GIS ГАЗИНФОРМ СЕРВИС

Программный комплекс управления конфигурациями и анализа защищенности «Efros Config Inspector» v.3

Описание применения

Санкт-Петербург 2020

Аннотация

В документе приведены сведения о программном комплексе управления конфигурациями и анализа защищенности «Efros Config Inspector» v.3 (далее по тексту – ПК «Efros Config Inspector» v.3 или комплекс).

Настоящий документ содержит описание назначения комплекса, описание функциональных возможностей, условий применения и решаемых комплексом задач, а также входные и выходные данные комплекса.

Содержание

1 Назначение ПК «Efros Config Inspector» v.3

Программный комплекс (ПК) управления конфигурациями и анализа защищенности «Efros Config Inspector» v.3 (далее, ПК «Efros Config Inspector» v.3 или ПК) предназначен для активного аудита сетевого оборудования, серверных и клиентских операционных систем (ОС), а также виртуальных сред. Активный аудит контролируемого оборудования осуществляется с использованием протоколов, указанных в таблице 1.

Таблица 1 – Протоколы, используемые на сервере ПК для аудита оборудования

Протокол	Где используется	Устройства/Функции	Поддерживаемые ОС
SSH	Модули взаимодействия с сетевыми устройствами	Сетевые устройства	Windows Server 2016 Astra Linux Special Edition v. 1.6, РЕД ОС v.7.2
Telnet	Модули взаимодействия с сетевыми устройствами		
LDAP	Модуль взаимодействия с Active Directory	Active Directory	Windows Server 2016
CPMI	Модуль взаимодействия с CheckPoint	CheckPoint SmartCenter	Windows Server 2016 Astra Linux Special Edition v. 1.6, РЕД ОС v.7.2
LEA			
REST (HTTP/HTTPS)	Модуль взаимодействия с устройствами Cisco ACS	Cisco ACS Cisco Firepower	Windows Server 2016 Astra Linux Special Edition v. 1.6, РЕД ОС v.7.2
Cisco Administrative XML (AXL)	Модуль взаимодействия с сетевыми устройствами Cisco UCM	Cisco UCM	Windows Server 2016 Astra Linux Special Edition v. 1.6, РЕД ОС v.7.2
XenAPI	Модуль взаимодействия с Citrix XenServer	Citrix XenServer	Windows Server 2016 Astra Linux Special Edition v. 1.6, РЕД ОС v.7.2
WMI	Модуль взаимодействия с Hyper-V	Загрузка настроек Hyper-V	Windows Server 2016
Powershell (WinRM)		Выполнение проверок соответствия Hyper-V	Windows Server 2016
SMB		Загрузка файлов ВМ Hyper-V	Windows Server 2016
Microsoft RTC API	Модуль отправки сообщений через MS Lync	Отправка сообщений в Lync	Windows Server 2016

Протокол	Где используется	Устройства/Функции	Поддерживаемые ОС
Microsoft Exchange Web Services Managed API	Модуль отправки сообщений через MS Exchange	Отправка писем Exchange	Windows Server 2016
SMTP	Модуль отправки писем по протоколу SMTP	Отправка писем SMTP	Windows Server 2016 Astra Linux Special Edition v. 1.6, РЕД ОС v.7.2
Syslog	Модуль отправки syslog-сообщений	Отправка Syslog-сообщений администраторам сети	Windows Server 2016 Astra Linux Special Edition v. 1.6, РЕД ОС v.7.2
	Модуль Syslog-сервер	Syslog-сервер приема сообщений	
SNMP	Сканер сети для последующего добавления найденных устройств в список устройств	Поиск устройств в сети (SNMP сканер)	Windows Server 2016 Astra Linux Special Edition v. 1.6, РЕД ОС v.7.2
VIX API (SOAP, HTTPS)	Модуль взаимодействия с vCenter	vCenter, загрузка настроек	Windows Server 2016
HTTPS		vCenter, загрузка файлов ВМ	Windows Server 2016
Проприетарный на базе HTTPS	Windows-агент	Сбор данных с ОС Windows от агента	Windows Server 2016 Astra Linux Special Edition v. 1.6, РЕД ОС v.7.2
		Прием сообщений от Windows-агента	Windows Server 2016 Astra Linux Special Edition v. 1.6, РЕД ОС v.7.2
	Сервер	Подключение консоли к серверу	Windows Server 2016 Astra Linux Special Edition v. 1.6, РЕД ОС v.7.2
		Взаимодействие между серверами в иерархии	Windows Server 2016 Astra Linux Special Edition v. 1.6, РЕД ОС v.7.2
	Коллекторы	Взаимодействие с коллекторами	Windows Server 2016

Список протоколов и модулей, с использованием которых на сервере ПК «Efros Config Inspector» v.3 может осуществляться активный аудит сетевого и серверного оборудования, может быть расширен за счет разработки и включения в программный комплекс соответствующих внешних модулей.

1.1 Структура ПК

ПК «Efros Config Inspector» v.3 построен на основе архитектуры «Клиент - Сервер» и состоит из:

– серверной части (далее – сервер) – устанавливается на выделенной ЭВМ под управлением ОС Windows, Astra Linux Special Edition (Smolensk) v. 1.6, РЕД ОС v.7.2;

– клиентской консоли – устанавливается на сервере под управлением ОС Windows, либо может быть установлена на других рабочих станциях под управлением ОС Windows и подключена к серверу по сети;

– windows-агента – устанавливается на контролируемом компьютере заказчика под управлением ОС Windows и подключен к серверу по сети;

– внешних модулей – устанавливаются вместе с серверной частью на сервере;

– коллектора задач (далее по тексту – коллектор) – устанавливается на других рабочих станциях и осуществляет подключение к серверной части программного комплекса.

Серверная часть обеспечивает выполнение основных функций ПК. Внешние модули и Windows-агент соединяют сервер ПК с устройствами по различным коммуникационным протоколам.

Клиентская консоль подключается к серверу по протоколу TLS и может работать одновременно на нескольких компьютерах. Управление контролируемыми устройствами, а также администрирование сервера ПК осуществляется из клиентской консоли.

Данные ПК «Efros Config Inspector» v.4 хранятся во внешней системе управления базами данных (СУБД). В качестве внешней СУБД поддерживаются: MySQL 5.5, PostgreSQL 9.4, Microsoft SQL Server 2012 (также поддерживаются новые версии данных СУБД) или защищенная СУБД «Jatoba» (ООО «Газинформсервис»). СУБД может быть установлена локально на сервере ПК либо на удаленном компьютере (далее – сервере БД) и подключена к серверу ПК по сети. Для обеспечения наилучшей производительности ПК рекомендуется использовать Microsoft SQL Server.

1.2 Функциональные возможности

Программный комплекс обеспечивает выполнение следующих функций:

- мониторинг уведомлений о событиях контроля и об ошибках выполнения заданий устройств в графическом и текстовом виде;
- ведение списка контролируемых на сервере ПК устройств и групп устройств;
- загрузка на сервер ПК текстовых конфигураций контролируемых устройств (текстовых файлов, выводов команд);
- контроль текущих статусов контролируемых устройств и групп устройств (просмотр уведомлений о событиях, зафиксированных для устройств и групп устройств, операциях, выполненных с устройствами и группами, и архива отчетов о событиях и операциях);

- загрузка и формирование отчетов по настройкам, локальным файлам и параметрам работы контролируемых устройств;
- выполнение действий с устройствами (загрузка отчетов, проверка соединения, конфигурирование и восстановление конфигураций контролируемых устройств) и группами устройств (обновление устройств, конфигурация устройств);
- ведение архива текстовых конфигураций и отчетов;
- контроль изменений текстовых конфигураций и отчетов;
- выполнение проверок соответствия конфигурации контролируемых устройств требованиям безопасности (compliance проверки);
- выполнение проверок наличия уязвимостей контролируемого оборудования;
- поиск устройств в сети (сканирование сети);
- сбор и обработка событий (сообщений) с контролируемых устройств;
- ведение журнала событий, включающий аудит действий пользователей комплекса, с возможностью настройки журнала (фильтрация, выборка, построение отчетов);
- выполнение проверок устройств и групп устройств по расписанию;
- возможность настройки реакции комплекса (выполнение проверок, отправка писем и сообщений) на события (как принятые с устройств, так и события системы);
- отправка писем, сообщений во внешние информационные системы;
- ведение списка пользователей комплекса с возможностью управления пользователями (добавление пользователей, групп пользователей, блокирование, активация, удаление учетной записи пользователя, смена пароля пользователя);
- идентификация и аутентификация пользователей комплекса на сервере ПК с использованием идентификатора и паролей. Применение защиты обратной связи «сервер ПК – пользователь» в процессе аутентификации;
- автоматическое блокирование идентификатора пользователя ПК после 45 дней его неиспользования;
- автоматическая проверка характеристик паролей при их создании, проверка сложности паролей, проверка паролей по истории паролей (запрет на использование пользователем любого из ранее использованных паролей при создании новых);
- ограничение времени действия паролей (максимальное и минимальное время);
- ролевое и дискреционное разграничение доступа пользователей комплекса к серверу ПК, к списку контролируемых на сервере ПК устройств, включая операции по чтению, записи (удалению) разрешённые к выполнению пользователям ПК при доступе к контролируемым устройствам и к операциям на подчиненных серверах;
- разделение полномочий (ролей) пользователей и администраторов комплекса, с предоставлением прав и привилегий по доступу к параметрам настройки исключительно администратору;
- настройки правил использования паролей и удаленной работы пользователей комплекса с сервером ПК;

- блокировка возможности подключений с IP-адреса на 15 минут, в случае четырех кратного ввода неверной идентификационной информации пользователя ПК;
- экспорт данных контроля оборудования в файл;
- настройка параметров запуска внешних программ, используемых для работы с контролируемым оборудованием: SSH-соединений, Telnet-соединений, HTTP-соединений, HTTPs-соединений;
- расширение списка, поддерживаемого комплексом оборудования за счет подключения к серверу ПК дополнительных модулей;
- хранение данных комплекса в реляционной БД с возможностью настройки сроков хранения;
- резервирование серверов.

Серверная часть ПК «Efros Config Inspector» v.3 обеспечивает выполнение функций ПК, в том числе и функций по настройке ПК:

- проверка/создание БД на сервере БД;
- подключение к сетевому и серверному оборудованию, Windows-агентам.

Клиентская консоль подключается к серверной части и предоставляет графический интерфейс для выполнения следующих функций:

Мониторинг уведомлений о событиях контроля и об ошибках выполнения заданий устройств в графическом и текстовом виде.

1) Работа с контролируемыми устройствами:
   – ведение списков устройств и групп устройств;
   – контроль текущих статусов устройств, (просмотр уведомлений о событиях, зафиксированных для устройств, операциях, выполненных с устройствами, и архива отчетов о событиях и операциях);
   – выполнение действий с устройствами (например, загрузка отчетов, проверка соединения, конфигурирование и восстановление конфигурации устройств);
   – обновление известных уязвимостей для устройств.

2) Сбор и обработка событий. Просмотр журнала событий с возможностью настройки журнала (фильтрация, выборка, построение отчетов).

3) Настройка ПК:

   а) настройки контроля:
      – задание триггеров для обработки событий, произошедших в системе и на устройствах;
      – управление профилями для гибкой настройки параметров контроля устройств;
      – управление отчетами, проверками, контролем конфигурации устройств и файловых объектов;
      – управление проверками устройств, настройка правил и исключений;

- настройка расписаний загрузки отчетов и выполнения операций с устройствами;
- настройка скрытия/разрешения загрузок и контроля целостности вычисляемых/получаемых с устройств отчетов;
- настройка политики межсетевых экранов при создании пользовательских правил проверок безопасности;

б) администрирование:

- настройка сроков хранения данных в БД ПК;
- подключение, отключение и настройка внешних модулей для работы с контролируемыми устройствами;
- управление пользователями ПК;
- настройка иерархии серверов;
- настройка резервирования серверов;
- настройка коллекторов;
- настройка параметров обновления базы данных уязвимостей (БДУ);
- управление лицензиями системы.

4) Настройка параметров запуска внешних программ: SSH-соединений, Telnet-соединений, HTTP-соединений, HTTPs-соединений.

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

Оборудование, поддерживаемое серверной частью «Efros Config Inspector» v.3, установленной на разные платформы (ОС Astra Linux Special Edition (Smolensk) v. 1.6, РЕД ОС v.7.2 и ОС Windows), представлено в таблице 2.

Таблица 2 – Перечень поддерживаемого оборудования серверной частью «Efros Config Inspector» v.3 установленной на различные платформы

Поддерживаемое оборудование	РЕД ОС v.7.2	Astra Linux SE (Smolensk) v. 1.6	Windows
3Com OS	ДА	ДА	ДА
AD Domain	НЕТ	НЕТ	ДА
AIX	ДА	ДА	ДА
Azimut (Marlin)	ДА	ДА	ДА
Allied-Telesis AT-GS950	ДА	ДА	ДА
Astra Linux	ДА	ДА	ДА
Avaya	ДА	ДА	ДА
Eltex (ESR, MES, WOP/WEP)	ДА	ДА	ДА
Huawei VRP	ДА	ДА	ДА
Cisco (ACS, ASA, AsyncOS, CatOS, FTD, FWSM Module, IOS, IOS XE, IOS XR, IPS, NX-OS, PIX, SMB, UCM 10.0, UCM 8.5, Unified Phone 78xx, Unified Phone 88xx, WAP, WLC).	ДА	ДА	ДА

Поддерживаемое оборудование	РЕД ОС v.7.2	Astra Linux SE (Smolensk) v. 1.6	Windows
Check Point (GAiA, R80 Management Server, SecurePlatform, SmartCenter)	ДА	ДА	ДА
Crossbeam XOS v.9	ДА	ДА	ДА
DATAPK	НЕТ	НЕТ	ДА
Dionis (LX, NX 1.1, NX 1.2, NX 2.0)	ДА	ДА	ДА
D-Link (DES, DGS)	ДА	ДА	ДА
Edge-Core ECS	ДА	ДА	ДА
Extreme 220 series	ДА	ДА	ДА
Fortinet FortiGate	ДА	ДА	ДА
FreeBSD	ДА	ДА	ДА
Hirschmann MAR	ДА	ДА	ДА
HP (BladeSystem HP, Comware Switch, Procurve, Virtual Connect, UX)	ДА	ДА	ДА
Juniper JUNOS	ДА	ДА	ДА
Korenix JetNet	ДА	ДА	ДА
Lenovo ENOS 8.4	ДА	ДА	ДА
Linux	ДА	ДА	ДА
Marlin	ДА	ДА	ДА
Mikrotik RouterOS	ДА	ДА	ДА
Moxa (EDS, MGate)	ДА	ДА	ДА
MS SCVMM (Virtual Machine Manager 2008 R2, 2012 R2, SCVMM Group, Hyper-V 2008 (R2 VM, R2 хост, R2 хост с контролем целостности), Hyper-V 2012 (R2 VM, R2 хост, R2 хост с контролем целостности), Standalone Hyper-V (2008 R2, 2012 R2))	НЕТ	НЕТ	ДА
Nateks (NX-5100, NXI-3030, NXI-3050)	ДА	ДА	ДА
NIS	ДА	ДА	ДА
Palo Alto Pan-OS	ДА	ДА	ДА
PKCC (OmniAccess 700, OmniSwitch 6850, OmniSwitch 7710, OmniSwitch 7750, OmniSwitch 9000, Onyx)	ДА	ДА	ДА
QTech QSW	ДА	ДА	ДА
Raisecom ISCOM	ДА	ДА	ДА
Rockwell Cisco IOS	ДА	ДА	ДА
Siemens Scalance X-300 series, X-400 series	ДА	ДА	ДА
S-Terra VPN Gate	ДА	ДА	ДА
SunOS	ДА	ДА	ДА
ViPNet Coordinator HW	ДА	ДА	ДА
VMWare vCenter (vCenter (VCSA, Windows), Standalone ESXi с контролем файлов по HTTPS (SSH), VM (5.0, 5.1, 5.5, 6.0, 6.5), Host, Host с контролем целостности файлов по SSH (HTTPS), Folder, Datacenter, vApp, Resource Pool, ESXi ОС с контролем файлов по HTTPS (SSH), Cluster)	НЕТ	НЕТ	ДА

Поддерживаемое оборудование	РЕД ОС v.7.2	Astra Linux SE (Smolensk) v. 1.6	Windows
WatchGuard Fireware (OS, XTM OS)	ДА	ДА	ДА
Windows	ДА	ДА	ДА
XenServer	ДА	ДА	ДА
Zelax M-1-MEGA	ДА	ДА	ДА
ZyXEL ZyNOS	ДА	ДА	ДА
Полигон (Арлан, Инзер)	ДА	ДА	ДА

Отличие функций ПК «Efros Config inspector» v.3 установленного на разные платформы (ОС Astra Linux Special Edition (Smolensk) v. 1.6, РЕД ОС v.7.2 и ОС Windows) представлено в таблице 3.

Таблица 3 – Функциональные различия ПК «Efros Config inspector» v.4 при развертывании на различных платформах

Функции	РЕД ОС v.7.2	Astra Linux SE (Smolensk) v. 1.6	Windows Server 2016
Идентификация и аутентификация пользователей под доменной учетной записью	НЕТ	НЕТ	ДА
Наличие клиентской консоли, для локальной установки совместно с сервером, реализующей графический интерфейс для управления функциями ПК	НЕТ (используется консоль, установленная на сервере под управлением ОС Windows Server 2016)	НЕТ (используется консоль, установленная на сервере под управлением ОС Windows Server 2016)	ДА

1.2.1 Обработка отчетов

Отчеты формируются путем загрузки с устройств или через преобразование из существующих отчетов.

Отчеты позволяют:

- просматривать данные устройств;
- выполнять фильтрацию и выборки;
- отслеживать изменение настроек устройств, хранить архив изменений;
- контролировать целостность настроек;
- проверять корректность настроек, использовать дополнительные проверки.

ПК позволяет создавать пользовательские отчеты, выбирая поля и записи из существующих отчетов. Такая возможность в комбинации с функциями контроля целостности создает новые сценарии использования ПК. Например, пользователь, может составить список допустимых процессов и проверять группу серверов на соответствие этому списку.

В ПК поддерживаются следующие форматы отчетов:

– отчеты о конфигурации, включающие в себя текстовые и структурированные отчеты;
– отчет о проверке.

На рисунке 1 приведены примеры представлений отчета, содержащего список пользователей, извлеченный из конфигурационного файла (КФ) Cisco IOS.

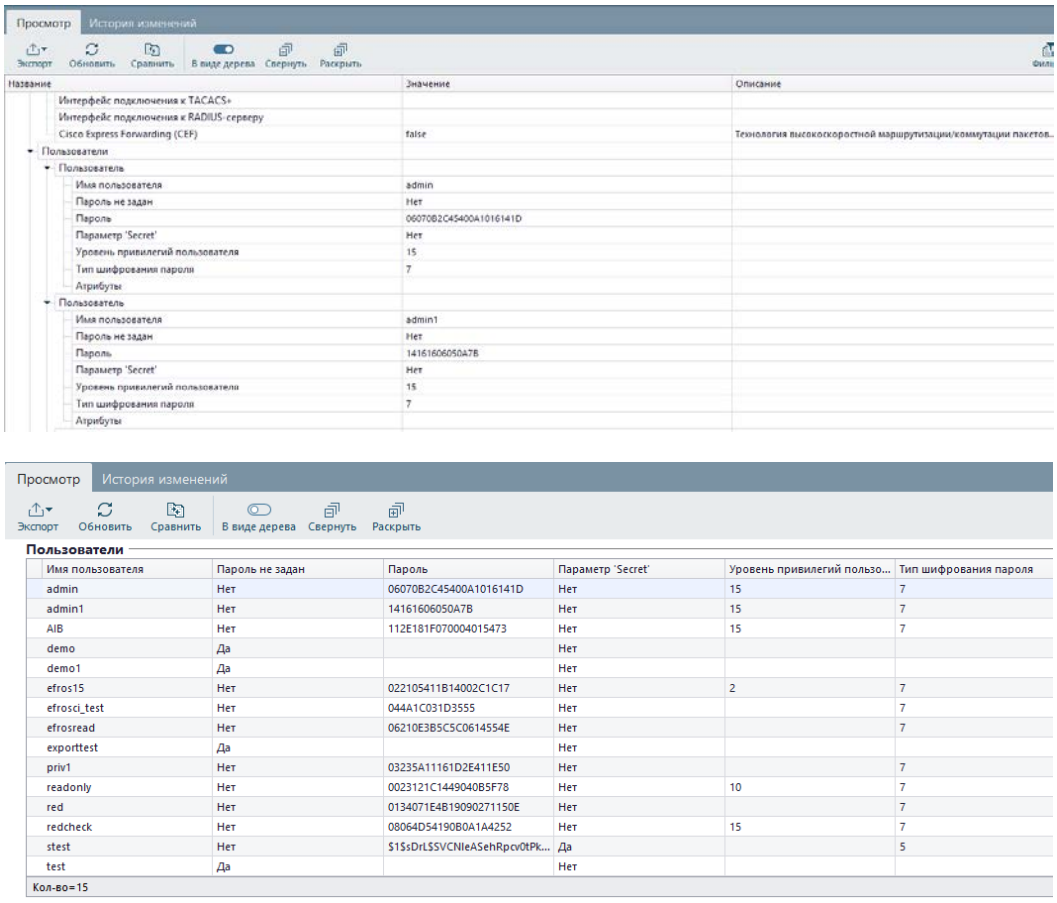

Рисунок 1 – Примеры представлений отчета, содержащего список пользователей, извлеченный из КФ Cisco IOS

1.2.2 Проверки

Проверки добавляются на сервер ПК вместе с подключением внешних модулей работы с устройствами, для которых они предназначены.

Проверки могут иметь различные назначения:

– **вопросы обслуживания**. Например, проверка синхронизации *running-* и *startup-* конфигураций Cisco IOS;

– **проверка соответствия (Compliance)**. Например, проверка аудита конфигурации Cisco IOS по правилам CIS;

– **уязвимости системы.** Например, вывод текущих уязвимостей для Cisco IOS по стандарту OVAL (https://oval.mitre.org/).

Для настройки проверок под нужды пользователя поддерживаются:

– возможность отключения проверки;

– возможность исключения одного или нескольких правил из проверки;

– возможность задания исключений для правил (например, исключение пользователя из правила ***Необходимо шифровать пароли пользователей***).

Пример отчета о результате проверки приведен на рисунке 2.

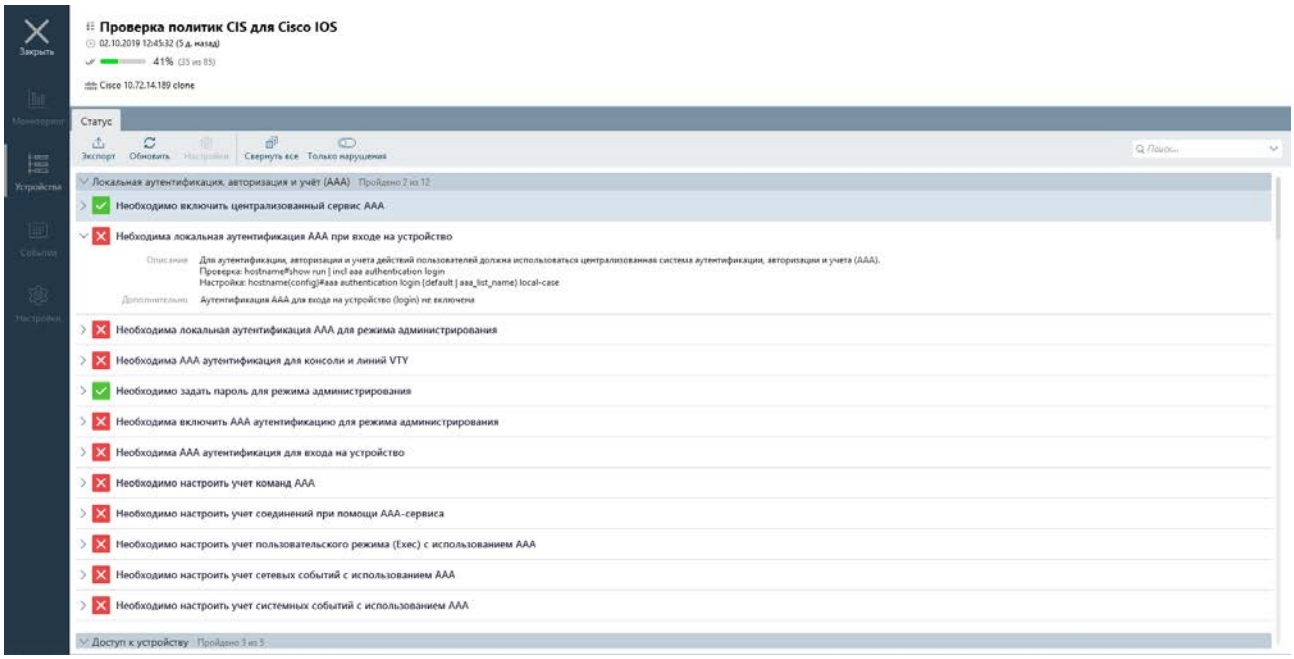

Рисунок 2 – Отчет о результате проверки

1.2.3 Сбор, обработка событий

ПК «Efros Config Inspector» v.3 поддерживает сбор и хранение событий, произошедших на сервере ПК или на контролируемом оборудовании.

События могут регистрироваться как самим ПК (например, при загрузке отчета), так и внешними модулями (например, Syslog-сообщения).

При этом комплекс поддерживает динамическое добавление новых типов событий. Помимо типа события также добавляются поля, которые содержит событие. Например, модуль Syslog-сервера регистрирует тип события Syslog-сообщение с полями *Facility*, *Severity*, *Address*, *Message*.

Перечень событий по умолчанию:

- запуск задания по расписанию;
- загрузка отчета;
- аудит;
- сохранение отчета в архив;
- выполнение проверки;
- нарушение целостности;
- выполнение операции;
- добавление, изменение устройства.

В дальнейшем, данные, содержащиеся в полях событий, могут использоваться для задания условий, как при фильтрации (рис. 3), так и при настройке обработчиков событий (триггеров) (рис. 4). Возможность создания триггеров доступна пользователям ПК «Efros Config Inspector» v.3 с ролями ***Администратор*** или ***Опытный пользователь.***

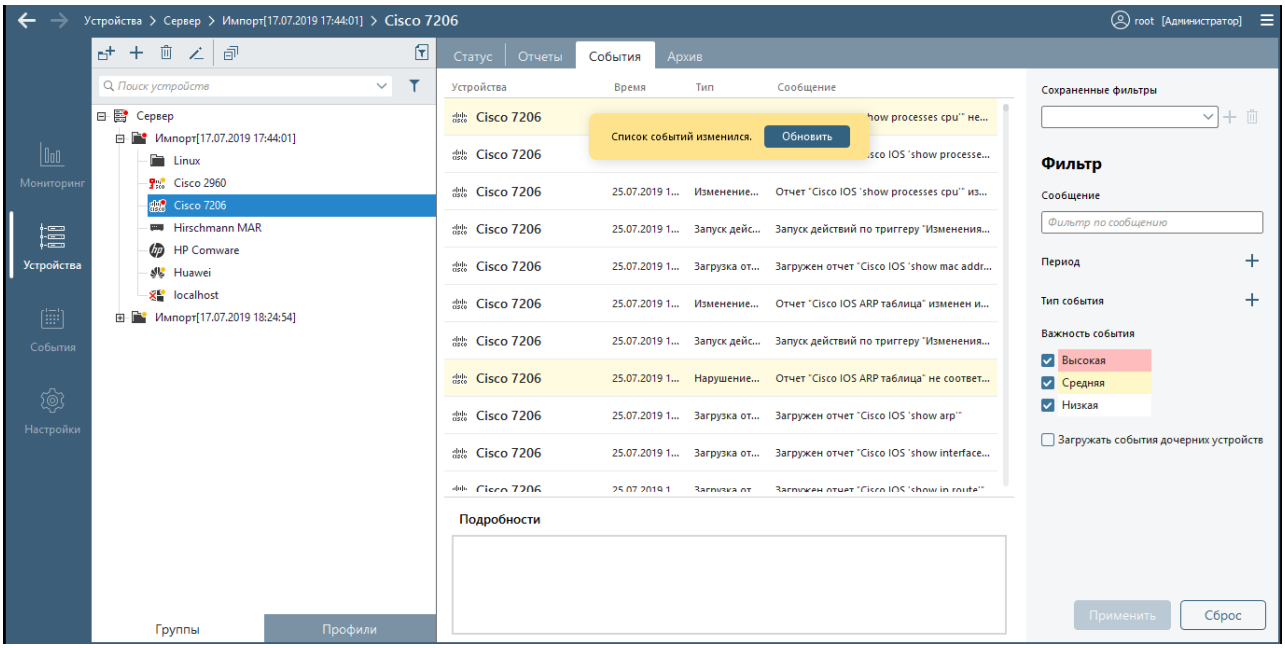

Рисунок 3 – Фильтрация событий

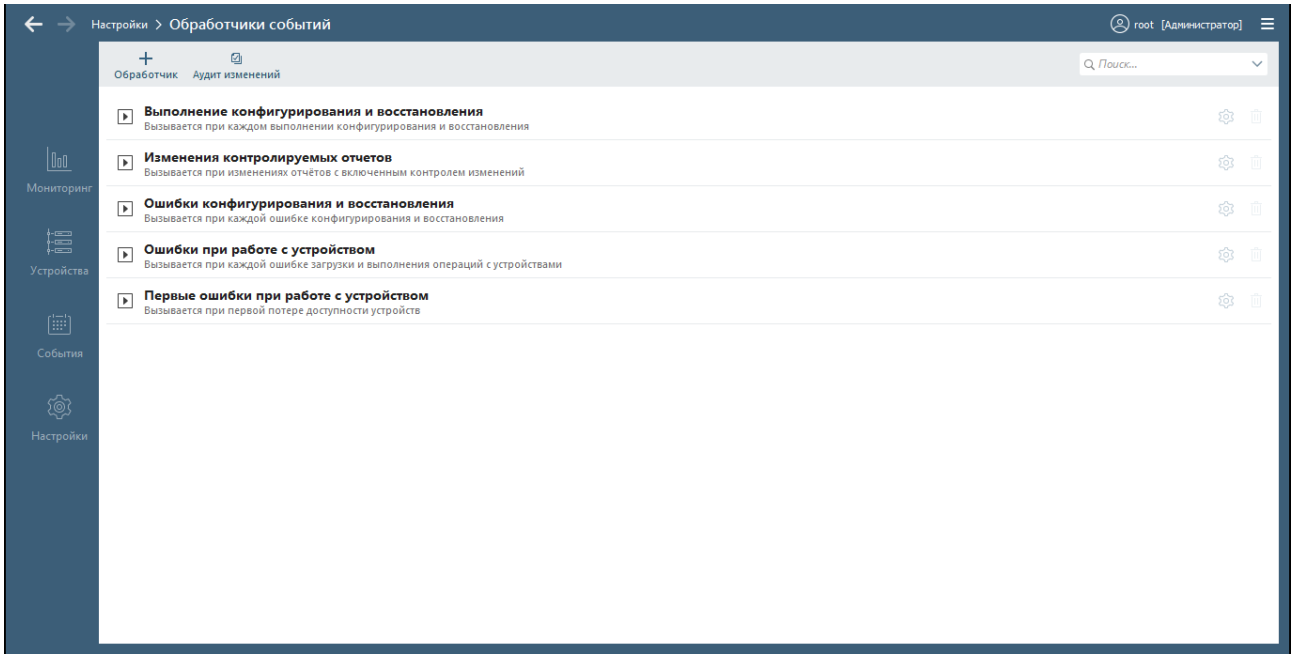

Рисунок 4 – Задание условий при настройке обработчика событий

При создании триггеров пользователь может выбирать типы событий и задавать условия к их полям.

При этом в качестве реакции системы возможны следующие варианты:

- создание уведомления (инцидента) в системе;
- выполнение операции «Проверить соединение»;
- отправка писем, Syslog сообщений с деталями события, писем через Exchange;
- запуск выполнения операций с устройствами;
- запуск загрузки отчетов;
- запуск зарегистрированных модулями действий (например, отправка сообщения в Microsoft Lync).

1.2.4 Поддержка операций управления устройствами

ПК «Efros Config Inspector» v.3 поддерживает выполнение операций с устройствами (например, операция копирования рабочей конфигурации в конфигурацию запуска для устройств Cisco IOS, изменение загрузочной конфигурации отдельных типов устройств, восстановление конфигураций сетевых устройств Cisco IOS, Cisco ASA, Huawei VRP с использованием сохраненных в архиве загрузочных конфигураций).

Операции управления устройствами добавляются на сервер ПК вместе с подключением внешних модулей работы с устройствами, для которых они предназначены.

С сервера ПК операции управления устройствами могут выполняться:

- по запросу пользователя;
- по расписанию;

– как результат обработки событий (по триггеру).

1.2.5 Резервирование сервера

В ПК «Efros Config Inspector» v.3 доступна настройка резервирования сервера.

Резервирование сервера осуществляется в случае выхода из строя основного сервера. При этом все функции основного сервера принимает на себя резервный.

Режим резервирования будет доступен при наличии одного и более резервных серверов.

При наличии нескольких серверных частей, ПК автоматически определяет основную. Все остальные являются резервными.

2 Условия применения

Минимальный состав технических средств электронно-вычислительной машины (ЭВМ)[1] для установки серверной части и внешних модулей ПК «Efros Config Inspector» v.3 рассчитывается на основе данных приведенных в таблицах 4–6.

Таблица 4 – Минимальные требования к производительности сервера ПК

Размер контролируемой сети	Характеристики сервера ПК
Малая (<100 активное сетевое оборудование; <50 др. объекты)	до 2Ghz CPU, Cores: 4, 8 GB RAM
Средняя (<300 активное сетевое оборудование; <200 др. объекты)	от 2Ghz CPU, Cores: 8, 16 GB RAM
Большая (>300 активное сетевое оборудование; >200 др. объекты)	от 2Ghz CPU, Cores: 16, 16GB RAM

Таблица 5 – Средние показатели параметров загрузки отчетов по типам устройств

Тип устройства	Среднее время загрузки, t (сек.)[2]	Увеличение объема данных, V (Mb\час)[2]
Network	120	0,05
ESXi	30	0,05
Unix	120	0,45
Windows	460	0,6

Таблица 6 – Средние значения коэффициента производительности сервера ПК

Размер контролируемой сети	Значение коэффициента (k)[2]
Малая	0,25
Средняя	0,15
Большая	0,1

Для приблизительного расчета минимального периода загрузки отчетов с контролируемых на сервере ПК устройств можно воспользоваться следующей формулой:

[1] Под ЭВМ понимается электронно-вычислительная машина, совместимая с архитектурой Intel x86 (x86_64).

[2] В таблицах 5 и 6, для расчета минимального периода опроса контролируемых устройств и минимального объема свободного дискового пространства, приведены ориентировочные (приблизительные) значения параметров, которые могут изменяться в зависимости от технических характеристик используемой ЭВМ.

$$(\sum t_n \cdot n) \cdot k,$$

где t_n – среднее время загрузки отчетов с контролируемого типа устройств (берется из таблицы 4);
n –количество контролируемых на сервере ПК устройств одного типа;
k – коэффициент производительности сервера ПК (берется из таблицы 6).

Например, для небольшой сети, в которой находится 15 сетевых устройств, 20 Unix-систем и 10 рабочих станций с ОС Windows, приблизительное время необходимое для загрузки отчетов на сервер ПК со всех контролируемых устройств составит:

$$(120 \cdot 15 + 120 \cdot 20 + 460 \cdot 10) \cdot 0{,}25 = 2200 \text{ сек} = 37 \text{ мин}$$

Для определения оптимальной периодичности автоматического выполнения операций с устройствами (загрузки отчетов по расписанию) необходимо:

1) После настройки комплекса и добавления всех контролируемых устройств на сервер ПК выполнить операцию загрузки отчетов со всех устройств.

2) Зафиксировать время, затраченное на загрузку отчетов со всех устройств.

3) К полученному времени добавить 20 процентов. Полученное значение установить в качестве периода времени между запусками расписания.

4) При добавлении на сервер ПК дополнительных устройств необходимо повторить п.1-3, корректируя установленную периодичность запуска расписания.

Свободное дисковое пространство ЭВМ необходимое для установки только серверной части ПК и внешних модулей, составляет 10 Гб.

При установке серверной части ПК и сервера баз данных на одну ЭВМ минимальный объем свободного дискового пространства рассчитывается на основе данных, приведенных в таблице 4 и заданного при настройке параметров работы сервера ПК периода очистки базы данных (Т).

Для расчета необходимого минимального объема свободного дискового пространства для хранения данных ПК в используемой базе данных нужно воспользоваться следующей формулой:

$$(\sum V_n \cdot n) \cdot T \cdot 24,$$

где V_n – среднее увеличение объема используемой базы данных в час в зависимости от типа контролируемых устройств (берется из таблицы 5);
n – количество контролируемых на сервере ПК устройств одного типа;
T – период очистки базы данных (устанавливается при настройке программного комплекса в клиентской консоли).

Например, для контролируемых на сервере ПК 15 сетевых устройств, 20 Unix-систем и 10 рабочих станций с ОС Windows и периода очистки базы данных в 30 дней, минимальный объем свободного дискового пространства составит приблизительно:

$$(0{,}05 \cdot 15 + 0{,}45 \cdot 20 + 0{,}6 \cdot 10) \cdot 720 = 11340 \text{ Mb}$$

Допускается установка серверной части ПК «Efros Config Inspector» v.3 на компьютеры, функционирующие под управлением операционных систем:

- Windows 7 с пакетом обновления 1 (SP1);
- Windows 8.1;
- Windows 10;
- Windows Server 2008R2 с пакетом обновления 1 (SP1);
- Windows Server 2012/2012R2;
- Windows Server 2016;
- Windows Server 2019;
- Astra Linux Special Edition (Smolensk) v. 1.6;
- РЕД ОС (Муром) v. 7.2.

Для установки серверной части и внешних модулей ПК «Efros Config Inspector» v.3, на ЭВМ под управлением ОС Windows, должен быть следующий минимальный состав программных средств:

– .NET Framework 4.5.2;

– СУБД (при установке локально): MySQL 5.5, PostgreSQL 9.4, Microsoft SQL Server 2012 (также поддерживаются новые версии данных СУБД) или Jatoba (ООО Газинформсервис);

Требования к настройке используемых СУБД приведены в подразделе 1.2.6 Руководства администратора ПК «Efros Config Inspector» v.3.

– SQL Server Native Client – при использовании СУБД MS SQL Server 2012, установленной на отдельном сервере баз данных;

– ПО Java (JRE) версия 1.6.0 (загрузить последнюю версию программного обеспечения Java (JRE) можно на сайте производителя http://java.com).

Перед установкой серверной части ПК на англоязычные ОС следует установить Русский язык в качестве Языка системы для программ, не поддерживающих Юникод.
Для обеспечения взаимодействия контролируемых ОС Windows с сервером ПК в используемом брандмауэре должны быть открыты TCP-порты: на сервере ПК – 20002, а на контролируемых ОС – 20001.

Для установки серверной части и внешних модулей ПК «Efros Config Inspector» v.4 на ЭВМ под управлением ОС Astra Linux Special Edition (Smolensk), РЕД ОС (Муром) необходим следующий минимальный состав программных средств:

- СУБД (при установке локально): пакеты MySQL 5.5, PostgreSQL 9.4 (также поддерживаются новые версии данных СУБД), Jatoba;
- СУБД MS SQL Server 2012 при установке на отдельном сервере баз данных под управлением ОС Windows;
- ПО Java (JRE) версия 1.6.0;

- systemd - подсистема инициализации Linux для запуска других демонов и управления ими в процессе работы системы.

СУБД может быть установлена локально на сервере ПК либо на удаленном компьютере и подключена к серверу ПК по сети. При подключении удаленной СУБД MySQL для обеспечения корректной работы необходимо, чтобы значение переменной max_allowed_packet сервера MySQL было не менее 512 М.

Для установки клиентской консоли ПК «Efros Config Inspector» v.3 ЭВМ должна иметь следующий минимальный состав технических и программных средств:

1) Аппаратное обеспечение:
– процессор двухъядерный с тактовой частотой 3 ГГц;
– оперативная память 4 Гб;
– свободное дисковое пространство не менее 2 Гб;
– сетевая карта Ethernet.
2) Программное обеспечение:
   а) Операционная система:
      - Windows 7 с пакетом обновления 1 (SP1);
      - Windows 8.1;
      - Windows 10;
      - Windows Server 2008R2 с пакетом обновления 1 (SP1);
      - Windows Server 2012/2012R2;
      - Windows Server 2016;
      - Windows Server 2019;
   б) .NET Framework 4.5.2.

Для сетевого взаимодействия клиентской консоли с сервером программного комплекса на рабочих станциях с установленной клиентской консолью должен быть открыт 20000 TCP-порт.

ЭВМ для установки windows-агента ПК «Efros Config Inspector» v.3 функционирует под управлением следующих операционных систем:

- Windows 7 с пакетом обновления 1 (SP1);
- Windows 8.1;
- Windows 10;
- Windows Server 2008R2 с пакетом обновления 1 (SP1);
- Windows Server 2012/2012R2;
- Windows Server 2016;
- Windows Server 2019.

Минимальные требования к производительности рабочей станции для установки windows-агента ПК:

– Процессор с тактовой частотой 1,6 ГГц или больше;
– ОЗУ объемом 1 ГБ (1,5 ГБ для работы на виртуальной машине);
– 100 МБ доступного пространства на жестком диске;

– сетевая карта Ethernet.

Для сетевого взаимодействия Windows-агента с сервером программного комплекса на контролируемых рабочих станциях должен быть открыт 20001 TCP-порт.

Для корректного функционирования компонентов ПК «Efros Config Inspector» v.3 при взаимодействии с установленным антивирусным ПО необходимо добавить в список исключений в настройках антивирусного ПО следующие программные модули программного комплекса:

– службу сервера (C:\Program Files (x86)\EFROS Config Inspector 3\Server\CIService.exe);

– клиентскую консоль (C:\Program Files (x86)\EFROS Config Inspector 3\Console\CIWPF.exe);

– службу Windows-агента (C:\Program Files (x86)\EFROS Config Inspector 3\Agent\WAService.exe).

Порядок настройки сетевого и серверного оборудования (в зависимости от производителя оборудования) для подключения его к серверу ПК по используемым протоколам указан в файле справки *ModulesDescripion.zip* (*ModulesDescripion.chm*), расположенном на дистрибутивном диске программного комплекса.

3 Решаемые задачи

ПК «Efros Config Inspector» v.3 решает следующие задачи:

- контроль активного сетевого оборудования разных производителей;
- проверка серверных ОС (Windows, Unix-like);
- мониторинг состояния объектов виртуальных инфраструктур;
- запуск проверок по расписанию;
- отправка писем и уведомлений администратору комплекса;
- отправка извещений сторонним средствам мониторинга;
- прием и хранение Syslog сообщений;
- аудит конфигураций контролируемых устройств по заданным профилям;
- конфигурирование устройств и групп устройств;
- восстановление конфигурации устройств;
- ведение журнала действий пользователей;
- возможность аутентификации на устройствах по протоколу SSH;
- контроль целостности файлов ОС;
- создание стандартов и настройка требований проверок безопасности для устройств;
- создание стандартов и настройка требований проверок безопасности межсетевых экранов;
- сбор данных об уязвимостях контролируемого оборудования и ПО;
- построение иерархии серверов и настройка подключения подчиненных серверов;
- резервирование серверов.

Прежде чем решать ту или иную задачу, администратору безопасности необходимо выполнить настройку комплекса.

3.1 Контроль активного сетевого оборудования разных производителей

Для контроля устройств необходимо при помощи клиентской консоли выполнить операцию ***Загрузить***. Данная операция запускается из меню устройства в ***Панели списка устройств***.

Полный список действий при выполнении данной операции включает:

1) загрузку на сервер ПК текстовых конфигураций контролируемых устройств (текстовых файлов, выводов команд);

2) загрузку и формирование отчетов по настройкам, локальным файлам и параметрам работы контролируемых устройств;

3) выполнение проверок наличия уязвимостей контролируемого оборудования;

4) выполнение проверок соответствия конфигурации контролируемых устройств требованиям безопасности (compliance проверки).

3.2 Запуск проверок по расписанию

Решение данной задачи заключается в настройке расписания проверки контролируемого оборудования. Расписание проверки задается в ***Форме настройки расписаний загрузки отчетов*** раздела **Настройки** клиентской консоли.

После выполнения настройки контроль устройств будет осуществляться строго по указанному расписанию.

3.3 Отправка писем администратору

В ПК «Efros Config Inspector» v.3 поддерживается отправка писем администратору с сообщениями о произошедших на сервере ПК и контролируемых устройствах событиях по протоколу *SMTP*.

Решение задачи отправки писем заключается в настройке параметров отправки писем. Настройка выполняется в ***Форме подключения, отключения и настройки внешних модулей*** раздела **Настройки** клиентской консоли для модуля ***Отправка писем по протоколу SMTP***.

3.4 Отправка извещений сторонним средствам мониторинга

В ПК «Efros Config Inspector» v.3 поддерживается отправка уведомлений на внешний сервер по протоколу *Syslog*.

3.5 Аудит конфигураций контролируемых устройств по политикам

В ПК «Efros Config Inspector» v.3 поддерживается аудит контроля конфигураций по заданным профилям.

Решение данной задачи заключается в:

- создании профилей политик контроля;
- проверке рабочей конфигурации устройств при загрузке на выполнение правил;
- анализе выполненных и невыполненных условий.

Операции выполняются администратором ПК в ***Форме управления профилями***, далее автоматически при загрузке отчетов.

3.6 Конфигурирование устройств и групп устройств

ПК поддерживает функцию конфигурирования устройств. Задача решается предоставлением пользователям доступа к конфигурированию отдельных устройств, поддерживающих данную функцию, в соответствии с уставленными правами доступа. Пользователи получают возможность внесения изменений в конфигурацию контролируемых устройств путем выдачи команд конфигурирования.

Поддерживается сохранение/изменение/удаление списков команд конфигурирования. Операция может выполняться как для одного устройства, так и для группы устройств.

Операция выполняться администратором с полным доступом или пользователями с доступом для выполнения операций на корневой группе устройств.

3.7 Восстановление конфигурации устройств

В ПК «Efros Config Inspector» v.3 для отдельных типов устройств решена задача восстановления конфигурации путем загрузки ранее сохраненных файлов конфигураций (эталонов) из архива ПК. В ходе восстановления возможно сравнение эталонной и текущей конфигурации устройства. Запуск восстановления конфигурации реализован на вкладке ***Статус*** раздела ***Устройства.***

3.8 Ведение журнала действий пользователей

В ПК «Efros Config Inspector» v.3 поддерживается фильтрация журнала событий по действиям различных пользователей ПК.

Решение задачи просмотра журнала действий оператора заключается в настройке фильтра. Настройка выполняется в разделе **События** путем фильтрации событий по типу события ***Аудит*** по условию ***Пользователь***.

3.9 Возможность аутентификации по протоколу SSH при подключении к устройствам

В ПК «Efros Config Inspector» v.3 при подключении к устройствам поддерживается протокол SSH версии 2.0.

Данная настройка доступна для ряда устройств – в свойствах контролируемого устройства есть возможность указать необходимый протокол взаимодействия.

3.10 Контроль файлов ОС

В программе поддерживается функция контроля целостности файлов операционной системы контролируемых устройств по требованию пользователя.

Данный функционал реализован во вкладке **Отчеты** раздела **Настройки** и настраивается путем создания пользовательских отчетов для операционной системы контролируемого оборудования, в которых перечислены полные пути к контролируемым файлам или указаны маски для типов контролируемых объектов.

3.11 Формирование пользовательских стандартов и настройка требований проверок безопасности для устройств

В ПК «Efros Config Inspector» v.3 реализована возможность формирования пользовательских стандартов проверок безопасности, на основании базы проверок

CIS, существующих пользовательских проверок (включая проверки с помощью регулярных выражений), а также путем копирования и последующего редактирования проверок, в том числе задание и редактирования исключений. При добавлении пользовательских стандартов возможен импорт настроек и требований пользовательского стандарта проверки безопасности из файла формата XML, а также добавления нового стандарта путем выбора требований из базы требований, формируемой из предустановленных требований при подключении внешних модулей оборудования или путем копирования из ранее добавленных стандартов.

Данный функционал реализован во вкладке **Проверка безопасности** раздела **Настройки.**

3.12 Анализ фильтрации трафика межсетевыми экранами

Для межсетевых экранов (МЭ) CheckPoint и Cisco ASA реализована возможность анализа движения трафика по зонам (подсетям). Анализ фильтрации трафика выполняется на основании заданных пользователем подсетей (источник, адресат), портов, протоколов и исключений. В результате формируется отчет, демонстрирующий запрещенные и разрешенные протоколы. Функция реализована во вкладке «Политики межсетевых экранов» раздела «Настройки» клиентской консоли.

Данный функционал реализован во вкладке **Политики межсетевых экранов** раздела **Настройки.**

3.13 Анализ правил межсетевых экранов

Механизм анализа правил межсетевых экранов CheckPoint и Cisco ASA выявляет избыточные и «теневые» правила МЭ. Избыточными считаются полностью или частично дублированные правила. «Теневые» правила не выполняются в силу вышестоящих правил с обратным действием, несут потенциальную угрозу безопасности. Итоговые отчеты содержат рекомендации по оптимизации правил МЭ.

3.14 Сбор данных об уязвимостях контролируемого оборудования и ПО

В ПК «Efros Config Inspector» v.3 реализовано обновление базы уязвимостей путем обмена через программный интерфейс с сервером, содержащим БДУ об известных уязвимостях в формализованном унифицированном виде. Полученные сведения об уязвимостях представляются по устройствам и программному обеспечению в виде отчета об уязвимостях, а также по типам устройств на вкладке **База уязвимостей** раздела **Настройки**.

3.15 Построение иерархии серверов

В ПК реализована функция построения иерархии серверов, добавление новых серверов, настройка режима работы подчиненных серверов и доступа

пользователей к ним. Также в **форме настойки иерархии** (открывается при переходе по ссылке **Иерархия** в разделе **Настройка),** при добавлении нового сервера, возможна настройка ограничения скорости при работе с подчиненными серверами.

3.16 Резервирование серверов

В случае выхода из строя основного сервера предусмотрено переключение выполнения всех функций резервным сервером. Для работы системы резервирования необходимо создание и настройка резервного сервера. Для этого серверная часть ПК «Efros Config Inspector» v.3 устанавливается на новый компьютер и выполняется настройка подключения сервера ПК к используемой базе данных комплекса. Порядок настройки режима резервирования сервера описан в п. 4.5 «Настройка режима резервирования сервера» документа «ПК «Efros Config Inspector» v.3 Руководство администратора».

В случае сбоя основного сервера, модули и настройки серверной части будут доступны на резервном сервере.

4 Входные и выходные данные

4.1 Входные данные

Входными данными для ПК «Efros Config Inspector» v.3 являются:

1) ***настройки:***

- сетевых устройств, серверов, виртуальных инфраструктур и групп данных объектов;
- программного комплекса «Efros Config Inspector» v.3 (настройки работы служб, сервера баз данных, отправки писем и извещений и др.);

2) ***данные (состав принимаемых данных зависит от состава включенных при настройке ПК внешних модулей):***

- принятые по протоколу Telnet;
- принятые по протоколу SSH;
- принятые по протоколу HTTPS;
- принятые по протоколу TLS;
- принятые Syslog сообщения;
- принятые по протоколу SNMP;
- принятые по протоколу VIX API (при работе с VMWare vCenter);
- принятые по протоколу WMI (при работе с Hyper-V);
- принятые по протоколу WinRM (при работе с Hyper-V);
- принятые по протоколу SMB (при работе с Hyper-V);
- принятые по протоколу AXL API (при работе с CISCO UCM);
- принятые по протоколу CPMI (при работе с устройствами CheckPoint);
- принятые по протоколу REST (при работе с устройствами Cisco ACS);
- принятые по протоколу XenAPI (при работе с устройствами Citrix XenServer);
- принятые по протоколу LDAP (при контроле ActiveDirectory);
- принятые по протоколу SNMP (при сканировании сети).

4.2 Выходные данные

Выходными данными для ПК «Efros Config Inspector» v.3 являются:

1) ***сохраненные в базе данных отчеты о конфигурации и состоянии контролируемых устройств;***

2) ***данные (состав выходных данных зависит от состава включенных при настройке ПК внешних модулей):***

- переданные по протоколу Telnet;
- переданные по протоколу SSH;
- принятые по протоколу HTTPS;
- переданные по протоколу TLS;

- переданные по протоколу SMTP;
- переданные по протоколу Microsoft Exchange Web Services Managed API (при отправке через MS Exchange);
- переданные по протоколу Microsoft Unified Communications Managed API (при отправке сообщений в MS Lync);
- переданные по протоколу Syslog;
- переданные по протоколу SNMP;
- переданные по протоколу VI API (при работе с VMWare vCenter);
- переданные по протоколу WMI (при работе с Hyper-V);
- переданные по протоколу WinRM (при работе с Hyper-V);
- переданные по протоколу AXL API (при работе с CISCO UCM);
- переданные по протоколу CPMI (при работе с устройствами CheckPoint);
- переданные по протоколу XenAPI (при работе с устройствами Citrix XenServer);
- переданные по протоколу LDAP (при контроле ActiveDirectory).

Перечень сокращений

HTTP (HyperText Transfer Protocol)	–	протокол прикладного уровня передачи данных. Основой HTTP является технология «клиент-сервер»
HTTPs (HyperText Transfer Protocol Secure)	–	расширение протокола HTTP, поддерживающее шифрование
Syslog	–	стандарт отправки сообщений о происходящих в системе событиях
SSH (Secure Shell)	–	сетевой протокол прикладного уровня, позволяющий производить удаленное управление и туннелирование сетевых соединений. В качестве транспорта используется TCP, при этом все передаваемые данные шифруются
SSL (Secure Socket Layer)	–	криптографический протокол. Использует асимметричную криптографию для аутентификации ключей обмена, симметричный шифр для сохранения конфиденциальности, коды аутентификации сообщений для целостности сообщений
TELNET (TELecommunication NETwork)	–	сетевой протокол для реализации текстового интерфейса по сети, в качестве транспорта используется TCP
TLS (Transport Layer Security)	–	криптографический протокол. Использует асимметричную криптографию для аутентификации ключей обмена, симметричный шифр для сохранения конфиденциальности, коды аутентичности сообщений для сохранения целостности сообщений
БД	–	база данных
ОС	–	операционная система
ПК	–	программный комплекс

Термины и определения

Отчет – загружаемые с устройств данные, а также результаты обработки загруженных данных, являются отчетами типа Отчет, Текстовый отчет. Результат проверки данных на соответствие заданным правилам – отчет типа Отчет о проверке

Проверка – отчет, сформированный ПК по результатам проверки загруженных или выбранных данных на соответствие заданным правилам

Профиль – поименованная совокупность настроек параметров контроля устройств, отчетов и проверок, доступных для устройств

Событие – зафиксированное в журнале программы действие сервера EFROS CI или пользователей программы

Статус – интерфейс, на котором отображены важные оповещения по ситуации и выведены основные операции с контролируемыми устройствами