ГАЗИНФОРМ СЕРВИС

Программный комплекс по защите системно-технической инфраструктуры «Efros Defence Operations»

Инструкция по экспорту данных из ПК «Efros CI» для ПК «Efros DO»

Санкт-Петербург, 2024

Аннотация

Данный документ представляет собой инструкцию по экспорту данных из программного комплекса управления конфигурациями и анализа защищенности «Efros Config Inspector» v.4 (ПК «Efros CI») для последующего импорта скачанных данных в программный комплекс по защите системно-технической инфраструктуры «Efros Defence Operations» (ПК «Efros DO»).

Документ содержит алгоритм выполнения экспорта, описание работы используемой утилиты и возможных ошибок при запуске утилиты.

Содержание

1 Алгоритм выполнения импорта

Импорт выполняется со всех поддерживаемых ПК «Efros CI» операционных систем (ОС) – Astra Linux, РЕДОС, Windows, а также со всех поддерживаемых систем управления базами данных (СУБД) – PostgreSQL\Jatoba, MySQL, MS SQL.

Перед выполнением импорта, в ПК «Efros DO» должна быть активирована лицензия на модули NA, FA, ICC, VC, сопоставимая по количеству объектов защиты используемому в ПК «Efros CI».

Алгоритм выполнения импорта включает следующие этапы:

1) Перед импортом необходимо выполнить обновление версии ПК «Efros CI» до актуальной версии, а также версий установленных в комплекс модулей поддержки устройств. Обновление выполняется в соответствии с разделом 3 «Обновление компонентов комплекса» документа «Программный комплекс управления конфигурациями и анализа защищенности «Efros Config Inspector. Руководство администратора».
2) После успешного обновления ПК «Efros CI» необходимо воспользоваться специальной утилитой *MakeEdoImportFile* для подготовки файла базы данных (БД) в формате SQLite, который в будущем будет импортирован в ПК «Efros DO».
3) Утилита запускается в командной строке из рабочей директории утилиты (установка утилиты не требуется, распаковывается из архива в любую директорию). Команда:

   cd /<директория утилиты>

   MakeEdoImportFile --features_folder="S:\tmp\tmp_modules" --output_file="S:\tmp\efrosci_edo.db" --db_type=DBTYPE --db_login=root --db_password=root --db_host=127.0.0.1 --db_schema=efrosci_4 --db_key_file_path="S:\tmp\tmp_modules\key.ecikey" --db_key_password=Gazprom09

Подробное описание утилиты приведено в разделе 2 «Описание работы утилиты *MakeEdoImportFile*».

4) Скопировать любыми доступными средствами файл БД, полученный в результате работы утилиты *MakeEdoImportFile*, на сервер ПК «Efros DO» в директорию «/opt/efros-do/backup».
5) На сервере ПК «Efros DO» запустить скрипт *edoctl* с аргументом «*--import*», который выполнит загрузку данных из файла БД в комплекс. Команда:

   sudo /opt/efros-do/edoctl --import

Подробное описание приведено в разделе 3 «Описание импорта данных в ПК «Efros DO».

2 Описание работы утилиты MakeEdoImportFile

Утилита *MakeEdoImportFile* выполняет проверку типа используемой ОС в БД сервера ПК «Efros CI» и производит обновление до ОС Astra Linux, а также замену модулей под целевую ОС.

Данные для работы утилиты:

- путь до формируемого выходного файла БД;
- параметры для подключения к БД;
- путь к папке с zip-архивами модулей для работы с ОС Astra Linux SE (v.1.6, v.1.7);
- параметр с числом дней для переноса записей событий.

2.1 Алгоритм действий утилиты

Алгоритм выполнения импортам включает следующие этапы:

1) Осуществляется подключение к БД и выполняются проверки:
   а) отключены ли модули «Отправка почты» и «Экспорт событий»;

   > В ПК «Efros DO» данные модули не поддерживаются. Имеются собственные инструменты, эквивалентные возможностям данных модулей.

   б) изначальный тип ОС в БД. Если тип ОС не Astra Linux, то:
   - проверяется, что все установленные модули присутствуют в папке с zip-архивами, подаваемой на вход;
   - заменяются модули под ОС Astra Linux из папки с zip-архивами:

     > Если модуль не найден в папке и модуль загружен, но не включен, то файлы модуля удаляются из БД. Если модуль не найден в папке, модуль загружен и включен – выполнение прерывается с ошибкой, что модуль не найден.

   - проводится обновление типа ОС в БД на целевую ОС.
2) Выполняется перенос данных из БД в формируемый выходной файл формата SQLite «*.db».
3) Выполняется тестовый запуск ядра, чтобы проверить возможность запуска с новыми данными.

2.2 Аргументы утилиты

Перечень аргументов утилиты *MakeEdoImportFile* приведен в таблице 1.

Таблица 1 – Перечень аргументов утилиты *MakeEdoImportFile*

Аргумент	Описание
features_folder	Путь к папке с zip-архивами модулей под ОС Astra Linux
output_file	Путь к выходному файлу (опционально). По умолчанию файл БД будет создан в рабочей директории утилиты с именем «efrosci_edo.db»
transfer_events_period_days	Количество дней, за которые будет выполнен перенос записей событий (по умолчанию 30, 0 – перенос всех событий) (опционально)
db_host	Адрес сервера БД
db_type	Тип БД (MYSQL, MSSQL, POSTGRESQL)
db_schema	Имя БД
db_login	Логин для подключения к БД
db_password	Пароль для подключения к БД
db_key_file_path	Путь к файлу с ключом (опционально)
db_key_password	Пароль ключа (опционально)

2.3 Пример запуска утилиты

Примеры запуска утилиты *MakeEdoImportFile*:

1) Со всеми аргументами:

   MakeEdoImportFile --features_folder=" C:\soft\EDO_migration\Modules" --output_file=" C:\soft\EDO_migration\eci_migration.db" --db_type=MYSQL --db_login=**** --db_password********* --db_host=10.72.11.105 --db_schema=efrosci_4 --db_key_file_path=" C:\soft\EDO_migration \key.ecikey" --db_key_password******* --transfer_events_period_days=0

При указании аргумента *transfer_events_period_days* равным «0», процесс подготовки файла БД и импорта данных из него в ПК «Efros DO» может занимать длительное время, а также значительно увеличит размер самого файла БД.

2) С минимальным набором аргументов (рисунок 1):

   MakeEdoImportFile --features_folder="C:\soft\EDO_migration\Modules" --db_type=MSSQL --db_login=**** --db_password********--db_host=10.72.11.105 --

db_schema=efrosci_4

Если аргумент *output_file* не указан, то файл БД будет создан в рабочей директории утилиты с именем по умолчанию «efrosci_edo.db».

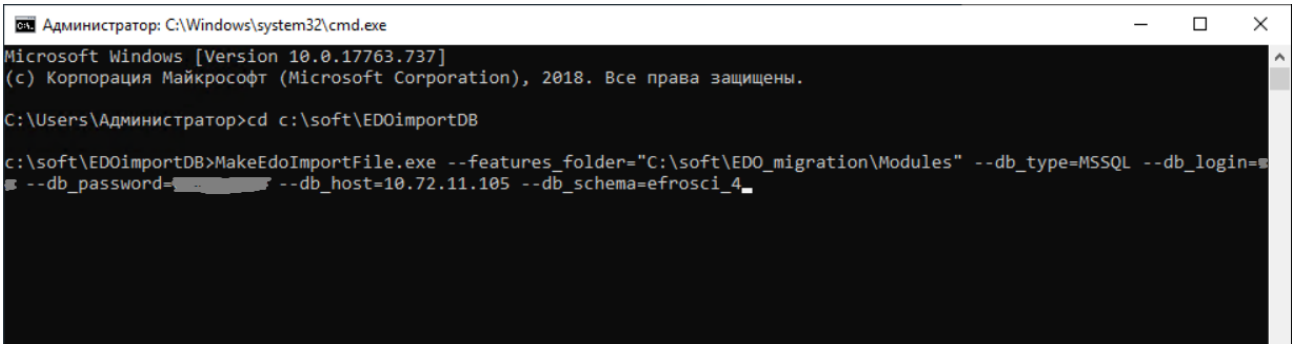

Рисунок 1 – Примеры запуска утилиты с минимальным набором аргументов

3 Возможные ошибки при выполнении

При выполнении утилиты *MakeEdoImportFile* могут возникнуть ошибки:

1) «Для продолжения требуется отключить встроенные модули» (рисунок 2).

Ошибка может быть вызвана тем, что в ПК «Efros CI» не отключены модули отправки писем и экспорта событий, работа которых не поддерживается в ПК «Efros DO».

Для устранения ошибки необходимо отключить указанные модули в подразделе ***Модули*** раздела **Настройки** клиентской консоли ПК «Efros CI» (рисунок 3).

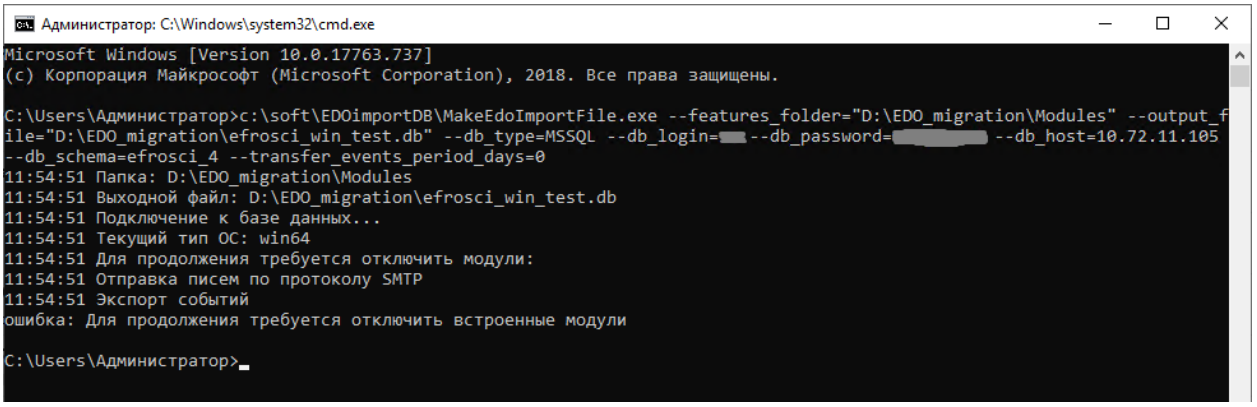

Рисунок 2 – Ошибка «Для продолжения требуется отключить встроенные модули»

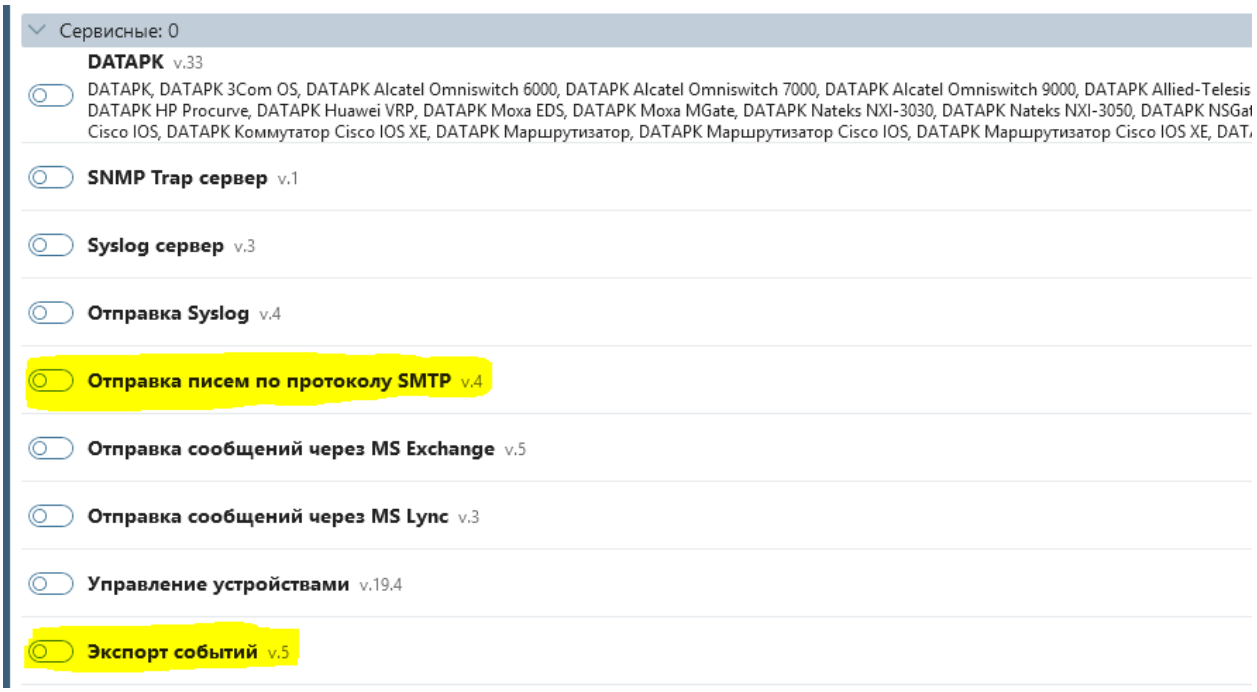

Рисунок 3 – Отключение модулей

2) «Не все установленные модули найдены в папке» (рисунок 4).

Ошибка может быть вызвана тем, что в папке с модулями найдены не все установленные модули. Возможно, требуется предварительно обновить используемые версии модулей либо модуль может не поддерживаться в сборке ПК «Efros DO».

Для устранения ошибки необходимо добавить zip-архив модуля в папку, либо отключить данный модуль в подразделе ***Модули*** раздела **Настройки** клиентской консоли ПК «Efros CI», если он не требуется (не используется).

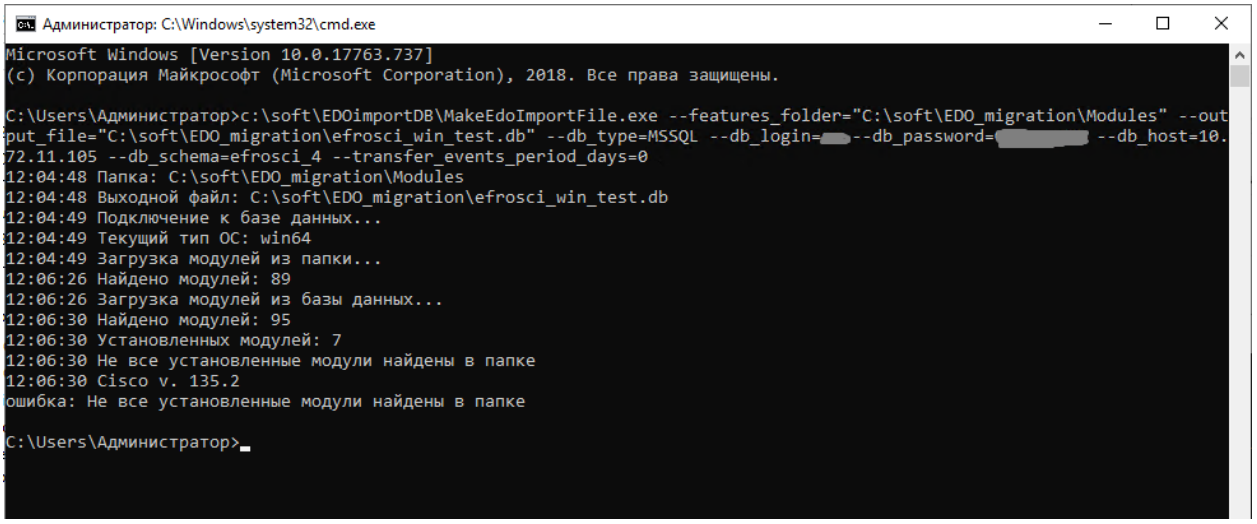

Рисунок 4 – Ошибка «Не все установленные модули найдены в папке»

Перечень сокращений

БД	–	База данных
ОС	–	Операционная система
ПК	–	Программный комплекс
СУБД	–	Система управления базами данных