Система анализа и мониторинга состояния ИБ DATAPK

Тема 7. Экспорт данных и работа с резервной копией. Отчеты.

udv|group

Резервное копирование

В DATAPK есть собственные механизмы резервного копирования

Уровень Management может скопировать (сервис **backup_manager**):

- информация об активах, конфигурации, правила сессий, внутренние события
- пользовательские конфигурационные файлы (manager.env и пр.);
- справочники (сканеры сбора, базы уязвимостей, задачи сбора);
- репозитории ПЛК (если есть модуль Version Control);
- опционально – сетевые соединения (флаг --include-nta)

Не копируются:

- внешние события (модуль EEM) – есть отдельный механизм архивации/восстановления индексов событий
- настройки узловой ОС (сетевые интерфейсы, пользователи ОС, настройки аудита ОС и пр.)

Запуск backup_manager – из консоли ОС. При запуске сервиса указывается пароль на РК (и для восстановления необходим этот пароль)

Не рекомендуется использовать спецсимволы в паролях к РК (особенно одиночные кавычки) – могут возникнуть проблемы с экранированием

Параметр machine-id – это уникальный идентификатор машины, который генерируется при установке ОС. Уникальность DATAPK определяется по этому идентификатору, поэтому его дублирование в инсталляции не допустимо (поэтому нельзя клонировать ВМ – в случае клонирования обязательно перегенерировать machine-id до запуска DATAPK)

Резервное копирование

Комплексы уровня Sensor не хранят данные, поэтому их резервное копирование заключается только в ручном сохранении следующих локальных файлов сенсора:

- **/etc/machine-id** – идентификатор текущего сенсора;
- **/usr/share/udv/datapk/sensor.env** – конфигурационный файл сенсора.
- **/usr/share/udv/zeek-wrapper/configs/general.dat** и **/usr/share/udv/zeek-wrapper/configs/ics-function.dat** – конфигурационные файлы модуля «Анализ промышленного сетевого трафика» (если он установлен на сенсоре).

Параметр machine-id – это уникальный идентификатор машины, который генерируется при установке ОС. Уникальность DATAPK определяется по этому идентификатору, поэтому его дублирование в инсталляции не допустимо (поэтому нельзя клонировать ВМ – в случае клонирования обязательно перегенерировать machine-id до запуска DATAPK)

Восстановление

- установить и настроить ОС (сетевые интерфейсы и пр.)
- если уровень Sensor:
  - поменять machine-id (заменить файл **/etc/machine-id** на файл из РК и сохранить файл machine-id в директории **/var/lib/dbus**)
  - установить пустой DATAPK Sensor (нужные модули)
  - поменять конфигурационные файлы (**sensor.env**, и **2 файла zeek** при наличии модуля iNTA), перезапустить машину
- если уровень Management:
  - положить архив с РК в **/var/backups** (если снималась копия сетевых соединений, то оба архива)
  - **/usr/bin/stop_services.sh** (останавливает все сервисы, кроме udv-postgresql)
  - если снималась копия сетевых соединений, то дополнительно выполнить запуск clickhouse (**systemctl restart udv-clickhouse-service)**
  - запустить команду восстановления с указанием названий файлов РК и пароля к бекапу (на этом этапе на машине подменится machine-id на тот, который в РК)
  - перезагрузить машину, опционально восстановить индексы внешних событий (если есть EEM/старые индексы)

Импорт и экспорт

Пользовательские справочники загружаются через страницу **Администрирование\Импорт и экспорт**

При импорте в режиме диалога предлагается выбрать:

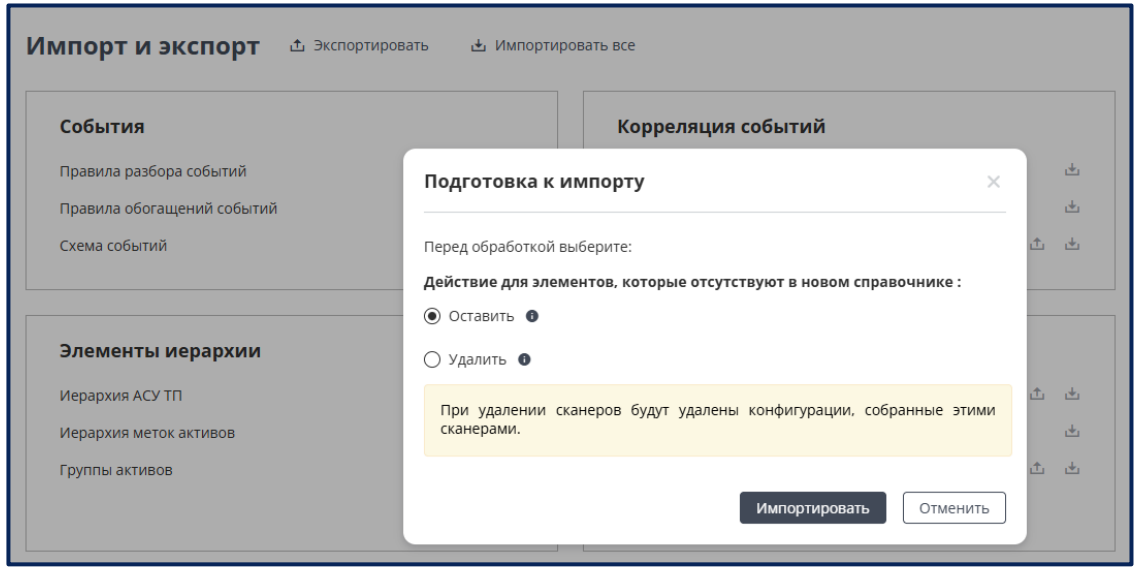
Оставить – новые данные добавляются; старые данные, которых нет в новом справочнике, остаются (типовой вариант)

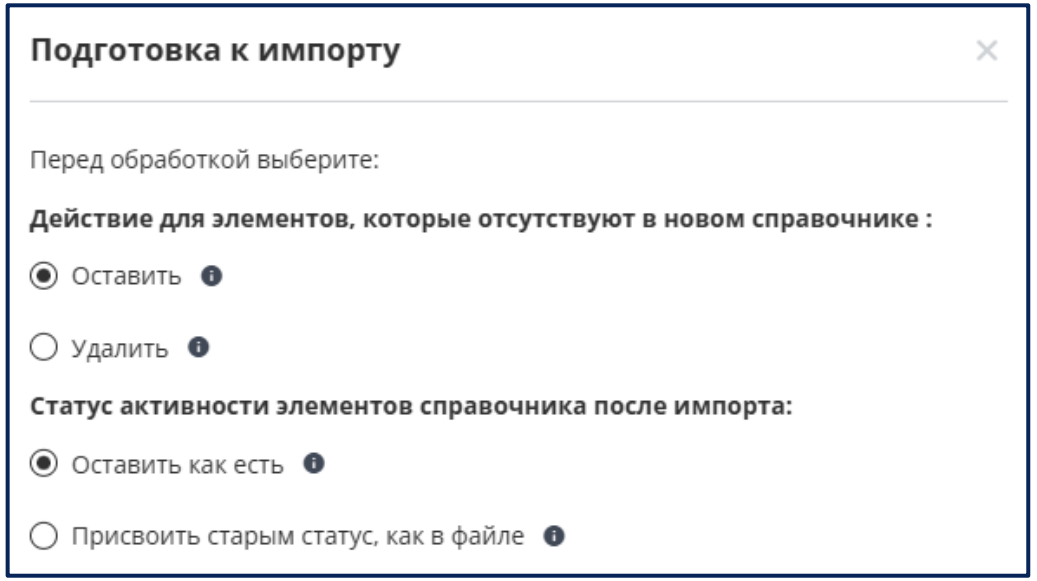
Удалить – новые данные добавляются, старые данные, которых нет в новом справочнике, удаляются (редко используемый вариант, но иногда полезен, если сформирован эталонный справочник, и хочется удалить все лишнее)

Дополнительно при импорте правил IDS (iNTA) и корреляции (EEM):

Оставить, как есть – при импорте не перетирается статус активности таких правил, но сами правила обновляются (основной сценарий – удобно, т.к. пользователь может сам включать/отключать правила)

Присвоить старым статус, как в файле – при импорте перетирается статус правил (берется из импортируемого файла) – более редкий кейс, используется нечасто





Отчеты

Так же можно создавать отчеты по выбранным активам, инцидентам в xlsx или html

Можно выбирать требуемые столбцы

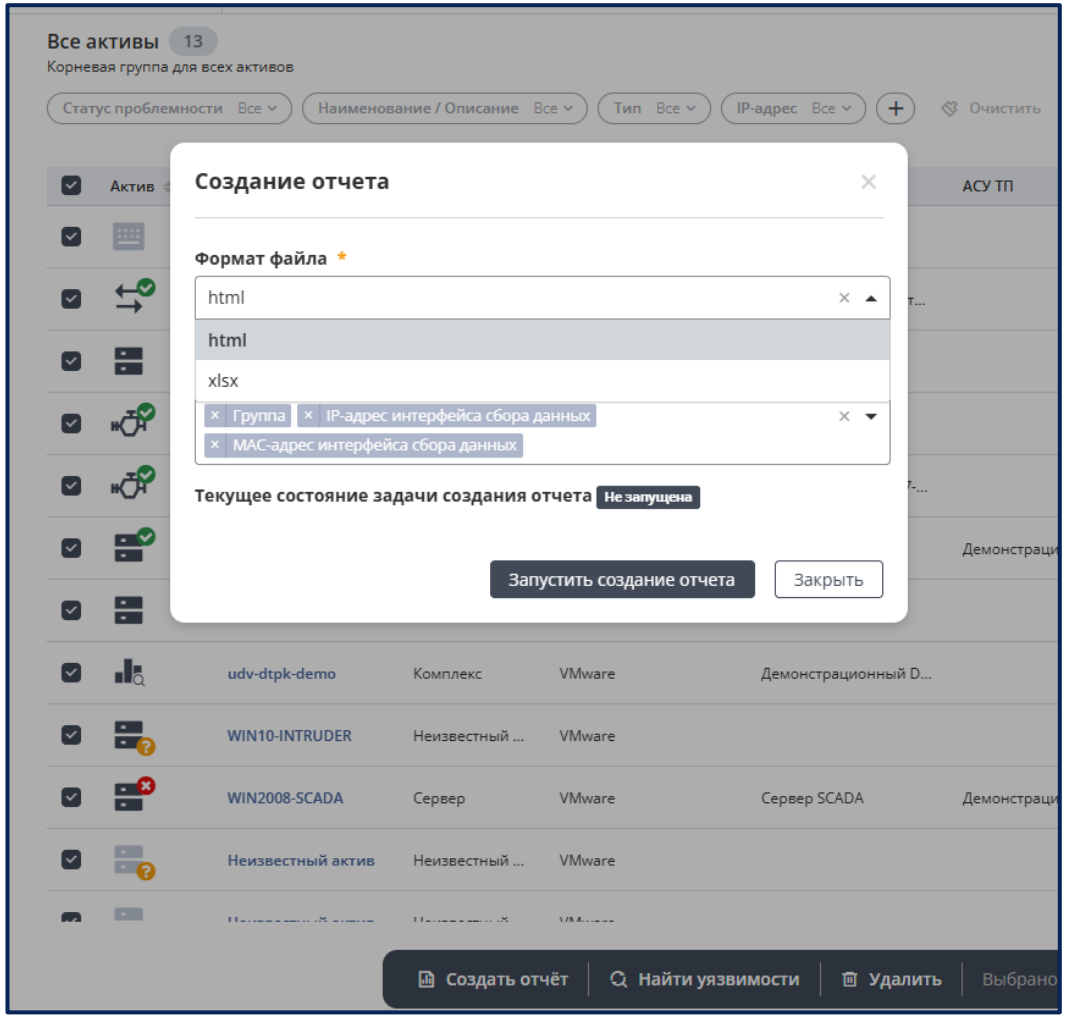
Отчет Активы

Создал: Иванов Иван None (datapktst)

Фильтры: Активы: Broadcast&Gateway, cisco, Historian, OPENPLC, S7-300, SCADABR, supervision-demo, u

Выгружено: 27.02.2026, 18:57:28

Наименование	Тип	Производитель	Описание
Broadcast&Gateway	Периферийное оборудование	VMware	
cisco	Коммутатор	VMware	Виртуальный коммутатор Cisco
Historian	Сервер	VMware	Сервер архивов
OPENPLC	ПЛК	VMware	OPENPLC
S7-300	ПЛК	VMware	Эмулятор Siemens S7-300
SCADABR	Сервер	VMware	Сервер SCADABR



Так же у продукта есть REST-API, можно забирать данные и обрабатывать внешними системами (в рамках курса не рассматривается)

Вопросы?

udv|group