

ПРОГРАММНЫЙ КОМПЛЕКС УПРАВЛЕНИЯ КОНФИГУРАЦИЯМИ И АНАЛИЗА ЗАЩИЩЕННОСТИ

«Efros Config Inspector» v.4

СОДЕРЖАНИЕ

1. Краткое описание программного комплекса 1
2. Дистрибутив 3
3. Установка 3
4. Запуск и проверка работы с «Альт Сервер 10» и «Альт Рабочая станция 10»..... 4

1. Краткое описание программного комплекса

ПК «Efros CI» предназначен для активного контроля сетевого оборудования, серверных и клиентских операционных систем (ОС), систем управления базами данных (СУБД), автоматизированных систем управления технологическим процессом (АСУ ТП), виртуальных сред, а также анализа правил межсетевых экранов.

Проект выполняется как клиент-серверное решение (рис.1).

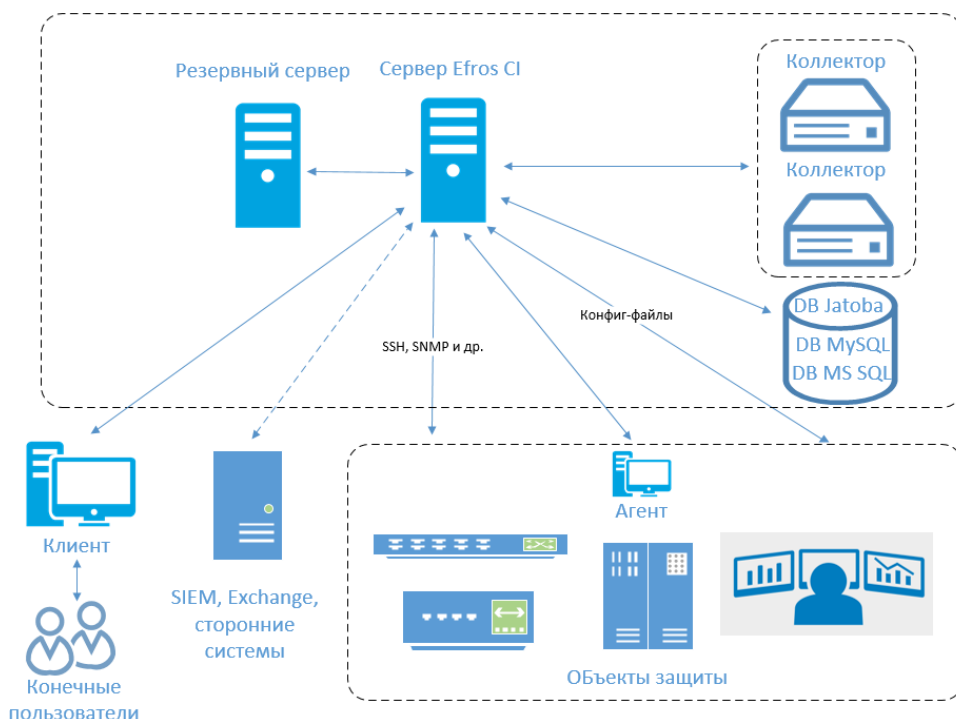


Рисунок 1 – Общая архитектура комплекса на физическом уровне

ПК «Efros CI» состоит из:

- серверной части – устанавливается на выделенном компьютере (далее – сервер), функционирующем под управлением ОС:
 - Astra Linux Special Edition (Smolensk) v. 1.6;
 - РЕД ОС v.7.2 (Муром);
 - серии Windows (64-разрядные):
- клиентской консоли – устанавливается на сервере ПК «Efros CI» либо на автоматизированных рабочих местах (АРМ), функционирующих под управлением ОС серии Windows, и подключается к серверной части посредством вычислительной сети; с помощью клиентской консоли осуществляется доступ к функциям конфигурирования сервера ПК «Efros CI» и к возможностям контроля его функционирования в различных режимах;
- Windows-агента – устанавливается на контролируемом объекте защиты под управлением ОС Windows и подключается к серверной части посредством вычислительной сети;
- внешних модулей – устанавливаются вместе с серверной частью на сервере программного комплекса. Функциональность, специфическая для каждого конкретного типа устройств, сосредоточена во внешних модулях. Каждый модуль представляет собой один или несколько исполняемых файлов и набор конфигурационных файлов. Внешние модули соединяют сервер с устройствами по различным коммуникационным протоколам;
- коллектора задач – устанавливаются на других электронных вычислительных машинах, функционирующих под управлением ОС Windows, и осуществляют подключение по вычислительной сети к серверной части для оптимизации рабочей нагрузки на программный комплекс.

ПК «Efros CI» хранит параметры своих настроек, информацию об учетных записях, перечни объектов защиты, файлы конфигураций объектов защиты, отчеты и прочие данные для функционирования во внешней базе данных (БД), находящейся под управлением СУБД, которая не входит в состав программного комплекса и поставляется отдельно.

Клиентская консоль может быть установлена на ЭВМ под управлением ОС серии Windows x64 и ОС серии Windows x86

Windows-агент ПК «Efros Config Inspector» v.4 функционирует под управлением 64-разрядных ОС серии Windows (аналогично серверной части).

Серверная часть ПК «Efros CI» обеспечивает выполнение функций по аудиту сетевого оборудования, серверных и клиентских ОС, СУБД, АСУ ТП, виртуальных сред, по анализу межсетевых экранов и по настройке комплекса.

Серверная часть запускается в виде службы «Config Inspector» совместно с внешними модулями. Служба обеспечивает удаленным клиентам доступ к функциям комплекса. Для передачи запросов используется HTTPS протокол. Для настройки службы используется программа настройки, позволяющая задать параметры настроек:

- 1) подключения к СУБД;
- 2) ведения электронных журналов (логов);
- 3) TCP-порта управления сервера ПК «Efros CI»;

- 4) запуска Java;
- 5) языка графического интерфейса сервера.

Служба содержит в себе ядро, которое выполняет основные функции комплекса:

- аудит сетевого оборудования, серверных и клиентских ОС, СУБД, АСУ ТП, виртуальных сред, анализ межсетевых экранов;
- управление конфигурациями активного сетевого оборудования (АСО);
- регистрация событий безопасности;
- формирование уведомлений о событиях контроля и ошибках выполнения заданий устройств в графическом и текстовом виде;
- функций по настройке комплекса, проверке/созданию БД на сервере БД, подключение к сетевому и серверному оборудованию, агентам.

Внешние модули устройств выполняют поддержку контролируемых устройств и оборудования.

Управление и контроль за результатами работы программного комплекса осуществляется из клиентской консоли. Клиентская консоль подключается к серверной части и предоставляет графический интерфейс для выполнения функций комплекса, реализуемых ядром.

Коллектор задач (далее по тексту – коллектор) ПК «Efros CI» подключается к серверной части программного комплекса. При наличии большого количества задач серверной части (например, загрузка отчетов), часть задач передается на выполнение коллектору.

Данные ПК «Efros CI» (конфигурации объектов защиты, электронные журналы, настройки и состояние всех программных модулей ПК) хранятся во внешней системе управления базами данных (СУБД).

В качестве внешней СУБД поддерживаются:

- PostgreSQL: 11, 12, 13, 14;
- Microsoft SQL Server: 2017
- MySQL: 8.0
- защищенная СУБД Jatoba v.1, v.2, v.3 (ООО «Газинформсервис»).

2. Дистрибутив

Для получения дистрибутива, необходимо обратиться в отдел продаж ООО «Газинформсервис» <https://www.gaz-is.ru/produkty/zashchita-it-infrastrukturi/efros-config-inspector.html#zakazat> или к вашему партнеру по интеграции.

3. Установка

Процесс установки описан в документе «Руководство администратора Efros CI 4». Документ доступен на сайте <https://www.gaz-is.ru/produkty/zashchita-it-infrastrukturi/efros-config-inspector.html>

4. Запуск и проверка работы с «Альт Сервер 10» и «Альт Рабочая станция 10»

4.1 Запуск консоли «Efros CI» и подключение к серверу «Efros CI».

Запуск клиентской консоли осуществляется из меню Пуск на панели задач. Для этого следует выбрать **Пуск** → **Все программы** → **Efros Config Inspector 4** → **Efros Config Inspector 4**. В поле **Сервер** – ввести IP-адрес сервера ПК или его DNS-имя. Если серверная и клиентская часть комплекса установлены на один компьютер, то в поле **Сервер** можно ввести *127.0.0.1* или *localhost*. В поля **Логин** и **Пароль** – ввести соответственно логин и пароль пользователя комплекса.

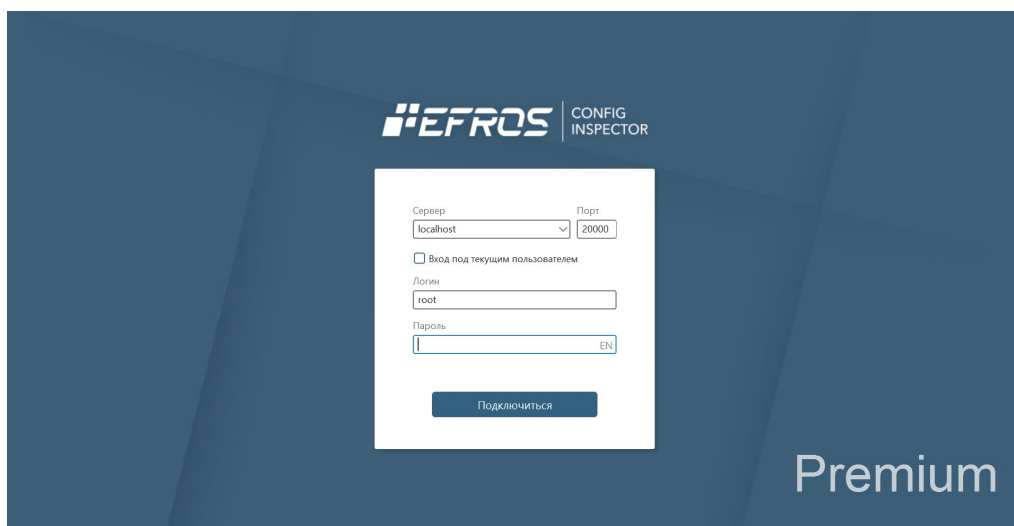


Рисунок 2 – Клиентская консоль, окно подключения

4.2 Загрузка и подключение модуля поддержки «Альт Сервер 10» и «Альт Рабочая станция 10».


Перейти в **Настройки**, затем на вкладку **Модули** и нажать кнопку **Загрузить** (↓). Откроется стандартное окно MS Windows «Открыть», в котором необходимо указать файл с модулем «Linux». После этого, в форме управления модулями комплекса (см. рис.3) выполните щелчок левой кнопкой «мыши» по переключателю , расположенному слева от имени модуля поддержки «Linux».



Рисунок 3 – Форма управления внешними модулями

4.3 Создание учетной записи в «Альт Сервер 10» и «Альт Рабочая станция 10»

Процесс создания учетной записи описан в документации к «Альт Сервер 10» и «Альт Рабочая станция 10»

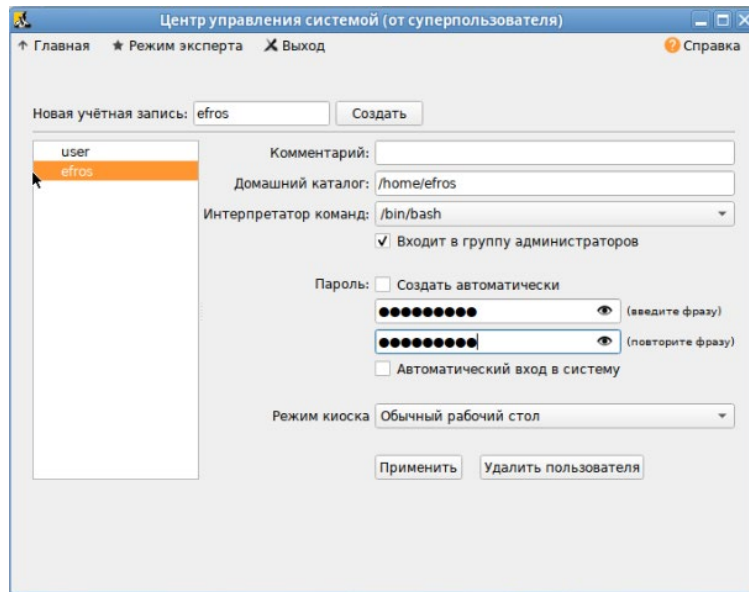


Рисунок 4 – Форма управления учетными записями в «Альт Сервер 10» и «Альт Рабочая станция 10»

4.4 Добавление устройства

При добавлении устройства, необходимо выбрать **тип «Linux»**. В **параметрах подключения** указать IP-адрес (DNS-имя) «Альт Сервер 10» или «Альт Рабочая станция 10». В разделе **Пользователь** указать имя учетной записи, созданной на предыдущем шаге. В способах аутентификации указать **по паролю** и пароль, заданный в пункте 4.3. В разделе порт SSH, указать порт на котором работает служба *sshd*. Нажать **Сохранить**. Процесс опроса «Альт Сервер 10» или «Альт Рабочая станция 10» и формирования отчётов запустится автоматически.

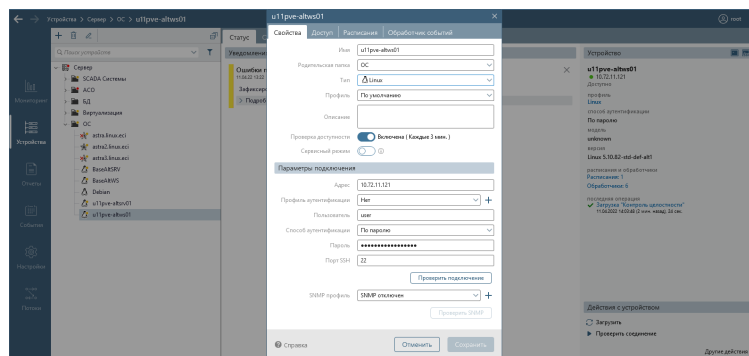


Рисунок 5 – Форма добавления устройства

4.5 Проверка загрузки отчетов

Убедиться, что все отчеты загружены успешно и их содержимое корректно.

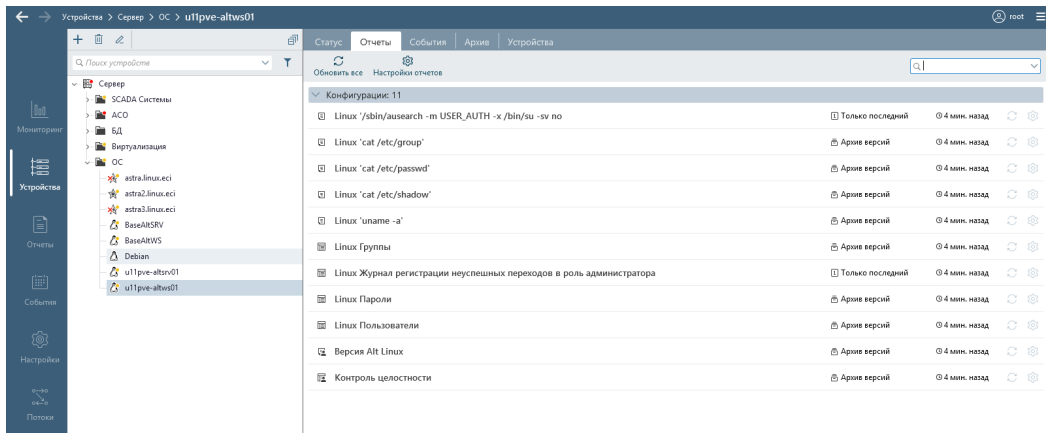


Рисунок 6 – Вкладка **Отчеты**

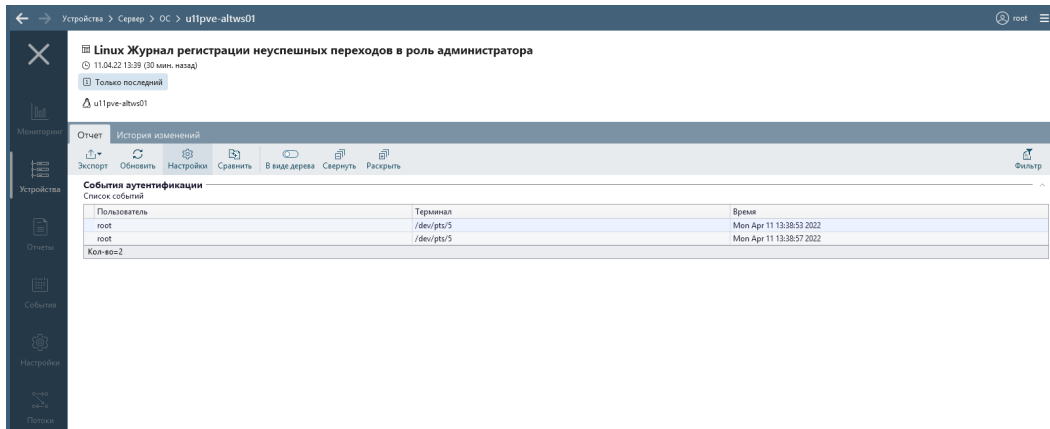


Рисунок 7 – Содержимое отчёта «Linux Журнал регистрации неуспешных переходов в роль администратора»

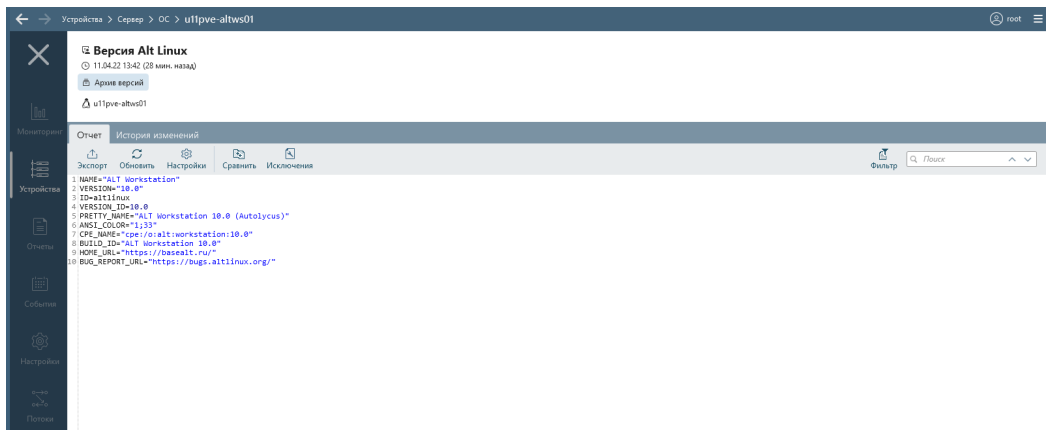


Рисунок 8 – Содержимое пользовательского отчёта «Версия Alt Linux»