



XSpider PRO

версия 1.1

Руководство администратора

© Positive Technologies, 2026.

Настоящий документ является собственностью Positive Technologies и защищен законодательством Российской Федерации и международными соглашениями об авторских правах и интеллектуальной собственности.

Копирование документа либо его фрагментов в любой форме, распространение, в том числе в переводе, а также их передача третьим лицам возможны только с письменного разрешения Positive Technologies.

Документ может быть изменен без предварительного уведомления.

Товарные знаки, использованные в тексте, приведены исключительно в информационных целях, исключительные права на них принадлежат соответствующим правообладателям.

Дата редакции документа: 11.09.2026

Содержание

1.	Об этом документе.....	8
2.	О сканере безопасности XSpider PRO	9
3.	Что нового в версии 1.1	10
4.	Аппаратные и программные требования	11
5.	Принципы безопасной работы.....	13
6.	Установка XSpider PRO.....	14
7.	Вход в XSpider PRO	18
8.	Активация продукта	19
9.	Лицензирование	22
10.	Начало работы.....	26
11.	Работа с задачами.....	33
11.1.	Обнаружение узлов в сети.....	36
11.2.	Настройка параметров сбора данных.....	39
11.2.1.	Профили сканирования	40
11.2.2.	Учетные записи для аудита	40
11.2.3.	Справочники для аудита	42
11.3.	Сбор данных в режиме пентеста.....	43
11.3.1.	Общие параметры сканирования.....	46
11.3.2.	Сканирование портов	47
11.3.3.	Сканирование UDP-служб	47
11.3.4.	Поиск уязвимостей — Подбор учетных данных — IBM DB2.....	48
11.3.5.	Поиск уязвимостей — Подбор учетных данных — Microsoft SQL Server	49
11.3.6.	Поиск уязвимостей — Подбор учетных данных — Oracle Database	49
11.3.7.	Поиск уязвимостей — Подбор учетных данных — Oracle Database, подбор SID.....	50
11.3.8.	Поиск уязвимостей — Подбор учетных данных — Oracle MySQL	50
11.3.9.	Поиск уязвимостей — Подбор учетных данных — SAP Sybase ASE	50
11.3.10.	Поиск уязвимостей — Подбор учетных данных — SAP через DIAG	51
11.3.11.	Поиск уязвимостей — Подбор учетных данных — SAP через RFC	51
11.3.12.	Поиск уязвимостей — Подбор учетных данных — Symantec pcAnywhere	52
11.3.13.	Поиск уязвимостей — Подбор учетных данных — Virtual Network Computing.....	52
11.3.14.	Поиск уязвимостей — Подбор учетных данных — VMware vSphere.....	52
11.3.15.	Поиск уязвимостей — Подбор учетных данных — По протоколу FTP	52
11.3.16.	Поиск уязвимостей — Подбор учетных данных — По протоколу NetBIOS	53
11.3.17.	Поиск уязвимостей — Подбор учетных данных — По протоколу POP3	53
11.3.18.	Поиск уязвимостей — Подбор учетных данных — По протоколу RDP	53
11.3.19.	Поиск уязвимостей — Подбор учетных данных — По протоколу SIP	53
11.3.20.	Поиск уязвимостей — Подбор учетных данных — По протоколу SMTP	54
11.3.21.	Поиск уязвимостей — Подбор учетных данных — По протоколу SNMP	54
11.3.22.	Поиск уязвимостей — Подбор учетных данных — По протоколу SSH	54
11.3.23.	Поиск уязвимостей — Подбор учетных данных — По протоколу Telnet.....	55
11.3.24.	Поиск уязвимостей — Подбор учетных данных — Фаматек RAdmin	55
11.3.25.	Поиск уязвимостей — Поиск файлов.....	55
11.3.26.	Поиск уязвимостей — Сканирование по LDAP	56

11.3.27.	Дополнительные параметры модуля Pentest	56
11.4.	Сбор данных в режиме аудита	58
11.4.1.	Сбор данных с использованием модуля Audit	60
11.4.1.1.	Сканирование систем — Check Point через OPSEC	62
11.4.1.2.	Сканирование систем — Microsoft SQL Server	62
11.4.1.3.	Сканирование систем — Oracle Database	63
11.4.1.4.	Сканирование систем — Oracle MySQL	64
11.4.1.5.	Сканирование систем — SAP через RFC	64
11.4.1.6.	Сканирование систем — VMware vSphere	65
11.4.1.7.	Сканирование систем — Windows	65
11.4.1.8.	Сканирование систем — По протоколу LDAP	66
11.4.1.9.	Сканирование систем — По протоколу SNMP	66
11.4.1.10.	Сканирование систем — Через терминал	67
11.4.1.11.	Дополнительные параметры модуля Audit	72
11.4.1.12.	Расширение сбора данных	74
11.4.2.	Команды, выполняемые при аудите узлов	74
11.5.	Сбор данных о веб-приложениях	145
11.5.1.	Сбор данных	148
11.5.2.	Подключение	149
11.5.3.	Дополнительные параметры модуля WebEngine	150
11.5.4.	Создание профилей на основе Web Scan Optimal для разных типов аутентификации ..	152
12.	Выпуск отчетов	155
13.	Администрирование мобильного сканера	160
13.1.	Обновление XSpider PRO	160
13.2.	Смена пароля служебной учетной записи администратора	161
13.3.	Обновление пакетов экспертизы	161
13.4.	Выдача прав на чтение пакетов экспертизы	165
13.5.	Удаление XSpider PRO с помощью сценария	166
14.	Справочник по настройке систем перед сканированием	167
14.1.	Антивирусное программное обеспечение	167
14.1.1.	Kaspersky Security Center 13–14.2: настройка узла	167
14.1.2.	Kaspersky Security Center 13–14.2: настройка XSpider PRO	169
14.1.2.1.	Добавление учетной записи для доступа к узлу через веб-API	170
14.1.2.2.	Создание задачи на аудит узла с профилем Web API Audit	170
14.2.	Межсетевые экраны	171
14.2.1.	Cisco ASA 8, 9: настройка узла	171
14.2.2.	Cisco ASA 8, 9: настройка XSpider PRO	172
14.2.2.1.	Добавление учетной записи для доступа по SSH	172
14.2.2.2.	Добавление пароля для повышения привилегий для аудита по SSH	173
14.2.2.3.	Создание задачи на аудит узла по SSH	173
14.3.	Операционные системы	173
14.3.1.	Microsoft Windows XP–11; Windows Server 2003–2022: настройка узла	174
14.3.2.	Microsoft Windows XP–11; Windows Server 2003–2022: настройка XSpider PRO	175
14.3.2.1.	Добавление учетной записи ОС	175
14.3.2.2.	Создание задачи на аудит узла	175

14.3.3.	Unix-подобные ОС: настройка узла	176
14.3.3.1.	Аудит с помощью учетной записи root	177
14.3.3.2.	Аудит с помощью повышения привилегий учетной записи через команду su	177
14.3.3.3.	Аудит с помощью учетной записи с sudo-привилегиями	180
14.3.4.	Unix-подобные ОС: настройка XSpider PRO	180
14.3.4.1.	Добавление учетной записи	181
14.3.4.2.	Создание и запуск задачи на аудит узла	181
14.4.	Системы виртуализации	182
14.4.1.	zVirt Engine 4.4–4.5: настройка узла	182
14.4.1.1.	Создание учетной записи для доступа к узлу через веб-API	183
14.4.1.2.	Создание и настройка роли для аудита	183
14.4.1.3.	Назначение роли учетной записи	183
14.4.1.4.	Снятие ограничений на сессии для учетной записи	184
14.4.2.	zVirt Engine 4.4–4.5: настройка XSpider PRO	184
14.4.2.1.	Добавление учетной записи для доступа к узлу через веб-API	185
14.4.2.2.	Добавление учетной записи для доступа к узлу по SSH	185
14.4.2.3.	Создание задачи на аудит узла с профилем Unix SSH Audit	185
14.4.2.4.	Создание задачи на аудит узла с профилем Web API Audit	186
14.5.	Системы мониторинга сети	187
14.5.1.	Microsoft System Center Configuration Manager (SCCM) 2012–2019: настройка узла ...	187
14.5.1.1.	Создание учетной записи Microsoft SQL Server	188
14.5.1.2.	Создание учетной записи Microsoft SQL Server с помощью запроса	190
14.5.2.	Microsoft System Center Configuration Manager (SCCM) 2012–2019: настройка XSpider PRO	191
14.5.2.1.	Добавление учетной записи для СУБД Microsoft SQL Server	191
14.5.2.2.	Создание задачи на аудит узла	192
14.6.	Другие источники	192
14.6.1.	Продукты Siemens: настройка XSpider PRO	193
14.6.1.1.	Добавление учетной записи	193
14.6.1.2.	Создание задачи на аудит узла	194
14.6.2.	«1С-Битрикс: Управление сайтом» 20.0.0 и выше: настройка узла	194
14.6.2.1.	Настройка удаленного доступа в MySQL	195
14.6.2.2.	Настройка СУБД MySQL	195
14.6.3.	«1С-Битрикс: Управление сайтом» 20.0.0 и выше: настройка XSpider PRO	196
14.6.3.1.	Добавление учетной записи	196
14.6.3.2.	Добавление учетной записи для СУБД Microsoft SQL Server	197
14.6.3.3.	Создание задачи на аудит узла	197
14.6.4.	AVEVA (Wonderware) Historian, Insight, InTouch, System Platform: настройка узла	198
14.6.5.	AVEVA (Wonderware) Historian, Insight, InTouch, System Platform: настройка XSpider PRO	199
14.6.5.1.	Добавление учетной записи	199
14.6.5.2.	Создание задачи на аудит узла	199
14.6.6.	JetBrains Hub 2018.1–2022: настройка узла	200
14.6.6.1.	Создание и настройка роли	200
14.6.6.2.	Создание и настройка учетной записи для доступа к активу	201

14.6.6.3.	Выпуск токена для учетной записи.....	201
14.6.7.	JetBrains Hub 2018.1—2022: настройка XSpider PRO.....	202
14.6.7.1.	Добавление учетной записи.....	202
14.6.7.2.	Создание задачи на аудит узла.....	203
14.6.8.	JetBrains YouTrack 2019: настройка узла.....	203
14.6.8.1.	Добавление новой роли.....	204
14.6.8.2.	Создание учетной записи.....	205
14.6.8.3.	Создание токена.....	205
14.6.9.	JetBrains YouTrack 2019: настройка XSpider PRO.....	206
14.6.9.1.	Добавление учетной записи.....	206
14.6.9.2.	Создание задачи на аудит узла.....	206
14.6.10.	JBrog Artifactory 6—6.23: настройка узла.....	207
14.6.10.1.	Создание учетной записи для доступа к узлу через веб-API.....	207
14.6.10.2.	Создание группы и добавление учетной записи в группу.....	208
14.6.10.3.	Выпуск токена доступа для учетной записи.....	208
14.6.11.	JBrog Artifactory 7 и выше: настройка узла.....	208
14.6.12.	JBrog Artifactory 6 и выше: настройка XSpider PRO.....	209
14.6.12.1.	Добавление учетной записи.....	209
14.6.12.2.	Создание задачи на аудит узла.....	210
14.6.13.	Yokogawa CENTUM VP R4—R6 и ProSafe-RS R2—R4: настройка узла.....	210
14.6.14.	Yokogawa CENTUM VP R4—R6 и ProSafe-RS R2—R4: настройка XSpider PRO.....	210
14.6.14.1.	Добавление учетной записи.....	211
14.6.14.2.	Создание задачи на аудит узла.....	211
14.7.	Стандартные операции для настройки источников.....	212
14.7.1.	Стандартные операции в Windows.....	212
14.7.1.1.	Включение правила межсетевого экрана Windows.....	212
14.7.1.2.	Создание учетной записи ОС.....	212
14.7.1.3.	Добавление учетной записи в локальную политику безопасности.....	213
14.7.1.4.	Добавление учетной записи в локальную группу пользователей.....	214
14.7.2.	Стандартные операции в ОС семейства Unix.....	214
14.7.2.1.	Создание учетной записи в ОС семейства Unix.....	215
14.7.2.2.	Определение используемой службы журналирования.....	216
14.7.2.3.	Перезапуск службы в ОС семейства Unix.....	216
14.7.2.4.	Установка ODBC-драйвера.....	216
14.7.2.5.	Настройка политики control для команд su и sudo в операционной системе «Альт».....	222
14.7.2.6.	Настройка уровня целостности для учетной записи в Astra Linux Special Edition.....	223
14.7.3.	Стандартные операции в системах виртуализации VMware.....	223
14.7.3.1.	Добавление учетной записи и назначение роли в VMware vCenter Server for Windows 5.5, 6.0.....	223
14.7.3.2.	Добавление учетной записи и назначение роли в VMware vCenter Server for Windows 6.5.....	224
14.7.3.3.	Создание учетной записи для VMware vCenter Server Appliance 6.7—8.0.....	225
14.7.3.4.	Назначение роли учетной записи в VMware vCenter Server Appliance 6.7—8.0.....	225

15. Решение проблем.....	226
16. О технической поддержке.....	227
17. Гарантийное обслуживание	231

1. Об этом документе

Руководство администратора содержит справочную информацию и инструкции по администрированию XSpider PRO (далее также — XSpider PRO). Руководство не содержит инструкций по установке XSpider PRO и использованию основных функций продукта.

Руководство адресовано специалистам, администрирующим XSpider PRO.

В документе приняты условные обозначения.

Таблица 1. Условные обозначения

Пример	Описание
Внимание! При выключении модуля снижается уровень защищенности сети	Предупреждения. Содержат информацию о действиях или событиях, которые могут иметь нежелательные последствия
Примечание. Вы можете создать дополнительные отчеты	Примечания. Содержат советы, описания важных частных случаев, дополнительную или справочную информацию, которая может быть полезна при работе с продуктом
► Чтобы открыть файл:	Начало инструкции выделено специальным значком
Нажмите OK	Названия элементов интерфейса (например, кнопок, полей, пунктов меню) выделены полужирным шрифтом
Выполните команду <i>Stop-Service</i>	Текст командной строки, примеры кода, прочие данные, которые нужно ввести с клавиатуры, выделены специальным шрифтом. Также выделены специальным шрифтом имена файлов и пути к файлам и папкам
Ctrl+Alt+Delete	Комбинация клавиш. Чтобы использовать комбинацию, клавиши нужно нажимать одновременно
<Название программы>	Переменные заключены в угловые скобки

2. О сканере безопасности XSpider PRO

С помощью XSpider PRO вы можете:

- обнаруживать узлы в сети;
- собирать и хранить сведения об узлах;
- собирать и хранить сведения об уязвимостях;
- выпускать отчеты и контролировать устранение уязвимостей.

Сканер XSpider PRO включает в себя интерфейс администратора. В состав сканера XSpider PRO включена база знаний, содержащая информацию о проверках и уязвимостях, модуль управления и сканирующее ядро. Данные сканирования хранятся во встроенной базе данных.

При сканировании XSpider PRO создает большой объем сетевого трафика, поэтому для работы необходимо высокоскоростное соединение между ним и исследуемыми объектами.

3. Что нового в версии 1.1

Главное в релизе

В этом разделе приведено краткое описание наиболее важных возможностей, появившихся в новой версии XSpider PRO.

Поддержка установки в инфраструктуре без внешнего DNS-сервера

Добавлена возможность выбрать локальный способ доступа к XSpider PRO. В этом случае FQDN и настройка DNS не требуются, а подключение к продукту выполняется с сервера установки.

Подробнее см. в разделе [Установка продукта \(см. раздел 6\)](#).

Обновление пакетов экспертизы

Теперь пользователи могут обновлять базы знаний модулей, используемых для обработки уязвимостей, вручную или с помощью сценария.

Подробнее см. в разделе [Обновление пакетов экспертизы \(см. раздел 13.3\)](#).

Улучшения

В XSpider PRO версии 1.1 появились следующие улучшения:

- Добавлен новый профиль для обнаружения уязвимостей в Unix-системах — **Unix Audit Vulnerabilities Discovery**. Этот профиль позволяет быстрее выполнять сканирование и уменьшить объем данных, записываемых на диск.
- Доработаны профили сканирования методом черного ящика: исправлены ошибки и улучшена производительность.

4. Аппаратные и программные требования

В этом разделе приведены аппаратные и программные требования к серверу XSpider PRO.

Требования к сетевой инфраструктуре

Для работы XSpider PRO должны быть доступны следующие TCP-порты:

- 4200 — для доступа к веб-интерфейсу управления (HTTPS);
- 22 — для административного доступа (SSH).

Требования к программному обеспечению

XSpider PRO поддерживает установку на 64-разрядные версии следующих ОС:

- Astra Linux Special Edition 1.7.5, 1.7.6 и 1.7.7 (только на базе ядра Linux версии 5.15 и выше в вариантах generic);
- Debian 11 и 12 (на базе ядра Linux версии 5.10 и выше).

Внимание! Установка XSpider PRO должна производиться на ОС, настроенные в соответствии с официальными рекомендациями производителя ОС. Использование модифицированных образов, нестандартных конфигураций ядра или отклонение от базовых параметров может привести к некорректной работе продукта. Positive Technologies не несет ответственности за работоспособность продукта в средах, не соответствующих стандартным конфигурациям указанных ОС.

Для работы в интерфейсе XSpider PRO рекомендуется использовать следующие браузеры:

- Chromium версии 90 или выше;
- Firefox версии 100 или выше;
- Google Chrome версии 90 или выше;
- Mozilla Firefox версии 78 (ESR) или выше;
- Яндекс Браузер версии 21.6 или выше.

Требования к аппаратному обеспечению

Таблица 2. Аппаратные требования к серверу XSpider PRO

Параметр	Минимальные требования	Рекомендуемые требования
Область применения	Сканирование сетей до 512 узлов с использованием модулей PenTest и WebEngine Периодический выпуск отчетов	Сканирование сетей до 512 узлов с использованием модулей Audit, PenTest и WebEngine Регулярный выпуск отчетов
Центральный процессор	Логические ядра: 4 Частота: 2,1 ГГц или выше	Логические ядра: 8 Частота: 2,1 ГГц или выше
Память (ОЗУ)	16 ГБ	32 ГБ или больше
Дисковое пространство	256 ГБ SSD (swap-раздел — 10 ГБ)	512 ГБ SSD
Скорость записи на диск	До 30 МБ/с (для выпуска отчетов об уязвимостях)	
Сетевой адаптер	1 порт со скоростью 1 Гбит/с	
Скорость обработки трафика	Входящий до 180 Кбит/с Исходящий до 30 Кбит/с	

Требования к сетевому взаимодействию компонентов

Межсетевой экран должен быть настроен таким образом, чтобы обеспечить следующие разрешения:

- исходящие TCP-соединения с целевыми узлами на портах 21, 22, 23, 25, 80, 443, 445, 3306, 3389, 8080, 8443;
- исходящие UDP-соединения на портах 53, 161;
- отправка сообщений ICMP Echo Request (ping) для проверки доступности узлов;
- доступ к DNS-серверу для разрешения доменных имен.

5. Принципы безопасной работы

Безопасная работа XSpider PRO гарантируется, если:

- Перед развертыванием XSpider PRO установлены все обновления безопасности для среды функционирования системы (операционное обеспечение).
- Система установлена и администрируется человеком, имеющим достаточную квалификацию и (или) прошедшим курс обучения работе с XSpider PRO и администрированию этого средства защиты информации.
- Работа с системой выполняется в соответствии с эксплуатационной документацией XSpider PRO.

6. Установка XSpider PRO

XSpider PRO может быть установлен как на физическом сервере, так и в виртуальной среде. XSpider PRO устанавливается через терминал с использованием архива <Название архива><Номер версии>.tar.gz из комплекта поставки.

Подготовка к установке

Перед началом установки продукта необходимо подготовить сервер, на который будет установлен продукт. Подробное описание каждого шага подготовки представлено в этом разделе. Сценарий подготовки к установке продукта включает следующие этапы:

1. Определить требуемый способ доступа к XSpider PRO: многопользовательский или локальный. Если планируется многопользовательский доступ, потребуется настроить DNS для разрешения имени сервера.
2. Если используется сервер с Astra Linux Special Edition, проверить состояние механизмов защиты (МКЦ, МРД и ЗПС). Перед началом установки они должны быть отключены.
3. Задать пароль учетной записи суперпользователя (root), если он не был установлен ранее.
4. Разрешить подключение по SSH для учетной записи суперпользователя (root).

Выбор способа доступа

При запуске установки вам будет предложено выбрать способ доступа к XSpider PRO:

- FQDN рекомендуется для удаленного и многопользовательского доступа. Для этого варианта необходимо заранее настроить разрешение доменного имени в IP-адрес сервера установки. Если DNS-сервер отсутствует, потребуется настроить локальную DNS-запись на сервере установки.

Внимание! Настройка DNS не входит в состав установки XSpider PRO и должна быть выполнена администратором инфраструктуры до начала установки продукта.

- Локальный доступ рекомендуется, если подключение к XSpider PRO требуется только с сервера установки. Компоненты продукта будут настроены на IP-адрес 172.17.0.1, используемый по умолчанию в качестве адреса шлюза bridge-сети Docker. Настройка DNS не требуется. Удаленное подключение к XSpider PRO при таком выборе недоступно.

Проверка состояния механизмов защиты Astra Linux

- Чтобы проверить состояние МКЦ, МРД и ЗПС:

1. В терминале выполните команды:

для МКЦ: `sudo astra-mic-control status`

для МРД: `sudo astra-mac-control status`

для ЗПС: `sudo astra-digsig-control status`

2. Убедитесь, что все механизмы отключены (находятся в состоянии НЕАКТИВНО).
3. Если один или несколько механизмов защиты включены, до начала установки XSpider PRO отключите их в соответствии [с документацией Astra Linux](#). Порядок отключения зависит от механизма защиты и используемой версии Astra Linux Special Edition.

Внимание! Состояние этих механизмов также проверяется автоматически при запуске сценария установки. Если состояние хотя бы одного из них не соответствует требованиям или его не удалось определить, установка не начнется.

Настройка пароля учетной записи root

Если пароль для учетной записи суперпользователя (root) не был установлен ранее, необходимо его задать.

- Чтобы задать пароль для учетной записи суперпользователя (root):

1. Выполните команду:
`sudo passwd root`
2. Введите новый пароль и нажмите Enter.
3. Повторно введите пароль для подтверждения.

Если пароль установлен успешно, в терминале появится сообщение `passwd: password updated successfully`.

Внимание! Заданный пароль потребуется во время установки XSpider PRO.

Настройка SSH

Для успешной установки XSpider PRO необходимо предварительно разрешить подключение по SSH для учетной записи суперпользователя (root).

- Чтобы настроить SSH:

1. Откройте файл конфигурации службы SSH:
`sudo nano /etc/ssh/sshd_config`
2. Для параметра `PermitRootLogin` установите значение:
`PermitRootLogin yes`
3. Если параметр отсутствует, добавьте его в конец файла.
4. Для параметра `PasswordAuthentication` установите значение:
`PasswordAuthentication yes`
5. Если параметр отсутствует, добавьте его в конец файла.
6. Сохраните изменения в файле, нажав комбинацию клавиш Ctrl+O и затем Enter.

7. Закройте файл, нажав комбинацию клавиш Ctrl+X.

8. Перезапустите службу SSH:

```
sudo systemctl restart ssh
```

Если служба имеет имя `sshd`, выполните команду `sudo systemctl restart sshd`.

9. Проверьте состояние службы SSH:

```
sudo systemctl status ssh
```

Если служба имеет имя `sshd`, выполните команду `sudo systemctl status sshd`.

В выводе команды должно отображаться состояние `Active: active (running)`.

Внимание! После завершения установки XSpider PRO рекомендуется вернуть значения параметров `PermitRootLogin` и `PasswordAuthentication` к значениям, соответствующим требованиям политики безопасности вашей организации.

Установка продукта

Внимание! Дистрибутив необходимо распаковывать в чистую папку.

Внимание! Если ранее у вас уже был установлен XSpider PRO, перед установкой новой версии необходимо [удалить продукт \(см. раздел 13.5\)](#), а также архив и распакованные каталоги, оставшиеся на сервере.

► Чтобы установить XSpider PRO:

1. Распакуйте архив `<Название архива><Номер версии>.tar.gz`:

```
tar -xf <Название архива><Номер версии>.tar.gz
```

2. Перейдите в каталог с распакованным дистрибутивом:

```
cd deploy
```

3. Разрешите запуск сценария:

```
chmod +x deploy.sh
```

4. Запустите сценарий установки:

```
./deploy.sh 2>&1 | tee -a install.log
```

5. Ознакомьтесь с условиями лицензионного соглашения и нажмите **Exit**.

6. В окне **Лицензионное соглашение** нажмите **Yes**, чтобы принять его условия.

7. В параметре **Задать FQDN стенда [y/n]?** выберите, какой адрес будет использоваться для настройки компонентов продукта, указав одно из значений:

Y — использовать FQDN сервера, где будет установлен продукт.

N — использовать IP-адрес `172.17.0.1`.

8. Если на предыдущем шаге вы указали значение **Y**, то в параметре **Адрес стенда** укажите FQDN сервера, где будет установлен продукт.

Внимание! Значение параметра **Адрес стенда** должно совпадать со значением, указанным в параметре **Имя домена** на этапе установки ОС.

9. В параметре **SSH пользователь стенда с правами sudo** оставьте значение по умолчанию (**root**).
10. В параметре **SSH password** введите пароль учетной записи суперпользователя.

Внимание! При ошибочном вводе пароля процесс установки продукта будет автоматически завершен без возможности ввести пароль повторно. В этом случае вам необходимо начать установку заново.

Начнется установка пакетов.

11. В параметре **Введите пароль для пользователя Administrator (output is hidden)** задайте пароль, который впоследствии будет использоваться для входа в веб-интерфейс продукта.

Внимание! Пароль должен содержать все из перечисленного: буквы латинского алфавита в верхнем и нижнем регистре, цифры и спецсимволы. Если в пароле не будет какого-то из этих элементов, процесс установки продукта будет автоматически завершен. В этом случае вам необходимо начать установку заново.

Внимание! Пароль P@ssw0rd запрещен.

Продолжится установка пакетов. По завершении появится сообщение **Установка продукта успешно завершена**.

После завершения установки XSpider PRO необходимо [войти в веб-интерфейс продукта \(см. раздел 7\)](#) и [активировать его \(см. раздел 8\)](#).

7. Вход в XSpider PRO

Веб-интерфейс продукта доступен по одному из адресов:

- `https://<FQDN сервера с установленным XSpider PRO>:4200` — если во время установки продукта был указан FQDN сервера;
- `https://172.17.0.1:4200` — если во время установки FQDN не был задан.

► Чтобы войти в XSpider PRO:

1. В адресной строке браузера введите ссылку для входа в интерфейс XSpider PRO.
2. В поле **Логин** введите `Administrator`.
3. В поле **Пароль** введите пароль, заданный на этапе установки продукта.

Примечание. Стандартная сессия пользователя в XSpider PRO длится 12 часов. Вы можете продлить сессию, установив флажок **Запомнить меня**: тогда она завершится только через 7 дней бездействия.

4. Нажмите **Войти**.

После первого входа в продукт вам потребуется [активировать его \(см. раздел 8\)](#) с использованием ZIP-файла ключа инсталляции из комплекта поставки.

8. Активация продукта

Вы можете активировать продукт при наличии и отсутствии доступа к интернету.

Онлайн-активация XSpider PRO

- ▶ Чтобы активировать XSpider PRO при наличии доступа к интернету:
 1. Войдите в веб-интерфейс XSpider PRO.
 2. На странице **Активация продукта** загрузите файл ключа инсталляции `installation_key_Positive Technologies_<Идентификационный номер>.zip` из комплекта поставки продукта.

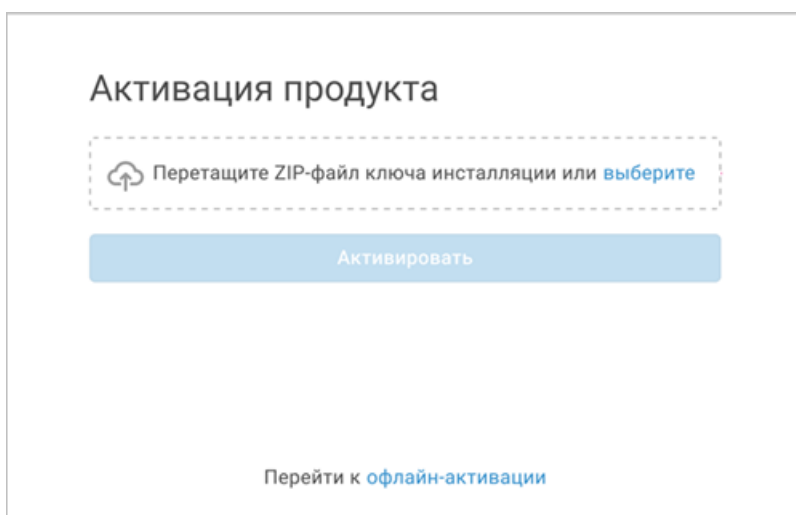


Рисунок 1. Онлайн-активация продукта

3. Нажмите **Активировать**.

Продукт активирован.

Офлайн-активация XSpider PRO

- ▶ Чтобы активировать XSpider PRO при отсутствии доступа к интернету:
 1. Войдите в веб-интерфейс XSpider PRO.
 2. Внизу страницы **Активация продукта** нажмите **Перейти к офлайн-активации**.
 3. На странице **Загрузка ключа инсталляции** выберите файл `installation_key_Positive Technologies_<Идентификационный номер>.zip` из комплекта поставки продукта.

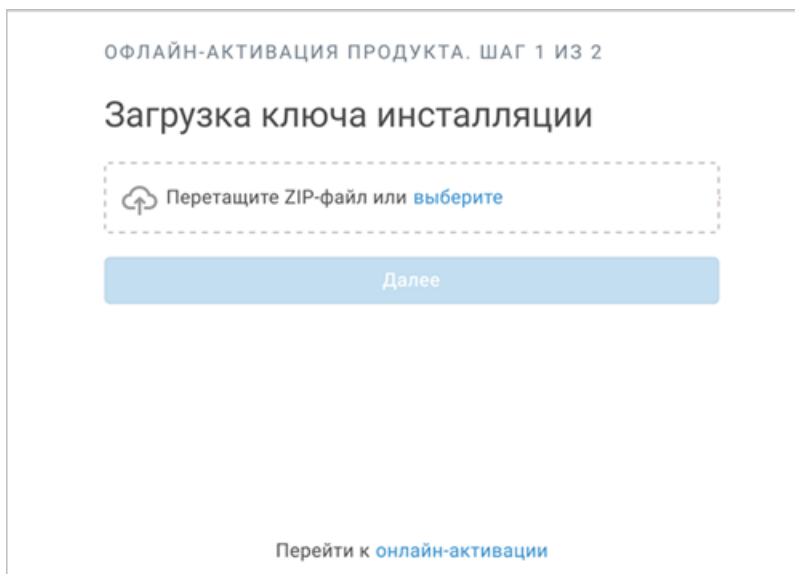


Рисунок 2. Загрузка ключа инсталляции

4. Нажмите **Далее**.
5. На странице **Передача отпечатка пальца и активация** нажмите **Скачать отпечаток пальца**.

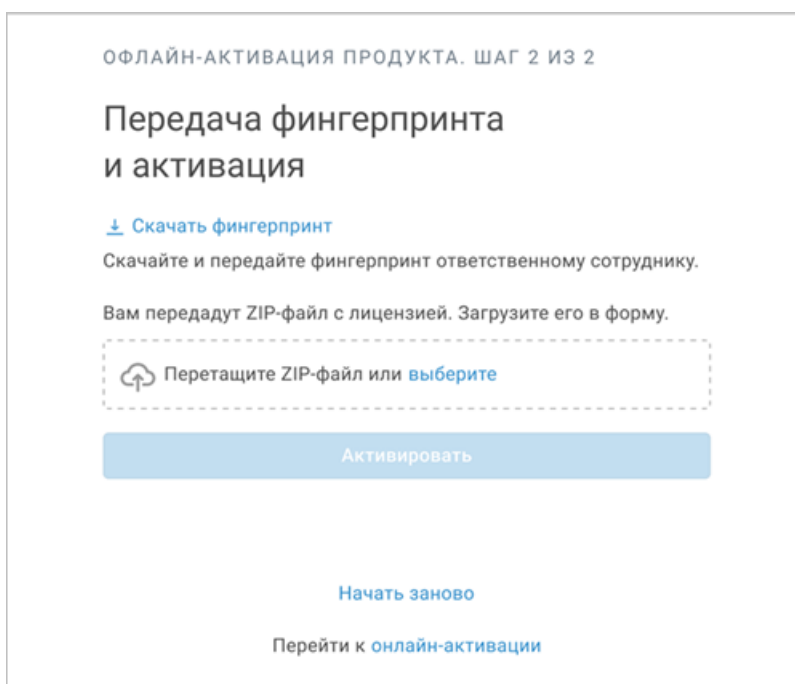


Рисунок 3. Скачивание файла отпечатка пальца

Начнется скачивание файла отпечатка пальца `fingerprint.zip`.

6. Отправьте файл отпечатка пальца менеджеру Positive Technologies.

После этого менеджер Positive Technologies передаст вам ZIP-файл с лицензией, который необходимо использовать на следующем шаге активации.

7. На странице **Передача отпечатка пальца и активация** загрузите полученный файл с лицензией `licenses_Positive Technologies_<Идентификационный номер>.zip`.

ОФЛАЙН-АКТИВАЦИЯ ПРОДУКТА. ШАГ 2 ИЗ 2

Передача отпечатка пальца и активация

[Скачать отпечаток пальца](#)

Скачайте и передайте отпечаток пальца ответственному сотруднику.

Вам передадут ZIP-файл с лицензией. Загрузите его в форму.

 license.zip 

Активировать

[Начать заново](#)

[Перейти к онлайн-активации](#)

Рисунок 4. Загрузка файла с лицензией

8. Нажмите **Активировать**.

Продукт активирован.

9. Лицензирование

Для работы мобильного сканера и его защиты от нелегального использования нужна действующая лицензия.

Одна лицензия может быть активирована только в одном экземпляре продукта. В одном экземпляре продукта одновременно может действовать только одна лицензия. Вы можете добавить еще одну лицензию, которая автоматически активируется и начнет действовать после истечения срока действия текущей лицензии.

Лицензия XSpider PRO содержит набор параметров, определяющих доступную функциональность продукта.

Таблица 3. Параметры и ограничения лицензии XSpider PRO

Параметр	Ограничение функциональности
Срок действия	После окончания срока действия лицензии становится невозможным запуск задач всех типов
Количество сканируемых узлов	Если результаты сканирования по задаче с профилем, отличным от HostDiscovery, содержат узел, не добавленный в лицензию, то невозможно выпустить отчет по этой задаче. При достижении лимита по количеству узлов становится невозможным добавление новых узлов для сканирования и выпуск отчетов по соответствующим задачам
Доступность модулей аудита	Если модули Audit и (или) AuditPLC не включены в лицензию, недоступен сбор данных в режиме аудита (см. раздел 11.4) по профилям соответствующих модулей и выпуск отчетов по соответствующим задачам

Информация о текущей лицензии доступна в интерфейсе XSpider PRO на странице **Параметры → Управление системой → О системе**. Там отображается информация о начале и окончании срока действия лицензии, количестве добавленных узлов и максимальном лимите, а также о доступных модулях.

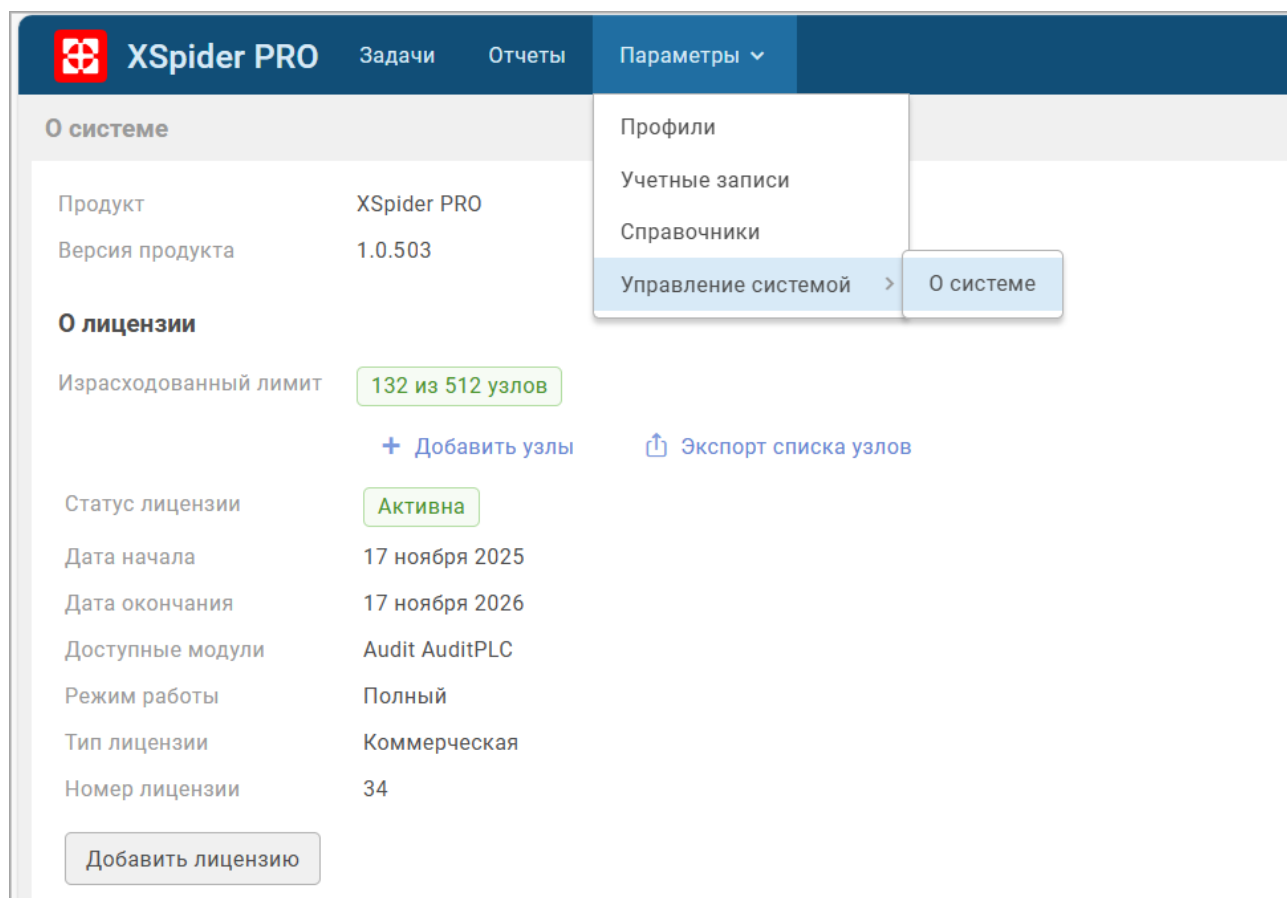


Рисунок 5. Информация о лицензии

Добавление узлов в лицензию

Вы можете загрузить в продукт CSV-файл со списком узлов, которые будут добавлены в лицензию. После этого станет возможным выпуск отчетов по задачам, у которых в качестве целей сбора данных указаны соответствующие узлы.

Вы можете сформировать такой файл вручную или на основе отчета типа [Инвентаризация узлов \(см. раздел 12\)](#), полученного в результате выполнения задачи на [обнаружение узлов в сети \(см. раздел 11.1\)](#) — в этом случае вам потребуется удалить из XLSX-файла отчета всю информацию, кроме списка идентификаторов узлов (FQDN и IP-адреса), и сохранить этот файл в формате CSV.

► Чтобы добавить узлы в лицензию XSpider PRO:

1. В главном меню выберите **Параметры** → **Управление системой** → **О системе**.
2. Нажмите **Добавить узлы**.
3. В открывшемся окне **Добавление узлов в лицензию** загрузите CSV-файл со списком узлов.

Внимание! Файл должен содержать только список FQDN и (или) IP-адресов узлов. Никакая другая информация (например сети, подсети, диапазоны) не должна присутствовать в файле. Вы можете скачать пример файла, чтобы ознакомиться с форматом или заменить значения в нем на узлы, которые вы хотите добавить в лицензию.

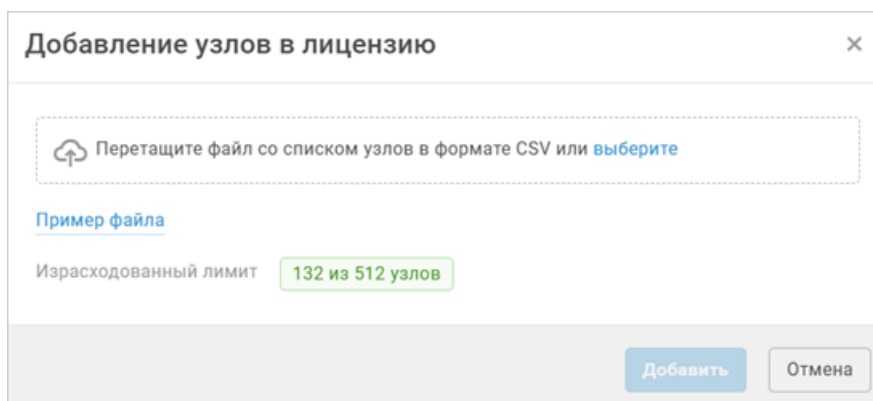


Рисунок 6. Добавление узлов в лицензию

Отобразится информация о количестве узлов, которые будут добавлены в лицензию.

Примечание. Учитываются только новые узлы, которые не добавлялись ранее.

4. Нажмите **Добавить**.

Вы можете скачать список добавленных в лицензию узлов, нажав **Экспорт списка узлов**. Если требуется, вы можете внести изменения в этот список и загрузить CSV-файл снова для добавления новых узлов.

Добавление новой лицензии

Для продолжения использования продукта после истечения срока действия лицензии необходимо добавить новую. Для этого вам потребуется получить от менеджера Positive Technologies новый файл лицензии и добавить его в систему. Вы можете добавить новую лицензию заранее, когда срок действия текущей лицензии еще не истек — в этом случае добавленная лицензия автоматически активируется и начнет действовать после истечения срока действия текущей.

► Чтобы добавить новую лицензию:

1. В главном меню выберите **Параметры** → **Управление системой** → **О системе**.
2. Нажмите **Добавить лицензию**.
3. Нажмите **Продолжить**.
4. Загрузите файл с новой лицензией `licenses_Positive Technologies_<Идентификационный номер>.zip`.

Добавление лицензии

[↓ Скачать фингерпринт](#)
Скачайте и передайте фингерпринт ответственному сотруднику.

Вам передадут ZIP-файл с лицензией. Загрузите его в форму.

 Перетащите ZIP-файл ключа инсталляции или [выберите](#)

Продолжить

Рисунок 7. Добавление лицензии

5. Нажмите **Продолжить**.

Обновление лицензии

 Когда новая лицензия начнет действовать, запускать задачи с некоторыми модулями будет невозможно, так как в новой лицензии модулей меньше, чем в предыдущей.

	Старая лицензия	Новая лицензия
Дата окончания	17 ноября	21 января 2027
Лимит	512 узлов	512 узлов
Доступные модули	Audit AuditPLC	Audit

Добавить лицензию

Рисунок 8. Сравнение лицензий

6. Нажмите **Добавить лицензию**.

10. Начало работы

Рекомендации и инструкции в этом разделе помогут вам быстро получить первые результаты после развертывания XSpider PRO.

Оперативное взаимодействие с ИТ-департаментом

► Чтобы подготовиться к сканированию инфраструктуры, рекомендуется наладить работу с ИТ-департаментом:

1. Предоставьте в ИТ-департамент IP-адреса серверов с установленным XSpider PRO.

С этих IP-адресов должны быть разрешены подключения ко всем портам и подсетям вашей инфраструктуры. Попросите коллег настроить соответствующие сетевые правила на аппаратных межсетевых экранах и других устройствах.

2. Запросите в ИТ-департаменте список подсетей, типов ОС и моделей оборудования ключевых узлов инфраструктуры.

Ключевые узлы — это элементы инфраструктуры, с которых за одно сканирование можно получить больше всего достоверных данных об инфраструктуре. Например, NGFW или коммутатор ядра.

3. Согласуйте учетные записи для аудита, чтобы в дальнейшем указать их в задачах сбора данных.

Стратегическое взаимодействие с ИТ-департаментом

Рекомендуем сразу согласовать с ИТ-командой требования по настройке серверов, рабочих станций и сетевого оборудования при вводе в эксплуатацию. Важно не только поставить задачу по разовой настройке, но и согласовать требования для системы подготовки новых узлов и управления изменениями.

Сканирование инфраструктуры профилем HostDiscovery

Чтобы собрать базовую информацию об узлах, рекомендуется просканировать инфраструктуру профилем HostDiscovery.

Профиль предназначен для поиска узлов в ИТ-инфраструктуре организации, не предназначен для поиска уязвимостей. Для проверки доступности узлов используется ICMP ping, TCP ping или оба метода одновременно.

При сканировании профилем HostDiscovery скорость поступления SYN-пакетов на сетевые устройства может резко возрасти. Кроме того, быстро растут списки подключений на устройствах. Это может нарушить работоспособность сетевых устройств. Чтобы этого не произошло, важно определить оптимальные значения параметров HostDiscovery для вашей инфраструктуры.

► Чтобы настроить HostDiscovery на оптимальную производительность:

1. Укажите в параметрах HostDiscovery скорость отправки 100 пакетов в секунду. Это безопасное значение для любых инфраструктур.
2. Согласуйте с ИТ-департаментом время начала сканирования и процедуру оперативной связи. ИТ-специалисты будут проводить мониторинг сетевой инфраструктуры в ходе сканирования.
3. Сообщите в ИТ-департамент о завершении сканирования.
4. В случае одобрения ИТ-специалистов увеличьте скорость отправки пакетов.

Повторите эту процедуру несколько раз, чтобы определить значения параметров модуля HostDiscovery, оптимальные с точки зрения скорости сканирования и нагрузки на сеть.

Первый поиск узлов в сети

Сканирование одного узла профилем HostDiscovery занимает до пяти минут. Рекомендуется сегментировать процесс поиска. Например, вы можете сегментировать поиск по подсетям, данные о которых предоставил ИТ-департамент.

► Чтобы найти узлы в инфраструктуре:

1. В главном меню выберите **Задачи**.
2. Нажмите **Создать задачу** → **Обнаружение узлов**.
3. Введите название задачи.
4. Отключите проверку с помощью эхо-запроса ICMP.
5. В поле **Порты TCP для проверки с помощью SYN-пакетов** укажите список часто используемых портов.

Пример:

21, 22, 25, 53, 80, 110, 123, 139, 143, 443, 445, 465, 631, 993, 995, 3389

Примечание. Рекомендуется согласовать список портов с ИТ-департаментом.

6. Включите отображение дополнительных параметров сбора данных.
7. Выберите **Параметры проверки узлов**.
8. Включите определение операционной системы.

Примечание. HostDiscovery может определить семейство ОС. Более точно определить ОС можно с помощью профиля Service Discovery.

9. Для параметров **Максимальная скорость отправки ARP-запросов** и **Максимальная скорость отправки пакетов** укажите значения 100.

Примечание. Эти значения в дальнейшем необходимо будет скорректировать на основе обратной связи от ИТ-департамента.

Параметры сбора данных

Импорт

Экспорт

Профиль

HostDiscovery

Способы проверки узлов

Параметры проверки узлов

Объем занимаемой памяти

Работа модуля

Параметры проверки узлов

Присваивать активам значения FQDN из целей сбора данных

Определение операционной системы

Проводить

Не проводить

Параметры проверок

Проверка с помощью ARP-запросов

Не проводить

Проводить

Считать узел активным при ответе на ARP-запрос

Считать узел активным при любом ответе

Сканирование активных узлов

Не проводить

Проводить

Максимальное количество неудачных проверок

2

Интервал между проверками

900

мс

Тайм-аут ответа

1000

мс

Максимальная скорость отправки ARP-запросов

100

пак./сек

Максимальная скорость отправки пакетов

100

пак./сек

Показывать дополнительные параметры

Рисунок 9. Параметры первого поиска узлов профилем HostDiscovery

10. В поле **Сетевые адреса** укажите одну или несколько подсетей, предоставленных ИТ-департаментом.

Внимание! Не рекомендуется указывать в качестве цели сбора данных подсети /8 и меньше. Для первого поиска узлов рекомендуется указывать подсети не меньше /16.

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

Указывая ограниченный список сканируемых портов TCP и только существующие подсети, вы можете максимально сократить время на первый поиск узлов.

Начало работы

28

Выпуск отчета об обнаруженных узлах

После успешного завершения задачи вы можете выпустить отчет **Инвентаризация узлов**, чтобы получить IP-адреса обнаруженных узлов.

Примечание. Отчет по результатам HostDiscovery содержит ограниченный набор информации, которая необходима при создании задач на сбор данных.

► Чтобы выпустить отчет по результатам завершенной задачи:

1. В главном меню выберите **Отчеты**.
2. Нажмите **Создать отчет** → **Инвентаризация узлов**.
3. Выберите задачу и ее результат.
4. Нажмите **Выпустить**.
5. После успешного выпуска сохраните отчет по ссылке в карточке.

Теперь вы можете перейти к сбору данных на обнаруженных узлах.

Определение ОС профилем Service Discovery

С помощью профиля Service Discovery можно быстро определить семейство ОС и службы, работающие на узлах. Профиль сканирует узлы без использования учетных записей (методом черного ящика).

Для определения семейств ОС и служб не требуется изменять значения параметров Service Discovery по умолчанию.

► Чтобы выполнить сканирование профилем Service Discovery:

1. В главном меню выберите **Задачи**.
2. Нажмите **Создать задачу** → **Сбор данных**.
3. Введите название задачи.
4. Выберите профиль **Service Discovery**.
5. Укажите цели для сбора данных на основе отчета **Инвентаризация узлов**.
6. Нажмите **Сохранить и запустить** → **Запустить сбор данных**.

После завершения задачи вы можете выпустить отчет **Операционные системы и открытые порты на узлах**. Зная семейство ОС и службы на узлах, вы можете определить ключевые узлы сети и выполнить их пентест или аудит.

Пентест ключевых узлов

Сканирование модулем PenTest выполняется без использования учетных записей (методом черного ящика). Позволяет проводить тестирование на проникновение, поиск уязвимостей и информации о связанном с ними ПО. Все профили пентеста сканируют порты и определяют работающие службы.

Доступны следующие стандартные профили модуля PenTest:

- **Bruteforce PenTest.** Для подбора учетных записей. Сканирует только стандартные порты служб (например, TCP 21–23, TCP 25 или TCP 80).
- **Full PenTest.** Для полного сканирования и поиска уязвимостей с использованием безопасных проверок и подбора учетных записей. Сканирование одного узла занимает до 8 минут.
- **Service Discovery.** Для быстрого определения семейства ОС и служб, работающих на узлах. Поиск уязвимостей не выполняется.

► Чтобы выполнить поиск уязвимостей методом черного ящика:

1. Создайте и выполните задачу на сбор данных с профилем **Bruteforce PenTest** или **Full PenTest**.
2. Выпустите отчет **Операционные системы и открытые порты на узлах** или отчет по уязвимостям на основе полученных результатов.

Аудит ключевых узлов

Внимание! Профили модулей Audit и AuditPLC доступны только при наличии соответствующей лицензии (см. раздел 9).

После определения семейств ОС на узлах вы можете выполнить их аудит. В ходе аудита узлы сканируются методом белого ящика. В параметрах задачи нужно указать учетную запись, которой предоставлены права на выполнение [команд для сбора данных](#) (см. раздел 11.4.2).

Доступны следующие стандартные профили модуля Audit:

- **SSH Network Device Audit.** Для аудита сетевых устройств по протоколу SSH. Профиль также может использоваться для сканирования сетевых устройств, не требующих повышения привилегий. Например, устройств Cisco.
- **Unix SSH Audit.** Для сканирования уязвимостей в Docker-контейнерах и их образах. Он выполняет автоматическую проверку конфигураций SSH-сервера в Unix-подобных системах на соответствие требованиям безопасности, а также анализирует установленные пакеты на предмет известных уязвимостей. Сканирование одного узла занимает до 5 минут.

Примечание. Профиль **Unix SSH Audit** требует большого количества вычислительных ресурсов и занимает продолжительное время. Рекомендуется использовать его только при крайней необходимости. Вместо него рекомендуется использовать профиль **Unix Audit Vulnerabilities Discovery**.

- **Windows Audit.** Для аудита Windows и ПО, установленного на узлах под управлением Windows, а также АСУ ТП. Сканирование одного узла 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.

Примечание. Профиль **Windows Audit** требует большого количества вычислительных ресурсов и занимает продолжительное время. Рекомендуется использовать его только при крайней необходимости. Вместо него рекомендуется использовать профиль **Windows Audit Vulnerabilities Discovery**.

- **Windows Audit Vulnerabilities Discovery.** Для поиска уязвимостей на узлах с Windows. Профиль собирает сведения об операционной системе и установленных приложениях, необходимые для обнаружения уязвимостей, но не выполняет полный аудит системы. Подходит для случаев, когда требуется только поиск уязвимостей без сбора дополнительных данных, доступных при сканировании с профилем **Windows Audit**. Не предназначен для аудита узлов АСУ ТП.

Примечание. По результатам тестирования сканирование с этим профилем выполнялось на 16% быстрее, чем с профилем **Windows Audit**, а результаты сканирования занимали на 30% меньше места на диске.

- **Unix Audit Vulnerabilities Discovery.** Для поиска уязвимостей на узлах с ОС семейства Unix. Профиль собирает сведения об операционной системе и установленных приложениях, необходимые для обнаружения уязвимостей, но не выполняет полный аудит системы. Подходит для случаев, когда требуется только поиск уязвимостей без сбора дополнительных данных, доступных при сканировании с профилем **Unix SSH Audit**. Не предназначен для аудита узлов АСУ ТП.

Примечание. По результатам тестирования сканирование с этим профилем выполнялось на 30% быстрее, чем с профилем **Unix SSH Audit**, а результаты сканирования занимали в 10 раз меньше места на диске. Пиковое потребление оперативной памяти процессом сканирования снизилось на 29%.

Доступны следующие стандартные профили модуля AuditPLC:

- S7ISO AuditPLC;
- S7TCP AuditPLC;
- SNMP AuditPLC;
- SNMP and S7TCP AuditPLC;
- SNMP and UMAS AuditPLC;
- UMAS AuditPLC.

► Чтобы добавить учетную запись в XSpider PRO:

1. В главном меню выберите **Параметры** → **Учетные записи**.
2. Нажмите **Добавить учетную запись** и выберите тип.
3. Заполните обязательные поля.

Примечание. В дополнение к названиям вы можете использовать метки, чтобы быстрее находить учетные записи.

- ▶ Чтобы выполнить поиск уязвимостей методом белого ящика:
 1. Создайте и выполните задачу на сбор данных с профилем аудита.
 2. Выпустите отчет по уязвимостям на основе полученных результатов, например, **Уязвимости по узлам**.

11. Работа с задачами

Для получения данных с ИТ-инфраструктуры организации в XSpider PRO необходимо создать задачу. В задаче необходимо указать цели, с которых нужно получить данные, например IP-адреса или FQDN.

Список всех задач, а также инструменты для работы с ними доступны на странице **Задачи** → **Задачи на сбор данных**. Вы можете создавать, копировать, изменять, удалять, запускать, ставить на паузу и останавливать задачи. При выборе задачи в списке справа открывается карточка с информацией о задаче и возможностью просмотреть историю запусков подзадач и [выпустить отчет по задаче \(см. раздел 12\)](#). По двойному нажатию задачи в списке вы также можете перейти к просмотру истории запусков подзадач и скачиванию различных отчетов, описанных ниже.

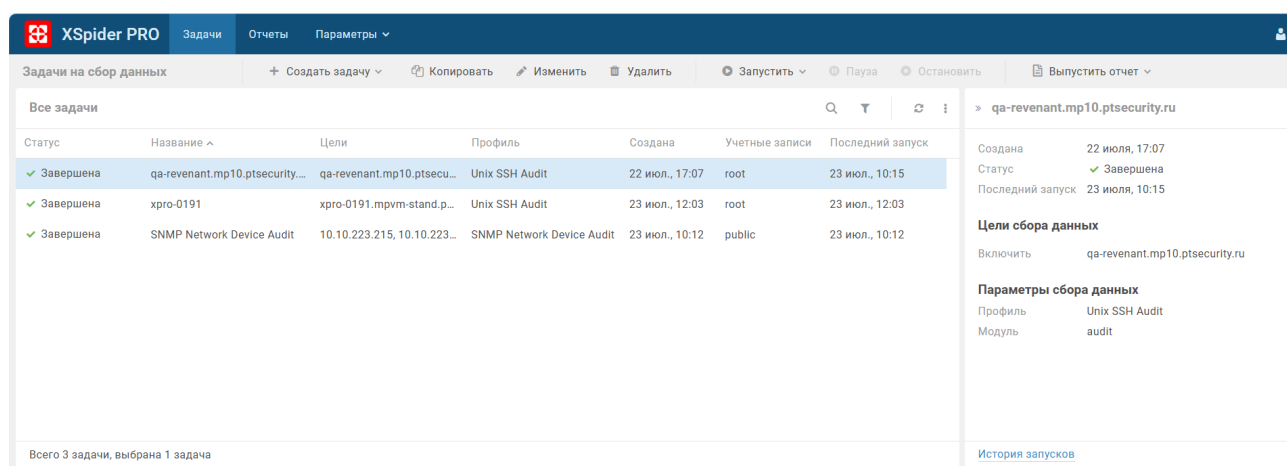


Рисунок 10. Страница задач

В зависимости от выбранного в задаче профиля XSpider PRO запускает соответствующий модуль для сбора данных.

В рамках задачи система создает подзадачи, которые выполняются автоматически.

Внимание! Существует ограничение на количество одновременно выполняемых подзадач — 3 для каждого из модулей. При достижении этого значения новые подзадачи ставятся в очередь.

Задачи могут использоваться для:

- **Обнаружения узлов.** Система обнаруживает активные узлы в рамках указанных IP-адресов, диапазонов IP-адресов, FQDN или подсетях.
- **Сканирования узлов методом черного ящика.** Система обнаруживает открытые порты и сетевые сервисы на этих портах.

- **Аудита узлов методом белого ящика.** Система определяет детальную конфигурацию операционной системы, установленной на узле, перечень установленного программного обеспечения, список открытых портов, перечень пользователей, которые зарегистрированы на узле. Формирует перечень уязвимостей.
- **Сканирования веб-приложений.** Система обнаруживает параметры веб-приложений, выявляет уязвимые параметры, формирует перечень уязвимых библиотек.
- **Сканирования Docker-контейнеров.** Система проверяет конфигурацию SSH-сервера в Unix-подобных системах на соответствие требованиям безопасности.

Скачивание отчета о выполнении задачи

На странице с историей запусков вы можете скачать отчет о результатах выполнения задачи по отдельному запуску. Отчет содержит информацию о выбранном запуске, запускаемой задаче и подзадачах, относящихся к ней, а также сообщения из подзадач с информацией об их источнике и времени получения.

► Чтобы скачать отчет о выполнении задачи:

1. В главном меню выберите **Задачи**.
2. Дважды нажмите задачу.
3. Выберите запуск задачи, по которому необходимо скачать отчет.
4. Нажмите  и выберите **Скачать отчет**.

Экспорт результатов выполнения задачи

Вы можете экспортировать результаты выполнения задачи на сбор данных.

► Чтобы экспортировать результаты выполнения задачи:

1. В главном меню выберите **Задачи**.
2. Дважды нажмите задачу.
3. Выберите запуск задачи, который необходимо экспортировать.
4. Нажмите  и выберите **Экспорт результатов сканирования**.

Будет сохранен файл в формате ZIP.

Просмотр и скачивание журнала выполнения подзадачи

Вы можете просмотреть и скачать детализированный отчет о ходе выполнения каждой из подзадач в виде журнала. Он может быть полезен, например, для анализа ошибок в процессе выполнения подзадачи.

► Чтобы скачать журнал выполнения подзадачи:

1. В главном меню выберите **Задачи**.
2. Дважды нажмите задачу.
3. Выберите подзадачу, журнал выполнения которой требуется скачать.
4. Нажмите **Скачать журнал**.

Начнется скачивание ZIP-архива, содержащего LOG-файл с журналом.

Вы также можете просмотреть журнал выполнения подзадачи в веб-интерфейсе продукта, нажав  **Журнал подзадачи**.

Проверка подключения для задач аудита

Перед запуском задачи аудита вы можете проверить для нее подключение к целевым узлам: доступность узлов и корректность указанной учетной записи для сканирования.

Для проверки в задаче должны быть настроены необходимые для выбранного профиля параметры. Проверка осуществляется для всех транспортов, которые используются в профиле выбранного для задачи модуля.

► Чтобы проверить подключение для задач аудита:

1. В главном меню выберите **Задачи**.
2. Выберите одну или несколько задач аудита.
3. Нажмите **Запустить** → **Проверить подключение**.
4. Выберите вариант проверки.

По завершении проверки статус задачи изменяется на **Завершена**. Цвет значка показывает результат проверки:



— все подзадачи завершены без ошибок.



— часть подзадач завершена с ошибками.



— все подзадачи завершены с ошибками.

Вы можете получить дополнительные сведения по подзадачам в истории запусков задачи.

В этом разделе

[Обнаружение узлов в сети \(см. раздел 11.1\)](#)

[Настройка параметров сбора данных \(см. раздел 11.2\)](#)

[Сбор данных в режиме пентеста \(см. раздел 11.3\)](#)

[Сбор данных в режиме аудита \(см. раздел 11.4\)](#)

[Сбор данных о веб-приложениях \(см. раздел 11.5\)](#)

11.1. Обнаружение узлов в сети

Чтобы собрать базовую информацию об узлах, рекомендуется просканировать инфраструктуру профилем HostDiscovery.

Профиль предназначен для поиска узлов в IT-инфраструктуре организации, не предназначен для поиска уязвимостей. Для проверки доступности узлов используется ICMP ping, TCP ping или оба метода одновременно.

Сканирование одного узла профилем HostDiscovery занимает до пяти минут.

Новая задача на обнаружение узлов

Название

Добавить описание

Параметры сбора данных

Импорт

Экспорт

Профиль

HostDiscovery

Способы проверки узлов

Параметры проверки узлов

Показывать дополнительные параметры

Способы проверки узлов

Проводить проверку с помощью эхо-запроса ICMP

Порты TCP для проверки с помощью SYN-пакетов

22;80;443;111;135

Цели сбора данных

Примеры допустимых адресов:

- IP-адрес v4 или v6 (192.168.0.0 или fe80::)
- диапазон IP-адресов (192.168.0.1-192.168.0.25)
- подсеть (192.168.0.0/24 или fe80::/10)
- FQDN (example.tuc.noao.ru)

Включить

Исключить

Сохранить

Сохранить и запустить

Отмена

Рисунок 11. Создание новой задачи на обнаружение узлов в сети

► Чтобы найти узлы в инфраструктуре:

1. В главном меню выберите **Задачи**.
2. Нажмите **Создать задачу** → **Обнаружение узлов**.
3. Введите название задачи.
4. Укажите **Параметры сбора данных**.
5. Укажите **Цели сбора данных**:

В поле **Включить** укажите IP-адреса или FQDN произвольных узлов, диапазонов, сетей и подсетей, в которых требуется выполнить поиск узлов.

В поле **Исключить** укажите IP-адреса или FQDN произвольных узлов, диапазонов, сетей и подсетей, которые требуется игнорировать при поиске узлов.

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

Настраивать параметры сканирования 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. Некоторые параметры становятся доступны после активации переключателя **Показывать дополнительные параметры**. Ниже приводятся описания параметров в каждой секции.

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 узлам значения FQDN из целей сбора данных** — при включении узлам, полученным в результате сканирования инфраструктуры, присваиваются FQDN, указанные в целях сбора данных. Включение позволяет избежать дублирования узлов 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 времени 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 сервере:

- **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** — при включении во время сбора событий, время регистрации которых значительно отличается от текущего времени (по умолчанию более чем на сутки), это время не будет заменяться временем сбора.
- **Интервал отправки уведомлений о состоянии** — поле для ввода интервала отправки уведомлений об активности модуля в миллисекундах.
- **Повторное подключение: максимальное количество попыток** — поле для ввода максимального количества попыток модуля восстановить связь в случае ее разрыва.
- **Повторное подключение: интервал между попытками** — поле для ввода времени между попытками модуля восстановить связь в миллисекундах.
- **Справочник с параметрами журналирования** — раскрывающийся список для выбора справочника XSpider PRO с параметрами журналирования работы модуля.
- **Сохранять статистику сбора данных** — при включении в журнале модуля сохраняется информация об объеме собранных модулем данных (в байтах), количестве пакетов с данными и их объеме (в байтах).

11.2. Настройка параметров сбора данных

С помощью параметров сбора данных вы можете:

- создавать пользовательские профили сканирования и сохранять параметры задач на сбор данных;
- управлять учетными записями для задач аудита, чтобы получать необходимые привилегии на узлах;
- добавлять справочники, чтобы расширить набор данных, собираемых при аудите.

В этом разделе

[Профили сканирования \(см. раздел 11.2.1\)](#)

[Учетные записи для аудита \(см. раздел 11.2.2\)](#)

[Справочники для аудита \(см. раздел 11.2.3\)](#)

11.2.1. Профили сканирования

Профиль — шаблон параметров задачи на поиск узлов или сбор данных.

Профили бывают стандартные и пользовательские. Стандартные профили предустановлены, вы не можете их изменять и удалять. На базе стандартных вы можете создавать пользовательские профили и настраивать параметры сбора данных.

На странице **Профили** вы можете создавать, изменять и удалять пользовательские профили. Пользовательские профили можно также экспортировать и импортировать. Файл экспорта сохраняется в формате JSON.

► Чтобы создать пользовательский профиль на базе стандартного:

1. В главном меню выберите **Параметры** → **Профили**.
2. В панели **Список профилей** выберите профиль.
3. Введите название профиля.
4. Если требуется, в панели **Параметры профиля** в раскрывающемся списке **Учетная запись** выберите учетную запись для сбора данных.

В зависимости от профиля для выбора учетной записи вам может потребоваться указать другие параметры профиля или выбрать другой пункт в иерархическом списке.

Примечание. В раскрывающемся списке **Учетная запись** отображаются учетные записи, при добавлении которых была выбрана метка используемого профилем метода сбора данных или не было выбрано никаких меток.

5. Если требуется, настройте другие параметры профиля.
6. Нажмите **Сохранить**.

11.2.2. Учетные записи для аудита

Учетные записи используются для авторизации на узле для проведения аудита. При добавлении учетной записи вы можете указать одну или несколько меток, соответствующих методу сбора данных, при котором она будет использоваться. Добавлять, изменять и удалять учетные записи вы можете на странице **Учетные записи**.

Поддерживаются учетные записи следующих типов:

- «логин — пароль»;
- «пароль»;
- «сертификат»;
- Local Administrator Password Solution (LAPS) версии 6.2.

► Чтобы добавить учетную запись типа «логин — пароль»:

1. В главном меню выберите **Параметры** → **Учетные записи**.
2. Нажмите **Добавить учетную запись** → **Логин — пароль**.
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**.

Примечание. При вводе различаются заглавные и строчные буквы.

6. Если для доступа к источнику используется доменная учетная запись, введите имя домена.
7. Нажмите **Сохранить**.

► Чтобы добавить учетную запись типа «пароль»:

1. В главном меню выберите **Параметры** → **Учетные записи**.
2. Нажмите **Добавить учетную запись** → **Пароль**.
3. Введите название учетной записи.
4. В поле **Пароль** введите пароль и подтвердите его в поле **Подтверждение пароля**.

Примечание. При вводе различаются заглавные и строчные буквы.

5. Нажмите **Сохранить**.

► Чтобы добавить учетную запись типа «сертификат»:

1. В главном меню выберите **Параметры** → **Учетные записи**.
2. Нажмите **Добавить учетную запись** → **Сертификат**.
3. В поле **Сертификат** введите путь к файлу сертификата.

Вы можете указать расположение файла сертификата по ссылке **Выбрать** или перетащить файл в поле **Сертификат**.

Внимание! Размер файла сертификата должен быть меньше 100 КБ.

4. Если требуется, в поле **Логин** введите логин учетной записи.

5. Если требуется, в поле **Пароль** введите пароль и подтвердите его в поле **Подтверждение пароля**.

Примечание. При вводе различаются заглавные и строчные буквы.

6. Нажмите **Сохранить**.

► Чтобы добавить учетную запись типа LAPS:

1. В главном меню выберите **Параметры** → **Учетные записи**.
2. Нажмите **Добавить учетную запись** → **LAPS**.
3. Введите название учетной записи.
4. В поле **Адрес** введите FQDN или IP-адрес контроллера домена Active Directory.
5. В поле **Порт** введите номер TCP-порта для подключения к контроллеру домена.
6. Если требуется, в поле **База поиска активов** введите фильтры для ускорения поиска активов в домене Active Directory.
7. Укажите учетную запись с правами на просмотр атрибутов объектов типа «Компьютер».
8. Введите логин для подключения к целевым активам.

Логин по умолчанию — `Administrator`.

9. Нажмите **Сохранить**.

11.2.3. Справочники для аудита

В справочниках могут храниться дополнительные данные и сценарии для расширения возможностей аудита и пентеста. Например, справочник `audit_expertise_extension` содержит сценарии на языке программирования Python, а справочник `mssql_accounts` — типичные комбинации логинов и паролей администратора БД для подбора.

Справочники бывают стандартные и пользовательские. Стандартные справочники предустановлены, вы не можете их изменять и удалять. Создавать, изменять и удалять пользовательские справочники вы можете на странице **Справочники**.

► Чтобы создать справочник:

1. В главном меню выберите **Параметры** → **Справочники**.
2. Нажмите **Создать**.
3. В поле **Название** введите название справочника.
4. В поле **Содержимое** введите текст для справочника.

Для деления текста на колонки вы можете использовать табуляцию (комбинация клавиш Alt+009). Вы также можете написать текст в любом текстовом редакторе и скопировать в поле **Содержание**.

5. Нажмите **Сохранить**.

Справочник можно выбрать в параметре **Расширение сбора данных** при создании задачи на аудит или при создании пользовательского профиля аудита.

11.3. Сбор данных в режиме пентеста

Сканирование модулем PenTest выполняется без использования учетных записей (методом черного ящика). Позволяет проводить тестирование на проникновение, поиск уязвимостей и информации о связанном с ними ПО. Все профили пентеста сканируют порты и определяют работающие службы.

Доступны следующие стандартные профили модуля PenTest:

- **Bruteforce PenTest**. Для подбора учетных записей. Сканирует только стандартные порты служб (например, TCP 21–23, TCP 25 или TCP 80).
- **Full PenTest**. Для полного сканирования и поиска уязвимостей с использованием безопасных проверок и подбора учетных записей. Сканирование одного узла занимает до 8 минут.
- **Service Discovery**. Для быстрого определения семейства ОС и служб, работающих на узлах. Поиск уязвимостей не выполняется.

Внимание! Перед началом сканирования систем Firebird, Microsoft SQL Server, MySQL, Oracle, PostgreSQL и ClickHouse с использованием профилей **Service Discovery**, **Bruteforce PenTest**, **Fast PenTest**, **Full PenTest** и **Safe PenTest** требуется предварительно [установить ODBC-драйвер \(см. раздел 14.7.2.4\)](#).

► Чтобы выполнить поиск уязвимостей методом черного ящика:

1. В главном меню выберите **Задачи**.
2. Нажмите **Создать задачу** → **Сбор данных**.
3. Введите название задачи.
4. Выберите профиль.
5. Укажите **Цели сбора данных**:

В поле **Включить** укажите IP-адреса или FQDN произвольных узлов, диапазонов, сетей и подсетей, которые требуется сканировать для сбора данных.

В поле **Исключить** укажите IP-адреса или FQDN произвольных узлов, диапазонов, сетей и подсетей, которые требуется игнорировать при сборе данных.

Новая задача на сбор данных

Название

Добавить описание

Параметры сбора данных

Импорт Экспорт

Профиль

Bruteforce PenTest

Общие параметры сканирования

Сканирование портов

Сканирование UDP-служб

Поиск уязвимостей

Подбор учетных данных

IBM DB2

Microsoft SQL Server

Oracle Database

Oracle Database, подбор SID

Oracle MySQL

PostgreSQL

SAP Sybase ASE

SAP через DIAG

Показывать дополнительные параметры

Общие параметры сканирования

Метод сканирования портов

SYN-пакеты

Подключение

Искать сетевые принтеры

Цели сбора данных

Примеры допустимых адресов:

- IP-адрес v4 или v6 (192.168.0.0 или fe80::)
- диапазон IP-адресов (192.168.0.1-192.168.0.25)
- подсеть (192.168.0.0/24 или fe80::/10)
- FQDN (example.tuc.noao.ru)

Включить

Исключить

Сохранить

Сохранить и запустить

Отмена

Рисунок 12. Создание задачи на сбор данных в режиме пентеста с профилем Bruteforce PenTest

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

По результатам задачи вы можете выпустить отчеты по уязвимостям на узлах. Если у вас есть предыдущие результаты пентеста тех же узлов, вы можете выпустить дифференциальный отчет по уязвимостям.

Настраивать параметры сканирования 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. Некоторые параметры становятся доступны после активации переключателя **Показывать дополнительные параметры**. Ниже приводятся описания параметров в каждой секции.

В этом разделе

[Общие параметры сканирования \(см. раздел 11.3.1\)](#)

[Сканирование портов \(см. раздел 11.3.2\)](#)

[Сканирование UDP-служб \(см. раздел 11.3.3\)](#)

[Поиск уязвимостей — Подбор учетных данных — IBM DB2 \(см. раздел 11.3.4\)](#)

[Поиск уязвимостей — Подбор учетных данных — Microsoft SQL Server \(см. раздел 11.3.5\)](#)

[Поиск уязвимостей — Подбор учетных данных — Oracle Database \(см. раздел 11.3.6\)](#)

[Поиск уязвимостей — Подбор учетных данных — Oracle Database, подбор SID \(см. раздел 11.3.7\)](#)

[Поиск уязвимостей — Подбор учетных данных — Oracle MySQL \(см. раздел 11.3.8\)](#)

[Поиск уязвимостей — Подбор учетных данных — SAP Sybase ASE \(см. раздел 11.3.9\)](#)

[Поиск уязвимостей — Подбор учетных данных — SAP через DIAG \(см. раздел 11.3.10\)](#)

[Поиск уязвимостей — Подбор учетных данных — SAP через RFC \(см. раздел 11.3.11\)](#)

[Поиск уязвимостей — Подбор учетных данных — Symantec pcAnywhere \(см. раздел 11.3.12\)](#)

[Поиск уязвимостей — Подбор учетных данных — Virtual Network Computing \(см. раздел 11.3.13\)](#)

[Поиск уязвимостей — Подбор учетных данных — VMware vSphere \(см. раздел 11.3.14\)](#)

[Поиск уязвимостей — Подбор учетных данных — По протоколу FTP \(см. раздел 11.3.15\)](#)

[Поиск уязвимостей — Подбор учетных данных — По протоколу NetBIOS \(см. раздел 11.3.16\)](#)

[Поиск уязвимостей — Подбор учетных данных — По протоколу POP3 \(см. раздел 11.3.17\)](#)

[Поиск уязвимостей — Подбор учетных данных — По протоколу RDP \(см. раздел 11.3.18\)](#)

[Поиск уязвимостей — Подбор учетных данных — По протоколу SIP \(см. раздел 11.3.19\)](#)

[Поиск уязвимостей — Подбор учетных данных — По протоколу SMTP \(см. раздел 11.3.20\)](#)

[Поиск уязвимостей — Подбор учетных данных — По протоколу SNMP \(см. раздел 11.3.21\)](#)

[Поиск уязвимостей — Подбор учетных данных — По протоколу SSH \(см. раздел 11.3.22\)](#)

[Поиск уязвимостей — Подбор учетных данных — По протоколу Telnet \(см. раздел 11.3.23\)](#)

[Поиск уязвимостей — Подбор учетных данных — Фаматек RAdmin \(см. раздел 11.3.24\)](#)

[Поиск уязвимостей — Поиск файлов \(см. раздел 11.3.25\)](#)

[Поиск уязвимостей — Сканирование по LDAP \(см. раздел 11.3.26\)](#)

[Дополнительные параметры модуля Pentest \(см. раздел 11.3.27\)](#)

11.3.1. 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.

11.3.2. 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.

11.3.3. 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).**

11.3.4. 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.
 - **Справочник с парами «логин — пароль»** — раскрывающийся список для выбора справочника XSpider PRO с парами «логин — пароль».

- **Подбирать имена баз данных** — по кнопке **Добавить** вы можете добавить поля для ввода имен, среди которых будет выполняться поиск имен БД, доступных в СУБД.
- **Максимальное количество потоков** — поле для ввода максимального количества параллельных потоков для подбора учетных данных.

11.3.5. Поиск уязвимостей — Подбор учетных данных — Microsoft SQL Server

Секция содержит следующие параметры для настройки подбора учетных данных пользователей СУБД Microsoft SQL Server:

- **Справочник с парами «логин — пароль»** — раскрывающийся список для выбора справочника XSpider PRO с парами «логин — пароль».
- **Максимальное количество потоков** — поле для ввода максимального количества параллельных потоков для подбора учетных данных.

11.3.6. 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 XSpider PRO (в секции параметров **Oracle Database, подбор SID**).
- **Подбирать пароли для найденных SID** — при включении выполняется подбор паролей для найденных SID или SERVICE_NAME.
 - **Справочник с парами «логин — пароль»** — раскрывающийся список для выбора справочника XSpider PRO с парами «логин — пароль».
- **Максимальное количество потоков** — поле для ввода максимального количества параллельных потоков для подбора учетных данных.

11.3.7. 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 XSpider PRO с SID или SERVICE_NAME.
- **Дополнительный справочник с SID или SERVICE_NAME** — раскрывающийся список для выбора справочника XSpider PRO с дополнительными SID или SERVICE_NAME.
- **Максимальное количество потоков** — поле для ввода максимального количества параллельных потоков для подбора SID или SERVICE_NAME.

11.3.8. Поиск уязвимостей — Подбор учетных данных — Oracle MySQL

Секция содержит следующие параметры для настройки подбора учетных данных пользователей СУБД Oracle MySQL:

- **Максимальное количество потоков** — поле для ввода максимального количества параллельных потоков для подбора учетных данных.

11.3.9. Поиск уязвимостей — Подбор учетных данных — SAP Sybase ASE

Секция содержит следующие параметры для настройки подбора учетных данных пользователей СУБД SAP Sybase ASE:

- **Справочник с парами «логин — пароль»** — раскрывающийся список для выбора справочника XSpider PRO с парами «логин — пароль».

11.3.10. 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.
 - **Справочник с парами «логин — пароль»** — раскрывающийся список для выбора справочника XSpider PRO с парами «логин — пароль».
- **Максимальное количество потоков** — поле для ввода максимального количества параллельных потоков для подбора учетных данных.

11.3.11. 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.
 - **Справочник с парами «логин — пароль»** — раскрывающийся список для выбора справочника XSpider PRO с парами «логин — пароль».
- **Максимальное количество потоков** — поле для ввода максимального количества параллельных потоков для подбора учетных данных.

11.3.12. Поиск уязвимостей — Подбор учетных данных — Symantec pcAnywhere

Секция содержит следующие параметры для настройки подбора учетных данных пользователей Symantec pcAnywhere:

- **Справочник с парами «логин — пароль»** — раскрывающийся список для выбора справочника XSpider PRO с парами «логин — пароль».
- **Максимальное количество потоков** — поле для ввода максимального количества параллельных потоков для подбора учетных данных.

11.3.13. Поиск уязвимостей — Подбор учетных данных — Virtual Network Computing

Секция содержит следующие параметры для настройки подбора учетных данных пользователей система удаленного доступа Virtual Network Computing:

- **Справочник с парами «логин — пароль»** — раскрывающийся список для выбора справочника XSpider PRO с парами «логин — пароль».

11.3.14. Поиск уязвимостей — Подбор учетных данных — VMware vSphere

Секция содержит следующие параметры для настройки подбора учетных данных пользователей систем VMware vSphere:

- **Справочник с парами «логин — пароль»** — раскрывающийся список для выбора справочника XSpider PRO с парами «логин — пароль».

11.3.15. Поиск уязвимостей — Подбор учетных данных — По протоколу FTP

Секция содержит следующие параметры для настройки подбора учетных данных пользователей по протоколу FTP:

11.3.16. Поиск уязвимостей — Подбор учетных данных — По протоколу NetBIOS

Секция содержит следующие параметры для настройки подбора учетных данных по протоколу NetBIOS:

- **Справочник с парами «логин — пароль»** — раскрывающийся список для выбора справочника XSpider PRO с парами «логин — пароль».
- **Подбирать пароли для найденных логинов** — при включении выполняется поиск паролей для найденных логинов.

11.3.17. Поиск уязвимостей — Подбор учетных данных — По протоколу POP3

Секция содержит следующие параметры для настройки подбора учетных данных по протоколу POP3:

- **Справочник с парами «логин — пароль»** — раскрывающийся список для выбора справочника XSpider PRO с парами «логин — пароль».

11.3.18. Поиск уязвимостей — Подбор учетных данных — По протоколу RDP

Секция содержит следующие параметры для настройки подбора учетных данных по протоколу RDP:

- **Справочник с парами «логин — пароль»** — раскрывающийся список для выбора справочника XSpider PRO с парами «логин — пароль».

11.3.19. Поиск уязвимостей — Подбор учетных данных — По протоколу SIP

Секция содержит следующие параметры для настройки подбора учетных данных по протоколу SIP:

- **Справочник с парами «логин — пароль»** — раскрывающийся список для выбора справочника XSpider PRO с парами «логин — пароль».

11.3.20. Поиск уязвимостей — Подбор учетных данных — По протоколу SMTP

Секция содержит следующие параметры для настройки подбора учетных данных по протоколу SMTP:

- **Справочник с парами «логин — пароль»** — раскрывающийся список для выбора справочника XSpider PRO с парами «логин — пароль».

11.3.21. 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:

Версия 3

Для протокола версии 3 доступны следующие параметры:

11.3.22. Поиск уязвимостей — Подбор учетных данных — По протоколу SSH

Секция содержит следующие параметры для настройки подбора учетных данных по протоколу SSH:

- **Справочник с парами «логин — пароль»** — раскрывающийся список для выбора справочника XSpider PRO с парами «логин — пароль».

11.3.23. Поиск уязвимостей — Подбор учетных данных — По протоколу Telnet

Секция содержит следующие параметры для настройки подбора учетных данных по протоколу Telnet:

- **Приглашения сервера на ввод логина** — раскрывающийся список для выбора справочника XSpider PRO содержащего запросы для определения приглашений сервера на ввод логина.
- **Приглашения сервера на ввод пароля** — раскрывающийся список для выбора справочника XSpider PRO содержащего запросы для определения приглашений сервера на ввод пароля.
 - **Справочник с парами «логин — пароль»** — раскрывающийся список для выбора справочника XSpider PRO с парами «логин — пароль».

11.3.24. Поиск уязвимостей — Подбор учетных данных — Фаматек RAdmin

Секция содержит следующие параметры для настройки подбора учетных данных пользователей ПО Фаматек RAdmin:

- **Справочник с парами «логин — пароль»** — раскрывающийся список для выбора справочника XSpider PRO с парами «логин — пароль».

11.3.25. 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 XSpider PRO с регулярными выражениями для имен и расширений файлов (по умолчанию filenames).
 - **Справочник с именами файлов для поиска через TFTP** — раскрывающийся список для выбора справочника XSpider PRO 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.

11.3.26. 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 количества записей Relative Distinguished Name, используемых сканировании.

11.3.27. 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 дампы данных сканирования** — при включении данные сканирования сохраняются в файле.
- **Использовать SQLite для хранения данных при сканировании** — при включении данные сканирования сохраняются не в памяти сервера, 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 сервере:

- **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** — при включении во время сбора событий, время регистрации которых значительно отличается от текущего времени (по умолчанию более чем на сутки), это время не будет заменяться временем сбора.
- **Интервал отправки уведомлений о состоянии** — поле для ввода интервала отправки уведомлений об активности модуля в миллисекундах.
- **Справочник с параметрами журналирования** — раскрывающийся список для выбора справочника XSpider PRO с параметрами журналирования работы модуля.
- **Сохранять статистику сбора данных** — при включении в журнале модуля сохраняется информация об объеме собранных модулем данных (в байтах), количестве пакетов с данными и их объеме (в байтах).

Отправка данных в систему

Секция содержит следующие параметры для настройки отправки данных в XSpider PRO:

- **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.

11.4. Сбор данных в режиме аудита

После определения семейств ОС на узлах вы можете выполнить их аудит. В ходе аудита узлы сканируются методом белого ящика. В параметрах задачи нужно указать учетную запись, которой предоставлены права на выполнение [команд для сбора данных \(см. раздел 11.4.2\)](#).

Внимание! Перед началом сканирования систем Firebird, Microsoft SQL Server, MySQL, Oracle, PostgreSQL и ClickHouse с использованием профиля **1C-Bitrix Audit** требуется предварительно [установить ODBC-драйвер \(см. раздел 14.7.2.4\)](#).

► Чтобы выполнить поиск уязвимостей методом белого ящика:

1. В главном меню выберите **Задачи**.
2. Нажмите **Создать задачу** → **Сбор данных**.
3. Введите название задачи.
4. Выберите профиль аудита.
5. Укажите **Цели сбора данных**:

В поле **Включить** укажите IP-адреса или FQDN произвольных узлов, диапазонов, сетей и подсетей, которые требуется сканировать для сбора данных.

В поле **Исключить** укажите IP-адреса или FQDN произвольных узлов, диапазонов, сетей и подсетей, которые требуется игнорировать при сборе данных.

Новая задача на сбор данных

Название

[Добавить описание](#)

Параметры сбора данных Импорт Экспорт

Профиль Windows Audit Vulnerabilities Discovery

▼ Сканирование систем: 1

Windows: Через WMI, RPC и RE

Расширение сбора данных

☐ Показывать дополнительные параметры

Сканирование систем

Windows x

Windows

windows

Цели сбора данных

Примеры допустимых адресов:

- IP-адрес v4 или v6 (192.168.0.0 или fe80::)
- диапазон IP-адресов (192.168.0.1-192.168.0.25)
- подсеть (192.168.0.0/24 или fe80::/10)
- FQDN (example.tuc.noao.ru)

Включить

Исключить

Сохранить Сохранить и запустить ▼ Отмена

Рисунок 13. Создание задачи на сбор данных в режиме аудита по профилю Windows Audit Vulnerabilities Discovery

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

По результатам задачи вы можете выпустить отчеты по уязвимостям на узлах или новый отчет **Инвентаризация узлов**. Если у вас есть предыдущие результаты аудита тех же узлов, вы можете выпустить дифференциальный отчет по уязвимостям.

Статусы проверки подключения

Для задач аудита вы можете проверять подключение, не запуская аудит. Так можно заранее убедиться, что к активам есть доступ с выбранной учетной записью.

► Чтобы проверить подключение:

1. В главном меню выберите **Сбор данных**.
2. Выберите задачу аудита.
3. Нажмите **Запустить** → **Проверить подключение**.
4. Дождитесь сообщения о выполнении проверки.

Если при проверке обнаружены ошибки, вы можете получить дополнительные сведения на странице задачи.

Настраивать параметры сканирования 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. Некоторые параметры становятся доступны после активации переключателя **Показывать дополнительные параметры**. Ниже приводятся описания параметров в каждой секции.

В этом разделе

[Сбор данных с использованием модуля Audit \(см. раздел 11.4.1\)](#)

[Команды, выполняемые при аудите узлов \(см. раздел 11.4.2\)](#)

11.4.1. Сбор данных с использованием модуля Audit

Доступны следующие стандартные профили модуля Audit:

- **SSH Network Device Audit**. Для аудита сетевых устройств по протоколу SSH. Профиль также может использоваться для сканирования сетевых устройств, не требующих повышения привилегий. Например, устройств Cisco.
- **Unix SSH Audit**. Для сканирования уязвимостей в Docker-контейнерах и их образах. Он выполняет автоматическую проверку конфигураций SSH-сервера в Unix-подобных системах на соответствие требованиям безопасности, а также анализирует установленные пакеты на предмет известных уязвимостей. Сканирование одного узла занимает до 5 минут.

Примечание. Профиль **Unix SSH Audit** требует большого количества вычислительных ресурсов и занимает продолжительное время. Рекомендуется использовать его только при крайней необходимости. Вместо него рекомендуется использовать профиль **Unix Audit Vulnerabilities Discovery**.

- **Windows Audit**. Для аудита Windows и ПО, установленного на узлах под управлением Windows, а также АСУ ТП. Сканирование одного узла 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.

Примечание. Профиль **Windows Audit** требует большого количества вычислительных ресурсов и занимает продолжительное время. Рекомендуется использовать его только при крайней необходимости. Вместо него рекомендуется использовать профиль **Windows Audit Vulnerabilities Discovery**.

- **Windows Audit Vulnerabilities Discovery.** Для поиска уязвимостей на узлах с Windows. Профиль собирает сведения об операционной системе и установленных приложениях, необходимые для обнаружения уязвимостей, но не выполняет полный аудит системы. Подходит для случаев, когда требуется только поиск уязвимостей без сбора дополнительных данных, доступных при сканировании с профилем **Windows Audit**. Не предназначен для аудита узлов АСУ ТП.

Примечание. По результатам тестирования сканирование с этим профилем выполнялось на 16% быстрее, чем с профилем **Windows Audit**, а результаты сканирования занимали на 30% меньше места на диске.

- **Unix Audit Vulnerabilities Discovery.** Для поиска уязвимостей на узлах с ОС семейства Unix. Профиль собирает сведения об операционной системе и установленных приложениях, необходимые для обнаружения уязвимостей, но не выполняет полный аудит системы. Подходит для случаев, когда требуется только поиск уязвимостей без сбора дополнительных данных, доступных при сканировании с профилем **Unix SSH Audit**. Не предназначен для аудита узлов АСУ ТП.

Примечание. По результатам тестирования сканирование с этим профилем выполнялось на 30% быстрее, чем с профилем **Unix SSH Audit**, а результаты сканирования занимали в 10 раз меньше места на диске. Пиковое потребление оперативной памяти процессом сканирования снизилось на 29%.

Внимание! При создании задач на сбор данных и выпуске отчетов профили модуля Audit доступны только при наличии соответствующей [лицензии \(см. раздел 9\)](#).

В этом разделе

[Сканирование систем — Check Point через OPSEC \(см. раздел 11.4.1.1\)](#)

[Сканирование систем — Microsoft SQL Server \(см. раздел 11.4.1.2\)](#)

[Сканирование систем — Oracle Database \(см. раздел 11.4.1.3\)](#)

[Сканирование систем — Oracle MySQL \(см. раздел 11.4.1.4\)](#)

[Сканирование систем — SAP через RFC \(см. раздел 11.4.1.5\)](#)

[Сканирование систем — VMware vSphere \(см. раздел 11.4.1.6\)](#)

[Сканирование систем — Windows \(см. раздел 11.4.1.7\)](#)

[Сканирование систем — По протоколу LDAP \(см. раздел 11.4.1.8\)](#)

[Сканирование систем — По протоколу SNMP \(см. раздел 11.4.1.9\)](#)

[Сканирование систем — Через терминал \(см. раздел 11.4.1.10\)](#)

[Дополнительные параметры модуля Audit \(см. раздел 11.4.1.11\)](#)

[Расширение сбора данных \(см. раздел 11.4.1.12\)](#)

11.4.1.1. 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 ввода 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).

11.4.1.2. 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 для 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.

11.4.1.3. Сканирование систем — Oracle Database

Секция содержит следующие параметры для настройки сбора данных из СУБД Oracle Database:

- **Учетная запись** — раскрывающийся список для выбора учетной записи для 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).

11.4.1.4. Сканирование систем — Oracle MySQL

Секция содержит следующие параметры для настройки сбора данных из СУБД Oracle MySQL:

- **Учетная запись** — раскрывающийся список для выбора учетной записи для 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.

11.4.1.5. 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 для 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.

11.4.1.6. Сканирование систем — VMware vSphere

Секция содержит следующие параметры для настройки сбора данных с VMware vCenter Server:

- **Учетная запись** — раскрывающийся список для выбора учетной записи для 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 сервере XSpider PRO необходимо штатными средствами ОС добавить этот сертификат в хранилище сертификатов от доверенных корневых центров сертификации.

11.4.1.7. Сканирование систем — Windows

Секция содержит параметры для настройки сбора данных из Windows с помощью следующих механизмов:

- WMI — инструменты управления Windows;
- RPC — удаленный вызов процедур;
- Remote Engine (RE) — удаленное выполнение сценариев (требуется WMI).

WMI

При выборе **WMI** доступны следующие параметры:

- **Учетная запись** — раскрывающийся список для выбора учетной записи для 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).

11.4.1.8. 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 для 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.

11.4.1.9. 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» для аутентификации на узле.

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 узле.

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

- **Аутентификация** — при включении используется аутентификация.
- **Шифрование** — при включении используется шифрование передаваемых данных.
 - **Учетная запись** — раскрывающийся список для выбора учетной записи.

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.

11.4.1.10. 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 для 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 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 ДН-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.

11.4.1.11. 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:

- **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** — при включении во время сбора событий, время регистрации которых значительно отличается от текущего времени (по умолчанию более чем на сутки), это время не будет заменяться временем сбора.
- **Интервал отправки уведомлений о состоянии** — поле для ввода интервала отправки уведомлений об активности модуля в миллисекундах.
- **Повторное подключение: максимальное количество попыток** — поле для ввода максимального количества попыток модуля восстановить связь в случае ее разрыва.
- **Повторное подключение: интервал между попытками** — поле для ввода времени между попытками модуля восстановить связь в миллисекундах.
- **Справочник с параметрами журналирования** — раскрывающийся список для выбора справочника XSpider PRO с параметрами журналирования работы модуля.
- **Сохранять статистику сбора данных** — при включении в журнале модуля сохраняется информация об объеме собранных модулем данных (в байтах), количестве пакетов с данными и их объеме (в байтах).

Отправка данных в систему

Секция содержит следующие параметры для настройки отправки данных в XSpider PRO:

- **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 дампы данных сканирования** — при включении данные сканирования сохраняются в файле.
- **Использовать SQLite для хранения данных при сканировании** — при включении данные сканирования сохраняются не в памяти сервера, а во временной базе SQLite. Это увеличивает время сканирования, но позволяет собирать большие объемы данных.

11.4.1.12. Расширение сбора данных

Содержит раскрывающийся список **Дополнительная экспертиза для аудита**, в котором по умолчанию выбран справочник `audit_expertise_extension`.

11.4.2. Команды, выполняемые при аудите узлов

Следует выбирать профиль аудита в соответствии с установленной на узле операционной системой. Для получения данных об узле 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 перечисленных команд.

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 4. Стандартные профили для аудита узлов

Узел	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

Узел	Версия	Профиль	Порт по умолчанию
Alcatel OmniSwitch	6.4.4	SSH Network Device Audit	— 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
Avaya (Nortel) NOS, серия ERS	5.1.0.015	SSH Network Device Audit	— 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
Cisco ACS	5	SSH Network Device Audit	— TCP 22; — UDP162
Cisco ADE-OS	—	SSH Network Device Audit	— TCP 22; — UDP 162
Cisco AireOS Wireless Controller	7.4.100, 7.6.130	SSH Network Device Audit	TCP 22
Cisco IOS XR, серия ASR9000	4.3.4, 6.1.1, 6.4.2	SSH Network Device Audit	TCP 22
Cisco ISE (Identity Services Engine)	2.3.0	SSH Network Device Audit	— TCP 22; — UDP 162
Cisco NX-OS	4–7	SSH Network Device Audit	— TCP 22; — UDP 162
Debian	7, 8, 9	Unix SSH Audit	TCP 22
Eltex, маршрутизаторы серии ESR	1.4.4	SSH Network Device Audit	TCP 22
Eltex, коммутаторы серий MES 1xxx, 2xxx, 3xxx, 51xx, 52xx	1.144, 4.0.9.3	SSH Network Device Audit	TCP 22
Fortinet FortiOS	5.4.2, 6.0.1	SSH Network Device Audit	TCP 22
FreeBSD	8–11	Unix SSH Audit	TCP 22

Узел	Версия	Профиль	Порт по умолчанию
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	Unix SSH Audit	TCP 22, 23
Huawei VRP, коммутаторы серии S, маршрутизаторы серий AR и NE	—	SSH Network Device Audit	— TCP 22; — UDP 162
IBM AIX	5.3, 6.1, 7.1–7.3	Unix SSH Audit	TCP 22, 23
Juniper JunOS	11–19	SSH Network Device Audit	— TCP 22; — UDP 162
Microsoft Windows	XP	Windows Audit, Windows Audit Vulnerabilities Discovery	TCP 1025–5000
Microsoft Windows Server	2003, 2003 R2	Windows Audit, Windows Audit Vulnerabilities Discovery	
Microsoft Windows	Vista, 7, 8, 8.1, 10	Windows Audit, Windows Audit Vulnerabilities Discovery	— 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, Windows Audit Vulnerabilities Discovery	
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	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

Команды для определения ОС на узле

При проведении аудита на узле выполняются следующие команды для определения установленной ОС:

```
show system vdom-property
end
- "\n config vdom\n edit ?\x15\n end\n"
- /usr/sbin/astra-modeswitch getname
- 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 на узле выполняются 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
- dmi decode
- dmi decode --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 '\n\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_path\n
\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|wicked-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 на узле выполняются следующие команды:

```
- |4
  ls -ltr /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
    end
  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
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 '\n\nclass
ProjectMemberForExport\n  attr_accessor :id\n  attr_accessor
  :type\n  attr_accessor :access_level\nend\n\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|wicked-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 на узле выполняются 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 на узле выполняются 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
  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
end

```

```

end
puts groups_for_export.to_json
,

- "gitlab-rails runner '\n
class ProjectMemberForExport\n  attr_accessor :id\n  attr_accessor
  :type\n  attr_accessor :access_level\nend\n\n
class ProjectForExport\n  attr_accessor
  :id\n  attr_accessor :name\n  attr_accessor :full_name\n  attr_accessor :full_path\n
  \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 на узле выполняются 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 '\n\nclass
ProjectMemberForExport\n  attr_accessor :id\n  attr_accessor
:type\n  attr_accessor :access_level\n\nend\n\n\nclass
ProjectForExport\n  attr_accessor

```

```

      :id\n attr_accessor :name\n attr_accessor :full_name\n attr_accessor :full_path\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
- lsvdisplay 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|wicked-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 на узле выполняются 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 snmp
- 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 на узле выполняются 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
end

- "gitlab-rails runner '\n
class 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
\n
\n  attr_accessor :visibility\n  attr_accessor :owner\n  attr_accessor :project_members\n
\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
\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
\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
\n  pr = ProjectForExport.new\n  pr.id = project.id\n  pr.name = project.name\n
\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 -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|wicked-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
- vdisplay 2>/dev/null
- who -r
- wicked test dhcp4 ?interface_id

```

CentOS

При проведении аудита на узле выполняются следующие команды:

```

- |4
  ls -ltr /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 /
- dhcpd --dumplease ?interface_id
- dhcpd --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
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 '\n\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_path\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
- lvddisplay 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,ttty,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
- vdisplay 2>/dev/null
- who -r
- wicked test dhcp4 ?interface_id

Cisco ACS

При проведении аудита на узле выполняются 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 на узле выполняются 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 на узле выполняются 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 IOS XR

При проведении аудита на узле выполняются 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 на узле выполняются 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 на узле выполняются 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 на узле выполняются 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
  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
end

```

```

end
puts groups_for_export.to_json
'

- "gitlab-rails runner '\n
class ProjectMemberForExport\n  attr_accessor :id\n  attr_accessor
  :type\n  attr_accessor :access_level\nend\n\n
class ProjectForExport\n  attr_accessor
  :id\n  attr_accessor :name\n  attr_accessor :full_name\n  attr_accessor :full_path\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|wicked-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
- vdisplay 2>/dev/null
- who -r
- wicked test dhcp4 ?interface_id

Eltex, маршрутизаторы серии ESR

При проведении аудита на узле выполняются 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 на узле выполняются 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 на узле выполняются 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

HPE Comware Software

При проведении аудита на узле выполняются 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 на узле выполняются 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 на узле выполняются 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 на узле выполняются 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 на узле выполняются 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 на узле выполняются 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 на узле выполняются 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

Oracle Linux

При проведении аудита на узле выполняются следующие команды:

- |4
ls -ltr /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 '\n
class ProjectMemberForExport\n  attr_accessor :id\n  attr_accessor
  :type\n  attr_accessor :access_level\nend\n\n
class ProjectForExport\n  attr_accessor
  :id\n  attr_accessor :name\n  attr_accessor :full_name\n  attr_accessor :full_path\n
  \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|wicked-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
- vdisplay 2>/dev/null
- who -r
- wicked test dhcp4 ?interface_id

```

Oracle Solaris

При проведении аудита на узле выполняются 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 на узле выполняются 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

Qtech QSW

При проведении аудита на узле выполняются 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 на узле выполняются следующие команды:

- |4

```
ls -ltr /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 '\n\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
\n
attr_accessor :visibility\n attr_accessor :owner\n attr_accessor :project_members\n
\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|wicked-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=%{SIGPGP: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 на узле выполняются 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 /
- dhcpd --dumplease ?interface_id
- dhcpd --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/dhcpd -type f -name 'dhcpd-*.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 '\n\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_path\n
    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
- lsvdisplay 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|wicked-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

```

11.5. Сбор данных о веб-приложениях

Модуль WebEngine предназначен для сбора данных о веб-приложениях в ИТ-инфраструктуре организации. В его состав входят встроенные модули для обнаружения различных веб-уязвимостей. Для модуля создан стандартный профиль **Web Scan Optimal**.

► Чтобы выполнить сканирование веб-приложений в ИТ-инфраструктуре:

1. В главном меню выберите **Задачи**.
2. Нажмите **Создать задачу** → **Сбор данных**.

3. Введите название задачи.
4. Выберите профиль сканирования.
5. Укажите **Цели сбора данных**:

В поле **Включить** укажите IP-адреса или FQDN произвольных узлов, диапазонов, сетей и подсетей, которые требуется сканировать для сбора данных.

В поле **Исключить** укажите IP-адреса или FQDN произвольных узлов, диапазонов, сетей и подсетей, которые требуется игнорировать при сборе данных.

Новая задача на сбор данных

Название

Добавить описание

Параметры сбора данных

Импорт

Экспорт

Профиль

Web Scan Optimal

Сбор данных

Подключение

Аутентификация

☐ Показывать дополнительные параметры

Сбор данных

Порты

80,443

Область сбора данных i

folder

Полнота сбора данных

optimal

Поиск стандартных каталогов

Режим поиска каталогов i

root

Цели сбора данных

Примеры допустимых адресов:

- IP-адрес v4 или v6 (192.168.0.0 или fe80::)
- диапазон IP-адресов (192.168.0.1-192.168.0.25)
- подсеть (192.168.0.0/24 или fe80::/10)
- FQDN (example.tuc.noao.ru)

Включить

Исключить

Сохранить

Сохранить и запустить ▼

Отмена

Рисунок 14. Создание задачи на сбор данных о веб-приложениях с профилем Web Scan Optimal

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

По результатам задачи вы можете выпустить отчеты по уязвимостям на узлах. Если у вас есть предыдущие результаты сканирования тех же веб-приложений, вы можете выпустить дифференциальный отчет по уязвимостям.

Настраивать параметры сканирования 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. Некоторые параметры становятся доступны после активации переключателя **Показывать дополнительные параметры**. Ниже приводятся описания параметров в каждой секции.

В этом разделе

[Сбор данных \(см. раздел 11.5.1\)](#)

[Подключение \(см. раздел 11.5.2\)](#)

[Дополнительные параметры модуля WebEngine \(см. раздел 11.5.3\)](#)

[Создание профилей на основе Web Scan Optimal для разных типов аутентификации \(см. раздел 11.5.4\)](#)

11.5.1. 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.
- **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.

11.5.2. 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 для 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.

11.5.3. 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 дампы данных сканирования** — при включении данные сканирования сохраняются в файле.
- **Использовать SQLite для хранения данных при сканировании** — при включении данные сканирования сохраняются не в памяти сервера, 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 сервере:

- **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** — при включении во время сбора событий, время регистрации которых значительно отличается от текущего времени (по умолчанию более чем на сутки), это время не будет заменяться временем сбора.
- **Интервал отправки уведомлений о состоянии** — поле для ввода интервала отправки уведомлений об активности модуля в миллисекундах.
- **Повторное подключение: максимальное количество попыток** — поле для ввода максимального количества попыток модуля восстановить связь в случае ее разрыва.
- **Повторное подключение: интервал между попытками** — поле для ввода времени между попытками модуля восстановить связь в миллисекундах.
- **Справочник с параметрами журналирования** — раскрывающийся список для выбора справочника XSpider PRO с параметрами журналирования работы модуля.
- **Сохранять статистику сбора данных** — при включении в журнале модуля сохраняется информация об объеме собранных модулем данных (в байтах), количестве пакетов с данными и их объеме (в байтах).

Отправка данных в систему

Секция содержит следующие параметры для настройки отправки данных в XSpider PRO:

- **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.

11.5.4. 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 **Параметры** → **Профили**.
2. Нажмите **Создать**.
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 поле **Адрес страницы входа** укажите адрес страницы, с которой выполняется вход на сайт.

Например:

`http://example.net/login.php`

8. 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 **Сохранить**.

Аутентификация с помощью веб-формы

► Чтобы создать профиль для аутентификации с помощью веб-формы:

1. В главном меню выберите **Параметры** → **Профили**.
2. Нажмите **Создать**.
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 поле **Адрес страницы входа** укажите адрес страницы, с которой выполняется вход на сайт.

Например:

`http://example.net/login.php`

8. 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. Введите логин и пароль.
 10. Введите идентификатор или имя кнопки входа.
- Например:
- `wp-submit`
11. 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 **Сохранить**.

HTTP-аутентификация

► Чтобы создать профиль для HTTP-аутентификации:

1. В главном меню выберите **Параметры** → **Профили**.
2. Нажмите **Создать**.
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. Выберите учетную запись, которую необходимо использовать для подключения.
8. Введите адрес страницы, которая будет открыта после входа.

Например:

`http://example.net/basic.php`

9. Нажмите **Сохранить**.

Аутентификация с помощью сессионных куки

► Чтобы создать профиль для аутентификации с помощью сессионных куки:

1. В главном меню выберите **Параметры** → **Профили**.
2. Нажмите **Создать**.
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 раскрывающемся списке **Куки (из заголовка запроса)** выберите учетную запись.
8. 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 **Сохранить**.

12. Выпуск отчетов

Отчеты позволяют анализировать результаты выполнения задач на сбор данных и обнаружение узлов.

Дифференциальный отчет позволяет анализировать динамику устранения уязвимостей.

Выпуск отчетов имеет следующие ограничения:

- Одновременно возможен выпуск только одного отчета. Новые созданные отчеты будут поставлены в очередь на выпуск. Если требуется поменять очередность выпуска отчетов, вы можете прервать выпуск текущего отчета, а затем выпустить копию этого отчета.
- Выпустить отчет повторно невозможно. Если требуется выпустить отчет с теми же параметрами, что у существующего, вы можете выпустить копию этого отчета.
- Изменить параметры созданного отчета невозможно. Вы можете выпустить копию отчета и изменить параметры в ней.
- Невозможен выпуск отчетов по задачам, у которых в качестве целей сбора данных указаны узлы, не добавленные [в лицензию \(см. раздел 9\)](#).
- Невозможен выпуск отчетов по задачам с профилями модуля AuditPLC. Этот модуль предназначен только для сбора данных о ПЛК.
- Во время установки пакетов экспертизы невозможен выпуск отчетов об уязвимостях.

В таблице отчетов в колонке **Статус отчета** отображается статус выпуска отчета. Существуют следующие статусы:

- **Выпускается** — отчет выпускается.
- **Ожидает выпуска** — отчет создан и находится в очереди на выпуск.
- **Выпуск прерван** — выпуск отчета был запущен и затем прерван. Продолжение выпуска этого отчета невозможно. Требуется выпустить его копию или создать новый отчет.
- **Выпущен** — отчет выпущен и доступен для скачивания в карточке справа.
- **Ошибка** — отчет не выпущен. Подробности о причине ошибки указаны в карточке справа.

XSpider PRO						
Задачи						
Отчеты						
Параметры						
Отчеты						
+ Выпустить отчет						
Выпустить копию						
Удалить						
Прервать выпуск						
Список отчетов						
Статус отчета	Название	Задача	Тип	Формат	Дата создания	
✓ Выпущен	Дифференциальный отчет по ...	qa-revenant.mp10.ptsecurity...	Дифференциальный отчет по уязвимостям на узлах	XLSX	Сегодня, 16:06	
✓ Выпущен	Уязвимости по узлам (23 июл....	xpro-0191	Уязвимости по узлам	XLSX	Сегодня, 15:21	
✓ Выпущен	Уязвимости по узлам (23 июл....	SNMP Network Device Audit	Уязвимости по узлам	XLSX	Сегодня, 13:25	
✓ Выпущен	Уязвимости по узлам (презент...	qa-revenant.mp10.ptsecurity...	Уязвимости по узлам (презентация)	HTML	Сегодня, 13:14	
✓ Выпущен	Уязвимости по узлам (22 июл....	qa-revenant.mp10.ptsecurity...	Уязвимости по узлам	XLSX	Вчера, 22:30	
✗ Ошибка ...	Уязвимости по узлам (22 июл....	qa-revenant.mp10.ptsecurity...	Уязвимости по узлам	XLSX	Вчера, 20:36	
✗ Ошибка ...	Уязвимости по узлам (22 июл....	qa-revenant.mp10.ptsecurity...	Уязвимости по узлам	XLSX	Вчера, 20:26	
Всего 7 отчетов, выбран 1 отчет						

Рисунок 15. Страница отчетов

► Чтобы выпустить отчет по результатам завершенной задачи:

1. В главном меню выберите **Отчеты**.
2. Нажмите **Создать отчет** и выберите тип отчета.
3. В поле **Задача** выберите задачу, которая содержит данные для формирования отчета.

Внимание! Узлы, указанные в задаче в качестве целей сбора данных, должны быть добавлены в лицензию (см. раздел 9).

Примечание. Выбор доступен из списка завершенных задач, имеющих результаты сканирования.

4. В поле **Результат** выберите дату и время получения результата сканирования.

Примечание. При выпуске дифференциального отчета необходимо выбрать два результата для сравнения: эталонный — данные которого будут взяты за основу для сравнения (по умолчанию это предпоследний результат сканирования) и изучаемый — данные которого будут сравниваться с эталонными (по умолчанию это последний результат сканирования). Результаты в дифференциальном отчете сопоставляются сначала по FQDN, затем по IP-адресу.

Новый отчет

Название	Дифференциальный отчет по уязвимостям на узлах (25 июл., 13:32)
Формат	XLSX
Описание	Динамика обработки уязвимостей между двумя сканированиями

Данные для отчета

Задача	Bruteforce PenTest
Эталонный результат (с чем сравнить)	23 июл., 17:20 Предпоследний
Изучаемый результат (что сравнить)	23 июл., 17:49 Последний

Выпустить **Отмена**

Рисунок 16. Создание нового дифференциального отчета по уязвимостям на узлах

5. Нажмите **Выпустить**.

Начнется выпуск отчета.

Вы можете скачать выпущенный отчет по ссылке в карточке справа.

Вы можете удалять отчеты. Для этого необходимо выбрать отчет в таблице и нажать **Удалить** в панели инструментов. Вы можете выбрать несколько отчетов, удерживая клавишу Ctrl или Shift.

Типы отчетов в XSpider PRO

Выбор отчета зависит от исходных данных решаемой задачи и целевой аудитории.

Таблица 5. Типы отчетов

Отчет	Исходные данные	Описание	Целевая аудитория
Уязвимости по узлам	Аудит, пентест или сканирование веб-приложений	Таблица с данными об уязвимостях с группировкой по узлам	ИТ-департамент
Уязвимости по узлам (презентация)	Аудит, пентест или сканирование веб-приложений	Данные об уязвимостях с группировкой по узлам в формате презентации. Примечание. После открытия скачанного HTML-файла отчет откроется в новой вкладке браузера. Вы можете сохранить отчет в формате PDF с помощью инструментов браузера (пункт меню Печать)	Руководство
Количество уязвимостей по приоритету	Аудит, пентест или сканирование веб-приложений	Информация о количестве уязвимостей на узлах с группировкой по приоритету	ИТ-департамент
Дифференциальный отчет по уязвимостям на узлах	Аудит, пентест или сканирование веб-приложений	Динамика обработки уязвимостей между двумя сканированиями. Уязвимости в отчете разделены на следующие группы: — Новые уязвимости — присутствуют в изучаемом результате сканирования и отсутствуют в эталонном. — Устраненные уязвимости — присутствуют в	ИТ-департамент

Отчет	Исходные данные	Описание	Целевая аудитория
		эталонном результате сканирования и отсутствуют в изучаемом. — Неустраненные уязвимости — присутствуют в обоих результатах сканирования	
Инвентаризация узлов	HostDiscovery, аудит, пентест или сканирование веб-приложений	Подробная информация об узлах: FQDN, версии ОС и ПО, службы, протоколы и порты. Без уязвимостей. Примечание. Этот отчет также доступен в форматах XML и JSON, что позволяет импортировать его в другие системы	ИТ-департамент
Операционные системы и открытые порты на узлах	Пентест или сканирование веб-приложений	Информация об операционных системах и открытых портах на узлах. Без уязвимостей	ИТ-департамент

13. Администрирование мобильного сканера

В этом разделе приводятся инструкции по администрированию XSpider PRO.

В этом разделе

[Обновление XSpider PRO \(см. раздел 13.1\)](#)

[Смена пароля служебной учетной записи администратора \(см. раздел 13.2\)](#)

[Обновление пакетов экспертизы \(см. раздел 13.3\)](#)

[Выдача прав на чтение пакетов экспертизы \(см. раздел 13.4\)](#)

[Удаление XSpider PRO с помощью сценария \(см. раздел 13.5\)](#)

13.1. Обновление XSpider PRO

Обновление продукта с версии 1.0 на 1.1

Если у вас установлен XSpider PRO версии 1.0, то для обновления до версии 1.1 необходимо придерживаться следующего порядка действий:

1. [Удалить продукт \(см. раздел 13.5\)](#);
2. [Установить продукт \(см. раздел 6\)](#) версии 1.1 с нуля в чистую папку.

Внимание! Установка XSpider PRO версии 1.1 без предварительного удаления версии 1.0 не поддерживается и приводит к потере данных.

Обновление продукта с версии 1.1.x на 1.1.y

► Чтобы обновить XSpider PRO:

1. Распакуйте архив <Название архива><Номер версии>.tar.gz:
`tar -xf <Название архива><Номер версии>.tar.gz`
2. Перейдите в каталог с распакованным дистрибутивом:
`cd deploy`
3. Разрешите запуск сценария:
`chmod +x deploy.sh`
4. Запустите сценарий обновления:
`./deploy.sh dockerRun false 2>&1 | tee -a install.log`
5. Ознакомьтесь с условиями лицензионного соглашения и нажмите **Exit**.
6. В окне **Лицензионное соглашение** нажмите **Yes**, чтобы принять его условия.
7. В параметре **Задать FQDN стенда [y/n]?** выберите, какой адрес будет использоваться для настройки компонентов продукта, указав одно из значений:

Y — использовать FQDN сервера, где будет установлен продукт.

N — использовать IP-адрес 172.17.0.1.

8. Если на предыдущем шаге вы указали значение **Y**, то в параметре **Адрес стенда** укажите FQDN сервера, где будет установлен продукт.

Внимание! Значение параметра **Адрес стенда** должно совпадать со значением, указанным в параметре **Имя домена** на этапе установки ОС.

9. В параметре **SSH пользователь стенда с правами sudo** оставьте значение по умолчанию (**root**).

См. также

[Удаление XSpider PRO с помощью сценария \(см. раздел 13.5\)](#)

[Установка XSpider PRO \(см. раздел 6\)](#)

13.2. Смена пароля служебной учетной записи администратора

В случае невозможности сменить пароль служебной учетной записи **Administrator** через веб-интерфейс (например, при утере пароля), вы можете сменить пароль в терминале Linux. Новый пароль должен быть не короче 8 символов и содержать как минимум одну строчную и одну прописную латинскую букву, одну цифру и один спецсимвол.

► Чтобы сменить пароль:

1. Выполните команды:

```
cd /var/lib/xpro-deploy/tools
chmod +x reset-password.sh
./reset-password.sh
```

В интерфейсе терминала появится сообщение:

```
Please enter new password
```

2. Введите новый пароль.

Начнется процесс смены пароля. По его завершении в интерфейсе терминала появится сообщение:

```
Password successfully changed
```

13.3. Обновление пакетов экспертизы

Экспертиза — это набор пакетов с актуальными сведениями об уязвимостях, продуктах, бюллетенях и условиях обнаружения. Экспертиза обновляется отдельно от сборки продукта, поэтому для получения новых данных не требуется переустанавливать XSpider PRO. Вы можете обновить пакеты экспертизы с помощью сценария `deploy_expertise.sh` или вручную.

Внимание! Инструкции необходимо выполнять на сервере от имени суперпользователя (root).

Обновление с помощью сценария

Сценарий `deploy_expertise.sh` поставляется в составе архива с пакетами экспертизы. Сценарий копирует пакеты в каталоги установки, устанавливает права доступа и перезапускает сервисы обработки уязвимостей (Vulnerabilities Processing) и сканирования (Scanning). Архив имеет плоскую структуру: сценарий, пакет экспертизы и обычные пакеты расположены в одном каталоге.

Внимание! Сценарий копирует файлы и перезапускает сервисы за несколько секунд, но фактическую установку пакетов выполняет модуль обработки уязвимостей асинхронно. При обычном обновлении установка занимает от 10 минут до 1 часа, при первой установке после активации лицензии — до 24 часов. Не перезапускайте сервисы и не прерывайте работу сценария до завершения установки.

► Чтобы обновить пакеты экспертизы с помощью сценария:

1. На [портале технической поддержки](#) скачайте tar-архив с пакетами экспертизы XSpider PRO.
2. Скопируйте архив на сервер XSpider PRO.
3. Распакуйте архив, например в каталог `/root`, с помощью команды:

```
tar -xf <Имя_архива>.tar
```

4. Перейдите в каталог с распакованными файлами и разрешите запуск сценария:

```
chmod +x deploy_expertise.sh
```

5. Запустите сценарий обновления пакетов экспертизы:

```
./deploy_expertise.sh
```

Сценарий проверит наличие пакетов и прав доступа, скопирует обычные пакеты в каталог `/var/lib/xpro-deploy/data/vulnerabilities.processing/data/vulnerability_packages/`, обновит словари Expertise Extension в каталоге `/var/lib/xpro-deploy/data/scanning/data/layer-updates/` и перезапустит сервисы. Ход выполнения записывается в файл `deploy_expertise.log` в текущем каталоге.

6. Проверьте код возврата сценария.

При успешном выполнении код равен 0, а в консоль и в файл `deploy_expertise.log` выводится сообщение об успешном копировании файлов. При ненулевом коде сверьтесь с таблицей ниже.

Таблица 6. Коды возврата сценария `deploy_expertise.sh`

Код	Статус	Причина и рекомендуемые действия
0	Успешно	Файлы скопированы, сервисы перезапущены, установка пакетов начата

Код	Статус	Причина и рекомендуемые действия
0	Частично успешно	Не удалось скопировать часть пакетов экспертизы. Сценарий выводит предупреждение со списком нескопированных пакетов в интерфейсе и в файле <code>deploy_expertise.log</code> . Повторите запуск и при необходимости обратитесь в техническую поддержку
0	Частично успешно	Не удалось перезапустить один из сервисов. Сценарий выводит предупреждение с именем сервиса в интерфейсе и в файле <code>deploy_expertise.log</code> . Для применения изменений может потребоваться ручной перезапуск сервиса. При необходимости обратитесь в техническую поддержку
1	Критическая ошибка	Не найдены пакеты экспертизы с расширением <code>.pkg</code> . Проверьте, что файлы с расширением <code>.pkg</code> находятся в одном каталоге со сценарием, и повторите запуск
2	Критическая ошибка	Не найден файл <code>expertise.extension.vm*.pkg</code> . Проверьте состав архива поставки и повторите запуск
3	Критическая ошибка	Недоступен каталог установки пакетов. Проверьте, что продукт установлен корректно и необходимые каталоги существуют
4	Критическая ошибка	Недостаточно прав доступа. Запустите сценарий от имени <code>root</code> и проверьте права на чтение файлов поставки и запись в каталоги установки
5	Критическая ошибка	Выполнение сценария прервано до завершения. Повторите запуск
6	Критическая ошибка	Не удалось скопировать ни один пакет экспертизы. Проверьте права доступа и свободное место на диске
7	Критическая ошибка	Непредвиденная ошибка. Сохраните файл <code>deploy_expertise.log</code> и обратитесь в техническую поддержку

Обновление вручную

► Чтобы обновить пакеты экспертизы вручную:

1. На [портале технической поддержки](#) скачайте tar-архив с пакетами экспертизы XSpider PRO.
2. Скопируйте архив на сервер XSpider PRO.
3. Скопируйте все файлы пакетов с расширением `.pkg` в каталог `/var/lib/xpro-deploy/data/vulnerabilities.processing/data/vulnerability_packages/`.

Внимание! Необходимо копировать файлы непосредственно в указанный выше каталог. Вложенные каталоги не поддерживаются.

4. Перезапустите модуль обработки уязвимостей (Vulnerabilities Processing). Для этого выполните команду:

```
docker restart $(docker ps -q -f name=vulnerabilities.processing)
```

После перезапуска начнется установка новых пакетов.

Контроль процесса и результата установки пакетов экспертизы

Независимо от того, как был запущен процесс обновления пакетов экспертизы (вручную или с помощью сценария), вы можете проверить, началась ли установка пакетов. При успешном запуске установки пакетов в веб-интерфейсе XSpider PRO в разделах **Задачи** и **Отчеты** будет отображаться информационный блок «Идет установка пакетов экспертизы».

Примечание. Информационный блок может появиться через 2-3 минуты после перезапуска сервиса. Блок обновляется каждые 5 минут.

Внимание! Длительность установки зависит от количества пакетов. При обычном обновлении она занимает от 10 минут до 1 часа. При первой установке после активации лицензии установка может занимать до 24 часов.

После завершения установки пакетов вы можете проанализировать результат. Признаки успешной установки пакетов экспертизы:

- информационный блок «Идет установка пакетов экспертизы» появился и исчез через указанное время;
- сообщения об ошибках не появились;
- отчеты об уязвимостях формируются.

Внимание! Убедитесь, что лицензия XSpider PRO активна. При проблемах с лицензией информационный блок может исчезнуть без сообщений об ошибке, однако расчет уязвимостей не будет выполняться и отчеты не будут формироваться.

Если результат отличается от успешного, ознакомьтесь с возможными причинами и рекомендуемыми действиями в разделе ниже.

Возможные проблемы при установке пакетов

Информационный блок «Идет установка пакетов экспертизы» не появился в течение 10-15 минут

Возможные причины:

- модуль обработки уязвимостей не запустился;
- пакеты отсутствуют в целевом каталоге;
- в браузере используются устаревшие данные.

Рекомендуемые действия:

1. Очистите кэш браузера.
2. Повторно выполните вход в систему.
3. Снова откройте раздел **Задачи** или **Отчеты**.
4. Если проблема сохраняется, выполните шаги 2 и 3 в другом браузере.
5. Если проблема сохраняется в другом браузере, обратитесь в техническую поддержку.

Информационный блок исчез и появилось сообщение вида «Не удалось установить X пакетов экспертизы из Y»

Возможная причина: ошибка установки одного или нескольких пакетов.

Рекомендуемое действие: обратитесь в техническую поддержку.

Информационный блок отображается более 24 часов

Если установка выполняется после активации лицензии и система обрабатывает большой объем пакетов, процедура может занимать до суток. Если информационный блок отображается больше суток, вероятно, произошла остановка процесса установки.

Рекомендуемое действие: не перезапускайте сервис и обратитесь в техническую поддержку.

Обращение в техническую поддержку

Для ускорения решения проблемы рекомендуется приложить к обращению в техподдержку:

- Версию XSpider PRO.
- Снимок экрана с сообщением об ошибке.
- Список пакетов, установка которых завершилась ошибкой.

13.4. Выдача прав на чтение пакетов экспертизы

Если при установке или обновлении пакетов экспертизы в интерфейсе XSpider PRO появляется ошибка доступа, это может означать, что сервис обработки уязвимостей (Vulnerabilities Processing) не может прочитать один или несколько файлов обновлений уязвимостей. Список файлов, к которым отсутствует доступ, можно посмотреть в окне ошибки.

► Чтобы выдать права на чтение пакетов экспертизы:

1. Подключитесь к серверу XSpider PRO по SSH:
`ssh user@<Адрес_сервера_XSpider_PRO>`
2. Перейдите в каталог с файлами пакетов экспертизы:
`cd /var/lib/xpro-deploy/data/vulnerabilities.processing/data/vulnerability_packages/`
3. Проверьте права доступа к файлам:
`ls -l`

Пример вывода:

```
-rw-r----- 1 root root ... vm.example.pkg
```

Права доступа указаны в первой части строки. Значение `-rw-r-----` означает, что владелец файла `root` может читать и изменять файл, группа `root` может читать файл, а остальные пользователи не имеют доступа к файлу. Если сервис обработки уязвимостей не запущен от имени пользователя `root` и не входит в группу `root`, он не сможет прочитать такой файл. Значение `-rw-r--r--` означает, что владелец файла `root` может читать и изменять файл, а группа `root` и остальные пользователи могут читать файл. Такие права позволяют сервису обработки уязвимостей прочитать файл.

4. Выдайте права на чтение всех файлов пакетов экспертизы:
`chmod o+r *.pkg`
5. Перезапустите сервис обработки уязвимостей:
`docker restart $(docker ps -q -f name=vulnerabilities.processing)`
6. Обновите страницу в интерфейсе XSpider PRO и убедитесь, что ошибка доступа больше не отображается.

13.5. Удаление XSpider PRO с помощью сценария

Удаление XSpider PRO производится с помощью сценария `uninstall.sh`, который доступен [по ссылке](#).

► Чтобы удалить XSpider PRO:

1. Поместите файл сценария в любой каталог на сервере, где установлен продукт.
2. Разрешите запуск сценария:
`chmod +x uninstall.sh`
3. Запустите сценарий удаления:
`./uninstall.sh`

Внимание! После удаления продукта на сервере могут остаться артефакты, например, установочный архив и распакованные каталоги. Необходимо удалить их вручную.

14. Справочник по настройке систем перед сканированием

Справочник по настройке систем перед сканированием содержит рекомендации по интеграции элементов IT-инфраструктуры организации с XSpider PRO для аудита узлов.

В этом разделе

[Антивирусное программное обеспечение \(см. раздел 14.1\)](#)

[Межсетевые экраны \(см. раздел 14.2\)](#)

[Операционные системы \(см. раздел 14.3\)](#)

[Системы виртуализации \(см. раздел 14.4\)](#)

[Системы мониторинга сети \(см. раздел 14.5\)](#)

[Другие источники \(см. раздел 14.6\)](#)

[Стандартные операции для настройки источников \(см. раздел 14.7\)](#)

14.1. Антивирусное программное обеспечение

Раздел содержит инструкции для настройки аудита поддерживаемого в XSpider PRO антивирусного программного обеспечения.

В этом разделе

[Kaspersky Security Center 13—14.2: настройка узла \(см. раздел 14.1.1\)](#)

[Kaspersky Security Center 13—14.2: настройка XSpider PRO \(см. раздел 14.1.2\)](#)

14.1.1. Kaspersky Security Center 13—14.2: настройка узла

Настройку узла нужно выполнять в Kaspersky Security Center Web Console или в Kaspersky Security Center для ОС Windows от имени учетной записи с ролью «Главный администратор».

Инструкции по настройке и установке см. на сайте kaspersky.ru.

Для аудита узла нужно:

1. На сервере Kaspersky Security Center необходимо разрешить доступ к порту TCP/13299 для сбора данных.
2. Создать учетную запись для доступа MP 10 Collector к узлу через веб-API.
3. Создать и настроить роль для учетной записи.
4. Назначить созданную роль учетной записи.

Настройка через Kaspersky Security Center (Windows)

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

1. Запустите приложение Kaspersky Security Center.
2. В списке выберите нужный сервер администрирования, нажмите правой кнопкой мыши на выбранный сервер и в контекстном меню выберите **Properties**.
Откроется окно **Свойства**.
3. В разделе **Роли пользователей** нажмите **Добавить**.
4. В открывшемся окне в разделе **Общие** введите имя новой роли.
5. В разделе **Права** перейдите в **Сервер администрирования Kaspersky Security Center** → **Общий функционал** → **Базовая функциональность** → **Чтение** и установите флажок **Разрешить**, нажмите **ОК**.
6. В разделе **Безопасность** нажмите **Внутренний пользователь**.
7. В открывшемся окне **Выбор пользователя** нажмите **Добавить пользователя**.
8. В открывшемся окне **Новый пользователь** введите имя учетной записи и пароль для новой учетной записи, нажмите **ОК**.
9. В окне **Выбор пользователя** выберите имя созданной на предыдущем шаге учетной записи, нажмите **ОК**.
Учетная запись появится в списке учетных записей в разделе **Безопасность**.
10. Выберите имя учетной записи в списке, в разделе **Разрешения** выберите вкладку **Роли** и нажмите **Добавить**.
11. В открывшемся окне **Роли пользователей** выберите роль, созданную ранее, и нажмите **ОК**.
12. В окне **Свойства** нажмите **Применить**, затем **ОК**.

Настройка через Kaspersky Security Center Web Console

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

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**.

14.1.2. Kaspersky Security Center 13—14.2: настройка XSpider PRO

Для аудита узла в XSpider PRO нужно добавить учетную запись для доступа к узлу, создать и запустить задачу на аудит.

В этом разделе

[Добавление учетной записи для доступа к узлу через веб-API \(см. раздел 14.1.2.1\)](#)

[Создание задачи на аудит узла с профилем Web API Audit \(см. раздел 14.1.2.2\)](#)

14.1.2.1. Добавление учетной записи для доступа к узлу через веб-API

► Чтобы добавить в XSpider PRO учетную запись для доступа к узлу:

1. В главном меню выберите **Параметры** → **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**.

14.1.2.2. Создание задачи на аудит узла с профилем Web API Audit

► Чтобы создать задачу на аудит узла:

1. В главном меню выберите **Задачи**.
2. Нажмите **Создать задачу** → **Сбор данных**.
3. Введите название задачи.
4. Выберите профиль **Web API Audit**.
5. Выберите **Сканирование систем** → **Через веб-API**.
6. Выберите тип аутентификации **Учетные данные**.
7. Выберите учетную запись для доступа к активу через веб-API.
8. Включите **Показывать дополнительные параметры**.
9. Укажите номер порта.
10. Укажите **Цели сбора данных**:

В поле **Включить** укажите IP-адреса или FQDN произвольных узлов, диапазонов, сетей и подсетей, которые требуется сканировать для сбора данных.

В поле **Исключить** укажите IP-адреса или FQDN произвольных узлов, диапазонов, сетей и подсетей, которые требуется игнорировать при сборе данных.

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

Задача на аудит узла с профилем Web API Audit создана.

14.2. Межсетевые экраны

Раздел содержит инструкции для настройки аудита поддерживаемых в XSpider PRO межсетевых экранов.

В этом разделе

[Cisco ASA 8, 9: настройка узла \(см. раздел 14.2.1\)](#)

[Cisco ASA 8, 9: настройка XSpider PRO \(см. раздел 14.2.2\)](#)

14.2.1. Cisco ASA 8, 9: настройка узла

Настройку узла 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 источника и узлом MP 10 Collector. Для проведения аудита узла по протоколу SSH используется порт TCP 22.

Для проведения аудита на узле 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 узлу:

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

3. Перейдите в режим конфигурирования:

```
configure terminal
```

4. Создайте учетную запись для доступа к узлу:

```
username <Логин> password <Пароль> privilege 15
```

Примечание. Если для ограничения доступа к узлу 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.

14.2.2. Cisco ASA 8, 9: настройка XSpider PRO

Для проведения аудита узла по протоколу SSH в XSpider PRO нужно добавить учетную запись для доступа к узлу, пароль для повышения привилегий (перехода в привилегированный режим EXEC) и создать задачу на проведение аудита.

В этом разделе

[Добавление учетной записи для доступа по SSH \(см. раздел 14.2.2.1\)](#)

[Добавление пароля для повышения привилегий для аудита по SSH \(см. раздел 14.2.2.2\)](#)

[Создание задачи на аудит узла по SSH \(см. раздел 14.2.2.3\)](#)

14.2.2.1. Добавление учетной записи для доступа по SSH

- Чтобы добавить в XSpider PRO учетную запись для доступа к узлу:

1. В главном меню выберите **Параметры** → **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 **Сохранить**.

Учетная запись добавлена.

14.2.2.2. Добавление пароля для повышения привилегий для аудита по SSH

► Чтобы добавить в XSpider PRO пароль для повышения привилегий:

1. В главном меню выберите **Учетные записи**.
2. Нажмите **Добавить учетную запись** → **Пароль**.
3. Введите название учетной записи.
4. В раскрывающемся списке **Метки** установите флажок **Terminal**.
5. Введите пароль и подтвердите его.
6. Нажмите **Сохранить**.

14.2.2.3. Создание задачи на аудит узла по SSH

► Чтобы создать задачу на проведение аудита узла:

1. В главном меню выберите **Задачи**.
2. Нажмите **Создать задачу** → **Сбор данных**.
3. Введите название задачи.
4. Выберите профиль **SSH Network Device Audit**.
5. Выберите пункт **Сканирование систем** → **Через терминал: SSH и Telnet**.
6. Выберите учетную запись для доступа к узлу.
7. Выберите учетную запись для повышения привилегий на узле.
8. Укажите **Цели сбора данных**:

В поле **Включить** укажите IP-адреса или FQDN произвольных узлов, диапазонов, сетей и подсетей, которые требуется сканировать для сбора данных.

В поле **Исключить** укажите IP-адреса или FQDN произвольных узлов, диапазонов, сетей и подсетей, которые требуется игнорировать при сборе данных.

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

Задача на проведение аудита узла создана.

14.3. Операционные системы

Раздел содержит инструкции для настройки аудита поддерживаемых в XSpider PRO операционных систем.

В этом разделе

[Microsoft Windows XP—11; Windows Server 2003—2022: настройка узла \(см. раздел 14.3.1\)](#)

[Microsoft Windows XP—11; Windows Server 2003—2022: настройка XSpider PRO \(см. раздел 14.3.2\)](#)

[Unix-подобные ОС: настройка узла \(см. раздел 14.3.3\)](#)

[Unix-подобные ОС: настройка XSpider PRO \(см. раздел 14.3.4\)](#)

14.3.1. Microsoft Windows XP—11; Windows Server 2003—2022: настройка узла

Настройку узла нужно выполнять от имени учетной записи администратора.

Внимание! В Windows XP по умолчанию отсутствует оболочка командной строки PowerShell. Для выполнения аудита требуется установить пакет обновлений KB968930, который включает в себя PowerShell 2, и перезагрузить компьютер.

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 узле нужно создать учетную запись для доступа MP 10 Collector к узлу. 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».

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»;
- «Настройка контроля локальных учетных записей (UAC)»;
- «Отключение контроля учетных записей (UAC)»;
- «Настройка подключения к службе WMI».

14.3.2. Microsoft Windows XP—11; Windows Server 2003—2022: настройка XSpider PRO

Для аудита узла в XSpider PRO нужно добавить учетную запись для доступа к узлу, создать и запустить задачу на проведение аудита с профилем **Windows Audit Vulnerabilities Discovery** или **Windows Audit**.

Примечание. Профиль **Windows Audit** требует большого количества вычислительных ресурсов и занимает продолжительное время. Рекомендуется использовать его только при крайней необходимости. Вместо него рекомендуется использовать облегченный профиль **Windows Audit Vulnerabilities Discovery**.

В этом разделе

[Добавление учетной записи ОС \(см. раздел 14.3.2.1\)](#)

[Создание задачи на аудит узла \(см. раздел 14.3.2.2\)](#)

14.3.2.1. Добавление учетной записи ОС

► Чтобы добавить в XSpider PRO учетную запись для доступа к источнику:

1. В главном меню выберите **Параметры** → **Учетные записи**.
2. Нажмите **Добавить учетную запись** → **Логин — пароль**.
3. Введите название учетной записи.
4. В раскрывающемся списке **Метки** установите флажок **WindowsAudit**.
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 **Сохранить**.

Учетная запись добавлена.

14.3.2.2. Создание задачи на аудит узла

► Чтобы создать задачу на проведение аудита узла:

1. В главном меню выберите **Задачи**.
2. Нажмите **Создать задачу** → **Сбор данных**.
3. Введите название задачи.
4. Выберите профиль **Windows Audit Vulnerabilities Discovery** или **Windows Audit**.

Примечание. Профиль **Windows Audit** требует большого количества вычислительных ресурсов и занимает продолжительное время. Рекомендуется использовать его только при крайней необходимости. Вместо него рекомендуется использовать облегченный профиль **Windows Audit Vulnerabilities Discovery**.

5. Выберите пункт **Сканирование систем** → **Windows**.

6. Укажите **Цели сбора данных**:

В поле **Включить** укажите IP-адреса или FQDN произвольных узлов, диапазонов, сетей и подсетей, которые требуется сканировать для сбора данных.

В поле **Исключить** укажите IP-адреса или FQDN произвольных узлов, диапазонов, сетей и подсетей, которые требуется игнорировать при сборе данных.

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

Задача на проведение аудита узла создана.

14.3.3. Unix-подобные ОС: настройка узла

Настройку узла 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 источника и узлом MP 10 Collector. Для проведения аудита узла по протоколу SSH используется порт TCP 22.

Поддерживается настройка аудита следующих ОС семейства Unix:

- «Альт» 9, 10;
- «Мос.ОС» (все версии);
- «РЕД ОС» 7.1–7.3;
- Astra Linux Common Edition 2.12;
- Astra Linux Special Edition 1.6, 1.7, 1.8;
- Canonical Ubuntu 16.04, 18.04, 20.04, 22.04;
- CentOS 7, 8;
- Debian 10, 11, 12;
- FreeBSD 12;
- HPE HP-UX 11.31;
- IBM AIX 7.3;
- macOS 11 и выше;
- Oracle Linux 7–9;
- Oracle Solaris 11;

- Photon OS 3.0—5.0;
- Platform V SberLinux OS Server (все версии);
- Red Hat Enterprise Linux 7—9;
- SUSE Linux Enterprise Server 15.

В этом разделе

[Аудит с помощью учетной записи root \(см. раздел 14.3.3.1\)](#)

[Аудит с помощью повышения привилегий учетной записи через команду su \(см. раздел 14.3.3.2\)](#)

[Аудит с помощью учетной записи с sudo-привилегиями \(см. раздел 14.3.3.3\)](#)

14.3.3.1. Аудит с помощью учетной записи root

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

Примечание. В macOS учетная запись root по умолчанию отключена. Для ее включения необходимо от имени пользователя, состоящего в группе администраторов, выполнить команду `dsenableroot`.

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 \(см. раздел 14.7.2.6\)](#).

14.3.3.2. 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.

Примечание. В macOS учетная запись `root` по умолчанию отключена. Для ее включения необходимо от имени пользователя, состоящего в группе администраторов, выполнить команду `dsenableroot`.

Настройка актива

► Чтобы настроить актив:

1. Если требуется, создайте учетную запись для доступа к активу.
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 \(см. раздел 14.7.2.5\)](#).

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.

14.3.3.3. Аудит с помощью учетной записи с sudo-привилегиями

Внимание! На активе должна быть установлена программа sudo.

Настройка актива

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

При проведении аудита с помощью доменной учетной записи:

- для входа на актив с macOS нужно указать имя пользователя;
- для входа на актив с другой ОС при использовании SSSD нужно указать доменное имя пользователя;
- для входа на актив с другой ОС при использовании Winbind, если в файле конфигурации /etc/samba/smb.conf параметр winbind use default domain установлен в значение yes, то нужно указать имя пользователя; если параметр установлен в значение no или отсутствует, то нужно указать доменное имя пользователя.

Примечание. Для используемой учетной записи в операционной системе Astra Linux Special Edition нужно дополнительно [настроить уровень целостности](#) (см. [раздел 14.7.2.6](#)).

Примечание. Для команды sudo в операционной системе «Альт» нужно дополнительно [настроить политику control](#) (см. [раздел 14.7.2.5](#)).

14.3.4. Unix-подобные ОС: настройка XSpider PRO

Для аудита узла в XSpider PRO нужно добавить учетную запись для доступа к узлу, создать и запустить задачу на проведение аудита с профилем Unix SSH Audit.

В этом разделе

[Добавление учетной записи \(см. раздел 14.3.4.1\)](#)

[Создание и запуск задачи на аудит узла \(см. раздел 14.3.4.2\)](#)

14.3.4.1. Добавление учетной записи

► Чтобы добавить в XSpider PRO учетную запись для доступа к источнику:

1. В главном меню выберите **Параметры** → **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**.

Учетная запись добавлена.

14.3.4.2. Создание и запуск задачи на аудит узла

► Чтобы создать задачу на проведение аудита узла:

1. В главном меню выберите **Задачи**.
2. Нажмите **Создать задачу** → **Сбор данных**.
3. Введите название задачи.
4. Выберите профиль **Unix SSH Audit**.
5. Выберите пункт **Сканирование систем** → **Через терминал: SSH**.
6. Выберите учетную запись для доступа к узлу.
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. Укажите **Цели сбора данных**:

В поле **Включить** укажите IP-адреса или FQDN произвольных узлов, диапазонов, сетей и подсетей, которые требуется сканировать для сбора данных.

В поле **Исключить** укажите IP-адреса или FQDN произвольных узлов, диапазонов, сетей и подсетей, которые требуется игнорировать при сборе данных.

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

Задача на проведение аудита узла создана.

14.4. Системы виртуализации

Раздел содержит инструкции для настройки аудита поддерживаемых в XSpider PRO систем виртуализации.

В этом разделе

[zVirt Engine 4.4—4.5: настройка узла \(см. раздел 14.4.1\)](#)

[zVirt Engine 4.4—4.5: настройка XSpider PRO \(см. раздел 14.4.2\)](#)

14.4.1. zVirt Engine 4.4—4.5: настройка узла

Настройку узла нужно выполнять от имени учетной записи администратора устройства.

Для аудита узла нужно:

1. Средствами ОС создать учетную запись для доступа MP 10 Collector к узлу 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 узлу по протоколу SSH в операционной системе, где установлен узел. Настройку нужно выполнять по инструкциям раздела «Unix-подобные ОС: настройка актива».

В этом разделе

[Создание учетной записи для доступа к узлу через веб-API \(см. раздел 14.4.1.1\)](#)

[Создание и настройка роли для аудита \(см. раздел 14.4.1.2\)](#)

[Назначение роли учетной записи \(см. раздел 14.4.1.3\)](#)

[Снятие ограничений на сессии для учетной записи \(см. раздел 14.4.1.4\)](#)

14.4.1.1. Создание учетной записи для доступа к узлу через веб-API

► Чтобы создать учетную запись для доступа к узлу:

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

14.4.1.2. Создание и настройка роли для аудита

► Чтобы создать и настроить роль:

1. Войдите в веб-интерфейс узла 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**.

14.4.1.3. Назначение роли учетной записи

► Чтобы назначить роль учетной записи:

1. Войдите в веб-интерфейс узла 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 узлу и нажмите **Поиск**.
6. В появившемся списке результатов поиска выберите учетную запись для доступа к узлу и нажмите **Добавить и закрыть**.

На странице **Пользователи** в списке учетных записей отобразится учетная запись для доступа к узлу.

7. В столбце **Имя пользователя** выберите логин учетной записи для доступа к узлу.
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**.

14.4.1.4. Снятие ограничений на сессии для учетной записи

► Чтобы снять ограничения на сессии для учетной записи:

1. Войдите в веб-интерфейс узла 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 узлу.
Откроется страница с параметрами учетной записи.
5. Нажмите **Управление ограничениями**.
6. В полях **Количество сессий** и **Время сессий (минуты)** укажите 0.
7. Нажмите **Сохранить**.

14.4.2. zVirt Engine 4.4—4.5: настройка XSpider PRO

Для аудита узла в XSpider PRO нужно добавить две учетные записи: одну для доступа к узлу 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 узлу через веб-API \(см. раздел 14.4.2.1\)](#)

[Добавление учетной записи для доступа к узлу по SSH \(см. раздел 14.4.2.2\)](#)

[Создание задачи на аудит узла с профилем Unix SSH Audit \(см. раздел 14.4.2.3\)](#)

[Создание задачи на аудит узла с профилем Web API Audit \(см. раздел 14.4.2.4\)](#)

14.4.2.1. Добавление учетной записи для доступа к узлу через веб-API

► Чтобы добавить в XSpider PRO учетную запись для доступа к узлу:

1. В главном меню выберите **Параметры** → **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**.

14.4.2.2. Добавление учетной записи для доступа к узлу по SSH

► Чтобы добавить в XSpider PRO учетную запись для доступа к узлу:

1. В главном меню выберите **Параметры** → **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**.

14.4.2.3. Создание задачи на аудит узла с профилем Unix SSH Audit

► Чтобы создать задачу на аудит узла:

1. В главном меню выберите **Задачи**.
2. Нажмите **Создать задачу** → **Сбор данных**.

3. Введите название задачи.
4. Выберите профиль **Unix SSH Audit**.
5. Выберите **Сканирование систем** → **Через терминал: SSH**.
6. Выберите учетную запись для доступа к активу по SSH.
7. Включите **Показывать дополнительные параметры**.
8. Укажите номер порта.
9. Укажите **Цели сбора данных**:

В поле **Включить** укажите IP-адреса или FQDN произвольных узлов, диапазонов, сетей и подсетей, которые требуется сканировать для сбора данных.

В поле **Исключить** укажите IP-адреса или FQDN произвольных узлов, диапазонов, сетей и подсетей, которые требуется игнорировать при сборе данных.

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

Задача на аудит узла с профилем Unix SSH Audit создана.

14.4.2.4. Создание задачи на аудит узла с профилем Web API Audit

► Чтобы создать задачу на аудит узла:

1. В главном меню выберите **Задачи**.
2. Нажмите **Создать задачу** → **Сбор данных**.
3. Введите название задачи.
4. Выберите профиль **Web API Audit**.
5. Выберите **Сканирование систем** → **Через веб-API**.
6. Выберите тип аутентификации **Учетные данные**.
7. Выберите учетную запись для доступа к активу через веб-API.
8. Включите **Показывать дополнительные параметры**.
9. Укажите номер порта.
10. Укажите **Цели сбора данных**:

В поле **Включить** укажите IP-адреса или FQDN произвольных узлов, диапазонов, сетей и подсетей, которые требуется сканировать для сбора данных.

В поле **Исключить** укажите IP-адреса или FQDN произвольных узлов, диапазонов, сетей и подсетей, которые требуется игнорировать при сборе данных.

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

Задача на аудит узла с профилем Web API Audit создана.

14.5. Системы мониторинга сети

Раздел содержит инструкции для настройки аудита поддерживаемых в XSpider PRO систем мониторинга сети.

В этом разделе

[Microsoft System Center Configuration Manager \(SCCM\) 2012–2019: настройка узла](#)
(см. раздел 14.5.1)

[Microsoft System Center Configuration Manager \(SCCM\) 2012–2019: настройка XSpider PRO](#)
(см. раздел 14.5.2)

14.5.1. Microsoft System Center Configuration Manager (SCCM) 2012–2019: настройка узла

Настройку узла 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 источника 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 XSpider PRO в качестве источников. Для каждого узла указывается информация о версии ОС и установленном ПО.

Для проведения аудита на узле нужно:

1. Создать [локальную](#) (см. раздел 14.7.1.2) или доменную учетную запись пользователя Windows.

Примечание. Данные этой учетной записи нужно указать при добавлении учетной записи в XSpider PRO.

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

2. Настроить локальную или групповую политику безопасности для удаленного доступа учетной записи.

3. Настроить локальную или групповую 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 \(см. раздел 14.5.1.1\)](#) или [с помощью запроса \(см. раздел 14.5.1.2\)](#).
5. Настроить порты TCP/IP для подключения к СУБД.
6. Настроить автоматический запуск SQL Server Browser.

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

[Создание учетной записи Microsoft SQL Server \(см. раздел 14.5.1.1\)](#)

[Создание учетной записи Microsoft SQL Server с помощью запроса \(см. раздел 14.5.1.2\)](#)

14.5.1.1. 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 выберите **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.

14.5.1.2. 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.

## 14.5.2. Microsoft System Center Configuration Manager (SCCM) 2012—2019: настройка XSpider PRO

Для проведения аудита в XSpider PRO нужно добавить учетную запись для доступа к активу, создать и запустить задачу на сбор данных с профилем MSSQL Audit.

### В этом разделе

[Добавление учетной записи для СУБД Microsoft SQL Server \(см. раздел 14.5.2.1\)](#)

[Создание задачи на аудит узла \(см. раздел 14.5.2.2\)](#)

### 14.5.2.1. Добавление учетной записи для СУБД Microsoft SQL Server

► Чтобы добавить в XSpider PRO учетную запись для доступа к источнику:

1. В главном меню выберите **Параметры** → **Учетные записи**.
2. Нажмите **Добавить учетную запись** → **Логин — пароль**.
3. Введите название учетной записи.
4. В раскрывающемся списке **Метки** установите флажки **DB\_MSSQL** и **WindowsAudit**.

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 **Сохранить**.

Учетная запись добавлена.

## 14.5.2.2. Создание задачи на аудит узла

► Чтобы создать задачу на проведение аудита узла:

1. В главном меню выберите **Задачи**.
2. Нажмите **Создать задачу** → **Сбор данных**.
3. Введите название задачи.
4. Выберите профиль **Windows Audit Vulnerabilities Discovery** или **Windows Audit**.

**Примечание.** Профиль **Windows Audit** требует большого количества вычислительных ресурсов и занимает продолжительное время. Рекомендуется использовать его только при крайней необходимости. Вместо него рекомендуется использовать облегченный профиль **Windows Audit Vulnerabilities Discovery**.

5. Выберите пункт **Сканирование систем** → **Windows**.
6. Укажите **Цели сбора данных**:

В поле **Включить** укажите IP-адреса или FQDN произвольных узлов, диапазонов, сетей и подсетей, которые требуется сканировать для сбора данных.

В поле **Исключить** укажите IP-адреса или FQDN произвольных узлов, диапазонов, сетей и подсетей, которые требуется игнорировать при сборе данных.

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

Задача на проведение аудита узла создана.

## 14.6. Другие источники

Раздел содержит инструкции для настройки сбора событий с других источников, поддерживаемых в XSpider PRO.

### В этом разделе

[Продукты Siemens: настройка XSpider PRO \(см. раздел 14.6.1\)](#)

[«1С-Битрикс: Управление сайтом» 20.0.0 и выше: настройка узла \(см. раздел 14.6.2\)](#)

[«1С-Битрикс: Управление сайтом» 20.0.0 и выше: настройка XSpider PRO \(см. раздел 14.6.3\)](#)

AVEVA (Wonderware) Historian, Insight, InTouch, System Platform: настройка узла (см. раздел 14.6.4)

AVEVA (Wonderware) Historian, Insight, InTouch, System Platform: настройка XSpider PRO (см. раздел 14.6.5)

JetBrains Hub 2018.1—2022: настройка узла (см. раздел 14.6.6)

JetBrains Hub 2018.1—2022: настройка XSpider PRO (см. раздел 14.6.7)

JetBrains YouTrack 2019: настройка узла (см. раздел 14.6.8)

JetBrains YouTrack 2019: настройка XSpider PRO (см. раздел 14.6.9)

JBfrog Artifactory 6—6.23: настройка узла (см. раздел 14.6.10)

JBfrog Artifactory 7 и выше: настройка узла (см. раздел 14.6.11)

JBfrog Artifactory 6 и выше: настройка XSpider PRO (см. раздел 14.6.12)

Yokogawa CENTUM VP R4—R6 и ProSafe-RS R2—R4: настройка узла (см. раздел 14.6.13)

Yokogawa CENTUM VP R4—R6 и ProSafe-RS R2—R4: настройка XSpider PRO (см. раздел 14.6.14)

## 14.6.1. Продукты Siemens: настройка XSpider PRO

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

### В этом разделе

[Добавление учетной записи \(см. раздел 14.6.1.1\)](#)

[Создание задачи на аудит узла \(см. раздел 14.6.1.2\)](#)

### 14.6.1.1. Добавление учетной записи

► Чтобы добавить в XSpider PRO 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.

## 14.6.1.2. Создание задачи на аудит узла

► Чтобы создать задачу на проведение аудита узла:

1. В главном меню выберите **Задачи**.
2. Нажмите **Создать задачу** → **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. Укажите **Цели сбора данных**:

В поле **Включить** укажите IP-адреса или FQDN произвольных узлов, диапазонов, сетей и подсетей, которые требуется сканировать для сбора данных.

В поле **Исключить** укажите IP-адреса или FQDN произвольных узлов, диапазонов, сетей и подсетей, которые требуется игнорировать при сборе данных.

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

Задача на проведение аудита узла создана.

## 14.6.2. «1С-Битрикс: Управление сайтом» 20.0.0 и выше: настройка узла

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.

Аудит «1С-Битрикс: Управление сайтом» поддерживается только при использовании веб-сервера Apache (HTTPD).

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».
2. Настроить удаленный доступ к СУБД MySQL.
3. Создать учетную запись СУБД с правом на чтение базы данных актива.

## В этом разделе

[Настройка удаленного доступа в MySQL \(см. раздел 14.6.2.1\)](#)

[Настройка СУБД MySQL \(см. раздел 14.6.2.2\)](#)

### 14.6.2.1. 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
```

### 14.6.2.2. 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 \(см. раздел 14.6.2.1\)](#).

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 XSpider PRO.

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;
```

### 14.6.3. «1С-Битрикс: Управление сайтом» 20.0.0 и выше: настройка XSpider PRO

Для аудита актива в XSpider PRO 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 1С-Bitrix Audit.

#### В этом разделе

[Добавление учетной записи \(см. раздел 14.6.3.1\)](#)

[Добавление учетной записи для СУБД Microsoft SQL Server \(см. раздел 14.6.3.2\)](#)

[Создание задачи на аудит узла \(см. раздел 14.6.3.3\)](#)

#### 14.6.3.1. Добавление учетной записи

- Чтобы добавить в XSpider PRO 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.

## 14.6.3.2. Добавление учетной записи для СУБД Microsoft SQL Server

► Чтобы добавить в XSpider PRO 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 **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.

## 14.6.3.3. Создание задачи на аудит узла

► Чтобы создать задачу на аудит узла:

1. В главном меню выберите **Задачи**.
2. Нажмите **Создать задачу** → **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. 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. Укажите **Цели сбора данных**:

В поле **Включить** укажите IP-адреса или FQDN произвольных узлов, диапазонов, сетей и подсетей, которые требуется сканировать для сбора данных.

В поле **Исключить** укажите IP-адреса или FQDN произвольных узлов, диапазонов, сетей и подсетей, которые требуется игнорировать при сборе данных.

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

Задача на аудит узла создана.

## 14.6.4. AVEVA (Wonderware) Historian, Insight, InTouch, System Platform: настройка узла

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 узле нужно создать учетную запись локального пользователя ОС для доступа MP 10 Collector к узлу. Данные этой учетной записи нужно указать при добавлении учетной записи в XSpider PRO.

## 14.6.5. AVEVA (Wonderware) Historian, Insight, InTouch, System Platform: настройка XSpider PRO

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

### В этом разделе

[Добавление учетной записи \(см. раздел 14.6.5.1\)](#)

[Создание задачи на аудит узла \(см. раздел 14.6.5.2\)](#)

### 14.6.5.1. Добавление учетной записи

► Чтобы добавить в XSpider PRO 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.

### 14.6.5.2. Создание задачи на аудит узла

► Чтобы создать задачу на проведение аудита узла:

1. В главном меню выберите **Задачи**.
2. Нажмите **Создать задачу** → **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. Укажите **Цели сбора данных**:

В поле **Включить** укажите IP-адреса или FQDN произвольных узлов, диапазонов, сетей и подсетей, которые требуется сканировать для сбора данных.

В поле **Исключить** укажите IP-адреса или FQDN произвольных узлов, диапазонов, сетей и подсетей, которые требуется игнорировать при сборе данных.

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

Задача на проведение аудита узла создана.

## 14.6.6. JetBrains Hub 2018.1—2022: настройка узла

Настройку узла нужно выполнять от имени учетной записи администратора устройства.

Для проведения аудита на узле 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

[Создание и настройка роли \(см. раздел 14.6.6.1\)](#)

[Создание и настройка учетной записи для доступа к активу \(см. раздел 14.6.6.2\)](#)

[Выпуск токена для учетной записи \(см. раздел 14.6.6.3\)](#)

### 14.6.6.1. 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.

## 14.6.6.2. 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 \(см. раздел 14.6.6.1\)](#).
11. В раскрывающемся списке **Scope** выберите проект **Global**.
12. Нажмите кнопку **Grant**.

Учетная запись создана.

## 14.6.6.3. Выпуск токена для учетной записи

Токен необходим для получения доступа к информации о событиях на узле 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.

## 14.6.7. JetBrains Hub 2018.1—2022: настройка XSpider PRO

Для аудита актива в XSpider PRO 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 \(см. раздел 14.6.7.1\)](#)

[Создание задачи на аудит узла \(см. раздел 14.6.7.2\)](#)

### 14.6.7.1. Добавление учетной записи

► Чтобы добавить в XSpider PRO учетную запись для доступа к источнику:

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.

## 14.6.7.2. Создание задачи на аудит узла

► Чтобы создать задачу на аудит узла:

1. В главном меню выберите **Задачи**.
2. Нажмите **Создать задачу** → **Сбор данных**.
3. В поле **Название** введите название задачи.
4. В раскрывающемся списке **Профиль** выберите **Web API Audit**.
5. В иерархическом списке выберите **Сканирование систем** → **Через веб-API**.
6. Выберите тип аутентификации **Токен доступа Bearer**.
7. Выберите учетную запись для доступа к активу через веб-API.
8. Включите **Показывать дополнительные параметры**.
9. Укажите номер порта.
10. Укажите **Цели сбора данных**:

В поле **Включить** укажите IP-адреса или FQDN произвольных узлов, диапазонов, сетей и подсетей, которые требуется сканировать для сбора данных.

В поле **Исключить** укажите IP-адреса или FQDN произвольных узлов, диапазонов, сетей и подсетей, которые требуется игнорировать при сборе данных.

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

Задача на аудит узла создана.

## 14.6.8. JetBrains YouTrack 2019: настройка узла

Настройку узла 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 источника и узлом MP 10 Collector. Для проведения аудита узла по протоколу HTTP/REST API используются порты TCP 80 и 443.

Для проведения аудита на узле 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 \(см. раздел 14.6.8.1\)](#)

[Создание учетной записи \(см. раздел 14.6.8.2\)](#)

[Создание токена \(см. раздел 14.6.8.3\)](#)

### 14.6.8.1. 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.

## 14.6.8.2. 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.

## 14.6.8.3. 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.

## 14.6.9. JetBrains YouTrack 2019: настройка XSpider PRO

Для аудита актива XSpider PRO 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 \(см. раздел 14.6.9.1\)](#)

[Создание задачи на аудит узла \(см. раздел 14.6.9.2\)](#)

### 14.6.9.1. Добавление учетной записи

► Чтобы добавить в XSpider PRO учетную запись для доступа к источнику:

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.

### 14.6.9.2. Создание задачи на аудит узла

► Чтобы создать задачу на аудит узла:

1. В главном меню выберите **Задачи**.
2. Нажмите **Создать задачу** → **Сбор данных**.
3. В поле **Название** введите название задачи.
4. В раскрывающемся списке **Профиль** выберите **Web API Audit**.
5. В иерархическом списке выберите **Сканирование систем** → **Через веб-API**.
6. Выберите тип аутентификации **Токен доступа Bearer**.
7. Выберите учетную запись для доступа к активу через веб-API.
8. Включите **Показывать дополнительные параметры**.

9. Укажите номер порта.

10. Укажите **Цели сбора данных**:

В поле **Включить** укажите IP-адреса или FQDN произвольных узлов, диапазонов, сетей и подсетей, которые требуется сканировать для сбора данных.

В поле **Исключить** укажите IP-адреса или FQDN произвольных узлов, диапазонов, сетей и подсетей, которые требуется игнорировать при сборе данных.

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

Задача на аудит узла создана.

## 14.6.10. JFrog Artifactory 6—6.23: настройка узла

Настройку узла нужно выполнять от имени учетной записи администратора устройства.

Для аудита на узле нужно:

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

[Создание учетной записи для доступа к узлу через веб-API \(см. раздел 14.6.10.1\)](#)

[Создание группы и добавление учетной записи в группу \(см. раздел 14.6.10.2\)](#)

[Выпуск токена доступа для учетной записи \(см. раздел 14.6.10.3\)](#)

### 14.6.10.1. Создание учетной записи для доступа к узлу через веб-API

► Чтобы создать учетную запись для доступа к узлу:

1. Войдите в веб-интерфейс узла 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**.

## 14.6.10.2. Создание группы и добавление учетной записи в группу

- ▶ Чтобы создать группу и добавить в нее учетную запись:
  1. Войдите в веб-интерфейс узла 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.

## 14.6.10.3. Выпуск токена доступа для учетной записи

**Внимание!** На узле 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 узле.
  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 узлу>" -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 XSpider PRO.

## 14.6.11. JFrog Artifactory 7 и выше: настройка узла

Для доступа MP 10 Collector к узлу используется токен доступа.

- ▶ Чтобы выпустить токен доступа:
  1. Войдите в веб-интерфейс узла 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 XSpider PRO.

## 14.6.12. JFrog Artifactory 6 и выше: настройка XSpider PRO

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

### В этом разделе

[Добавление учетной записи \(см. раздел 14.6.12.1\)](#)

[Создание задачи на аудит узла \(см. раздел 14.6.12.2\)](#)

### 14.6.12.1. Добавление учетной записи

► Чтобы добавить в XSpider PRO учетную запись для доступа к источнику:

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.

## 14.6.12.2. Создание задачи на аудит узла

► Чтобы создать задачу на аудит узла:

1. В главном меню выберите **Задачи**.
2. Нажмите **Создать задачу** → **Сбор данных**.
3. В поле **Название** введите название задачи.
4. В раскрывающемся списке **Профиль** выберите **Web API Audit**.
5. В иерархическом списке выберите **Сканирование систем** → **Через веб-API**.
6. Выберите тип аутентификации **Токен доступа Bearer**.
7. Выберите учетную запись для доступа к активу через веб-API.
8. Включите **Показывать дополнительные параметры**.
9. Укажите номер порта.
10. Укажите **Цели сбора данных**:

В поле **Включить** укажите IP-адреса или FQDN произвольных узлов, диапазонов, сетей и подсетей, которые требуется сканировать для сбора данных.

В поле **Исключить** укажите IP-адреса или FQDN произвольных узлов, диапазонов, сетей и подсетей, которые требуется игнорировать при сборе данных.

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

Задача на аудит узла создана.

## 14.6.13. Yokogawa CENTUM VP R4—R6 и ProSafe-RS R2—R4: настройка узла

Настройку узла нужно выполнять от имени учетной записи администратора устройства.

Для проведения аудита на узле нужно создать учетную запись локального пользователя ОС для доступа MP 10 Collector к узлу. Данные этой учетной записи нужно указать при добавлении учетной записи в XSpider PRO.

## 14.6.14. Yokogawa CENTUM VP R4—R6 и ProSafe-RS R2—R4: настройка XSpider PRO

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

## В этом разделе

[Добавление учетной записи \(см. раздел 14.6.14.1\)](#)

[Создание задачи на аудит узла \(см. раздел 14.6.14.2\)](#)

### 14.6.14.1. Добавление учетной записи

► Чтобы добавить в XSpider PRO 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.

### 14.6.14.2. Создание задачи на аудит узла

► Чтобы создать задачу на проведение аудита узла:

1. В главном меню выберите **Задачи**.
2. Нажмите **Создать задачу** → **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. Укажите **Цели сбора данных**:

В поле **Включить** укажите IP-адреса или FQDN произвольных узлов, диапазонов, сетей и подсетей, которые требуется сканировать для сбора данных.

В поле **Исключить** укажите IP-адреса или FQDN произвольных узлов, диапазонов, сетей и подсетей, которые требуется игнорировать при сборе данных.

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

Задача на проведение аудита узла создана.

## 14.7. Стандартные операции для настройки источников

Раздел содержит инструкции для стандартных операций, выполняемых при настройке сбора событий с источников.

### В этом разделе

[Стандартные операции в Windows \(см. раздел 14.7.1\)](#)

[Стандартные операции в ОС семейства Unix \(см. раздел 14.7.2\)](#)

[Стандартные операции в системах виртуализации VMware \(см. раздел 14.7.3\)](#)

### 14.7.1. Стандартные операции в Windows

Раздел содержит инструкции для стандартных операций, выполняемых в Windows.

#### В этом разделе

[Включение правила межсетевого экрана Windows \(см. раздел 14.7.1.1\)](#)

[Создание учетной записи ОС \(см. раздел 14.7.1.2\)](#)

[Добавление учетной записи в локальную политику безопасности \(см. раздел 14.7.1.3\)](#)

[Добавление учетной записи в локальную группу пользователей \(см. раздел 14.7.1.4\)](#)

#### 14.7.1.1. 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.

#### 14.7.1.2. Создание учетной записи ОС

► Чтобы создать учетную запись пользователя ОС:

1. Откройте панель управления Windows.
2. Выберите **Администрирование** → **Управление компьютером**.

3. В левой части окна выберите узел **Управление компьютером** → **Локальные пользователи и группы** → **Пользователи**.
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.

### 14.7.1.3. 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 **ОК**.
11. В окне **Свойства <Имя политики>** нажмите **ОК**.

### 14.7.1.4. Добавление учетной записи в локальную группу пользователей

- Чтобы добавить учетную запись в локальную группу пользователей:
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. Нажмите **Добавить**.
  7. Нажмите **Размещение**.
  8. В открывшемся окне выберите:
    - если используется локальная учетная запись — имя узла;
    - если используется доменная учетная запись — имя домена.
  9. Нажмите **ОК**.
  10. В поле **Введите имена выбираемых объектов** введите логин учетной записи и нажмите **ОК**.
  11. В окне **Свойства <Имя группы>** нажмите **ОК**.

## 14.7.2. Стандартные операции в ОС семейства Unix

Раздел содержит инструкции для стандартных операций, выполняемых в ОС семейства Unix.

### В этом разделе

[Создание учетной записи в ОС семейства Unix \(см. раздел 14.7.2.1\)](#)

[Определение используемой службы журналирования \(см. раздел 14.7.2.2\)](#)

[Перезапуск службы в ОС семейства Unix \(см. раздел 14.7.2.3\)](#)

[Установка ODBC-драйвера \(см. раздел 14.7.2.4\)](#)

[Настройка политики control для команд su и sudo в операционной системе «Альт» \(см. раздел 14.7.2.5\)](#)

[Настройка уровня целостности для учетной записи в Astra Linux Special Edition \(см. раздел 14.7.2.6\)](#)

## 14.7.2.1. 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>
```

## 14.7.2.2. 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 --get-selections | grep syslog
```

```
rpm -qa *syslog*
```

- если SUSE Linux Enterprise Server:

```
zypper search *syslog* --installed-only | grep 'i |'
```

На экране появится название используемой службы.

## 14.7.2.3. 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.

## 14.7.2.4. 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. Если в инструкции не указана версия драйвера, рекомендуется использовать наиболее актуальную версию из доступных.

**Внимание!** Инструкции разработаны на основе документации вендоров СУБД и предназначены для установки ODBC-драйвера на узел с Debian 12. В других ОС команды и пути к файлам могут отличаться.

## Подготовка к установке

- Чтобы подготовить узел к установке ODBC-драйвера:

1. Запустите терминал на компьютере, где установлен XSpider PRO.

2. Выполните команду:

```
docker ps | grep core.agent
```

Отобразится список контейнеров.

3. Скопируйте ID или имя контейнера.

4. Перейдите в контейнер с правами суперпользователя, выполнив команду:

```
docker exec -it -u root <ID_или_имя_контейнера> /bin/bash
```

**Внимание!** Все дальнейшие действия по установке ODBC-драйвера необходимо выполнять внутри контейнера.

5. После завершения установки ODBC-драйвера перезапустите контейнер, выполнив команду:

```
docker restart <ID_или_имя_контейнера>
```

## Для СУБД Microsoft SQL Server

- Чтобы установить ODBC-драйвер:

1. Добавьте репозиторий для Debian:

```
curl https://packages.microsoft.com/keys/microsoft.asc | apt-key add -
curl https://packages.microsoft.com/config/debian/<Версия Debian>/prod.list > /etc/apt/sources.list.d/mssql-release.list
```

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
```

## Для СУБД Firebird

► Чтобы установить ODBC-драйвер:

1. Обновите данные о пакетах:

```
apt update
```

2. Скачайте с сайта [firebirdsql.org](https://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
```

3. Переместите файл `libOdbcFb.so` в каталог для библиотек:

```
mv libOdbcFb.so /usr/lib64/libOdbcFb.so
```

4. Запустите установку библиотеки `libfbclient2`:

```
apt install libfbclient2
```

5. 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
```

6. Откройте файл `/etc/odbcinst.ini`.

7. Добавьте в файл строки:

```
[Firebird]
Description=InterBase/Firebird ODBC Driver
Driver=/usr/lib64/libOdbcFb.so
Setup=/usr/lib64/libOdbcFb.so
Threading=1
FileUsage=1
CPOutput=
CPReuse=
```

8. Сохраните изменения и закройте файл.

## Для СУБД MySQL

► Чтобы установить ODBC-драйвер:

1. Установите необходимые пакеты:

```
apt-get install -y curl gnupg unixodbc-dev libssl-dev
```

2. Скачайте с сайта [mysql.com](https://dev.mysql.com) ODBC-драйвер:

Например:

```
curl -LO https://dev.mysql.com/get/Downloads/Connector-ODBC/mysql-connector-odbc-8.0.26-linux-glibc2.12-x86-64bit.tar.gz
```

3. Распакуйте архив:

```
tar -xzf mysql-connector-odbc-8.0.26-linux-glibc2.12-x86-64bit.tar.gz
```

4. Скопируйте исполняемые файлы драйвера в системный каталог:  

```
cp mysql-connector-odbc-8.0.26-linux-glibc2.12-x86-64bit/bin/* /usr/local/bin/
```
5. Откройте файл `/etc/odbcinst.ini`.
6. Добавьте в файл строки:  

```
[MySQL ODBC 8.0 ANSI Driver]
Description=MySQL ODBC 8.0 ANSI Driver
Driver=/usr/local/lib/libmyodbc8a.so
[MySQL ODBC 8.0 Unicode Driver]
Description=MySQL ODBC 8.0 Unicode Driver
Driver=/usr/local/lib/libmyodbc8w.so
```
7. Сохраните изменения и закройте файл.

## Для СУБД Microsoft SQL Server

### ► Чтобы установить ODBC-драйвер:

1. Обновите данные о пакетах:  

```
apt update
```
2. Установите ODBC-драйвер:  

```
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
```

## Для СУБД Oracle Database

► Чтобы установить ODBC-драйвер:

1. Скачайте с сайта [oracle.com](https://www.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](https://www.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 ~
```

## Для СУБД PostgreSQL

► Чтобы установить ODBC-драйвер:

1. Скачайте с сайта [postgresql.org](https://www.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/psqlodbc.a.so
```

4. Сохраните изменения и закройте файл.

## Для СУБД ClickHouse

► Чтобы установить ODBC-драйвер:

1. Скачайте с сайта [github.com](https://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:

```
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:

```
sudo mv clickhouse-odbc-1.1.10-Linux/share/doc/clickhouse-odbc/config/* /var/lib/clickhouse-odbc/doc/
```

5. Откройте 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
```

## 14.7.2.5. 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.

### 14.7.2.6. 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>
```

## 14.7.3. Стандартные операции в системах виртуализации VMware

Раздел содержит инструкции для стандартных операций, выполняемых в системах виртуализации VMware.

### В этом разделе

[Добавление учетной записи и назначение роли в VMware vCenter Server for Windows 5.5, 6.0 \(см. раздел 14.7.3.1\)](#)

[Добавление учетной записи и назначение роли в VMware vCenter Server for Windows 6.5 \(см. раздел 14.7.3.2\)](#)

[Создание учетной записи для VMware vCenter Server Appliance 6.7–8.0 \(см. раздел 14.7.3.3\)](#)

[Назначение роли учетной записи в VMware vCenter Server Appliance 6.7–8.0 \(см. раздел 14.7.3.4\)](#)

### 14.7.3.1. 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**.

### 14.7.3.2. 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**.

### 14.7.3.3. 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**.

### 14.7.3.4. 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**.

## 15. Решение проблем

### Не удается войти в учетную запись XSpider PRO

При попытке входа в учетную запись XSpider PRO появляется ошибка.

Для решения проверьте правильность имени пользователя и пароля.

Если ошибки в данных нет, обратитесь [в службу технической поддержки \(см. раздел 16\)](#).

## 16. О технической поддержке

Гарантийная поддержка доступна для всех владельцев действующих лицензий на XSpider PRO 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 гарантийной 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 и сроки 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 portalу 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.

Поддержка на портале предоставляется на русском и английском языках.

## Условия предоставления гарантийной поддержки

Для получения гарантийной 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 гарантийной 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 гарантийной поддержке продукта не включают в себя услуги по переустановке продукта, решению 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 гарантийной 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 службы 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.

## 17. Гарантийное обслуживание

Гарантийное обслуживание осуществляют сотрудники компании Positive Technologies.

Условия гарантийного обслуживания определены пользовательским соглашением.

Заявки на гарантийное обслуживание регистрируются через обращение в службу технической поддержки.



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. Positive Technologies — первая и единственная компания из сферы кибербезопасности на Московской бирже (MOEX: POSI). Количество акционеров превышает 220 тысяч.