ГАЗИНФОРМ СЕРВИС

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

Описание релиза v. 3.1.400

Санкт-Петербург, 2019

Описание релиза программного комплекса управления конфигурациями и анализа защищенности «Efros Config Inspector» v.3.1.400

Программный комплекс «Efros Config Inspector» релиз 3.1.400 (далее ПК «Efros Config Inspector» v.3).

О релизе:

Основными нововведениями релиза являются:

- ограничение скорости при работе с подчиненными серверами;
- механизм контроля действий пользователя с устройствами;
- поддержка локальных групп пользователей;
- доработанные модули поддержки сред виртуализации;
- расширена поддержка английского языка;
- построение карты сети с применением SNMP.

Также добавлен ряд функциональных улучшений, расширена поддержка устройств. Выполнены доработки для упрощения работы пользователей и оптимизации работы системы.

Обновлен перечень проверок уязвимостей для поддерживаемых устройств.

Новые возможности:

1. Ограничение скорости при работе с подчиненным сервером

Для ограничения канала связи между главным и подчиненным сервером была добавлена опция, в которой можно указать скорость для загрузки данных и отдельно для загрузки событий подчиненного сервера. Находится данная опция в клиентской консоли, раздел “Настройки-Иерархия”, редактор подчиненного сервера.

2. Механизм контроля действий пользователя с устройствами

Добавлен новый триггер для устройств Cisco и Huawei, который автоматически срабатывает при получении syslog или SNMP-Trap сообщения о изменении конфигурации устройства. После получения сообщения запускается загрузка текущей конфигурации устройства для проверки на изменения. В случае обнаружения изменений формируется событие, к которому прикрепляется информации о пользователях, которые могли внести изменения.

3. Поддержка локальных групп пользователей

Добавлены группы пользователей для удобного разграничения прав по группам.
Добавлена возможность редактирования группы, механизм добавления/удаления пользователей группы.
Добавлено отображение групп и "вложенных" пользователей.
Добавлена проверка уникальности имени пользователя/группы.

4. Виртуализация

Расширен набор контролируемых параметров виртуализации VMware и Microsoft.
Расширена поддержка vCenter.
Добавлена загрузка аппаратной составляющей для гипервизоров Microsoft и VMWare.
Добавлена поддержка Distributed Virtual Switch, Virtual Switch, VM Networks.
Добавлена поддержка загрузки списка пользователей из Lockdown Mode Exception User List.
Расширена поддержки SCVMM и Hyper-V.
Добавлен отчет об аппаратной составляющей BM, сетевой составляющей SCVMM.

5. Локализация

Выполнена английская локализация модулей LinuxGeneral модулей LinuxGeneral, SendMail, PaloAlto, Polygon, Sterra, vCenter, ModulesCodeGen, PaloAlto, Polygon, Sterra, CiscoGeneral, Eltex, GeneralNetworkDevices, SNMPScanner, SNMPServer.
Обновлен словарь переводов.

6. Поддержка устройств

Добавлена поддержка:

Zelax M-1 Mega;

Cisco Firepower;

ExtremeNetworks;

Edgecore ECS;

Allied Telesis AlliedWare Plus.

Обновлен перечень проверок уязвимостей для поддерживаемых устройств.

7. Карта сети с применением SNMP

Реализовано построение карты сети на основании данных SNMP, что обеспечивает удобство контроля и полноту карты сетевых устройств.

8. Общие доработки

Добавлен ряд улучшений интерфейса:

- настроек сервера;
- настроек пользователей;
- настроек доступа для группы и устройств;

- вкладки Доступ, раздел Настройки-Иерархия;
- вкладки добавление/редактирование сервера, раздел Настройки-Иерархия;
- расписаний и обработчиков событий, окно Свойства устройства;
- истории изменения отчета;
- Настройки, названия разделов,
- Профили подключения;
- Дерево устройств, раздел Устройства.

Выполнена оптимизация дерева устройств, для ускорения работы при большом количестве устройств.

Исправленные ошибки:

- Утилита настройки сервера. Английская локализация. Ошибки и неточности.
- Утилита настройки агента. Английская локализация. Ошибки и неточности.
- Утилита настройки коллектора. Английская локализация. Ошибки и неточности.
- Консоль. Некорректно работает переключение языка на английский.
- Модуль vCenter. Корректировка перевода правил.
- Ошибка вывода подсети 127.0.0.0 на карту сети при использовании SNMP Probe модуля.
- Ошибки при установке агента и коллектора.
- Консоль. Ошибки\неточности в обновленном инсталляторе.
- Сервер. Ошибки\неточности в обновленном инсталляторе.
- Агент. Ошибки\неточности в обновленном инсталляторе.
- Обновление. Не удалось обновить структуру базы данных. Обновить сервер с 3.1.2.3 на 300.
- Лишний текст в окне инсталлятора клиента. На этапе инсталляции продукта, в окне установки клиента, отображается слово progress.
- Отсутствие обновления списка устройств подчиненного сервера при изменении группы пользователя.
- Консоль. Ошибки при добавлении нового сервера.
- Ошибка при добавлении устройства в случае отсутствия модулей.
- Зависание консоли при подключении к подчиненному серверу с удаленным устройством.
- Авторизация. Сообщение об ошибке не поместилось в окно.
- Внешний вид. Отсутствует заголовок у окна ошибки.
- Невозможно добавить устройство из списка результатов сканирования сети.
- Некорректный выбор типов при создании нового отчета.
- Наложение текста при небольшом размере окна консоли при входе.
- Консоль. Английская локализация. Ошибки\неточности\комментарии по переводу.
- Опечатка на вкладке "Мониторинг".
- Отсутствуют названия отчетов в уведомлениях о нарушении целостности.

- Консоль. Английская локализация. Ошибки\неточности\комментарии по переводу.
- Некорректная проверка версионности парсера модулей позволяет добавить неподдерживаемые модули в старые версии сервера.
- Модули виртуализации. Не все типы устройств доступны для создания новой проверки.
- Модули виртуализации. vCenter v1, Hyper-V v1. Ошибки\неточности\примечания.
- Выпадающий список выбора подчиненного сервера отображается по-разному.
- Профилирование нагрузки при проверке большего количества устройств.
- Иерархия. После запуска управляющего сервера не выводятся устройства с отключённых серверов.
- Отсутствует кнопка «Обновить все модули» пока не обновлен хотя бы один модуль.
- Не загружается отчет «Вложенные устройства» на SCVMM 2008 R2.
- У отчета Windows-драйверы фильтр от отчета Windows-службы.
- У модуля vCenter v. 1 история изменений от v. 8
- Отсутствует история изменений модуля Hyper-V
- Модуль vCenter v. 1. Исполняемые файлы модуля не совпадают по имени.
- Клиент Windows не прошел проверку после обновления. Остановка службы.
- Не работает резервирование серверов.
- Отсутствие индикации режима, подчиненного в пассивном режиме для новых добавленных устройств.
- Ошибки загрузки отчета «Cisco IOS running-startup difference» после обновления
- Не работает миграция базы данных.
- Ошибка переноса БД на postgres с учетной записью на встроенного администратора.
- Вкладка Устройства перестает работать если в строку поиска ввести знак «\».
- Ошибки при открытии удаленного пользовательского отчета из архива.
- Отсутствия ограничения длинны имени пользователя
- Присутствия предустановленного поля в модуле Cisco UCM
- Ошибка загрузки отчетов SCVMM 2012 при наличии хостов ESXi
- Предупреждение об отличии версии схемы БД при создании новой БД
- Множественные опечатки в историях изменений модулей
- Устранение проблемы со шрифтами и отступами в справке.
- Ошибка определения приглашения (HP Procurve)
- Ошибка подключения по telnet (3Com)
- Нет обработки Cisco UCM.
- Ошибки при включении модулей
- Многократное сообщение об ошибке при добавлении подчиненного сервера
- Отсутствие описания изменений модуля Windows для версии 23.
- Отчет «Уязвимости Windows». Для каждой уязвимости текст описания повторяется дважды.

- Множественные ошибки при использовании профилей после обновлений 3.1.23 cent.
- Ошибка при загрузке отчетов Cisco UCM 11.
- Отсутствует описание изменений модуля Cisco UCM для версии 30.
- Миграция. Ошибка миграции с MySQL на Postgres.
- Ошибки в консоли после неудачной попытки установки текущих модулей Hyper-V и vCenter параллельно с устаревшими.
- Текст сообщения дублируется на английском в отправляемых письмах.
- Непонятный тип сообщения об ошибке из-за отсутствия библиотек UCM API 4.0 Runtime при отправке сообщений через Lynk.
- Для устройств Windows имя интерфейсов дублируется в 16-ричном виде в отчете "Интерфейсы (SNMP)".
- Отключенный сетевой интерфейс исчезает из отчета "Интерфейсы (SNMP)".
- Ошибка загрузки сертификатов агентом в режиме read only.
- Читаемое сообщение об ошибке при ошибке загрузки событий агентом.