртуализации VMware

Раздел содержит инструкции для стандартных операций, выполняемых в системах виртуализации VMware.

В этом разделе

17.7.1. Добавление учетной записи и назначение роли в VMware vCenter Server for Windows 5.5, 6.0

- Чтобы добавить учетную запись в VMware vCenter Server for Windows и назначить ей роль:

  1. Войдите в веб-интерфейс VMware vCenter Server for Windows от имени учетной записи с правами администратора.
  2. В иерархическом списке выберите узел сервера.
  3. Выберите вкладку **Manage**.
  4. Нажмите **Permissions**.
  5. В панели инструментов нажмите  .
  6. В открывшемся окне нажмите **Add**.
  7. Если используется доменная учетная запись, в раскрывающемся списке **Domain** выберите домен учетной записи.
  8. В списке выберите учетную запись и нажмите **Add**.
  9. Нажмите **OK**.
  10. В окне **<Имя сервера> — Change Role On Permissions** в раскрывающемся списке выберите **Read-only**.
  11. Нажмите **OK**.

17.7.2. Добавление учетной записи и назначение роли в VMware vCenter Server for Windows 6.5

- Чтобы добавить учетную запись в VMware vCenter Server for Windows и назначить ей роль:

  1. Войдите в веб-интерфейс VMware vCenter Server for Windows от имени учетной записи с правами администратора.
  2. В левой части страницы нажмите **Hosts and Clusters**.
  3. В иерархическом списке выберите узел сервера.
  4. Выберите вкладку **Permissions**.
  5. В панели инструментов вкладки нажмите  .
  6. В открывшемся окне нажмите **Add**.
  7. Если используется доменная учетная запись, в раскрывающемся списке **Domain** выберите домен.
  8. В списке выберите учетную запись и нажмите **Add**.
  9. Нажмите **OK**.
  10. В окне **<Имя сервера> — Add Permission** в раскрывающемся списке выберите **Read-only**.
  11. Нажмите **OK**.

17.7.3. Создание учетной записи для VMware vCenter Server Appliance 6.7—8.0

- Чтобы создать учетную запись для VMware vCenter Server Appliance:

  1. Войдите в веб-интерфейс VMware vCenter Server Appliance от имени учетной записи с правами администратора.
  2. Нажмите **Menu** → **Administration**.
  3. В левой части страницы выберите раздел **Single Sign On** → **Users and Groups**.
  4. Выберите вкладку **Users**.
  5. В раскрывающемся списке **Domain** выберите SSO-домен VMware vCenter (по умолчанию **vsphere.local**).
  6. Нажмите **ADD USER**.
  7. Введите логин учетной записи.

8. Введите пароль и подтвердите его.
9. Нажмите **ADD**.

17.7.4. Назначение роли учетной записи в VMware vCenter Server Appliance 6.7—8.0

- Чтобы назначить роль учетной записи:

1. Войдите в веб-интерфейс VMware vCenter Server Appliance от имени учетной записи с правами администратора.
2. В левой части страницы нажмите **Hosts and Clusters**.
3. В иерархическом списке выберите узел сервера.
4. Выберите вкладку **Permissions**.
5. В панели инструментов вкладки нажмите + .
6. В раскрывающемся списке **User** выберите домен и в поле ниже введите логин учетной записи.
7. В раскрывающемся списке **Role** выберите **Read-only**.
8. Установите флажок **Propagate to children**.
9. Нажмите **OK**.

18. Параметры модулей

Раздел содержит описание параметров работы модулей MP 10 Collector для сканирования активов.

В этом разделе

18.1. Модули для сбора информации об активах

Раздел содержит описание параметров модулей для сканирования активов, поиска и импорта информации об активах.

> **Внимание!** Если MP 10 Collector установлен на Linux, MaxPatrol VM не сможет выполнять поиск файлов в режиме пентеста. Использование протокола Kerberos доступно с ограничениями и зависит от профиля для сбора данных. Производительность MP 10 Collector, установленного на Linux, в режиме пентеста в целом на 15—40% ниже, чем установленного на Microsoft Windows.

В этом разделе

18.1.1. 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).

> **Внимание!** Для выполнения аудита Windows и Microsoft Active Directory с помощью MP 10 Collector, установленного на Linux, необходимо указывать полное доменное имя (FQDN) цели.
>
> **Примечание.** При сканировании по протоколу LDAP помощью MP 10 Collector, установленного на Linux, аутентификация по протоколу NTLM не поддерживается.

Для модуля созданы стандартные профили:

- **Checkpoint Management Server SSH Audit.** Для аудита сервера управления систем информационной безопасности Check Point GAIA или Check Point SPLAT 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. Собирает данные о версии и конфигурации СУБД Microsoft SQL.
- **Oracle Audit.** Для аудита СУБД Oracle Database. Собирает данные о версии и конфигурации 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 протоколу SSH. Профиль также может использоваться для сканирования устройств Cisco, не требующих повышения привилегий.
- **Unix SSH Audit.** Для аудита ОС семейства Unix и ПО, установленного на активах с такими ОС. Сканирование одного актива занимает до 5 минут.

  Примечание. При проведении аудита ОС семейства Unix с профилем Unix SSH 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.
- **Unix SSH and Web API Audit.** Для аудита ПО, установленного на активах с ОС семейства Unix. Сканирование осуществляется одновременно через веб-API и по протоколу SSH.
- **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 и ПО, установленного на активах под управлением Windows. Сканирование одного актива занимает до 15 минут. Собирает данные о приложениях и ОС, необходимые для поиска уязвимостей на узлах с Windows. Не выполняет аудит ресурсов службы каталогов Microsoft Active Directory.

  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 по протоколам LDAP и RPC.

— **Windows Updates Discovery.** Для обновления данных о приложениях и ОС, необходимых для поиска уязвимостей на узлах с Windows. Задачи с этим профилем собирают ограниченный объем информации. Сканирование одного актива занимает до 2 минут.

Также в состав модуля Audit входит встроенный модуль AuditCheck для проверки подключения к целевым активам и транспортам.

Настраивать параметры модуля вы можете при создании пользовательского профиля на базе стандартного или при создании задачи на сбор данных. Для этого в панели с параметрами профиля в иерархическом списке нужно выбрать секцию параметров. Ниже приводятся описания параметров в каждой секции.

По умолчанию для модуля Audit могут одновременно выполняться не больше 20 подзадач, а для встроенного модуля AuditCheck — не больше 40. Вы можете изменить это значение на странице **Управление системой** на вкладке **Коллекторы** в панели **Модули и потоки**.

В этом разделе

Сканирование систем — Check Point через OPSEC (см. раздел 18.1.1.1)

Сканирование систем — Microsoft SQL Server (см. раздел 18.1.1.2)

Сканирование систем — Oracle Database (см. раздел 18.1.1.3)

Сканирование систем — Oracle MySQL (см. раздел 18.1.1.4)

Сканирование систем — SAP через RFC (см. раздел 18.1.1.5)

Сканирование систем — VMware vSphere (см. раздел 18.1.1.6)

Сканирование систем — Windows (см. раздел 18.1.1.7)

Сканирование систем — По протоколу LDAP (см. раздел 18.1.1.8)

Сканирование систем — По протоколу SNMP (см. раздел 18.1.1.9)

Сканирование систем — Через веб-API (см. раздел 18.1.1.10)

18.1.1.1. 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).

18.1.1.2. 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 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.

18.1.1.3. 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).

18.1.1.4. 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.

18.1.1.5. 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 манданта клиента** — поле для ввода номера манданта 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.

18.1.1.6. 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.

18.1.1.7. 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).

18.1.1.8. 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.

— **Фильтр для объектов** — при включении для сбора данных используются поисковые фильтры LDAP. Доступна фильтрация групп, учетных записей и компьютеров. Условия фильтрации нужно указать самостоятельно, используя стандартный синтаксис поисковых запросов LDAP. Примеры фильтров для каждого вида объектов:

- `(&(objectCategory=group)(description=*))` — группы, у которых есть описание;
- `(&(objectCategory=person)(objectClass=user)(pwdLastSet=0))` — учетные записи, для которых не задан пароль;
- `(&(objectCategory=computer)(operatingSystem=*server*))` — компьютеры с операционной системой Windows Server.

18.1.1.9. 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.

18.1.1.10. 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.

18.1.1.11. 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).

— **Разделитель команд** — поле для ввода последовательности символов в конце каждой команды.

— **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. Если ни одной команды не добавлено, все команды считаются разрешенными. Для ввода команд нужно использовать только регулярные выражения. Если в секции 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. Для ввода команд нужно использовать только регулярные выражения. Если в секцию добавлена выполняемая команда, 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.

18.1.1.12. Дополнительные параметры модуля Audit

В этом разделе описаны дополнительные параметры профиля модуля сканирования данных.

Особенности сканирования систем

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.

Область сбора данных

Секция содержит параметр **Частичный сбор данных** для отладки сбора данных об активах. При его 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.

— **По идентификаторам проверок** — фильтрация данных при заполнении модели активов выполняется по указанным идентификаторам проверок. Для этого вида сканирования доступен параметр **Идентификаторы проверок**: по кнопке **Добавить** вы можете добавить поля для ввода идентификаторов проверок, выполняемых при частичном сканировании.

Объем занимаемой памяти

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).

Работа модуля

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 18.3).

— **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).

Отправка данных в систему

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.

Отладка сканирования

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.

18.1.1.13. Расширение сбора данных

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 SSH Audit.

18.1.2. Модуль AuditPLC

Модуль предназначен для диагностики программируемых логических контроллеров (ПЛК) с подключением по протоколам S7COMM (S7ISO и S7TCP), SNMP и UMAS.

Для модуля созданы стандартные профили:

— S7ISO AuditPLC;

— S7TCP AuditPLC;

— SNMP AuditPLC;

— SNMP and S7TCP AuditPLC;

— SNMP and UMAS AuditPLC;

— UMAS AuditPLC.

Сканирование ПЛК по протоколу S7COMM

Протокол S7COMM предназначен для обмена данными с ПЛК производства Siemens. MaxPatrol VM поддерживает две версии протокола S7COMM: S7ISO для сканирования по сетевому протоколу ISO и S7TCP для сканирования по протоколу TCP.

Для сканирования ПЛК по протоколу S7COMM при создании задачи на сбор данных можно выбрать профиль S7ISO AuditPLC или S7TCP AuditPLC. Секция содержит раскрывающийся список для выбора сетевого протокола.

Если выбран сетевой протокол ISO, нужно указать следующие параметры:

— **Сетевой интерфейс** — поле для ввода имени сетевого интерфейса, по которому узел MP 10 Collector подключен к ПЛК. Если узел работает под управлением Linux, список сетевых интерфейсов можно получить с помощью команды `netstat -i`. На узле под управлением Windows список сетевых интерфейсов можно получить с помощью команды Windows Powershell `Get-NetAdapter`.

  Внимание! При сканировании по протоколу S7ISO необходимо выбрать подключение к активам по FQDN, а в качестве цели указать MAC-адреса ПЛК.

— **Тайм-аут ответа** — поле для ввода времени ожидания ответа ПЛК в секундах.

Если выбран сетевой протокол TCP, нужно указать следующие параметры:

— **Порт** — поле для ввода номера TCP-порта ПЛК.

— **Тайм-аут ответа** — поле для ввода времени ожидания ответа ПЛК в секундах.

Сканирование ПЛК по протоколу SNMP

Секция содержит раскрывающийся список для выбора версии протокола SNMP.

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.

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**.

Блок дополнительных параметров сбора данных 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.

Сканирование ПЛК по протоколу UMAS

Протокол UMAS предназначен для обмена данными с ПЛК производства Schneider Electric. Для сканирования ПЛК по протоколу UMAS достаточно указать время ожидания ответа от ПЛК в поле **Тайм-аут ответа**. Время ожидания по умолчанию — 3 секунды.

Дополнительные параметры

Дополнительные параметры модуля AuditPLC аналогичны параметрам модуля Audit. Подробности см. в разделах «Область сбора данных (дополнительные параметры)», «Объем занимаемой памяти (дополнительные параметры)», «Работа модуля (дополнительные параметры)», «Отправка данных в систему (дополнительные параметры)» и «Отладка сканирования (дополнительные параметры)».

18.1.3. 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, не предназначен для поиска уязвимостей. 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. Сканирование одного актива занимает до 5 минут.

— **Inventory Profile.** Для поиска активов. Актив обнаруживается по открытым на нем TCP-портам или ответу на запрос по протоколу ICMP. Профиль не определяет FQDN актива вне зависимости от того, указан для этого актива IP-адрес или FQDN.

— **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. Профиль не определяет FQDN актива вне зависимости от того, указан для этого актива IP-адрес или FQDN.

  Примечание. Все ОС семейства Linux определяются, как Linux с указанием диапазона версий ядра системы.

Внимание! Не рекомендуется использовать этот профиль для сканирования сетей, в которых установлены средства защиты (например, межсетевой экран) и любые сетевые устройства, которые изменяют TCP-заголовки пакетов, так как они могут препятствовать корректному определению ОС.

— **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 при создании задачи на сбор данных. Для этого в панели с параметрами профиля в иерархическом списке нужно выбрать секцию параметров. Ниже приводятся описания параметров в каждой секции.

По умолчанию для модуля HostDiscovery может одновременно выполняться не больше одной подзадачи. Вы можете изменить это значение на странице **Управление системой** на вкладке **Коллекторы** в панели **Модули и потоки**.

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.

Параметры проверки узлов

Секция содержит следующие параметры для настройки проверок портов:

- **Присваивать активам значения FQDN из целей сбора данных** — при включении активам, полученным в результате сканирования инфраструктуры, присваиваются FQDN, указанные в целях сбора данных. Включение позволяет избежать дублирования активов с указанным FQDN, обнаруженных с помощью модуля Audit.
- **Определение операционной системы** — при включении на активных узлах проводится определение версии ОС.
- **Проверка с помощью ARP-запросов** — дополнительный параметр, при включении которого 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** — дополнительный 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.

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).

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 18.3).
- **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).

18.1.4. 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 при создании задачи на сбор данных. Для этого в панели с параметрами профиля в иерархическом списке нужно выбрать секцию параметров. Ниже приводятся описания параметров в каждой секции.

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.

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.

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 18.3).

— **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).

18.1.5. 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. Все профили модуля сканируют порты и определяют работающие службы. Для модуля созданы следующие стандартные профили:

- **Bruteforce PenTest.** Для подбора учетных записей. Сканирует только стандартные порты служб (например, TCP 21—23, TCP 25 или TCP 80).
- **Database Discovery.** Для быстрого поиска и инвентаризации сетевых устройств с базами данных.
- **Fast PenTest.** Для быстрого поиска уязвимостей методом SYN-сканирования (см. раздел 18.1.5.1) ограниченного числа портов (часто встречающихся). Аудит с этим профилем быстрее, чем с Full PenTest и Unsafe PenTest.
- **Full PenTest.** Для полного сканирования и поиска уязвимостей с использованием безопасных проверок и подбора учетных записей. Сканирование одного актива занимает до 8 минут.
- **Http Servers Discovery.** Для быстрого поиска и инвентаризации веб-ресурсов с использованием безопасных проверок. Сканирует только стандартные TCP-порты (например, 80, 443, 8080). Сканирование одного актива занимает до 8 минут.
- **Mail Servers Discovery.** Для быстрого поиска и инвентаризации почтовых служб.
- **Remote Management Discovery**. Для быстрого поиска и инвентаризации устройств с включенным удаленным управлением.
- **Safe PenTest**. Для тестирования на проникновение с использованием безопасных проверок. В Safe PenTest задан более широкий диапазон портов, чем в Fast PenTest. Сканирует стандартные порты (в соответствии с распределением портов IANA) наиболее популярных служб и приложений. Не ищет уязвимости методом подбора учетных записей.
- **SAP Discovery.** Для быстрого поиска и инвентаризации продуктов компании SAP.
- **Service Discovery.** Для обнаружения активных узлов, открытых на них портов и определения работающих служб. Не ищет уязвимости.
- **Service Discovery on well-known ports.** Для быстрого обнаружения активных узлов, открытых на них портов и определения работающих служб. Не ищет уязвимости. Аудит с этим профилем требует меньше времени, чем с профилем Service Discovery, за счет того, что не проверяются UDP-службы.
- **SNMP Scan.** Для быстрого обнаружения активных узлов в сети и поиска на них уязвимостей по протоколу SNMP.

— **Unsafe PenTest.** Для тестирования на проникновение с использованием небезопасных проверок, при которых уязвимости обнаруживаются с помощью атак типа «отказ в обслуживании» (DoS).

— **Windows Discovery.** Для обнаружения активных узлов с Windows, поиска на них открытых портов и определения работающих служб.

Внимание! Сканирование с профилем Unsafe PenTest может привести к недоступности отдельных сервисов или узлов. Возможны ложные срабатывания в случае проблем с соединением.

Настраивать параметры модуля вы можете при создании пользовательского профиля на базе стандартного или при создании задачи на сбор данных. Для этого в панели с параметрами профиля в иерархическом списке нужно выбрать секцию параметров. Ниже приводятся описания параметров в каждой секции.

По умолчанию для модуля Pentest могут одновременно выполняться не больше 20 подзадач. Вы можете изменить это значение на странице **Управление системой** на вкладке **Коллекторы** в панели **Модули и потоки**.

В этом разделе

18.1.5.1. 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 сканирования. Этот метод сканирования менее заметен для некоторых сетевых устройств.

  Внимание! Сканирование с помощью SYN-пакетов увеличивает нагрузку на сетевую инфраструктуру из-за большого количества полуоткрытых соединений. При сканировании одного порта может устанавливаться до трех соединений, которые остаются полуоткрытыми в течение некоторого времени, поэтому растет количество таких соединений. Для уменьшения количества полуоткрытых соединений необходимо уменьшить максимальное количество потоков.

- **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.

18.1.5.2. 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.

18.1.5.3. 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)**.

18.1.5.4. 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 уязвимостей. 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 уязвимостей. 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.

18.1.5.5. 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.

18.1.5.6. 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.

18.1.5.7. 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.

18.1.5.8. 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.

18.1.5.9. 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.

18.1.5.10. 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».

18.1.5.11. 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 мандантов клиентов** — по кнопке **Добавить** вы можете добавить поля для ввода номеров мандантов клиентов SAP, для которых будут подбираться учетные данные.
- **Проверить все номера мандантов от 000 до 999** — при включении учетные данные подбираются для клиентов SAP с любыми мандантами.

— **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.

18.1.5.12. 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 мандантов клиентов** — по кнопке **Добавить** вы можете добавить поля для ввода номеров мандантов клиентов SAP, для которых будут подбираться учетные данные.

— **Проверить все номера мандантов от 000 до 999** — при включении учетные данные подбираются для клиентов SAP с любыми мандантами.

— **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.

18.1.5.13. 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.

18.1.5.14. 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».

18.1.5.15. 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».

18.1.5.16. 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.

18.1.5.17. 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.

18.1.5.18. 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».

18.1.5.19. 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».

18.1.5.20. 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».

18.1.5.21. 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».

18.1.5.22. 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.

18.1.5.23. 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».

18.1.5.24. 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».

18.1.5.25. 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».

18.1.5.26. 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.

18.1.5.27. 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.

18.1.5.28. Дополнительные параметры модуля Pentest

В этом разделе описаны дополнительные параметры профиля модуля сканирования данных.

Отладка сканирования

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.

Объем занимаемой памяти

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).

Работа модуля

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 18.3).

— **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).

Отправка данных в систему

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.

18.1.6. Модуль WebEngine

Модуль предназначен для сбора данных о веб-приложениях в IT-инфраструктуре организации. В состав модуля WebEngine входят встроенные модули для обнаружения различных веб-уязвимостей. Запуск задач на сбор данных с модулем WebEngine доступен только на коллекторах, установленных на Linux. Для модуля создан стандартный профиль Web Scan Optimal.

Внимание! Для просмотра данных, полученных в результате сбора данных с профилем Web Scan Optimal, необходимо создать динамическую группу активов с фильтром на основе корневой сущности WebSite.

Настраивать параметры модуля вы можете при создании пользовательского профиля на базе стандартного или при создании задачи на сбор данных. Для этого в панели с параметрами профиля в иерархическом списке нужно выбрать секцию параметров. Ниже приводятся описания параметров в каждой секции.

По умолчанию для модуля WebEngine могут одновременно выполняться не больше 4 подзадач. Вы можете изменить это значение на странице **Управление системой** на вкладке **Коллекторы** в панели **Модули и потоки**.

В этом разделе

Сбор данных (см. раздел 18.1.6.1)

Подключение (см. раздел 18.1.6.2)

Дополнительные параметры модуля WebEngine (см. раздел 18.1.6.3)

Создание профилей на основе Web Scan Optimal для разных типов аутентификации (см. раздел 18.1.6.4)

18.1.6.1. Сбор данных

Секция содержит параметры для настройки сбора событий с веб-приложений.

Сбор данных

Блок содержит следующие параметры:

— **Порты** — поле для ввода номеров портов подключения. Несколько портов нужно указывать через точку с запятой.

— **Область сбора данных** — раскрывающийся список для выбора области сбора данных:

- **path** — сбор данных в пределах пути указанного URL. Параметры указанного URL могут не совпадать с параметрами остальных URL, сканируемых в пределах указанного пути. Например, если указана цель `https://www.example.test:8443/crm/index.php?action=welcome&next=guide`, то в область сканирования также попадают `https://www.example.test:8443/crm/index.php` и `https://www.example.test:8443/crm/index.php?action=logout`;
- **folder** — сбор данных из каталога указанной страницы и вложенных в него каталогов. Например, если указана цель `https://www.example.test:8443/crm/indexphp?action=welcome&next=guide`, то в область сканирования также попадают `https://www.example.test:8443/crm/`, `https://www.example.test:8443/crm/admin.php`, `https://www.example.test:8443/crm/admin/index.php`;

- **domain** — сбор данных в пределах указанного домена. Например, если указана цель `https://www.example.test:8443/crm/index.php?action=welcome&next=guide`, то в область сканирования также попадает `http://www.example.test:8080/api/v1/users`;
- **base_domain** — сбор данных в пределах основного домена указанного URL и его поддоменов. Например, если указана цель `https://www.example.test:8443/crm/index.php?action=welcome&next=guide`, то в область сканирования также попадают `http://example.test/` и `https://admin.example.test:1337/foo/bar`. Основным считается домен, следующий за доменом из списка **Public Suffix List**.

— **Полнота сбора данных** — раскрывающийся список для выбора режима сбора данных:

- **fast** — быстрый сбор данных. Включает в себя проверку со следующими встроенными модулями WebEngine: xss_r, xss_s, fileupload, appfingerprint, sqli, xxe, csrf, ssi;
- **optimal** — оптимальный сбор данных. Включает в себя проверку со следующими встроенными модулями WebEngine: xss_r, xss_s, fileupload, appfingerprint, sqli, xxe, csrf, ssi, fileops, infoexposure, rce, oscmd, shellshock, httpheaderinj. Предусмотрен по умолчанию;
- **full** — полный сбор данных. Включает в себя проверку со всеми встроенными модулями WebEngine.

Внимание! Сбор данных в режиме **full** может занять длительное время.

Поиск стандартных каталогов

Блок содержит параметр **Режим поиска каталогов** — раскрывающийся список для выбора области поиска каталогов со стандартными именами:

— **root** — поиск только в корневом каталоге сайта;

— **directory** — поиск в каждом каталоге первого уровня.

18.1.6.2. Подключение

Секция содержит раскрывающийся список для настройки подключения к веб-приложению.

Аутентификация

При выборе значения **Аутентификация** доступен раскрывающийся список для выбора типа аутентификации:

— **Веб-форма (автоматический поиск)** — при выборе значения доступны следующие параметры:

- **Адрес страницы входа** — поле для ввода адреса страницы, с которой выполняется вход на сайт;
- **Учетная запись** — раскрывающийся список для выбора учетной записи, которая будет использоваться MP 10 Collector при аутентификации в ОС.
- **Проверка входа** — поле для ввода текста, с помощью которого можно определить, что вход на сайт выполнен успешно. Если текст не указан, проверяется только открытие страницы.

— **Веб-форма** — при выборе значения доступны следующие параметры:

- **Адрес страницы входа** — поле для ввода адреса страницы, с которой выполняется вход на сайт;
- **XPath-выражение для формы входа** — поле для ввода XPath-выражения, которое позволяет найти форму входа на странице аутентификации. Определить XPath-выражение формы входа можно с помощью инструментов браузера;
- **Логин**, **Пароль**, **Кнопка входа** — поле для ввода атрибутов идентификатора или имени DOM-элемента;
- **Учетная запись** — раскрывающийся список для выбора или добавления учетной записи;
- **Проверка входа** — поле для ввода текста, с помощью которого можно определить, что вход на сайт выполнен успешно. Если текст не указан, проверяется только открытие страницы.

— **HTTP-аутентификация** — при выборе значения доступны следующие параметры:

- **Учетная запись** — раскрывающийся список для выбора или добавления учетной записи. При добавлении учетной записи обязательны для заполнения следующие параметры: **Тип**, **Название**, **Логин**, **Пароль**, **Подтверждение пароля** и **Домен**;
- **Адрес страницы для проверки входа** — поле для ввода адреса страницы, которая будет открыта после входа. Если она откроется, вход будет считаться успешным и запустится процесс сканирования.

— **Сессионные куки** — при выборе значения доступны следующие параметры:

- **Куки (из заголовка запроса)** — раскрывающийся список для выбора или добавления учетной записи. При добавлении учетной записи в полях **Пароль** и **Подтверждение пароля** необходимо ввести сессионные куки, доступ к которым можно получить с

помощью средств разработчика. В качестве формата куки поддерживается формат значения заголовка Set-Cookie HTTP-ответа. Может быть использован список значений куки: по одному значению на каждый элемент списка;

- **Адрес страницы для проверки входа** — поле для ввода адреса страницы, которая будет открыта после входа. Если она откроется, вход будет считаться успешным и запустится процесс сканирования;
- **Проверка входа** — поле для ввода текста, с помощью которого можно определить, что вход на сайт выполнен успешно. Если текст не указан, проверяется только открытие страницы.

Прокси-сервер (дополнительные параметры)

При выборе значения **Прокси-сервер** доступны следующие параметры:

— **Тип** — раскрывающийся список для выбора типа прокси-сервера (http, socks4, socks5, socks5h).

— **Адрес** — раскрывающийся список для выбора типа адреса прокси-сервера:

- **FQDN** — полное доменное имя;
- **IPv4** — IP-адрес версии 4.
- **IPv6** — IP-адрес версии 6.

— **Порт** — дополнительное поле для ввода номера порта прокси-сервера.

— **Учетная запись для подключения к прокси-серверу** — раскрывающийся список для выбора или добавления учетной записи.

18.1.6.3. Дополнительные параметры модуля WebEngine

В этом разделе описаны дополнительные параметры профиля модуля сканирования данных.

Отладка сканирования

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.

Объем занимаемой памяти

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).

Работа модуля

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 18.3).

— **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).

Отправка данных в систему

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.

18.1.6.4. Создание профилей на основе Web Scan Optimal для разных типов аутентификации

Аутентификация с помощью веб-формы (автоматический поиск)

► Чтобы создать профиль для аутентификации с помощью веб-формы (автоматический поиск):

1. В главном меню выберите **Сбор данных** → **Профили**.

   Откроется страница **Профили**.

2. В панели инструментов нажмите кнопку **Создать**.

   Откроется страница **Новый профиль**.

3. Введите название профиля.
4. В раскрывающемся списке **Создать на основе** выберите **Web Scan Optimal**.
5. В панели **Параметры профиля** в иерархическом списке выберите **Аутентификация**.
6. В раскрывающемся списке **Аутентификация** выберите **Веб-форма (автоматический поиск)**.
7. В блоке параметров **Веб-форма (автоматический поиск)** в поле **Адрес страницы входа** укажите адрес страницы, с которой выполняется вход на сайт.

   Например:

   ```
   http://example.net/login.php
   ```

8. В раскрывающемся списке **Учетная запись** выберите учетную запись, которую необходимо использовать для входа на сайт.
9. В поле **Проверка входа** введите текст, с помощью которого можно определить, что вход на сайт выполнен успешно.

   Например:

   ```
   Вход выполнен успешно
   ```

   Примечание. Если текст не указан, проверяется только открытие страницы.

10. Нажмите кнопку **Сохранить**.

Аутентификация с помощью веб-формы (автоматический поиск) настроена.

Аутентификация с помощью веб-формы

- Чтобы создать профиль для аутентификации с помощью веб-формы:

1. В главном меню выберите **Сбор данных** → **Профили**.

   Откроется страница **Профили**.

2. В панели инструментов нажмите кнопку **Создать**.

   Откроется страница **Новый профиль**.

3. Введите название профиля.
4. В раскрывающемся списке **Создать на основе** выберите **Web Scan Optimal**.
5. В панели **Параметры профиля** в иерархическом списке выберите **Аутентификация**.
6. В раскрывающемся списке **Аутентификация** выберите **Веб-форма**.
7. В блоке параметров **Веб-форма** в поле **Адрес страницы входа** укажите адрес страницы, с которой выполняется вход на сайт.

   Например:

   `http://example.net/login.php`

8. В поле **XPath-выражение для формы входа** укажите XPath-выражение, которое позволяет найти форму входа на странице аутентификации.

   Например:

   `//[@id="id01"]/form`

   Примечание. Вы можете определить XPath-выражение формы входа с помощью инструментов браузера.

9. В блоке параметров **Названия элементов** введите логин и пароль.
10. В поле **Кнопка входа** введите идентификатор или имя кнопки входа.

    Например:

    `wp-submit`

11. В раскрывающемся списке **Учетная запись** выберите учетную запись, которую необходимо использовать для входа на сайт.
12. В поле **Проверка входа** введите текст, с помощью которого можно определить, что вход на сайт выполнен успешно.

    Например:

    `Вход выполнен успешно`

    Примечание. Если текст не указан, проверяется только открытие страницы.

13. Нажмите кнопку **Сохранить**.

Аутентификация с помощью веб-формы настроена.

HTTP-аутентификация

- Чтобы создать профиль для HTTP-аутентификации:

  1. В главном меню выберите **Сбор данных** → **Профили**.

     Откроется страница **Профили**.

  2. В панели инструментов нажмите кнопку **Создать**.

     Откроется страница **Новый профиль**.

  3. Введите название профиля.
  4. В раскрывающемся списке **Создать на основе** выберите **Web Scan Optimal**.
  5. В панели **Параметры профиля** в иерархическом списке выберите **Аутентификация**.
  6. В раскрывающемся списке **Аутентификация** выберите **HTTP-аутентификация**.
  7. В блоке параметров **HTTP-аутентификация** в раскрывающемся списке **Учетная запись** выберите учетную запись, которую необходимо использовать для подключения.
  8. В поле **Адрес страницы для проверки входа** введите адрес страницы, которая будет открыта после входа.

     Например:
     `http://example.net/basic.php`
  9. Нажмите кнопку **Сохранить**.

  HTTP-аутентификация настроена.

Аутентификация с помощью сессионных куки

- Чтобы создать профиль для аутентификации с помощью сессионных куки:

  1. В главном меню выберите **Сбор данных** → **Профили**.

     Откроется страница **Профили**.

  2. В панели инструментов нажмите кнопку **Создать**.

     Откроется страница **Новый профиль**.

  3. Введите название профиля.
  4. В раскрывающемся списке **Создать на основе** выберите **Web Scan Optimal**.
  5. В панели **Параметры профиля** в иерархическом списке выберите **Аутентификация**.
  6. В раскрывающемся списке **Аутентификация** выберите **Сессионные куки**.
  7. В блоке параметров **Сессионные куки** в раскрывающемся списке **Куки (из заголовка запроса)** выберите учетную запись.

8. В поле **Адрес страницы для проверки входа** введите адрес страницы, которая будет открыта после входа.

   Например:
   `http://example.net/basic.php`

9. В поле **Проверка входа** введите текст, с помощью которого можно определить, что вход на сайт выполнен успешно.

   Например:
   `Вход выполнен успешно`

   Примечание. Если текст не указан, проверяется только открытие страницы.

10. Нажмите кнопку **Сохранить**.

Аутентификация с помощью сессионных куки настроена.

18.2. Модуль для выполнения сценариев на удаленных узлах, RemoteExecutor

Модуль предназначен для выполнения сценариев на удаленных узлах. Для него созданы стандартные профили:

- **PowershellExecutor.** Для выполнения указанного сценария с помощью Windows PowerShell и получения результата выполнения.
- **RemoteExecutor.** Для выполнения указанного сценария и получения результата выполнения.

Настраивать параметры модуля вы можете при создании пользовательского профиля на базе стандартного или при создании задачи на сбор данных. Для этого в панели с параметрами профиля в иерархическом списке нужно выбрать секцию параметров. Ниже приводятся описания параметров в каждой секции.

В этом разделе

18.2.1. 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.

18.2.2. 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.

18.3. 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**.

Журналы модулей сохраняются в папке компонента MP 10 Collector:

— если коллектор установлен на Windows — `C:\ProgramData\Positive Technologies\MaxPatrol 10 Agent\log\modules\<Название модуля>`;

— если коллектор установлен на ОС семейства Unix — `/var/log/core-agent/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 6. 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

Параметр	Модуль (компонент)
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)
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

Параметр	Модуль (компонент)
`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
`WMINotification`	Модуль WmiNotification

19. О технической поддержке

Базовая техническая поддержка доступна для всех владельцев действующих лицензий на MaxPatrol VM в течение периода предоставления обновлений и включает в себя следующий набор услуг.

Предоставление доступа к обновленным версиям продукта

Обновления продукта выпускаются в порядке и в сроки, определяемые Positive Technologies. Positive Technologies поставляет обновленные версии продукта в течение оплаченного периода получения обновлений, указанного в бланке лицензии приобретенного продукта Positive Technologies.

Positive Technologies не производит установку обновлений продукта в рамках технической поддержки и не несет ответственности за инциденты, возникшие в связи с некорректной или несвоевременной установкой обновлений продукта.

Восстановление работоспособности продукта

Специалист Positive Technologies проводит диагностику заявленного сбоя и предоставляет рекомендации для восстановления работоспособности продукта. Восстановление работоспособности может заключаться в выдаче рекомендаций по установке продукта заново с потенциальной потерей накопленных данных либо в восстановлении версии продукта из доступной резервной копии (резервное копирование должно быть настроено заблаговременно). Positive Technologies не несет ответственности за потерю данных в случае неверно настроенного резервного копирования.

> **Примечание.** Помощь оказывается при условии, что конечным пользователем продукта соблюдены все аппаратные, программные и иные требования и ограничения, описанные в документации к продукту.

Устранение ошибок и дефектов в работе продукта в рамках выпуска обновленных версий

Если в результате диагностики обнаружен дефект или ошибка в работе продукта, Positive Technologies обязуется включить исправление в ближайшие возможные обновления продукта (с учетом релизного цикла продукта, приоритета дефекта или ошибки, сложности требуемых изменений, а также экономической целесообразности исправления). Сроки выпуска обновлений продукта остаются на усмотрение Positive Technologies.

Рассмотрение предложений по доработке продукта

При обращении с предложением по доработке продукта необходимо подробно описать цель такой доработки. Вы можете поделиться рекомендациями по улучшению продукта и оптимизации его функциональности. Positive Technologies обязуется рассмотреть все предложения, однако не принимает на себя обязательств по реализации каких-либо

доработок. Если Positive Technologies принимает решение о доработке продукта, то способы ее реализации остаются на усмотрение Positive Technologies. Заявки принимаются на портале технической поддержки.

Портал технической поддержки

На портале технической поддержки вы можете круглосуточно создавать и обновлять заявки и читать новости продуктов.

Для получения доступа к порталу технической поддержки нужно создать учетную запись, используя адрес электронной почты в официальном домене вашей организации. Вы можете указать другие адреса электронной почты в качестве дополнительных. Добавьте в профиль название вашей организации и контактный телефон — так нам будет проще с вами связаться.

Техническая поддержка на портале предоставляется на русском и английском языках.

Условия предоставления технической поддержки

Для получения технической поддержки необходимо оставить заявку на портале технической поддержки и предоставить следующие данные:

— номер лицензии на использование продукта;

— файлы журналов и наборы диагностических данных, которые требуются для анализа;

— снимки экрана.

Positive Technologies не берет на себя обязательств по оказанию услуг технической поддержки в случае вашего отказа предоставить запрашиваемую информацию или отказа от внедрения предоставленных рекомендаций.

Если заказчик не предоставляет необходимую информацию по прошествии 20 календарных дней с момента ее запроса, специалист технической поддержки имеет право закрыть заявку. Оказание услуг может быть возобновлено по вашей инициативе при условии предоставления запрошенной ранее информации.

Услуги по технической поддержке продукта не включают в себя услуги по переустановке продукта, решение проблем с операционной системой, инфраструктурой заказчика или сторонним программным обеспечением.

Заявки могут направлять уполномоченные сотрудники заказчика, владеющего продуктом на законном основании (включая наличие действующей лицензии). Специалисты заказчика должны иметь достаточно знаний и навыков для сбора и предоставления диагностической информации, необходимой для решения заявленной проблемы.

Услуги по технической поддержке оказываются в отношении поддерживаемых версий продукта. Информация о поддерживаемых версиях содержится в «Политике поддержки версий программного обеспечения» и (или) иных информационных материалах, размещенных на официальном веб-сайте Positive Technologies.

Время реакции и приоритизация заявок

При получении заявки ей присваивается регистрационный номер, специалист службы технической поддержки классифицирует ее (присваивает тип и уровень значимости) и выполняет дальнейшие шаги по ее обработке.

Время реакции рассчитывается с момента получения заявки до первичного ответа специалиста технической поддержки с уведомлением о взятии заявки в работу. Время реакции зависит от уровня значимости заявки. Специалист службы технической поддержки оставляет за собой право переопределить уровень значимости в соответствии с приведенными ниже критериями. Указанные сроки являются целевыми, но возможны отклонения от них по объективным причинам.

Таблица 7. Время реакции на заявку

Уровень значимости заявки	**Критерии значимости заявки**	**Время реакции на заявку**
Критический	Аварийные сбои, приводящие к невозможности штатной работы продукта (исключая первоначальную установку) либо оказывающие критически значимое влияние на бизнес заказчика	До 4 часов
Высокий	Сбои, проявляющиеся в любых условиях эксплуатации продукта и оказывающие значительное влияние на бизнес заказчика	До 8 часов
Средний	Сбои, проявляющиеся в специфических условиях эксплуатации продукта либо не оказывающие значительного влияния на бизнес заказчика	До 8 часов
Низкий	Вопросы информационного характера либо сбои, не влияющие на эксплуатацию продукта	До 8 часов

Указанные часы относятся к рабочему времени (рабочие дни с 9:00 до 18:00 UTC+3) специалистов технической поддержки. Под рабочим днем понимается любой день за исключением субботы, воскресенья и дней, являющихся официальными нерабочими днями в Российской Федерации.

Обработка и закрытие заявок

По мере рассмотрения заявки и выполнения необходимых действий специалист технической поддержки сообщает вам:

— о ходе диагностики по заявленной проблеме и ее результатах;

— планах выпуска обновленной версии продукта (если требуется для устранения проблемы).

Если по итогам обработки заявки необходимо внести изменения в продукт, Positive Technologies включает работы по исправлению в ближайшее возможное плановое обновление продукта (с учетом релизного цикла продукта, приоритета дефекта или ошибки, сложности требуемых изменений, а также экономической целесообразности исправления). Сроки выпуска обновлений продукта остаются на усмотрение Positive Technologies.

Специалист закрывает заявку, если:

— предоставлены решение или возможность обойти проблему, не влияющие на критически важную функциональность продукта (по усмотрению Positive Technologies);

— диагностирован дефект продукта, собрана техническая информация о дефекте и условиях его воспроизведения, исправление дефекта запланировано к выходу в рамках планового обновления продукта;

— заявленная проблема вызвана программным обеспечением или оборудованием сторонних производителей, на которые не распространяются обязательства Positive Technologies;

— заявленная проблема классифицирована специалистами Positive Technologies как неподдерживаемая.

Примечание. Если продукт приобретался вместе с аппаратной платформой в виде программно-аппаратного комплекса (ПАК), решение заявок, связанных с ограничением или отсутствием работоспособности аппаратных компонентов, происходит согласно условиям и срокам, указанным в гарантийных обязательствах (гарантийных талонах) на такие аппаратные компоненты.

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.

Для сканирования систем через терминал в панели **Параметры сбора данных** вы можете добавить разрешенные и запрещенные команды (см. раздел 18.1.1.11), используя регулярные выражения. Операторы регулярных выражений должны быть экранированы.

> **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 8. Стандартные профили для аудита активов

Актив	Версия	Профиль	Порт по умолчанию
«Базальт СПО», «Альт СП»	8	Unix SSH Audit	TCP 22
«Базальт СПО», «Альт Рабочая станция»	9, 10	Unix SSH Audit	TCP 22
«РЕД СОФТ», «РЕД ОС»	7.1—7.3	Unix SSH Audit	TCP 22
Alcatel OmniSwitch	6.4.4 [1]	SSH Network Device Audit, SNMP Network Device Audit [2]	— TCP 22; — UDP 162
Astra Linux Common Edition	2.12	Unix SSH Audit	TCP 22
Astra Linux Special Edition	1.6, 1.7	Unix SSH Audit	TCP 22
Atlassian Confluence	7.13 и выше	SSH Network Device Audit	TCP 22

1 Указаны версии ПО, на которых производилась проверка аудита. Корректная работа аудита на других версиях не гарантируется.

2 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
Avaya (Nortel) NOS, серия ERS	5.1.0.015 [1]	SSH Network Device Audit, SNMP Network Device Audit [2]	— TCP 22; — UDP 162
Canonical Ubuntu	16.04, 18.04, 20.04, 22.04	Unix SSH Audit	TCP 22
CentOS	6, 7	Unix SSH Audit	TCP 22
Check Point GAiA OS	76, 77.10—81.10	Checkpoint Management Server SSH Audit, Checkpoint OPSEC Audit	TCP 22, 18190
Check Point SPLAT	R75.40 [1]	SSH Network Device Audit, Checkpoint OPSEC Audit	TCP 22, 18190
Cisco ACS	5	SSH Network Device Audit, SNMP Network Device Audit [2]	— TCP 22; — UDP162
Cisco ADE-OS	—	SSH Network Device Audit, SNMP Network Device Audit [2]	— TCP 22; — UDP 162
Cisco AireOS Wireless Controller	7.4.100, 7.6.130 [1]	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 [2]	— TCP 22; — UDP 162
Cisco IOS XE	12, 15, 16	SSH Cisco Audit in Enable Mode, SNMP Network Device Audit [2]	— TCP 22; — UDP 162
Cisco IOS XR, серия ASR9000	4.3.4, 6.1.1, 6.4.2 [1]	SSH Network Device Audit	TCP 22
Cisco ISE (Identity Services Engine)	2.3.0 [1]	SSH Network Device Audit, SNMP Network Device Audit [2]	— TCP 22; — UDP 162
Cisco NX-OS	4—7	SSH Network Device Audit, SNMP Network Device Audit [2]	— TCP 22; — UDP 162
Debian	7, 8, 9	Unix SSH Audit	TCP 22
Eltex, маршрутизаторы серии ESR	1.4.4 [1]	SSH Network Device Audit	TCP 22

Актив	Версия	Профиль	Порт по умолчанию
Eltex, коммутаторы серий MES 1xxx, 2xxx, 3xxx, 51xx, 52xx	1.1.44, 4.0.9.3 [1]	SSH Network Device Audit	TCP 22
Fortinet FortiOS	5.4.2, 6.0.1 [1]	SSH Network Device Audit	TCP 22
FreeBSD	8—11	Unix SSH Audit	TCP 22
HPE Comware Software	5, 7	SSH Network Device Audit	TCP 22
HPE Integrated Lights-Out (iLO)	3—5	SSH Network Device Audit	TCP 22
HPE UX	11.31 [1]	Unix SSH Audit	TCP 22, 23
Huawei VRP, коммутаторы серии S, маршрутизаторы серий AR и NE	—	SSH Network Device Audit, SNMP Network Device Audit [2]	— TCP 22; — UDP 162
IBM AIX	5.3, 6.1, 7.1—7.3	Unix SSH Audit	TCP 22, 23
JetBrains Hub	2018.1—2022	Web API Audit	TCP 80, 443
JetBrains YouTrack	2019	Web API Audit	TCP 80, 443
Juniper JunOS	11—19	SSH Network Device Audit, SNMP Network Device Audit [2]	— TCP 22; — UDP 162
Microsoft System Center Configuration Manager (SCCM)	2012—2019	MSSQL Audit	TCP 1433
Microsoft Windows	XP	Windows Audit	TCP 1025—5000
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; — UDP 135, 137, 138, 445
Microsoft Windows Server	2008, 2008 R2, 2012, 2012 R2, 2016, 2019	Windows Audit	

Актив	Версия	Профиль	Порт по умолчанию
Oracle Linux	6, 7	Unix SSH Audit	TCP 22
Oracle Solaris	9, 10, 11	Unix SSH Audit	TCP 22, 23
Palo Alto Networks PAN-OS	6.1—8.1 [1]	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 SSH Audit	TCP 22
SUSE Linux Enterprise Server	11, 12	Unix SSH Audit	TCP 22
VMware vCenter Server	5.5—7.0	vSphere Audit	TCP 443
VMware vSphere Hypervisor (ESXi)	5.5, 6.0, 6.5, 6.7 [1]	vSphere Audit	TCP 443

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 2>/dev/null
- fw ver -k
- get system status
- ifconfig -a
- ip addr show
- ip address
- oslevel -s
- racadm getversion
- rpm -qa '*release*' 2>/dev/null
- show /map1
- show /map1/dnsendpt1
- show banner static
- show inventory
- show run-config
- show running-config
- show security-gateway version
- show system
- show system info
```

```
- show system info | match model
- show system information
- show system unit ?unit
- show version
- show version all
- show version brief
- show version detail
- show version | no-more
- system identity print
- system license print
- system package print
- system resource print
- system routerboard print
- terminal length 0
- terminal pager 0
- uname
- uname -a
- uname -a > /dev/null
- uname -s
- ver
- version
```

«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
- show arp dynamic all
- show arp static all
- show asset all
- show backups
- show bgp summary
- show config-state
- show configuration
- show configuration core-dump
- show installer package ?num
- show interfaces all
- show ipv6-state
- show mfc summary
- show password-controls all
- show password-controls deny-on-fail block-admin
- show rip interfaces
- show route
- show router-id
- show security-gateway version
- show snapshot ?name all
- show snapshots
- show snmp usm user ?username
```

- show system info
- show version all
- 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
- route ptint
- show security-gateway version
- show system info
- show version all
- ver

Check Point SPLAT

При проведении аудита модуль audit выполняет на активе следующие команды:

- cpstat fw
- cpstat os
- cpstat vpn
- fw ver -k
- hostname
- idle
- ifconfig -a
- lockout show
- netstat -nr
- route print
- show security-gateway version
- show system info
- show version all
- 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
- route print
- show aaa-server
- 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 network
- show ntp status
- show ospf
- show ospf interface
- show rip database
- show route
- show running-config
- show running-config all
- show running-config all policy-map
- show running-config view full
- show snmp group
- show snmp host
- show snmp user
- show ssh
- show startup-config
- show system info
- 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 crypto ikev2 sa detailed
- show crypto ipsec sa detail
- show crypto isakmp sa detail
- show crypto key mypubkey all
- show crypto key mypubkey rsa
- show dhcp lease
- show dmvpn
- 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 nhrp
- show ip ospf
- show ip ospf interface
- show ip protocols
- show ip protocols vrf ?vrf
- show ip route vrf *
- show ip ssh
- show ipv6 access-list
- 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 system info
- show version
- show vlan brief
- show vrf
- show vrrp
- show vstack config
- show vtp password
- show vtp status

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 crypto ikev2 sa detailed
- show crypto ipsec sa detail
- show crypto isakmp sa detail
- show crypto key mypubkey all
- show crypto key mypubkey rsa
- show dhcp lease
- show dmvpn
- 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 nhrp
- show ip ospf
- show ip ospf interface
- show ip protocols
- show ip protocols vrf ?vrf
- show ip route vrf *
- show ip ssh
- show ipv6 access-list
- 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 system info
- show version
- show vlan brief
- show vrf
- show vrrp
- show vstack config
- show vtp password
- show vtp status

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 running-config all
- show running-config view full
- show snmp
- show snmp group
- show snmp view
- show version brief
- show version detail
- 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:

```
- interf bridge monitor ?name once
- interface bridge print detail without-paging
- interface bridge vlan print detail without-paging
- route print
- 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 logging origin-id
- 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 system info
- 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 startup-config
- show system
- show system id
- show system unit ?unit
- 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 interfaces
- show ip interfaces vrf ?vrf_name
- show ip route
- show ip route vrf ?vrf
- show ip vrf
- show running-config
- show running-config access-list
- show startup-config
- show system
- show system info
- show user accounts
- show vlan
- show vrrp
- show vrrp ?id
- show vrrp vrf ?vrf_name

FortiNet FortiOS

При проведении аудита модуль audit выполняет на активе следующие команды:

- get hardware nic ?interface_id
- get log memory global-setting
- get log syslogd?number filter
- get log syslogd?number setting
- get system password-policy
- show system admin
- show system interface
- show system vdom-property
- diag netlink aggregate name ?interface_id
- diagnose firewall fqdn list
- diagnose firewall fqdn list-ip
- diagnose firewall ipgeo ip-list ?name
- diagnose ip address list
- diagnose netlink dstmac list

```
- get log memory filter
- get log memory setting
- get router info routing-table all
- get router multicast
- get system arp
- show
- show user local
- diag netlink aggregate name ?interface_id
- diagnose firewall fqdn list
- diagnose firewall fqdn list-ip
- diagnose firewall ipgeo ip-list ?name
- diagnose ip address list
- diagnose netlink dstmac 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
- route print
- show
- show system admin
- show system info
- 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 current-configuration configuration dnat-address-group ?address-group
- display current-configuration configuration nat-static
- display destination-nat address-group name ?pool
- display domain-set verbose ?name
- display geo-location verbose ?name
- display geo-location-set verbose ?name
- 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 nat address-group name ?pool
- display ospf brief
- display patch-information
- display port vlan
- display predefined-service
- 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 chassis mac-addresses
- 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 set | no-more | display inheritance
- show configuration | display xml | no-more | display inheritance
- show ethernet-switching table
- show interfaces ?name media
- 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 system info
- 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:

```
- run request resolve address ?name
- run set system setting target-vsys ?vsys
- run show running security-policy
- run set system setting target-vsys none
- run set system setting target-vsys ?vsys_name
- run show pbf rule name ?name
- run show pbf rule name ?name
- run show running security-policy
- show
- show ?kind ?object ?name
- show ?object ?name
- show predefined default-security-rules
- show predefined region ?region
- show predefined service
- show predefined service-group
- show rulebase default-security-rules
- show vsys ?name rulebase default-security-rules
- show vsys ?vsys ?object ?name
- show arp all
- show arp management
- show interface ?name
- show interface hardware
- show interface logical
- show interface management
- show routing route
- show system info
- configure\nshow\nexit
- set cli pager off
- set cli terminal width 500
- set cli config-output-format xml
- show interface .*
```

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
```

См. также

Сканирование систем — Через терминал (см. раздел 18.1.1.11)

Предметный указатель

A

B

C

D

E

F

H

J

K

L

M

N

O

P

Q

R

S

U

V

W

Y

Z

П

positive
technologies

Positive Technologies — один из лидеров в области 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 около 3000 организаций по всему миру. Positive Technologies — первая и единственная компания из сферы кибербезопасности на Московской бирже (MOEX: POSI). Количество акционеров превышает 220 тысяч.