Система анализа и мониторинга состояния ИБ DATAPK

Тема 3. Настройка подсистемы сбора конфигураций активов.

udv|group

Понятие сбора данных

Сбор данных – взаимодействие с объектом защиты в режиме запрос-ответ с целью получения определенных конфигураций (и иногда событий), а также их последующим анализом в ПК DATAPK.

Для того, чтобы собрать данные с актива, узел должен в первую очередь отдавать эти данные по запросу DATAPK. Для этого нужно настраивать актив. Без настройки узлов функционал сбора данных работать не будет.

В сборе данных фигурирует модуль **Configuration Management (CM)**. Для отображения собранных событий с активов нужен модуль **External Events Management (EEM)**.

Настройка актива под управлением Windows

Для полноценной работы функционала сбора данных и анализа защищенности необходимо создавать УЗ с правами локального администратора.
DATAPK поддерживает сбор данных с ОС Windows по следующим протоколам:

- WMI (Windows Management Instrumentation)
- MS-EVEN (версии 4 и 6) – только при наличии модуля **EEM**
- WinRM (Windows Remote Management) – основной протокол для современных Windows (7/2008 и новее)
- Winexe (для старых Windows – XP/2000/2003) – требуется дополнительный пакет **udv-terminal-connector-old-protocols**

MSI

WMI (Windows Management Instrumentation) – инструментарий управления Windows, одна из базовых технологий для централизованного управления и слежения за работой различных частей компьютерной инфраструктуры под управлением платформы Windows.

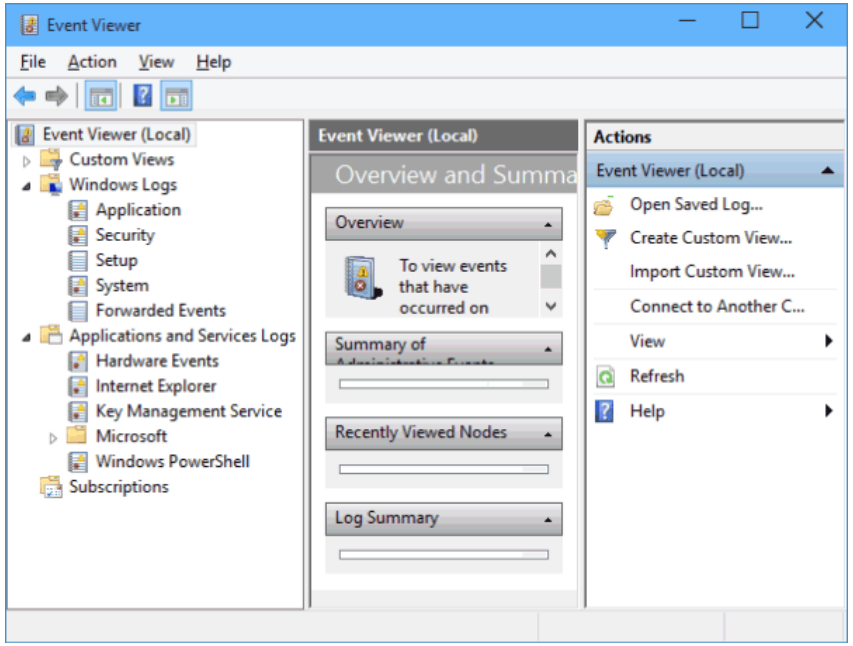
Для обращения к объектам WMI используется специфический язык запросов WMI Query Language (WQL), который является одной из разновидностей SQL. Основное его отличие от ANSI SQL — это невозможность изменения данных, то есть с помощью WQL возможна лишь выборка данных с помощью команды SELECT. Помимо ограничений на работу с объектами, WQL не поддерживает такие операторы как DISTINCT, JOIN, ORDER, GROUP, математические функции. Конструкции IS и NOT IS применяются только в сочетании с константой NULL.

На практике используется нечасто, т.к. WinRM работает стабильнее на современных Windows и не требует открытых High-портов на межсетевом экране

CyberLympha®

MS-EVEN

MS-EVEN – технология для получения журналов Windows посредством Microsoft RPC.



Достоинства сбора данных по WMI/MS-EVEN:

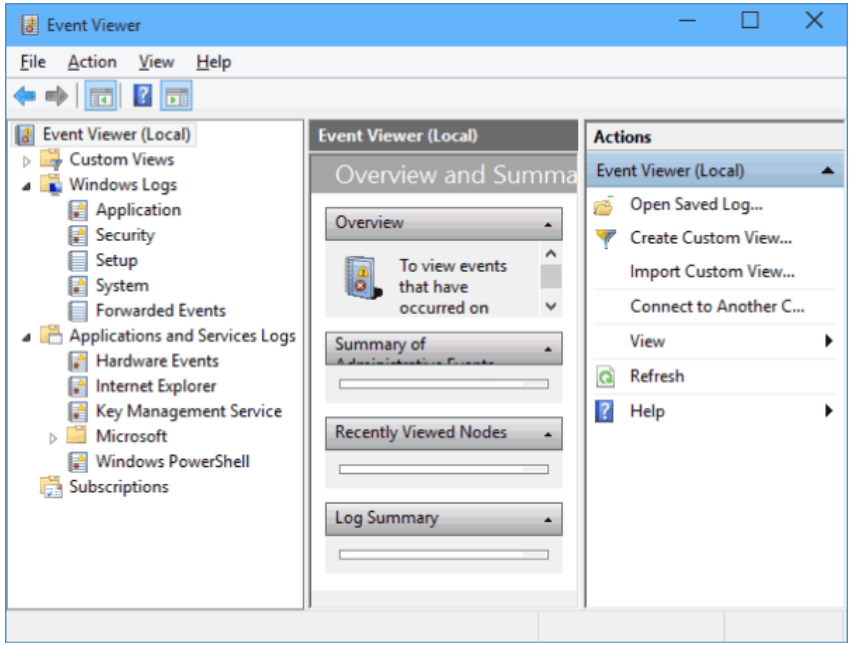
- встроенный функционал Windows;
- позволяет простыми запросами получить большое количество различных данных в табличном представлении;
- можно протестировать запросы встроенной утилитой wbemtest;
- единственный способ безагентного сбора журналов для Windows XP/Server 2003 и старше.

CyberLympha®

MS-EVEN

Недостатки сбора данных по WMI/MS-EVEN:

- некоторые запросы выполняются долго (либо не укладываются в таймаут);
- не всегда отдает все необходимые данные (в частности – отдает не все установленное ПО, а лишь ПО, установленное посредством Windows Installer);
- большое количество нюансов при настройке – не всегда механизм корректно отрабатывает на объектах защиты, бывают сбои работы компонента WMI на конкретных ОЗ;
- закрытая спецификация, не всегда удается собрать данные сторонними библиотеками;
- взаимодействует по TCP 135 и High-портам (разные у разных машин), у MS-EVEN еще TCP 445 – сложности с прописыванием сетевых доступов на МСЭ.



CyberLympha®

Сетевые доступы

Сетевые доступы для WMI и MS-EVEN

Источник трафика	Порт назначения	Узел назначения
DATAPK Sensor	TCP 135, TCP 445, TCP 1024-5000	Объекты защиты (ОЗ) на базе Windows XP и старше
	TCP 135, TCP 445, TCP 49152-65535	Объекты защиты (ОЗ) на базе Windows Vista и новее

CyberLympha®

WinRM

WinRM (Windows Remote Management) – встроенный функционал Windows, позволяет системам получать доступ к управляющей информации или обмениваться ею через общую сеть, используя объекты сценариев или встроенный инструмент командной строки.

Функционал доступен в ОС Windows 7 (Vista) и новее.

У протокола WinRM есть 2 вариации:

- Без шифрования (WinRM over HTTP), работает на порту 5985/TCP – данные передаются по сети в нешифрованном виде, не работает в неопознанных, общественных сетях. Рекомендуется к использованию в Windows XP, поскольку там не поддерживаются современные алгоритмы шифрования.
- С шифрованием (WinRM over HTTPS)), работает на порту 5986/TCP – данные передаются в шифрованном виде, может работать в неопознанных, общественных сетях. Рекомендуется к использованию в Windows 7 и новее.

CyberLympha®

WinRM

Для работы WinRM на Windows XP нужно установить обновление KB968930. Однако установка обновлений на СВТ АСУ ТП далеко не всегда возможна. Работы по установке обновлений ОС нужно отдельно согласовывать с эксплуатирующей организацией.

Достоинства сбора данных по WinRM:

- встроенный функционал Windows;
- позволяет выполнять произвольные cmd/powershell запросы;
- позволяет собирать события журналов Windows, которые не отдает MS-EVEN 4 (например, журнал службы печати).

Недостатки сбора данных по WinRM:

- по умолчанию доступен, начиная с Windows 7;
- DATAPK поддерживает только Basic и NTLM-авторизацию WinRM;
- более сложный синтаксис сканеров сбора данных, поскольку приходится вручную парсить вывод из cmd или powershell.

CyberLympha®

Winexe

Winexe – сторонняя служба winexesvc, позволяющая выполнять консольные команды на ОЗ под управлением Windows. Альтернатива PsExec, запускающаяся с узлов под управлением ОС Linux.

При обращении к ОЗ по Winexe сперва происходит инициализация службы, далее выполняется команда на ОЗ. По завершении соединения служба удаляется.

DATAPK поддерживает 2 версии протокола Winexe – 0.8 и 1.0. Версия 0.8 – основная, поддерживает сбор с более широкого перечня ОЗ (в частности, есть скрипты для сбора с Windows 2008 и новее). Для части ОЗ необходимо использовать версию Winexe 1.0 в случае ошибок при работе с Winexe 0.8.

Требуется дополнительный пакет **udv-terminal-connector-old-protocols**

Ввиду постепенного импортозамещения или перехода на новые Windows протокол используется нечасто

CyberLympha®

Сетевые доступы

Сетевые доступы для Winexe

Источник трафика	Порт назначения	Узел назначения
DATAPK	TCP 139, TCP 445	Объекты защиты (ОЗ) на базе Windows

Производитель DATAPK не рекомендует использовать Winexe при возможности сбора данных по WinRM. Поддержка скриптов Winexe для ОС Windows 7 и новее не производится.

Допускается использование данного механизма лишь для сбора данных с ОЗ под управлением Windows XP и Windows 2000.

CyberLympha®

Winexe

Достоинства сбора данных по Winexe:

- позволяет собирать данные с активов под управлением Windows 2000 и Windows XP в качестве альтернативы WinRM;
- очень часто не требует настройки активов (за исключением создания ОЗ).

Недостатки сбора данных по Winexe:

- сбор данных обязателен с УЗ локального администратора, нельзя ограничить полномочия;
- доступны не все команды cmd/powershell, в частности – не доступна команда wmic;
- сторонняя служба, не являющаяся встроенным функционалом Windows;
- менее стабильная работа по сравнению с WMI, WinRM;
- предоставляет мало информации для диагностики ошибок.

CyberLympha®

Необходимые настройки на ОС Windows

- Создана УЗ с необходимыми правами (обычно локальный администратор).
- Службы «Сервер» (LanmanServer) и «Инструментарий управления Windows» (Winmgmt) д.б. в статусе «Выполняется» и с автоматическим типом запуска.
- Д.б. отключен удаленный контроль учетных записей (Remote UAC) на Windows Vista и новее (параметр HKLM\SOFTWATE\Microsoft\Windows\CurrentVersion\Policies\System\LocalAccountTokenFilterPolicy, значение 1, тип DWORD).
- Правила межсетевого экранирования (при включенном брандмауэре Windows).
- «Панель управления» – «Администрирование» – «Локальная политика безопасности» – «Локальные политики» – «Параметры безопасности» – «Сетевой доступ: модель общего доступа и безопасности для локальных учетных записей» – Д.б. установлен параметр: «Обычная – локальные пользователи удостоверяются как они сами».
- «Панель управления» – «Администрирование» – «Локальная политика безопасности» – «Политики диспетчера списка сетей» – «Неопознанные сети» – Установить параметр: «Тип расположения»: «Личное» (для Windows Vista и новее при использовании WinRM over HTTP – Vista и новее, при использовании WinRM over HTTPS настройка избыточна).

CyberLympha®

Необходимые настройки на ОС Windows

Настроена служба «Инструментарий управления Windows» (winrm) при использовании сбора с использованием WinRM.

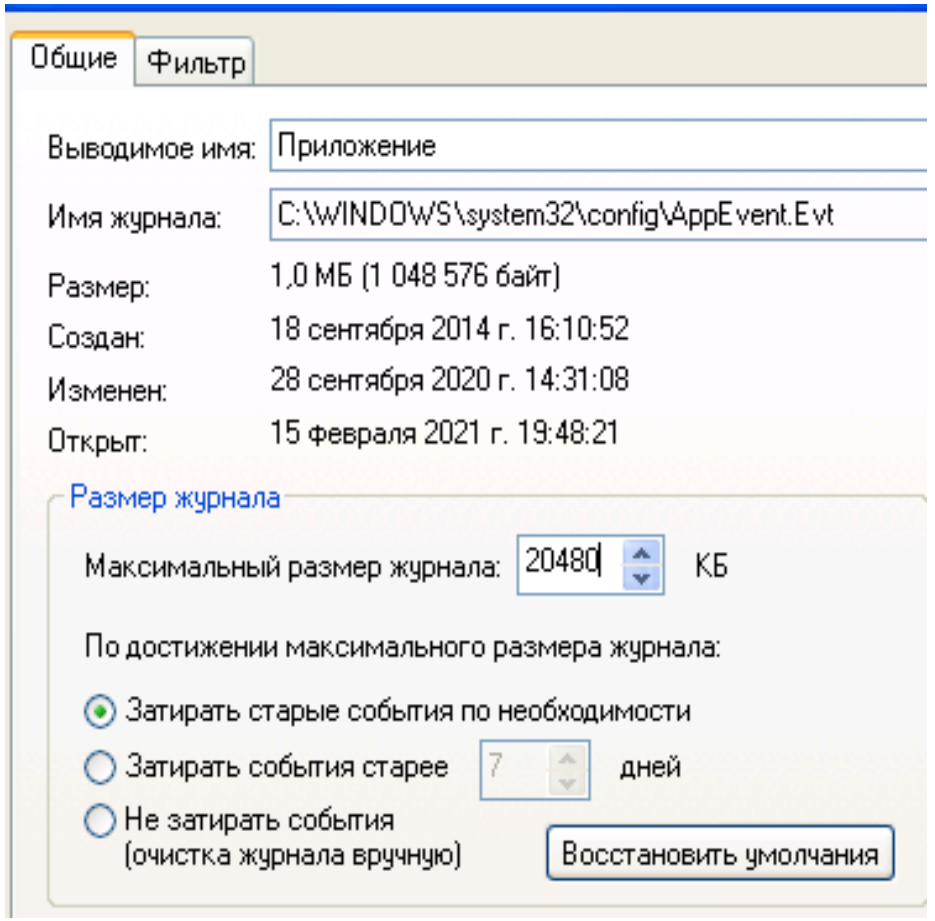
Настроен аудит для сбора событий. Рекомендуемые значения:

- «Аудит входа в систему»: «Успех, Отказ»;
- «Аудит доступа к объектам»: «Нет аудита»;
- «Аудит доступа к службе каталогов»: «Нет аудита»;
- «Аудит изменения политики»: «Успех, Отказ»;
- «Аудит использования привилегий»: «Нет аудита»;
- «Аудит отслеживания процессов»: «Нет аудита»;
- «Аудит системных событий»: «Успех, Отказ»;
- «Аудит событий входа в систему»: «Успех, Отказ»;
- «Аудит управления учетными записями»: «Успех, Отказ».

CyberLympha®

Необходимые настройки на ОС Windows

Проверить настройки журналов Windows (Панель управления \ Администрирование \ Просмотр событий) – д.б. установлена настройка «При достижении максимального размера: затирать старые события при необходимости». Рекомендуемый максимальный размер журнала 20 МБ. В ОС Windows Vista и новее данные настройки по умолчанию установлены корректно, но проверить не помешает.



CyberLympha®

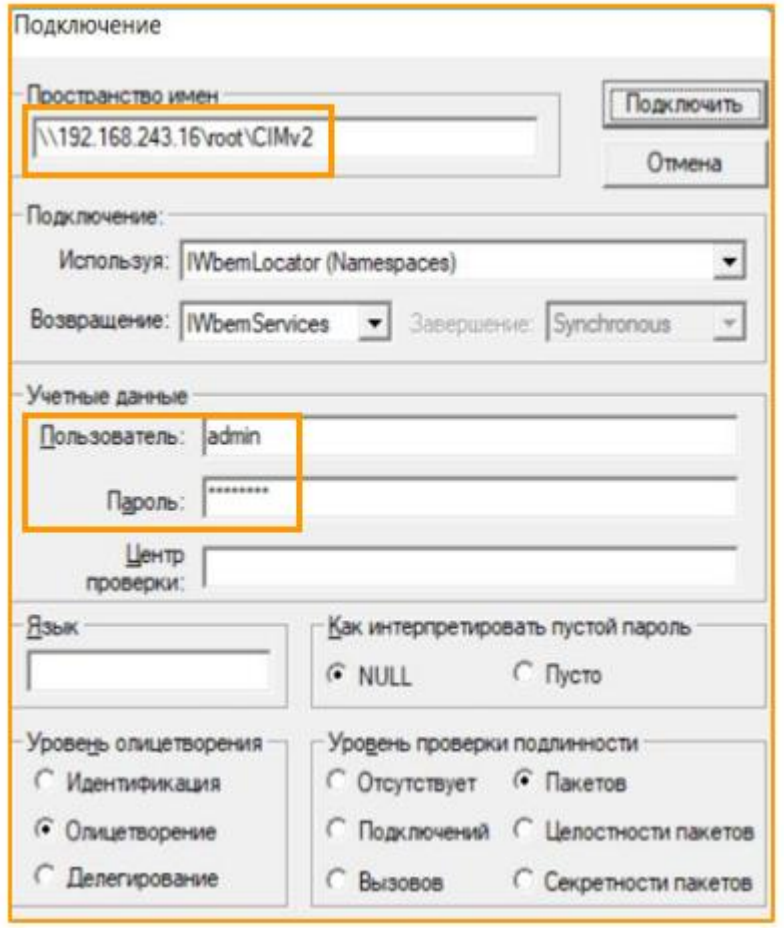
Необходимые настройки на ОС Windows

После выполнения настроек необходима перезагрузка СВТ.

Проверка подключения:

Доступ по WMI удобно проверять встроенной утилитой wmemtest на ОС Windows.

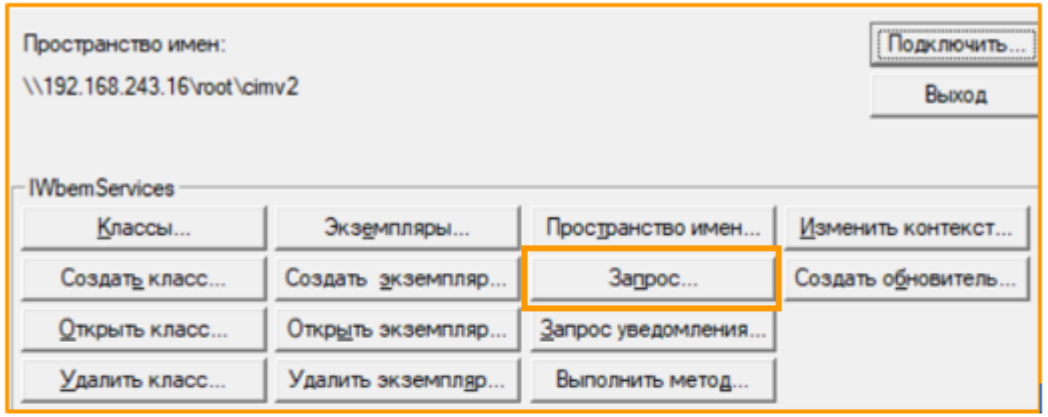
Для подключения к удаленному ОЗ необходимо в пространстве имен набрать \\IP\root\CIMv2 и ввести логин и пароль пользователя. Далее – нажать «Подключить».

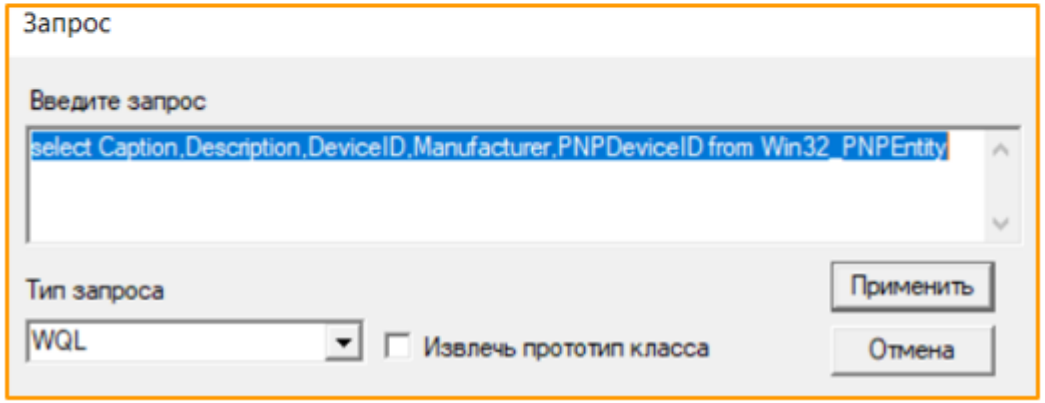


CyberLympha®

Необходимые настройки на ОС Windows

Далее выбрать «Запрос», ввести тестовый WMI-запрос и нажать «Применить».





Примеры тестовых WQL запросов (работают в т.ч на Windows 2000):

- select * from Win32_PNPEntity – запрос списка устройств
- select * from Win32_Process – запрос списка процессов

Прочие WQL-запросы можно посмотреть в скриптах сбора данных DATAPK.

Можно попробовать протестировать подключение посредством cmd, например командой вида **wmic /user:"Administrator" /password:"P@ssword" /node:"192.168.243.19" process list brief**.

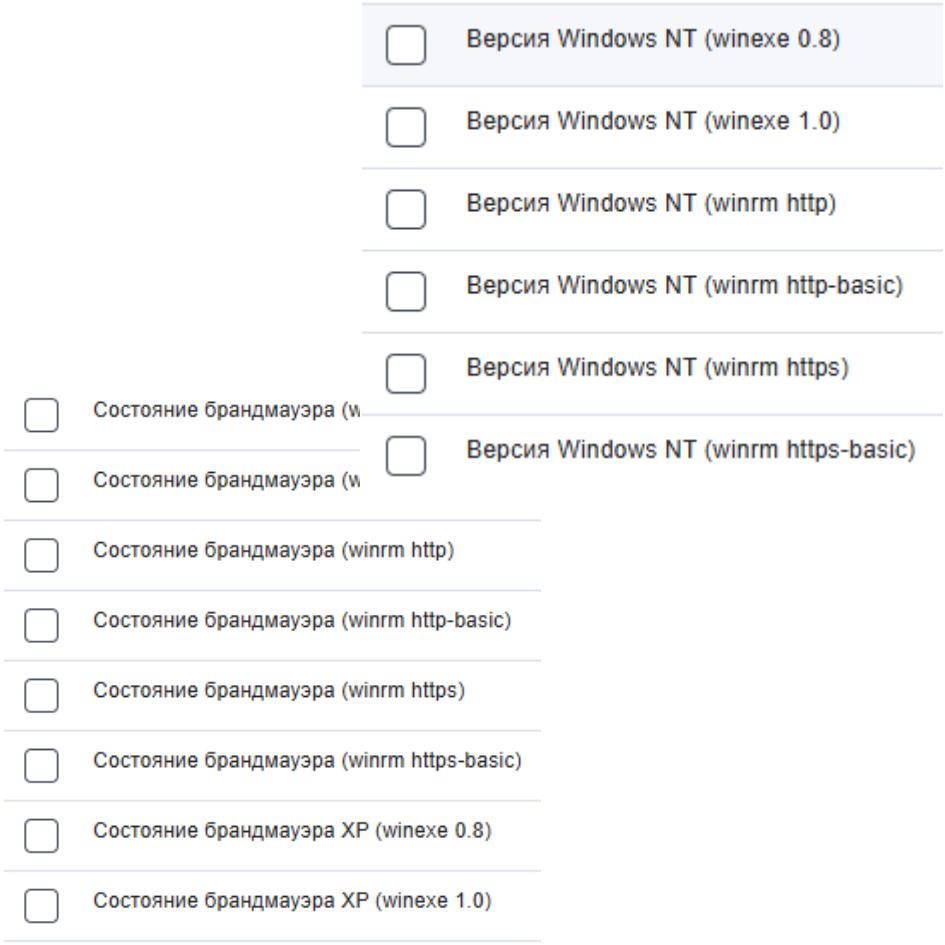
Сканеры под ОС Windows

В сканерах в скобках указан протокол опроса (иногда еще семейство для старых ОС).

Basic – это basic-авторизация для WinRM (с доменными УЗ не работает, при WinRM HTTP учетные данные в BASE64 без доп. шифрования)

Если просто WinRM – это NTLM-авторизация (более безопасный алгоритм, работает в т.ч. с доменными УЗ – указывать надо в формате FQDN (например username@company.local))

Тег используется **admin**



CyberLympha®

Настройка ОЗ под управлением Unix

Сбор с ОС Linux поддерживается по протоколу SSH версии 2.

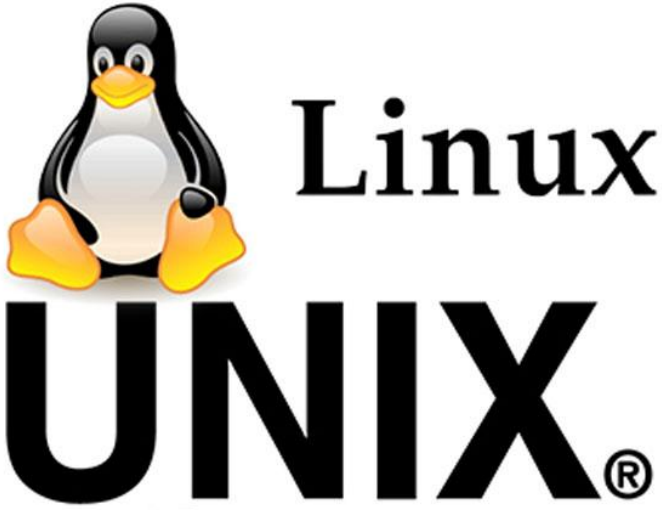
На ОЗ под управлением Linux нужно настроить службу ssh и создать учетную запись для DATAPK. В общем случае – нужны права на чтение файлов и выполнения перечня команд.

Для сбора большинства параметров хватает обычной пользовательской УЗ.

При необходимости повышения прав для получения конфигурации возможно использовать утилиту sudo. Для этого необходимо прописать разрешения через visudo (либо добавить пользователя в группу wheel или аналогичную).

Также возможно повышение привилегий путем вызова команды su и ввода пароля суперпользователя. Данный вариант не рекомендован к использованию, однако в некоторых случаях – это единственно возможный вариант получения конфигураций (например, для сбора запланированных задач Cron в ОС Solaris).

В случае отсутствия возможности сбора по SSH (отсутствие пакета в ОС) допускается сбор по telnet. В частности, по telnet собираются конфигурации ОС QNX 4.25.



CyberLympha®

Сетевые доступы, настройки и проверка

Сетевые доступы для Unix-like дистрибутивов

Источник трафика	Порт назначения	Узел назначения
DATAPK Sensor	TCP 22	Объекты защиты (ОЗ) на базе Unix – сбор по SSH
	TCP 23	Объекты защиты (ОЗ) на базе Unix – сбор по telnet

Необходимые настройки на ОС Linux:

- создана УЗ;
- настроен доступ по SSH (в редких случаях – Telnet);
- разрешено выполнение всех требуемых команд (при необходимости УЗ добавлена в sudoers/wheel);
- настроена отправка интересующих событий по syslog в сторону DATAPK (rsyslog или аналогичная служба).

Проверка подключения:

- **ssh login@ip_address** из консоли DATAPK для проверки доступа по SSH;
- **telnet ip_address** из консоли DATAPK для проверки доступа по Telnet (утилита не всегда есть в составе ОС), **curl -v telnet://ip_address:port** – проверка доступности порта (номер порта для telnet по умолчанию 23, можно опустить в команде).

Сканеры под Unix

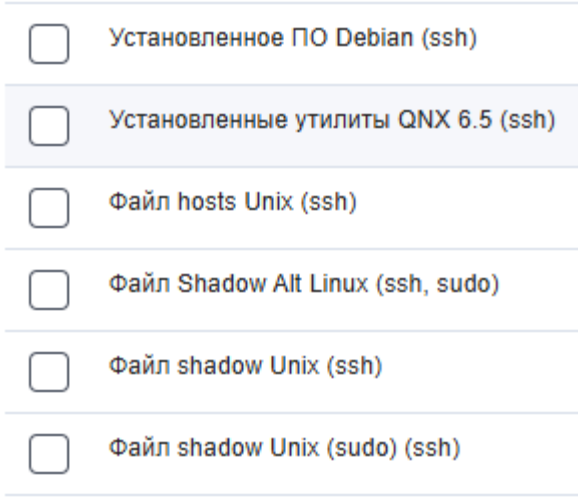
Если сканеры под Linux содержат приписку sudo – это значит, что выполняется команда с повышением привилегий

Если приписки нет – команда выполняется от имени пользователя без повышения привилегий

В некоторых случаях уточняется семейство ОС (если это критично для выполнения)

Для Astra подходит большинство Debian-сканеров, для РЕД ОС – большинство CentOS-сканеров

Тег используется **admin**



Настройка АСО

Сбор данных с использованием командной оболочки (CLI).

Для сбора конфигураций с активного сетевого оборудования рекомендуется использовать протокол SSH 2.0.

В случае отсутствия возможности подключения по SSH версии 2 есть возможность сбора данных по протоколу SSH версии 1 или telnet. Для сбора по SSHv1 нужен пакет **udv-terminal-connector-old-protocols**

Для сбора данных нужно создать УЗ для DATAPK на сетевом оборудовании. Также для сбора данных нужны привилегии на выполнение команд просмотра текущей и начальной конфигурации АСО.

В частности, в некоторых случаях для этого требуется ввод пароля на вход в привилегированный (enable) режим. Такие скрипты есть для АСО Cisco в стандартной поставке.

CyberLympha®

Настройка АСО

Поддерживаемое DATAPK сетевое оборудование:

- Cisco, Cisco ASA;
- Eltex;
- Huawei;
- Nateks;
- Zelax и пр.

Также есть примеры скриптов для Hirschmann, NsGate NIS, Moxa, Fortinet, Checkpoint.

CyberLympha®

Сетевые доступы

Сетевые доступы для АСО

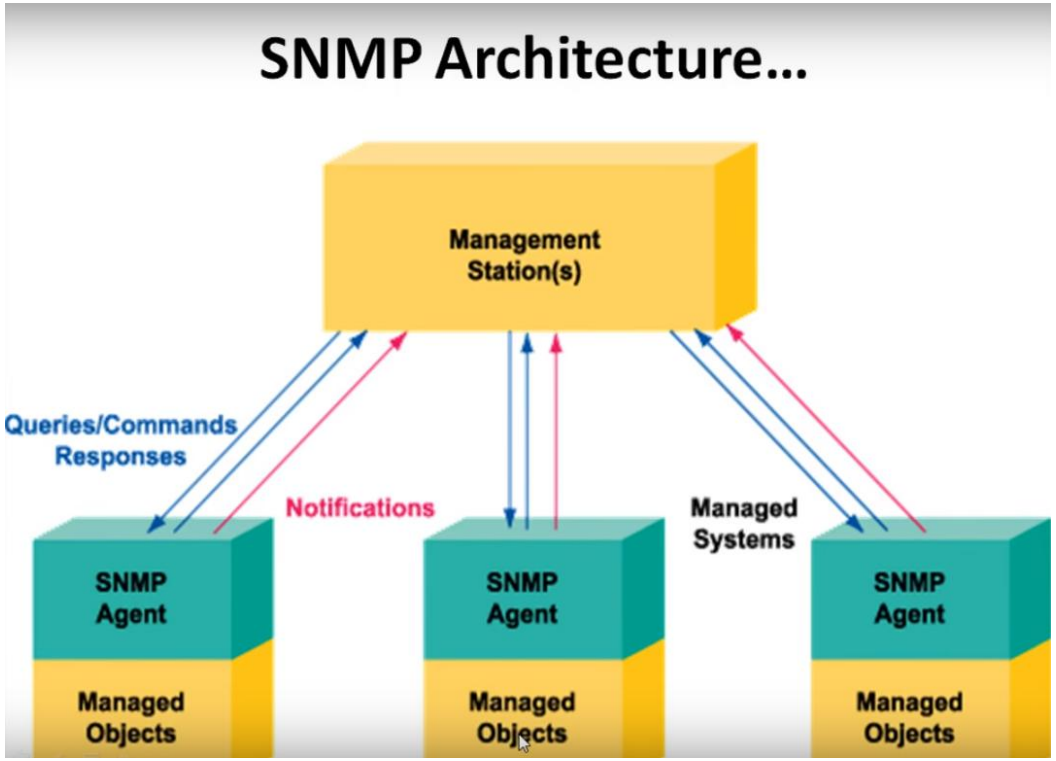
Источник трафика	Порт назначения	Узел назначения
DATAPK Sensor	TCP 22	АСО, сбор по SSH
	TCP 23	АСО, сбор по telnet

CyberLympha®

Сбор данных по SNMP

DATAPK позволяет собирать данные с сетевых устройств с использованием SNMP.

Поддерживаются версии SNMP 1, 2c, 3. Также посредством данных сканеров можно собрать список всех интерфейсов АСО и назначить найденные интерфейсы объекту защиты. Полезно для функционала автоматической привязки неизвестных ОЗ с MAC-адресами маршрутизирующих устройств существующим ОЗ.



CyberLympha®

Сетевые доступы

Сетевые доступы для SNMP

Источник трафика	Порт назначения	Узел назначения
DATAPK Sensor	UDP 161	АСО, сбор по SNMP

CyberLympha®

Необходимые настройки на АСО

- создана УЗ
- настроен доступ по SSH (в редких случаях – Telnet)
- разрешено выполнение всех требуемых команд (в некоторых случаях – через привилегированный режим)
- настроен snmp-сервер версии 1 или 2c, рекомендуется отдельная группа (community) с правами на чтение для подключения DATAPK. В случае использования snmpv3 нужно указать дополнительные параметры (алгоритм шифрования и пр.)
- настроена отправка интересующих событий по syslog в сторону DATAPK
- при необходимости – отправка SNMP-trap версии 1 или 2c в сторону DATAPK (зачастую избыточно при настроенной отправки syslog)

- **ssh login@ip_address** из консоли DATAPK для проверки доступа по SSH;
- **telnet ip_address** из консоли DATAPK для проверки доступа по Telnet (при наличии утилиты), доступность порта можно проверить командой **curl -v telnet://ip_address**;
- **snmpwalk -v snmp_version -c community_name ip_address** из консоли DATAPK для проверки доступа по SNMP.

Настройка ПЛК

Поддерживаются следующие протоколы:

- S7comm для ПЛК Siemens;
- UMAS (расширенный Modbus) для ПЛК Schneider Electric;
- EthernetIP для ПЛК Allen Bradley;
- OPC UA для ПЛК Регул, ТРЭИ и пр..

Также есть возможность написания скриптов сбора значений регистров по протоколу Modbus, написания скриптов сбора данных с ПЛК по протоколам SSH, Telnet, SNMP, FTP.

CyberLympha®

Сетевые доступы

Для получения данных с ПЛК нужны следующие сетевые доступы

Источник трафика	Порт назначения	Узел назначения
DATAPK Sensor	TCP 102	ПЛК Siemens
	TCP 502	ПЛК Schneider Electric либо произвольный ПЛК с поддержкой Modbus
	TCP 44818	ПЛК Allen Bradley
	TCP 48010	ПЛК Регул (OPC UA) – порт довольно часто разный у разных вендоров

Необходимые настройки на ПЛК

- настроен доступ к ПЛК по интересующему протоколу;
- есть служебная УЗ / уточнено значение стойки (Rack) и ячейки (Slot) для подключения к ПЛК;
- уточнены номера программных блоков и блоков данных для мониторинга (для Siemens);
- в некоторых случаях – внесены изменения в программу ПЛК, чтобы она отдавала контрольные суммы/иную информацию.

Для проверки доступа: **curl -v telnet://ip_address:port**

CyberLympha®

Общая структура сбора данных

Конфигурация актива — набор параметров актива, связанных с состоянием информационной безопасности. Как правило, каждому набору параметров соответствует своя конфигурация. Например, для ПЛК могут проверяться конфигурации по протоколу S7comm на соответствие эталонным настройкам системы, ее версии и контрольным суммам блоков.

Сбор информации о конфигурациях ведется при помощи задач сбора данных, сбор данных может быть как разовым, так и периодическим.

Группа сканеров — совокупность сканеров для совместного или раздельного сбора данных о конфигурациях и в некоторых случаях событиях.

Сканер — исполняемый python-скрипт сбора данных. Для безопасности обсчитывается контрольная сумма сканера (цифровая подпись) во избежание несанкционированного внесения изменений

Скрипт — это последовательность действий, описанных с помощью скриптового языка программирования Python, для сбора данных с объектов защиты.

Запускать сканеры сбора можно только при согласовании с заказчиком.

Интегратор (или заказчик) целиком и полностью несут ответственность в случае выполнения самописных сканеров сбора данных.

Общая структура сбора данных

У сканеров 4 типа:

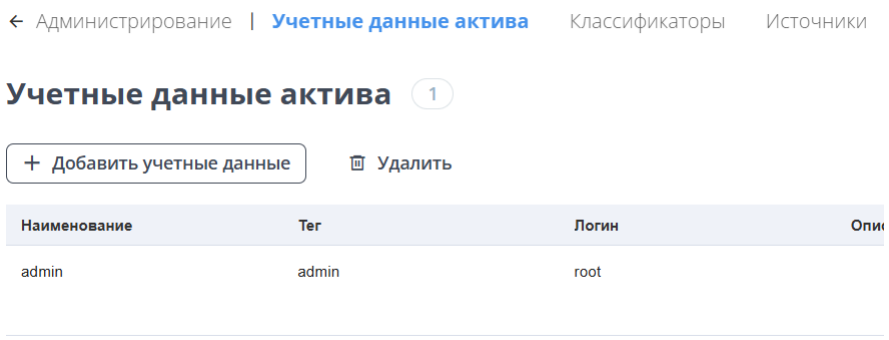
- конфигурации;
- версия ОС;
- установленное ПО;
- события (требуется дополнительно модуль EEM)

- В одну группу не рекомендуется добавлять более 10 сканеров
- Все сканеры в группе должны выполняться на одном типе ОЗ – новые Windows либо Linux/ПЛК Siemens/... (в идеале использовать один и тот же протокол сбора данных)

Учетные записи

Учетная запись (УЗ) – объект в DATAPK, позволяющий использовать в сканерах сбора данных авторизационные данные.

Создание учетных записей происходит в блоке «Администрирование», страница Учетные данные актива.



CyberLympha®

Атрибуты УЗ

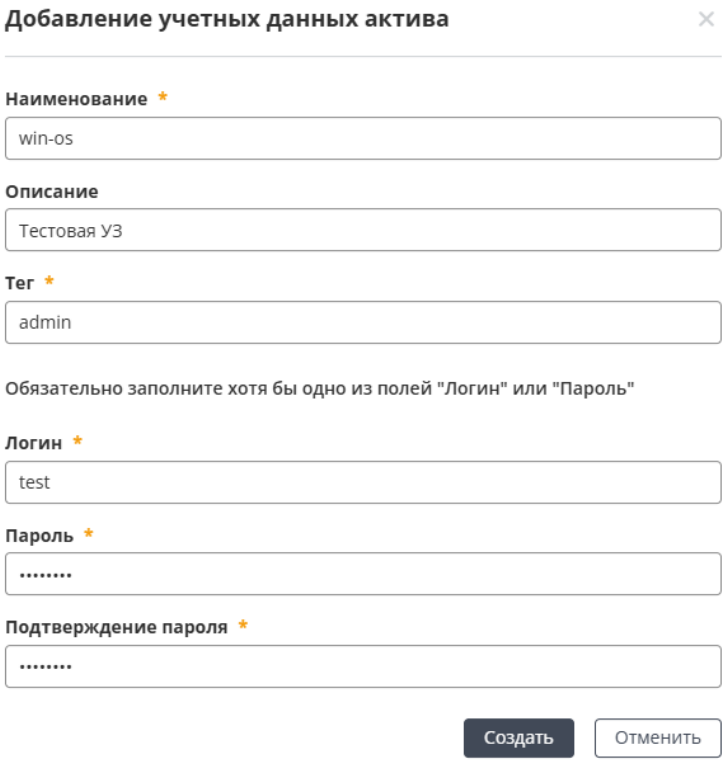
- **Наименование** – обязательное уникальное поле с произвольным названием учетной записи
- **Описание** – опциональное поле для ввода текстового описания УЗ
- **Тег** – текстовое поле для ввода признака УЗ (тега), по которому к ней может обратиться скрипт сбора данных. Тег должен совпадать со значением, указанным в сканере сбора данных.
- **Логин** – опциональное поле – наименование (логин) УЗ, по которому планируется обращение к ОЗ
- **Пароль** – опциональное поле. Пароль для обращения к ОЗ. Введенный пароль намеренно скрывается

CyberLympha®

Атрибуты УЗ

Например, нужно создать УЗ для подключения к активу под управлением Windows с логином test и паролем.

Тег в этом случае admin (используется в скриптах сбора данных под ОС Windows).



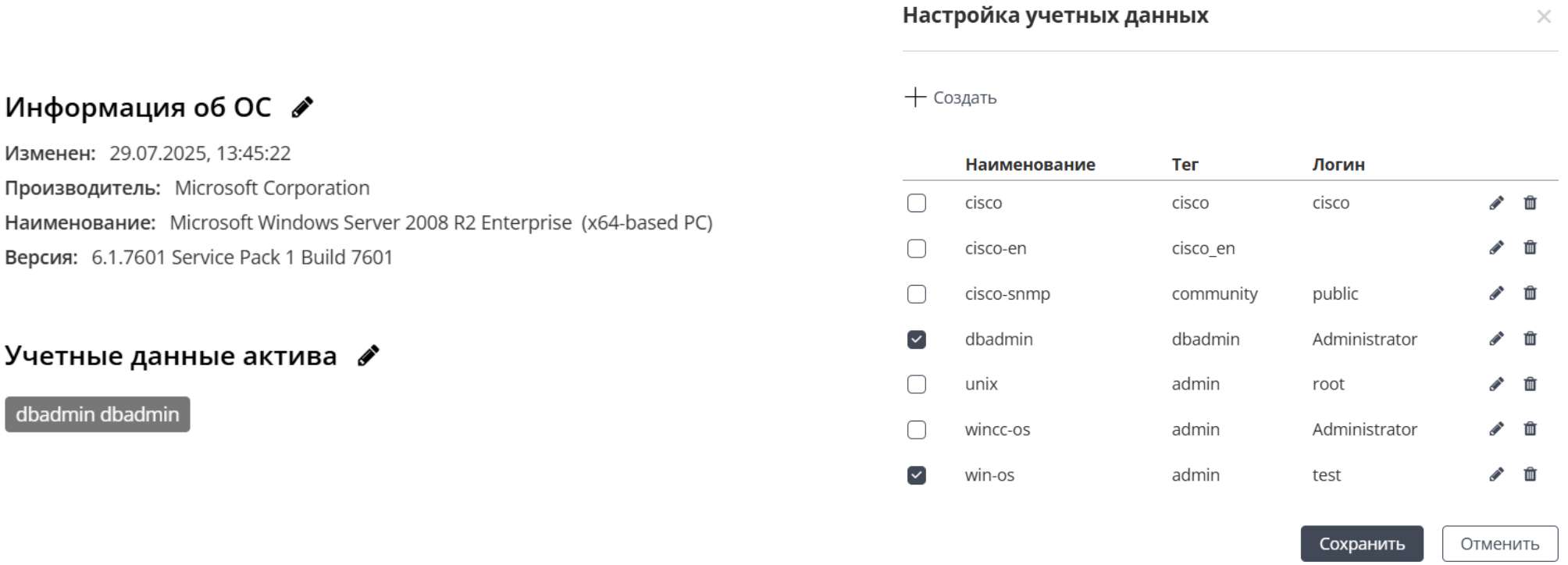

```
        return credentials[user]
    except KeyError:
        raise KeyError('Учетные данные для %s не найдены' % user)
def get_admin_credentials(credentials: dict):
    return get_credentials(credentials, 'admin')
def get_oval_credentials(credentials: dict) -> dict:
    oval_credentials = credentials.get(
```

Атрибуты УЗ

Учетные записи можно редактировать и удалять на этой же странице.

Назначить учетную запись ОЗ можно через его карточку в блоке «Учетные данные актива».

Активу можно назначать несколько УЗ с разными тегами (для сбора по разным протоколам). В примере ниже собираются конфигурации MSSQL (отдельная УЗ, тег dbadmin) и с ОС Windows по WinRM (тег admin)



Python-скрипт сбора данных

Скрипт сбора данных – это последовательность действий, описанных с помощью скриптового языка программирования Restricted Python, для сбора данных с объектов защиты. В скриптах запрещен импорт пакетов.

Скрипт необходимо сохранять в файле формата *.py (кодировка – UTF-8 без BOM). В скриптах сбора данных необходимо следить за отступами (требования Python). Также запрещено использовать табуляцию.

Для просмотра и редактирования скриптов сбора данных рекомендуется использовать текстовые редакторы Notepad++, Visual Studio Code или аналогичные. Запрещено редактировать скрипты с использованием встроенного блокнота, поскольку в этом случае возможны проблемы с кодировкой и переносом строк.

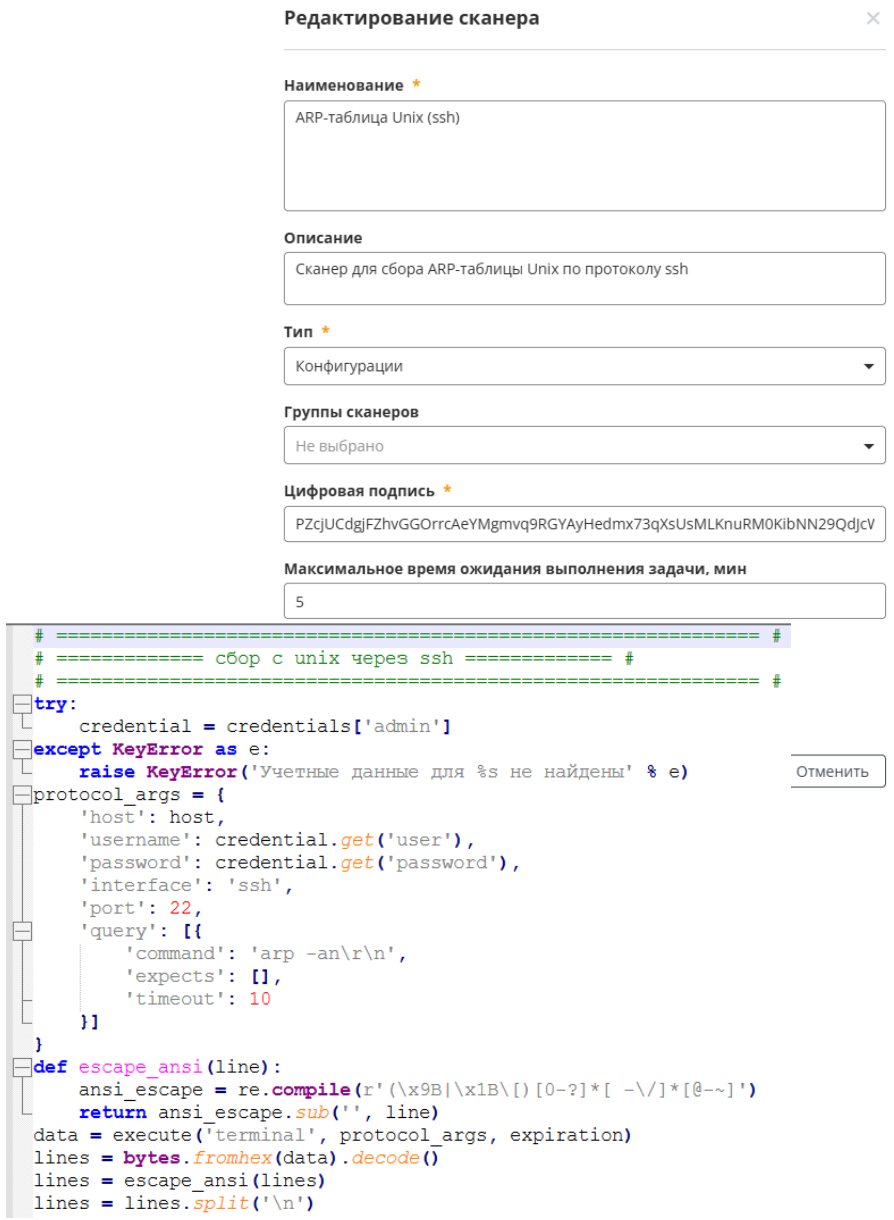
Скрипт выполняется внутри функции compile_restricted_function. Результат выполнения функции есть результат выполнения скрипта, т.е. результат выполнения необходимо вернуть с помощью оператора return.

В рамках технической поддержки производитель DATAPK помогает готовить сканеры сбора данных.

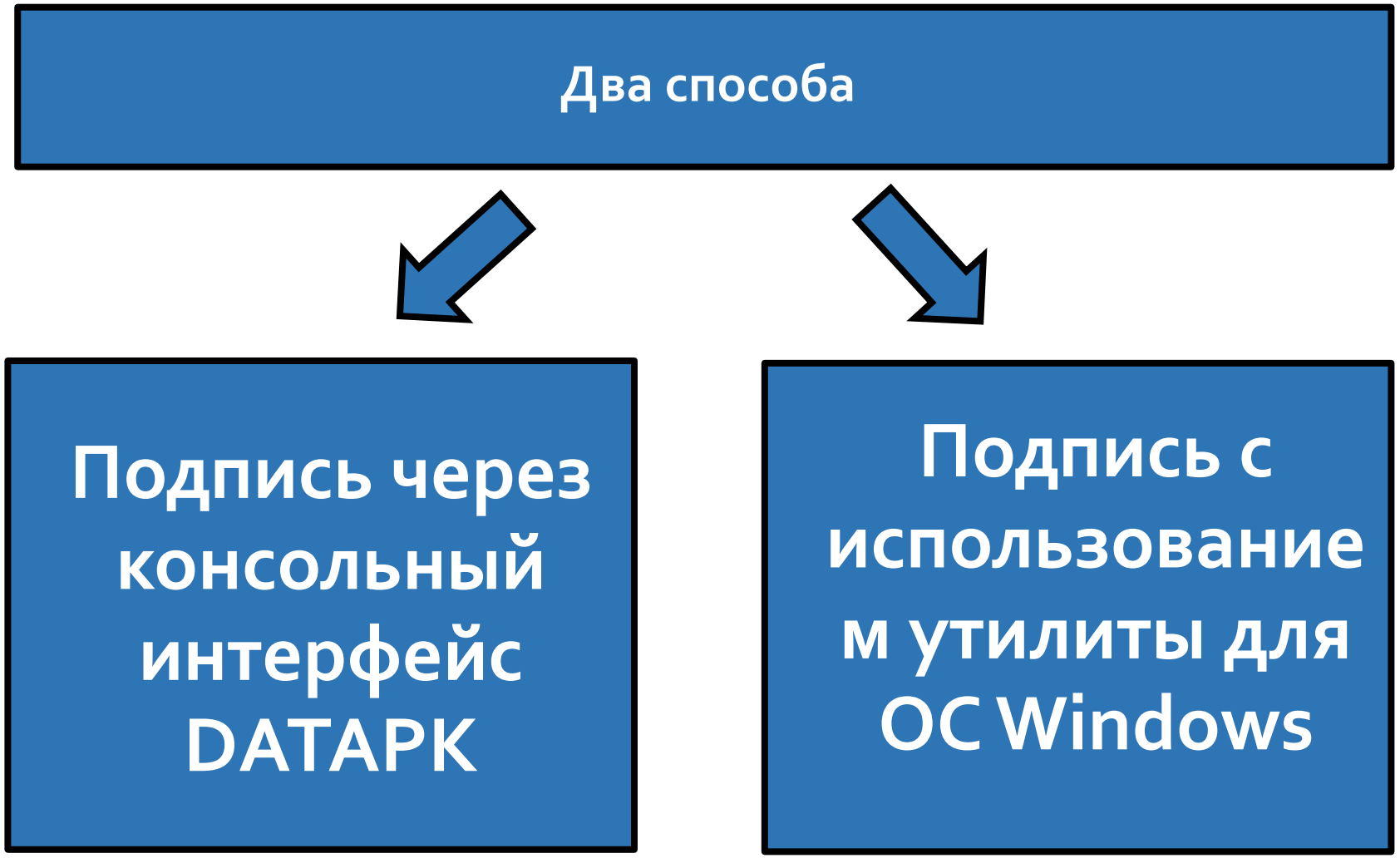
Скрипт сбора данных

Основные переменные в скриптах сбора данных:

- **host** – IP-адрес объекта защиты, на котором выполняется сбор данных. Берется из карточки узла (из сетевого интерфейса по умолчанию, оттуда же берется идентификатор сенсора, который выполняет скрипт сбора);
- **credentials** – словарь (dict) с реквизитами доступа к объекту защиты; значение данной переменной – словарь с двумя ключами (user, password). Сканер получает данные о ключах из учетной записи объекта защиты DATAPK, тег которой совпадает с названием словаря;
- **store** – (any, dict) сохраненные данные с предыдущего запуска скрипта. Если скрипт запускается первый раз, то store = None, применяется в скриптах сбора событий;
- **timeout – максимальное время выполнения запроса**
- **expiration** – максимальное общее время выполнения скрипта (задается через веб в настройках сканера);
- **execute** – метод, выполняющий запрос к коннектору.



Подпись скрипта сбора данных



CyberLympha®

Подпись через консольный интерфейс (редкий кейс)

Можно подписать скрипт при помощи команды, явно указывая пути к закрытому ключу и скрипту. Сертификат по умолчанию находится в каталоге **/usr/share/udv/scripts-certs/** (для подписи он не нужен). Закрытый ключ поставляется производителем DATAPK по запросу. При необходимости вендор может выпустить отдельную пару сертификат-закрытый ключ.

Алгоритм подходит для любой Linux-машины с библиотекой openssl.

Для этого нужно скопировать файл python-скрипта сбора данных и файл ключа в отдельный каталог, например **/opt/scanners** (предварительно его нужно создать командой **mkdir /opt/scanners**).

Далее – перейти в директорию в режиме командной строки (**cd /opt/scanners** в нашем примере).

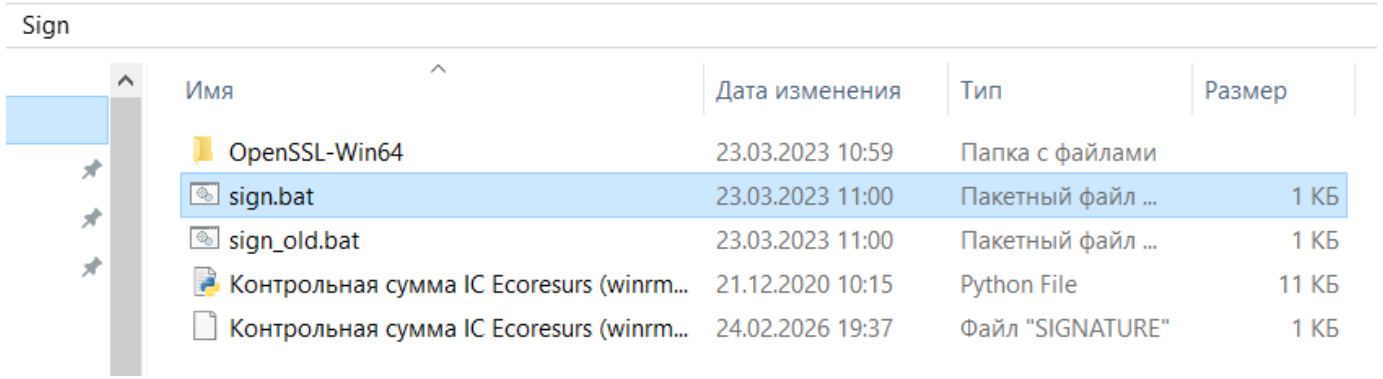
Далее – создать цифровую подпись скрипта с использованием команды **openssl dgst -sha256 -sign datapk_script.key 'имя_py-файла' | openssl enc -base64 -in /dev/stdin**

```
[root@datapk-demo scripts-certs]# openssl dgst -sha256 -sign datapk_script.key 'audit.py' | openssl en
c -base64 -in /dev/stdin
jR+HfLTMW55vYkAIdky7BKEdt2vB3Q9gPQfBjfYaA8nKOi8Fdc6DxpWoUpFLStJi
AAh5tFY7OvmsNarIbwG14oCiGnVjFQkJMVIriJUJwu4gCRYoUrMFn/EFrfIIxwXm
2ulM9FDypqbbiRPQ9Z133YaEuozE0VHmsaa2um38jqL8CEZGg5Ee1WmxkQ2axtap
UQ/Q1pSYoYAwlimlGgroFJClhKopwosNNUNElJ4PsaxIV+IZuCC9rPWStULqS4B5
agLhj1+DxqsCb9IbwJBqIKKqpDgF6evIxLBC1HDkMOrX/hXX+N7sHiqsmNss7clP
t+S9P99eAXYaU/M7eTe0ZA==
```

Подпись с использованием утилиты для ОС Windows

Если вы используете Windows, можно воспользоваться утилитой для подписи скриптов.

Для этого нужно распаковать архив Sign.rar и положить файл с python-скриптом в каталог утилиты. После этого нужно запустить скрипт для подписи двойным кликом на файл “sign.bat”, этот скрипт проходится по всем файлам в папке с расширением «*.py» и выполняет команду для подписи скриптов. Для каждого файла результат выполнения команды сохраняется в текстовый файл с именем «<полное имя файла>.signature».



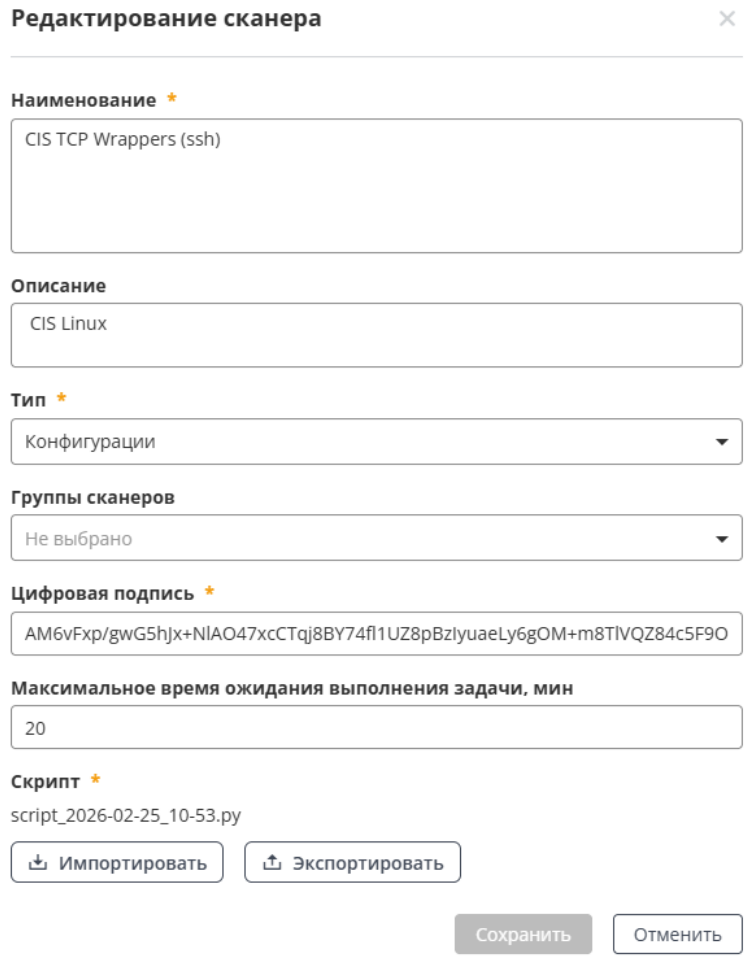
Создание и редактирование сканеров

Для создания одиночного скрипта нужно:

Перейти на страницу Администрирование\Сканеры, нажать кнопку «Создать сканер» и заполнить WEB-форму.

Для редактирования – нажать кнопку редактирования сканеры и внести изменения в форме.

Производитель DATAPK поставляет уже подписанные сканеры в json, их надо импортировать через страницу «Импорт и экспорт»



CyberLympha®

Основные блоки сканеров

Каждый сканер в DATAPK можно разделить на 3 логических этапа:

- **Формирование запроса к объекту защиты (по указанному протоколу)**
- **Обработка полученных данных (с использованием регулярных выражений)**
- **Формирование ответа в специальном виде**

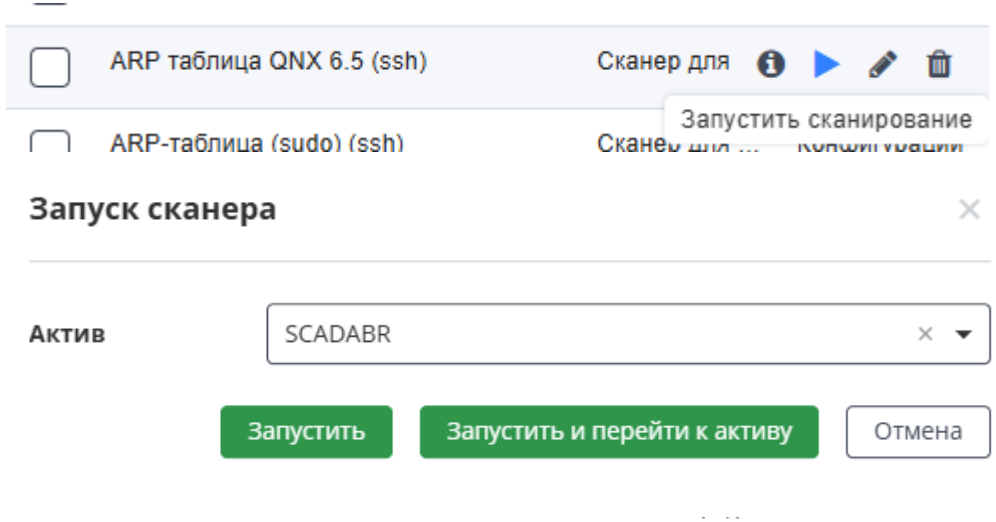
CyberLympha®

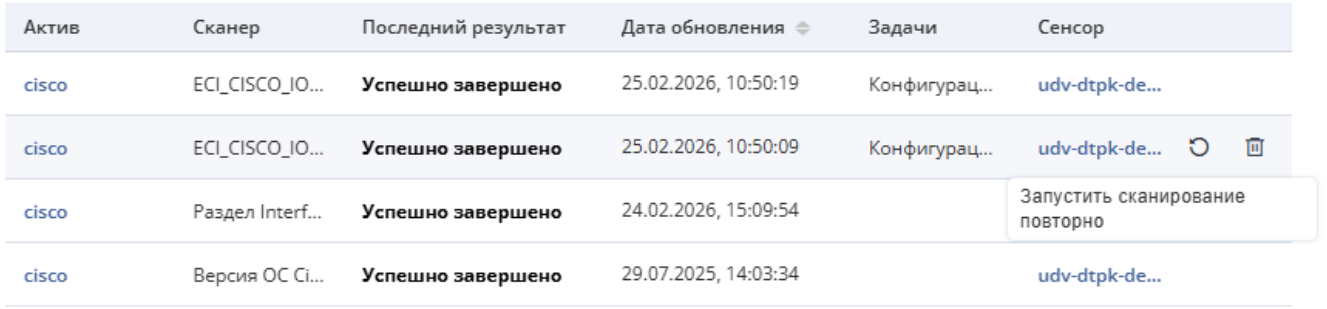
Пример результата сбора

№	Параметр	Значение
9	Наименование ПЛК	SIMATIC 300(1)
10	Наименование модуля	CPU 317-2 PN/DP
11	Состояние ПЛК	S7CpuStatusRun
12	Количество программных блоков	129
13	Позиция селектора	В состоянии: RUN
14	Параметры уровня защиты	Пароль Селектора
15	Уровень защиты ЦПУ	Предоставлен доступ
16	Переключатель запуска	Неизвестно или недоступно
17	Уровень защиты селектора	Доступно только чтение

Запуск сканера

Для разового выполнения со страницы сканеров можно нажать на кнопку Play рядом с соответствующем сканером и выбрать в диалоговом окне DATAPK и объект защиты, где запустить данный сканер сбора данных.





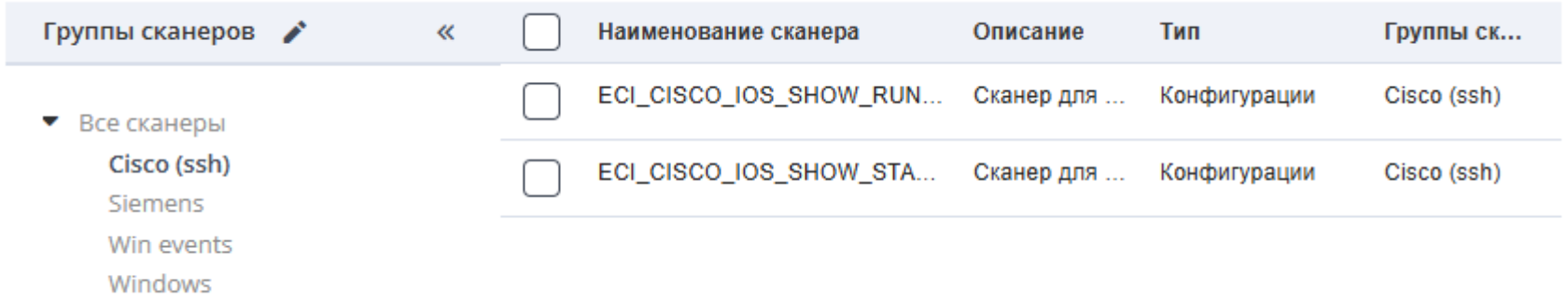
Так же можно повторно запускать сканер со страницы «Статус сбора»

Создание и редактирование групп сканеров

Для создания группы нужно на странице «Администрирование\Сканеры» создать группу. Далее поместить нужные сканеры в эту группу

Группы м.б. вложенные. В этом случае родительская группа выполняет все подчиненные сканеры (на практике используется редко)

- *В одну группу не рекомендуется добавлять более 10 сканеров*
- *Все сканеры в группе должны выполняться на одном типе ОЗ – новые Windows либо Linux/ПЛК Siemens/… (в идеале использовать один и тот же протокол сбора данных)*



Настройка задач сбора данных

Задача сбора – это группа сканеров, которая выполняется на группе активов в заданное время.

Есть разовые, есть периодические задачи.

Назначать можно точечно на активы, можно на группу

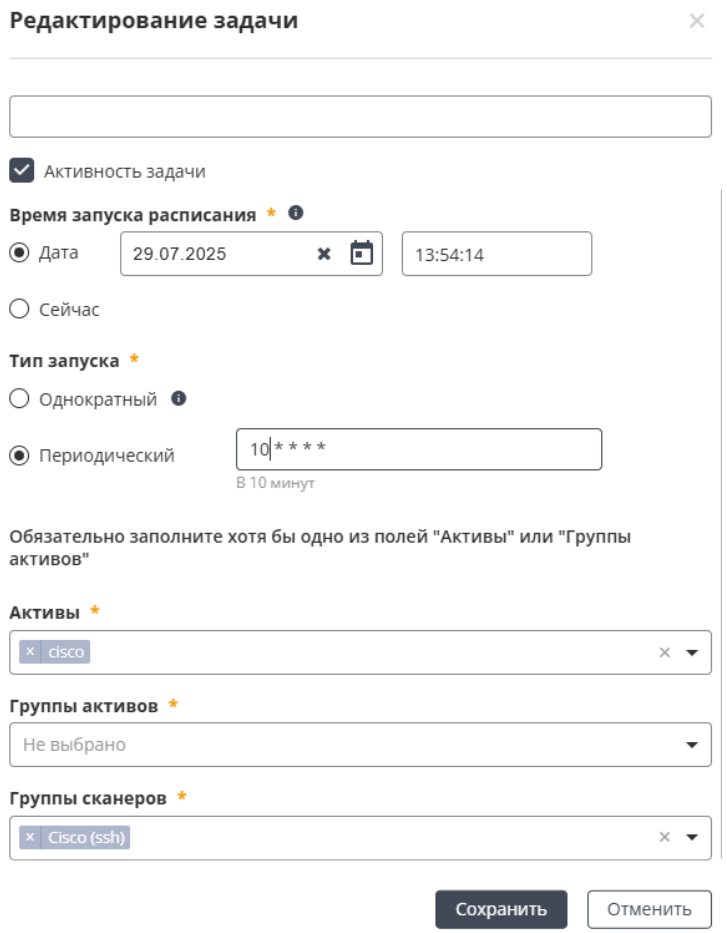
Расписание для периодических задач задается через cron (с точностью до минут, секунды не поддерживаются). Чаще, чем раз в 4 часа, опрашивать конфигурации не имеет смысла (только в демонстрационных целях можно делать более частый опрос)

Рекомендуется задачи сбора разносить по времени (в 1 момент времени выполняется 1 задача сбора):

0 */4 * * * – каждые 4 часа (часы кратны 4 – 0, 4, 8, …) в 0 минут сбор конфигураций с коммутаторов

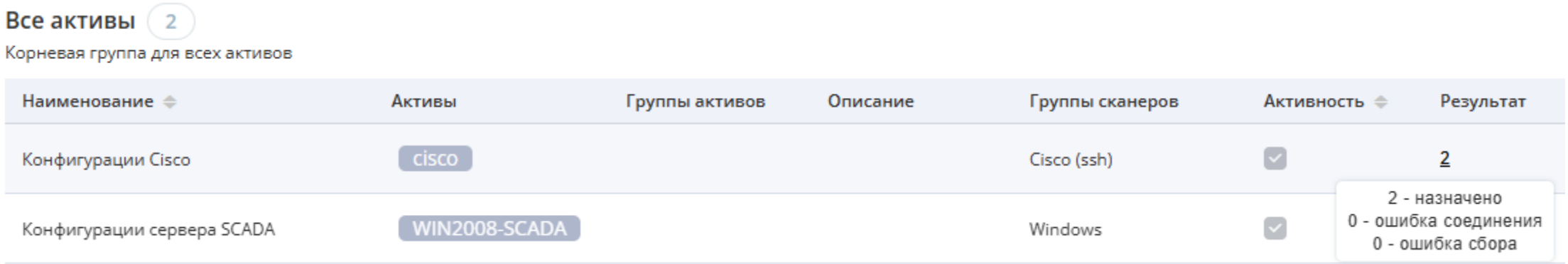
20 */4 * * * – каждые 4 часа в 20 минут сбор конфигураций с Windows

30 1/4 * * * – каждые 4 часа, начиная с 1 (1, 5, 9, 13, …) в 30 минут сбор с Linux

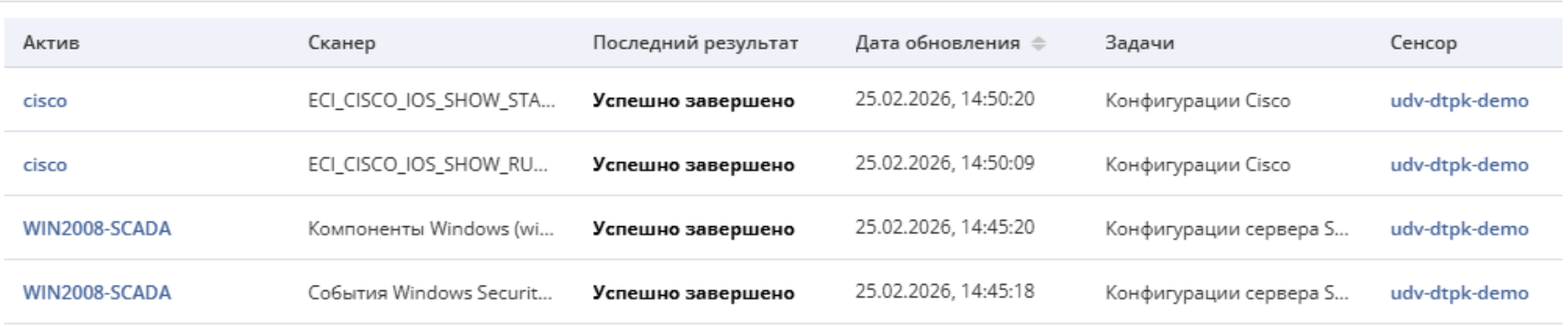


Просмотр результатов сбора данных

Результаты сбора данных отображаются на странице «Задачи сбора»



Результаты по выполнению сканеров (как запущенных отдельно, так и в составе задач) – на странице «Статус сбора»



CyberLympha®

Просмотр результатов сбора данных

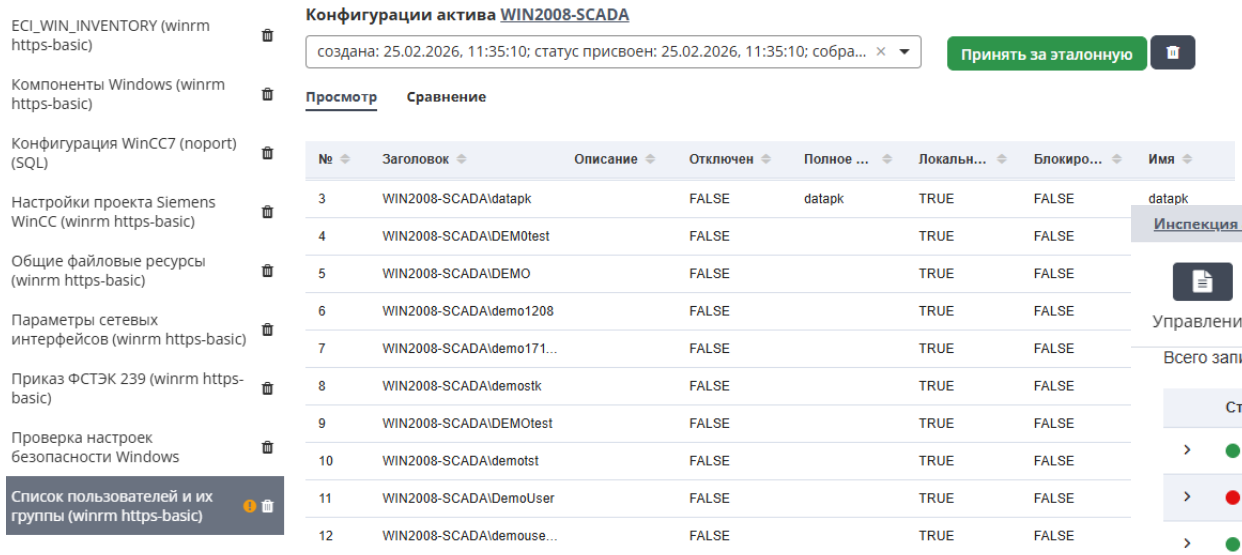
На что реагировать: есть ошибки сбора – в идеале их быть не должно

Ошибки могут свидетельствовать:

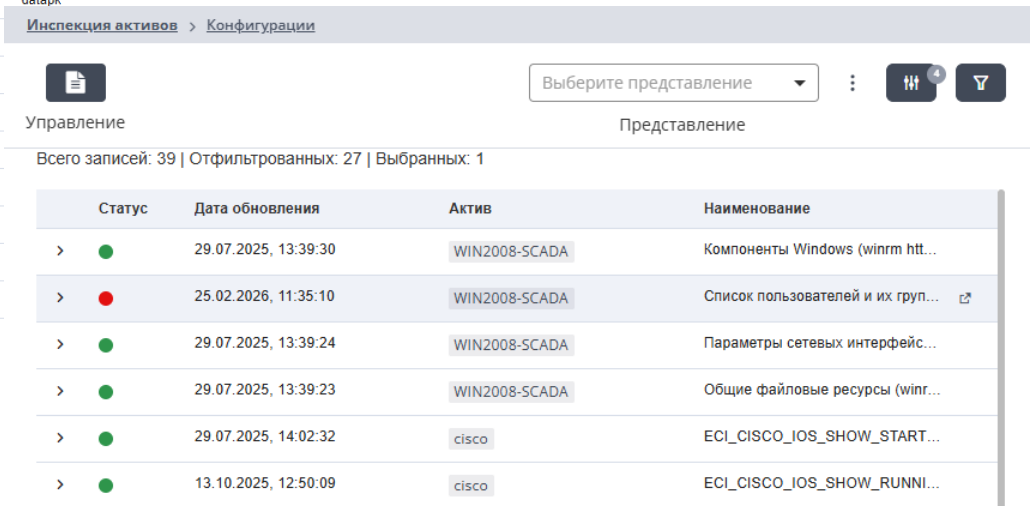
- об отсутствии доступа к узлу/некорректных учетных записях;
- о внесении изменений в узел, что с него перестали собираться конфигурации;
- о некорректных настроек задач/групп сканеров (пытаемся собрать не теми сканерами не по тому протоколу), пытаемся собирать слишком часто (сканер выполняется 5 минут, а мы пытаемся собрать раз в 4 минуты и пр.), не разносим задачи по времени
- о необходимости внести изменения в сканер сбора данных (выполняем не ту команду, не так обрабатываем вывод и пр.)

Просмотр конфигурации

Для просмотра конфигурации необходимо из карточки нужного актива перейти в блок «Конфигурации». После этого откроется страница «Конфигурации актива» с собранными конфигурациями.



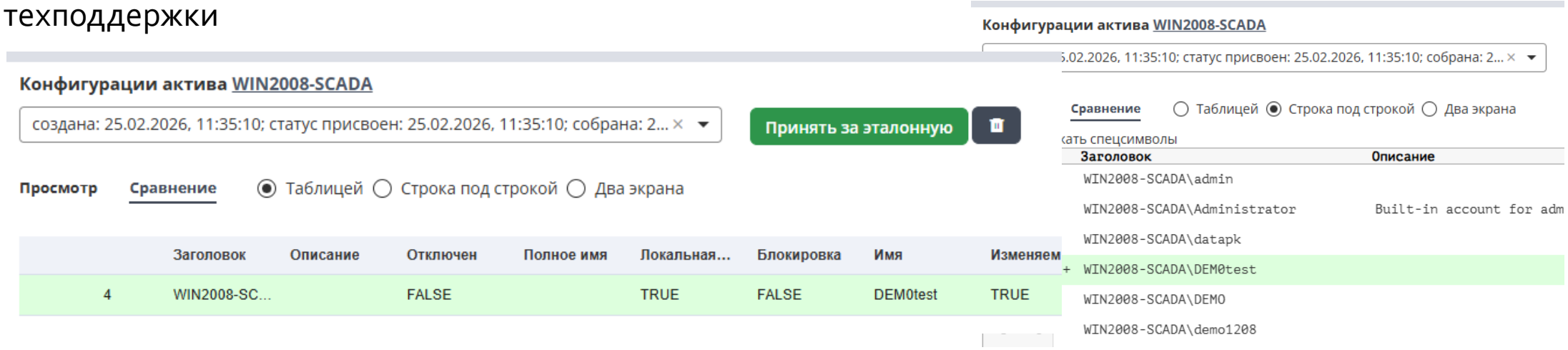
К конфигурациям активов можно также перейти через блок «Инспекция активов», страница «Конфигурации».



Конфигурации. Сравнение с эталоном

На что реагировать: есть отклонения от эталона. Необходимо проанализировать отклонения и принять новую конфигурацию за эталон (если изменения легитимны) или разобраться в причинах изменения/вернуть конфигурацию на активе в требуемый вид/отключить сбор конфигурации.

Не всегда изменение конфигурации – реальный инцидент – иногда отклонения вызваны некорректным выборам сканера сбора (собираем то, что вполне легитимно меняется), в этом случае нужно исключить сбор данных параметров или внести изменения в сканер (исключить меняющуся неинформативные строки). Помощь в корректировке сканеров оказывается производителем DATAPK в рамках техподдержки



CyberLympha®

Ошибки при сборе данных

- **Ошибка выполнения команды (No route to host)** - нет доступа (либо в принципе данный механизм сбора не применим к активу)
- **Учетные данные для пользователя не найдены** - УЗ не привязана к активу/ УЗ не с тем тегом
- **Ошибка выполнения команды», «the specified credentials were rejected by the server»** – неверные учетные данные или не хватает прав на активе
- **Ошибка выполнения команды. Соединение неожиданно закрылось** – любая ошибка для протокола WinEXE (неверные УЗ, нехватка прав на активе и пр.)
- **Превышено время ожидания выполнения задачи сбора событий» или «Превышено время ожидания выполнения задачи сбора данных / Превышено время ожидания, ошибка выполнения сканера, не удалось получить ожидаемое сообщение** – сканер сбора не успел выполниться за таймаут – проверить доступы, если ок – увеличить таймаут или переписать сканер (иногда из-за ошибок в регулярных выражениях возникает)
- **Ошибка выполнения команды rpc_s_access_denied** – некорректные учетные данные или недостаточно прав для WMI/MS-EVEN запроса

Вопросы?

udv|group