UserGate Log Analyzer 6

Руководство администратора

Оглавление

1 ВВЕДЕНИЕ

UserGate Log Analyzer (UserGate LogAn, LogAn) - это вспомогательный компонент для универсального шлюза UserGate, с помощью которого администратор может выполнить следующие задачи:

- Уменьшить нагрузку на шлюз, переложив обработку журналов, создание отчетов и процессинг других статистических данных на внешний сервер LogAn, обеспечив таким образом больше ресурсов для выполнения шлюзом задач защиты и фильтрации.
- Объединить журналы с нескольких шлюзов UserGate для общего анализа.
- Увеличить глубину журналирования за счет большего размера хранилища на серверах LogAn.
- Собирать по SNMP и анализировать информацию со сторонних устройств.

LogAn поставляется в виде программно-аппаратного комплекса (ПАК, appliance) либо в виде образа виртуальной машины (virtual appliance), предназначенного для развертывания в виртуальной среде.

2 ЛИЦЕНЗИРОВАНИЕ USERGATE LOGAN

UserGate LogAn лицензируется по количеству настроенных сенсоров, с которых он собирает информацию. В качестве сенсора может выступать шлюз UserGate, либо любое другое устройство, которое может отправлять информацию по протоколу SNMP на сервер LogAn.

Лицензия на UserGate LogAn дает право бессрочного пользования продуктом.

Дополнительно лицензируются следующие модули:

Наименование	Описание
Модуль Security Update (SU)	Модуль SU дает право на получение: • обновлений ПО UserGate LogAn. • технической поддержки. Модуль выписывается на 1 год, по истечении данного срока для получения обновлений ПО и технической поддержки необходимо приобрести продление лицензии.
Сенсоры	Данный модуль определяет количество сенсоров, с которых LogAn может собирать информацию. Данный модуль выписывается сроком на 1 год и требует ежегодного продления.

Для регистрации продукта необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Перейти в Дашборд	Нажать на пиктограмму **Дашборд** в правом верхнем углу.
Шаг 2. В разделе **Лицензия** зарегистрировать продукт	В разделе **Лицензия** нажать на ссылку **Нет лицензии**, ввести ПИН-код и заполнить регистрационную форму.

Посмотреть статус установленной лицензии можно в разделе **Дашборд** в виджете **Лицензия**.

3 ПЕРВОНАЧАЛЬНАЯ НАСТРОЙКА

UserGate LogAn поставляется в виде программно-аппаратного комплекса (ПАК, appliance) либо в виде образа виртуальной машины (virtual appliance), предназначенного для развертывания в виртуальной среде. В случае виртуальной машины UserGate LogAn поставляется с двумя Ethernet-интерфейсами. В случае поставки в виде ПАК UserGate LogAn может содержать 8 или более Ethernet-портов.

3.1 Развертывание программно-аппаратного комплекса

В случае поставки решения в виде ПАК, программное обеспечение уже загружено и готово к первоначальной настройке. Перейдите к главе Подключение к UserGate LogAn для дальнейшей настройки.

3.2 Развертывание виртуального образа

UserGate LogAn Virtual Appliance позволяет быстро развернуть виртуальную машину, с уже настроенными компонентами. Образ предоставляется в формате OVF (Open Virtualization Format), который поддерживают такие вендоры как VMWare, Oracle VirtualBox. Для Microsoft Hyper-v и KVM поставляются образы дисков виртуальной машины.

Примечание

Для корректной работы виртуальной машины рекомендуется использовать минимум 8 Гб оперативной памяти и 2-ядерный виртуальный процессор. Гипервизор должен поддерживать работу 64-битных операционных систем.

Для начала работы с виртуальным образом, выполните следующие шаги:

Наименование	Описание
Шаг 1. Скачайте образ и распакуйте	Скачайте последнюю версию виртуального образа с официального сайта https://www.usergate.com/ru.
Шаг 2. Импортируйте образ в свою систему виртуализации	Инструкцию по импорту образа вы можете посмотреть на сайтах VirtualBox и VMWare. Для Microsoft Hyper-v и KVM необходимо создать виртуальную машину и указать в качестве диска скачанный образ, **после чего отключить службы интеграции** в настройках созданной виртуальной машины.
Шаг 3. Настройте параметры виртуальной машины	Увеличьте размер оперативной памяти виртуальной машины. Используя свойства виртуальной машины, установите минимум 8Gb.
Шаг 4. Важно! Увеличьте размер диска виртуальной машины	Размер диска по умолчанию составляет 100Gb, что обычно недостаточно для хранения всех журналов и настроек. Используя свойства виртуальной машины, установите размер диска в 300Gb или более. Рекомендованный размер - 1000Gb или более.

Шаг 5. Настройте виртуальные сети	UserGate LogAn поставляется с двумя интерфейсами, назначенными в зоны: • **Management** - первый интерфейс виртуальной машины. • **Trusted** - второй интерфейс виртуальной машины.
Шаг 6. Выполните сброс к заводским настройкам	Запустите виртуальную машину UserGate Log Analyzer. Во время загрузки выберите **Support Tools** и выполните **Factory reset**. **Этот шаг крайне важен**. Во время этого шага настраивает сетевые адаптеры и увеличивает размер раздела на жестком диске до полного размера диска, увеличенного в 4-м пункте.

3.3 Подключение к UserGate LogAn

Интерфейс port0 настроен на получение IP-адреса в автоматическом режиме (DHCP) и назначен в зону **Management**. Первоначальная настройка осуществляется через подключение администратора к веб-консоли через интерфейс port0.

Если нет возможности назначить адрес для Management-интерфейса в автоматическом режиме с помощью DHCP, то его можно явно задать, используя CLI (Command Line Interface). Более подробно об использовании CLI смотрите в главе Интерфейс командной строки (CLI).

Остальные интерфейсы отключены и требуют последующей настройки.

Первоначальная настройка требует выполнения следующих шагов:

Наименование	Описание
Шаг 1. Подключиться к интерфейсу управления	**При наличии DHCP-сервера** Подключить интерфейс port0 в сеть предприятия с работающим DHCP-сервером. Включить UserGate LogAn. После загрузки UserGate LogAn укажет IP-адрес, на который необходимо подключиться для дальнейшей активации продукта. **Статический IP-адрес** Включить UserGate LogAn. Используя CLI (Command Line Interface), назначить необходимый IP-адрес на интерфейс port0. Детали использования CLI смотрите в главе Интерфейс командной строки (CLI)**.** Подключиться к веб-консоли UserGate LogAn по указанному адресу, он должен выглядеть примерно следующим образом: https://UserGate_LogAn_IP_address:8010.
Шаг 2. Выбрать язык	Выбрать язык, на котором будет продолжена первоначальная настройка.
Шаг 3. Задать пароль	Задать логин и пароль для входа в веб-интерфейс управления.
Шаг 4. Зарегистрировать систему	Ввести ПИН-код для активации продукта и заполнить регистрационную форму. Для активации системы необходим доступ UserGate LogAn в интернет. Если на данном этапе выполнить регистрацию не удается, то ее следует повторить после настройки сетевых интерфейсов на шаге 8.
Шаг 5. Настроить зоны, IP-адреса интерфейсов,	В разделе **Интерфейсы** включить необходимые интерфейсы, установить корректные IP-адреса, соответствующие вашим сетям, и назначить интерфейсы соответствующим

подключить UserGate LogAn в сеть предприятия	зонам. Подробно об управлении интерфейсами читайте в главе Настройка интерфейсов. Система поставляется с предопределенными зонами: • Зона Management (сеть управления), интерфейс port0. • Зона Trusted (LAN). Предполагается, что через зону Trusted LogAn будет подключен в сеть, через которую шлюзы UserGate будут отсылать на него журналы, а также через которую LogAn получит доступ в интернет. Для работы UserGate LogAn достаточно одного настроенного интерфейса. Разделение функций управления устройством и сбора данных на разные сетевые интерфейсы рекомендовано для обеспечения безопасности, но не является жестким требованием.
Шаг 6. Настроить шлюз в интернет	В разделе **Шлюзы** указать IP-адрес шлюза в интернет на интерфейсе, имеющим доступ в интернет, как правило, это зона **Trusted**. Подробно о настройке шлюзов в интернет читайте в главе Настройка шлюзов.
Шаг 7. Указать системные DNS-серверы	В разделе **DNS** укажите IP-адреса серверов DNS, вашего провайдера или серверов, используемых в вашей организации. Подробно об управлении DNS читайте в главе Общие настройки.
Шаг 8. Зарегистрировать продукт (если не был зарегистрирован на шаге 4)	Зарегистрировать продукт с помощью ПИН-кода. Для успешной регистрации необходимо подключение к интернету и выполнение предыдущих шагов. Более подробно о лицензировании продукта читайте в главе Лицензирование UserGate LogAn.
Шаг 9. Подключить шлюзы UserGate для сбора и анализа журналов	В разделе **Сенсоры --> Сенсоры UserGate** добавить существующие сервера UserGate.
Шаг 10. Создать дополнительных администраторов (опционально)	В разделе **Администраторы** создать дополнительных администраторов системы, наделить их необходимыми полномочиями (ролями).

После выполнения вышеперечисленных действий UserGate LogAn готов к работе. Для более детальной настройки обратитесь к необходимым главам справочного руководства.

4 НАСТРОЙКА USERGATE LOGAN

4.1 Общие настройки

Раздел **Общие настройки** определяет базовые установки UserGate LogAn:

Наименование	Описание
Часовой пояс	Часовой пояс, соответствующий вашему местоположению. Часовой пояс используется в расписаниях, применяемых в правилах, а также для корректного отображения времени и даты в отчетах, журналах и т.п.
Язык интерфейса по умолчанию	Язык, который будет использоваться по умолчанию в консоли.
Настройка времени сервера	Настройка параметров установки точного времени. **Использовать NTP –** использовать сервера NTP из указанного списка для синхронизации времени. **Основной сервер NTP** – адрес основного сервера точного времени. Значение по умолчанию - pool.ntp.org **Запасной сервер NTP** – адрес запасного сервера точного времени. **Время на сервере** – позволяет установить время на сервере. Время должно быть указано в часовом поясе UTC.
Системные DNS-серверы	Укажите корректные IP-адреса серверов DNS.
Состояние Log Analyzer	Отображается текущее состояние сервера Log Analyzer: • **Состояние** – показывает текущее состояние сервиса статистики. • **Версия устройства** – версия UserGate Log Analyzer.

4.2 Управление устройством

Раздел **Управление устройством** определяет следующие установки UserGate LogAn:

- Настройки диагностики.
- Операции с сервером.
- Экспорт настроек..

4.2.1 Диагностика

В данном разделе задаются параметры диагностики сервера, необходимые службе технической поддержки UserGate при решении возможных проблем.

Наименование	Описание
Детализация диагностики	• **Off** - ведение журналов диагностики отключено. • **Error** - журналировать только ошибки работы сервера. • **Warning** - журналировать только ошибки и предупреждения. • **Info** - журналировать только ошибки, предупреждения и дополнительную информацию. • **Debug** - максимум детализации. Рекомендуется установить значение параметра **Детализация диагностики** в **Error** (только ошибки) или **Off** (Отключено), если техническая поддержка UserGate не попросила вас установить иные значения. Любые значения, отличные от Error (только ошибки) или Off (Отключено), негативно влияют на производительность UserGate LogAn.
Журналы диагностики	• **Скачать журналы** - скачать диагностические журналы для передачи их в службу поддержки UserGate. • **Очистить журналы** - очистить содержимое журналов.
Удаленный помощник	• **Включено/Отключено** - включение/отключение режима удаленного помощника. Удаленный помощник позволяет инженеру технической поддержки UserGate, зная значения идентификатора и токена удаленного помощника, произвести безопасное подключение к серверу UserGate LogAn для диагностики и решения проблем. Для успешной активации удаленного помощника ЦК UserGate должен иметь доступ к серверу удаленного помощника компании UserGate по протоколу SSH. • **Идентификатор удаленного помощника** - полученное случайным образом значение. Уникально для каждого включения удаленного помощника. • **Токен удаленного помощника** - полученное случайным образом значение токена. Уникально для каждого включения удаленного помощника.

4.2.2 Операции с сервером

Данный раздел позволяет произвести следующие операции с сервером:

Наименование	Описание
Операции с сервером	• **Перезагрузить** - перезагрузка сервера UserGate LogAn. • **Выключить** - выключение сервера UserGate LogAn.
Обновления	Выбор канала обновлений ПО UserGate LogAn: • **Стабильные** - проверка наличия стабильных обновлений ПО. • **Бета** - проверка наличия экспериментальных обновлений.

Компания UserGate постоянно работает над улучшением качества своего программного обеспечения и предлагает обновления продукта UserGate LogAn в рамках подписки на модуль лицензии Security Update (подробно о лицензировании смотрите в разделе Лицензирование UserGate LogAn). При наличии обновлений в разделе **Управление продуктом** отобразится соответствующее оповещение. Обновление

продукта может занять довольно длительное время, рекомендуется планировать установку обновлений с учетом возможного времени простоя UserGate LogAn.

Для установки обновлений необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Создать файл резервного копирования	Создать резервную копию состояния UserGate LogAn. Данный шаг рекомендуется всегда выполнять перед применением обновлений, поскольку он позволит восстановить предыдущее состояние устройства в случае возникновения каких-либо проблем во время применения обновлений.
Шаг 2. Установить обновления	В разделе **Управление устройством** при наличии оповещения **Доступны новые обновления** нажать на ссылку **Установить сейчас**. Система установит скачанные обновления, по окончании установки UserGate LogAn будет перезагружен.

4.2.3 Экспорт настроек

Администратор имеет возможность сохранить текущие настройки UserGate LogAn в файл и впоследствии восстановить эти настройки на этом же или другом сервере UserGate LogAn. В отличие от резервного копирования, экспорт/импорт настроек не сохраняет текущее состояние всех компонентов комплекса, сохраняются только текущие настройки.

Примечание

Экспорт/импорт настроек не восстанавливает состояние интерфейсов и информацию о лицензии. После окончания процедуры импорта необходимо повторно зарегистрировать UserGate LogAn с помощью имеющегося ПИН-кода и настроить интерфейсы.

Для экспорта настроек необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Экспорт настроек	В разделе **Управление устройством --> Экспорт настроек** нажмите **Экспорт** и выберите **Экспортировать все настройки** или **Экспортировать сетевые настройки**. Система сохранит: • текущие настройки сервера под именем: logan_core-logan_core@nodename_version_YYYYMMDD_HHMMSS.bin • сетевые настройки под именем: network-logan_core-logan_core@nodename_version_YYYYMMDD_HHMMSS.bin nodename – имя узла UserGate LogAn. version – версия UserGate LogAn. YYYYMMDD_HHMMSS – дата и время выгрузки настроек в часовом поясе UTC. Например, logan_core-logan_core@ranreahattha_6.1.8.13494RS-1_20211227_091350.bin или network-logan_core-logan_core@ranreahattha_6.1.8.13494RS-1_20211227_091407.bin.

Для применения созданных ранее настроек необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Импорт настроек	В разделе **Управление устройством** нажать на ссылку **Экспорт настроек --> Импорт** и указать путь к ранее созданному файлу настроек. Указанные настройки применятся к серверу, после чего сервер будет перезагружен.

Дополнительно администратор может настроить сохранение настроек на внешние серверы (FTP, SSH) по расписанию. Для создания расписания выгрузки настроек необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Создать правило экспорта	В разделе **Управление устройством --> Экспорт настроек** нажать кнопку **Добавить**, указать имя и описание правила.
Шаг 2. Указать параметры удаленного сервера	Во вкладке правила **Удаленный сервер** указать параметры удаленного сервера: • **Тип сервера** - FTP или SSH. • **Адрес сервера** - IP-адрес сервера. • **Порт** - порт сервера. • **Логин** - учетная запись на удаленном сервере. • **Пароль/Подтверждение пароля** - пароль учетной записи. • **Путь на сервере** - путь на сервере, куда будут выгружены настройки.
Шаг 3. Выбрать расписание выгрузки	Во вкладке правила **Расписание** указать необходимое время отправки настроек. В случае задания времени в CRONTAB-формате, задайте его в следующем виде: (минуты:0-59) (часы:0-23) (дни месяца:0-31) (месяц:0-12) (день недели:0-6, 0-воскресенье) Каждое из первых пяти полей может быть задано следующим образом: • Звездочка (*)- обозначает весь диапазон (от первого до последнего); • Дефис (-) - обозначает диапазон чисел. Например, "5-7" будет означать 5,6 и 7; • Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23"; • Звездочка и тире используются для пропусков в диапазонах. Шаг указывается после косой черты. Например, "2-10/2" будет значить "2,4,6,8,10", а выражение "*/2" в поле "часы" будет означать "каждые два часа.

4.3 Администраторы

Доступ к веб-консоли UserGate LogAn регулируется с помощью создания дополнительных учетных записей администраторов, назначения им профилей доступа, создания политики управления паролями администраторов и настройки доступа к веб-консоли на уровне разрешения сервиса в свойствах зоны сети.

Примечание

При первоначальной настройке UserGate LogAn создается локальный суперпользователь Admin.

Для создания дополнительных учетных записей администраторов устройства необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Создать профиль доступа администратора	В разделе **Администраторы --> Профили администраторов** нажать кнопку **Добавить** и указать необходимые настройки.
Шаг 2. Создать учетную запись администратора и назначить ей один из созданных ранее профилей администратора	В разделе **Администраторы** нажать кнопку **Добавить** и выбрать необходимый вариант: • **Добавить локального администратора** - создать локального пользователя, задать ему пароль доступа и назначить созданный ранее профиль доступа. • **Добавить пользователя LDAP** - добавить пользователя из существующего домена. Для этого должен быть корректно настроен LDAP-коннектор в разделе **Серверы аутентификации**. При входе в консоль администрирования необходимо указывать имя пользователя в формате user@domain. Назначить созданный ранее профиль. • **Добавить группу LDAP** - добавить группу пользователей из существующего домена. Для этого должен быть корректно настроен LDAP-коннектор в разделе **Серверы аутентификации**. При входе в консоль администрирования необходимо указывать имя пользователя в формате user@domain. Назначить созданный ранее профиль.

При создании профиля доступа администратора необходимо указать следующие параметры:

Наименование	Описание
Название	Название профиля.
Описание	Описание профиля.
Разрешения для API	Список объектов, доступных для делегирования доступа при работе через программный интерфейс (API). Объекты описаны документации API. В качестве доступа можно указать: • Нет доступа. • Чтение. • Чтение и запись.
Разрешения для веб-консоли	Список объектов дерева веб-консоли, доступных для делегирования. В качестве доступа можно указать: • Нет доступа. • Чтение.

	• Чтение и запись.
Разрешения для CLI	Позволяет разрешить доступ к CLI. В качестве доступа можно указать: • Нет доступа. • Чтение. • Чтение и запись.

Администратор UserGate LogAn может настроить дополнительные параметры защиты учетных записей администраторов, такие, как сложность пароля и блокировку учетной записи на определенное время при превышении количества неудачных попыток аутентификации.

Для настройки этих параметров необходимо:

Наименование	Описание
Шаг 1. Настроить политику паролей	В разделе **Администраторы --> Администраторы** нажать кнопку **Настроить**
Шаг 2. Заполнить необходимые поля	Указать значения следующих полей: • **Сложный пароль** - включает дополнительные параметры сложности пароля, задаваемые ниже, такие как - минимальная длина, минимальное число символов в верхнем регистре, минимальное число символов в нижнем регистре, минимальное число цифр, минимальное число специальных символов, максимальная длина блока из одного и того же символа. • **Число неверных попыток аутентификации** - количество неудачных попыток аутентификации администратора, после которых учетная запись заблокируется на **Время блокировки**. • **Время блокировки** - время, на которое блокируется учетная запись.

В разделе **Администраторы --> Сессии администраторов** отображаются все администраторы, выполнившие вход в веб-консоль администрирования UserGate LogAn. При необходимости любую из сессий администраторов можно сбросить (закрыть).

Администратор может указать зоны, с которых будет возможен доступ к сервису веб-консоли (порт TCP 8010).

Примечание

Не рекомендуется разрешать доступ к веб-консоли для зон, подключенных к неконтролируемым сетям, например, к сети интернет.

Для разрешения сервиса веб-консоли для определенной зоны необходимо в свойствах зоны в разделе контроль доступа разрешить доступ к сервису **Консоль администрирования**. Более подробно о настройке контроля доступа к зонам можно прочитать в разделе Настройка зон.

4.4 Управление сертификатами

UserGate LogAn использует защищенный протокол HTTPS для управления устройством. Для выполнения данной функции UserGate LogAn использует сертификат типа **SSL веб-консоли**.

Для того чтобы создать новый сертификат, необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Создать сертификат	Нажать на кнопку **Создать** в разделе **Сертификаты**.
Шаг 2. Заполнить необходимые поля	Указать значения следующих полей: • **Название** - название сертификата, под которым он будет отображен в списке сертификатов. • **Описание** - описание сертификата. • **Страна** - страна, в которой выписывается сертификат. • **Область или штат** - область или штат, в котором выписывается сертификат. • **Город** - город, в котором выписывается сертификат. • **Название организации** - название организации, для которой выписывается сертификат. • **Common name** - имя сертификата. Рекомендуется использовать только символы латинского алфавита для совместимости с большинством браузеров. • **E-mail** - e-mail вашей компании.
Шаг 3. Указать, для чего будет использован данный сертификат	После создания сертификата необходимо указать его роль в UserGate LogAn. Для этого необходимо выделить необходимый сертификат в списке сертификатов, нажать на кнопку **Редактировать** и указать тип сертификата - SSL веб-консоли. После этого UserGate LogAn перезагрузит сервис веб-консоли и предложит вам подключиться уже с использованием нового сертификата.

UserGate LogAn позволяет экспортировать созданные сертификаты и импортировать сертификаты, созданные на других системах, например, сертификат, выписанный доверенным удостоверяющим центром вашей организации.

Для экспорта сертификата необходимо:

Наименование	Описание
Шаг 1. Выбрать сертификат для экспорта	Выделить необходимый сертификат в списке сертификатов.
Шаг 2. Экспортировать сертификат	Выбрать тип экспорта: • **Экспорт сертификата** - экспортирует данные сертификата в der-формате без экспортирования приватного ключа сертификата. Используйте файл, полученный в результате экспорта сертификата для инспектирования SSL, для установки его в качестве локального удостоверяющего центра на компьютеры пользователей. • **Экспорт CSR** - экспортирует CSR сертификата, например, для подписи его

	удостоверяющим центром.

Примечание

Рекомендуется сохранять сертификат для возможности его последующего восстановления.

Примечание

В целях безопасности UserGate LogAn не разрешает экспорт приватных ключей сертификатов.

Для импорта сертификата необходимо иметь файлы сертификата и - опционально - приватного ключа сертификата и выполнить следующие действия:

Наименование	Описание
Шаг 1. Начать импорт	Нажать на кнопку **Импорт**.
Шаг 2. Заполнить необходимые поля	Указать значения следующих полей: • Название - название сертификата, под которым он будет отображен в списке сертификатов. • Описание - описание сертификата. • Загрузите файл, содержащий данные сертификата. • Загрузите файл, содержащий приватный ключ сертификата. • Пароль для приватного ключа, если таковой требуется. • Цепочка сертификатов – файл, содержащий сертификаты вышестоящих центров сертификации, которые участвовали в создании сертификата. Необязательное поле.

4.5 Профили оповещений

Профиль оповещения указывает транспорт, с помощью которого оповещения могут быть доставлены получателям. Поддерживается 2 типа транспорта:

- SMTP, доставка сообщений с помощью e-mail.
- SMPP, доставка сообщений с помощью SMS практически через любого оператора сотовой связи или через большое количество SMS-центров рассылки.

Для создания профиля сообщений SMTP необходимо нажать на кнопку **Добавить** в разделе **Профили оповещений**, выбрать вариант **Добавить профиль оповещения SMTP** и заполнить необходимые поля:

Наименование	Описание
Название	Название профиля.
Описание	Описание профиля.
Хост	IP-адрес сервера SMTP, который будет использоваться для отсылки почтовых сообщений.
Порт	Порт TCP, используемый сервером SMTP. Обычно для протокола SMTP используется порт 25, для SMTP с использованием SSL - 465. Уточните данное значение у администратора почтового сервера.
Безопасность	Варианты безопасности отправки почты, возможны варианты: Нет, STARTTLS, SSL.
Аутентификация	Включает аутентификацию при подключении к SMTP-серверу.
Логин	Имя учетной записи для подключения к SMTP-серверу.
Пароль	Пароль учетной записи для подключения к SMTP-серверу.

Для создания профиля сообщений SMPP необходимо нажать на кнопку **Добавить** в разделе **Профили оповещений**, выбрать вариант **Добавить профиль оповещения SMPP** и заполнить необходимые поля:

Наименование	Описание
Название	Название профиля.
Описание	Описание профиля.
Хост	IP-адрес сервера SMPP, который будет использоваться для отсылки SMS сообщений.
Порт	Порт TCP, используемый сервером SMPP. Обычно для протокола SMPP используется порт 2775, для SMPP с использованием SSL – 3550.
SSL	Использовать или нет шифрацию с помощью SSL.
Логин	Имя учетной записи для подключения к SMPP-серверу.
Пароль	Пароль учетной записи для подключения к SMPP-серверу.
Правила трансляции номеров	В некоторых случаях SMPP-провайдер ожидает номер телефона в определенном формате, например, в виде 89123456789. Для соответствия требованиям провайдера можно указать замену первых символов номеров с одних на другие. Например, заменить все номера, начинающиеся на +7, на 8.

4.6 Серверы аутентификации

Серверы аутентификации - это внешние источники учетных записей пользователей для авторизации в веб-консоли управления LogAn. LogAn поддерживает только сервер аутентификации LDAP-коннектор. LDAP-коннектор позволяет:

- Получать информацию о пользователях и группах Active Directory или других LDAP-серверов. Поддерживается работа с LDAP-сервером FreeIPA.
- Осуществлять авторизацию пользователей через домены Active Directory/FreeIPA.

Для создания LDAP-коннектора необходимо нажать на кнопку **Добавить**, выбрать **Добавить LDAP-коннектор** и указать следующие параметры:

Наименование	Описание
Включено	Включает или отключает использование данного сервера аутентификации.
Название	Название сервера аутентификации.
SSL	Определяет, требуется ли SSL-соединение для подключения к LDAP-серверу.
Доменное имя LDAP или IP-адрес	IP-адрес контроллера домена, FQDN контроллера домена или FQDN домена (например, test.local). Если указан FQDN, то UserGate получит адрес контроллера домена с помощью DNS-запроса. Если указан FQDN домена, то при отключении основного контроллера домена, UserGate будет использовать резервный.
Bind DN («login»)	Имя пользователя, которое необходимо использовать для подключения к серверу LDAP. Имя необходимо использовать в формате DOMAIN\username или username@domain. Данный пользователь уже должен быть заведен в домене.
Пароль	Пароль пользователя для подключения к домену.
Домены LDAP	Список доменов, которые обслуживаются указанным контроллером домена, например, в случае дерева доменов или леса доменов Active Directory.
Пути поиска	Список путей в сервере LDAP, начиная с которых система будет осуществлять поиск пользователей и групп. Необходимо указывать полное имя, например, ou=Office,dc=example,dc=com.

После создания сервера необходимо проверить корректность параметров, нажав на кнопку **Проверить соединение**. Если параметры указаны верно, система сообщит об этом либо укажет на причину невозможности соединения.

Настройка LDAP-коннектора завершена.

5 ОФЛАЙН ОПЕРАЦИИ С СЕРВЕРОМ

Некоторые операции с сервером проводятся, когда сервер не выполняет свою функцию и находится в офлайн режиме. Для выполнения таких операций необходимо во время загрузки сервера выбрать раздел меню **Support menu** и затем одну из требуемых операций. Для получения доступа к этому меню необходимо подключить монитор к разъему VGA(HDMI), клавиатуру к разъему USB (при наличии соответствующих разъемов на устройстве) или используя специальный кабель для последовательного порта или переходник USB-Serial, подключить свой компьютер к UserGate LogAn. Запустить терминал, позволяющий подключение через последовательный порт, например, Putty для Windows. Установить подключение через последовательный порт, указав параметры подключения 115200 8n1.

Во время загрузки администратор может выбрать один из нескольких пунктов загрузки в boot-меню:

Наименование	Описание
1. UserGate LogAn (serial console)	Загрузка UserGate LogAn с выводом диагностической информации о загрузке в последовательный порт.
2. UserGate LogAn (verbouse mode)	Загрузка UserGate LogAn с выводом диагностической информации о загрузке в консоль tty1 (монитор).
3. Support menu	Войти в раздел системных утилит с выводом информации в консоль tty1 (монитор).
4. Support menu (serial console)	Войти в раздел системных утилит с выводом информации в последовательный порт. При подключении через последовательный порт загрузочное меню не отображается. Для выбора раздела **Support menu** необходимо во время загрузки нажимать клавишу “**4**“. Для выбора одного из пунктов меню в разделе **Support menu** необходимо нажать клавишу, соответствующую первой букве названия пункта меню, например, для выбора **Restore backup,** необходимо нажать клавишу “**R**”, затем клавишу “**Ввод**”.
5. Memory test	Запуск проверки оперативной памяти устройства.

Раздел системных утилит (Support menu) позволяет выполнить следующие действия:

Наименование	Описание
Check filesystems	Запуск проверки файловой системы устройства на наличие ошибок и их автоматическое исправление.
Clear logs	Очистка диагностических журналов для освобождения пространства на системном разделе. Журналы UserGate LogAn не очищаются (журналы веб-доступа, трафика, событий, СОВ и т.п.).
Export logs	Выгрузка диагностических журналов на внешний USB носитель. Все данные на внешнем носителе будут удалены.
Expand log partition	Увеличение раздела для журналов на весь выделенный диск. Эта операция обычно используется после увеличения дискового пространства, выделенного гипервизором для виртуальной машины UserGate LogAn. Данные и настройки UserGate LogAn не сбрасываются.

Backup full	Создать полную копию диска UserGate LogAn на внешний USB носитель. Все данные на внешнем носителе будут удалены.
Backup system only	Создать копию системного раздела UserGate LogAn, исключая журналы (журналы веб-доступа, трафика, событий, СОВ и т.п.) на внешний USB носитель. Все данные на внешнем носителе будут удалены.
Restore from backup	Восстановление UserGate LogAn с внешнего USB носителя.
Update from USB	Установка обновления ПО UserGate LogAn с внешнего USB носителя. Обновление должно быть скопировано в корень съемного диска, диск должен иметь формат NTFS или FAT32. Название файла обновления должно быть в следующем формате: **update_xxxxx** (где xxxxx – номер версии).
Refresh NIC names	Упорядочивание имен сетевых портов в необходимом порядке. Упорядочивание производится в соответствии с номером порта на шине PCI. Эту операцию необходимо выполнять после добавления сетевых портов в настроенный аплаенс UserGate LogAn, например, после установки дополнительной сетевой карты в физический аплаенс или после добавления портов в виртуальный аплаенс. Данные и настройки UserGate LogAn не сбрасываются.
Factory reset	Сброс состояния UserGate LogAn к первоначальному состоянию системы. Все данные и настройки будут утеряны.
Exit	Выход и перезагрузка устройства.

6 НАСТРОЙКА СЕТИ

В данном разделе описаны сетевые настройки UserGate LogAn.

6.1 Настройка зон

Зона в UserGate LogAn - это логическое объединение сетевых интерфейсов. Политики безопасности UserGate LogAn используют зоны интерфейсов, а не непосредственно интерфейсы.

Рекомендуется объединять интерфейсы в зоне на основе их функционального назначения, например, зона LAN-интерфейсов, зона интернет-интерфейсов, зона интерфейсов управления.

По умолчанию UserGate LogAn поставляется со следующими зонами:

Наименование	Описание
Management	Зона для подключения доверенных сетей, из которых разрешено управление UserGate LogAn.
Trusted	Зона для подключения доверенных сетей, например, LAN-сетей. Предполагается, что через зону Trusted LogAn будет подключен в сеть, через которую межсетевые экраны UserGate будут отсылать на него журналы, а также через которую LogAn получит доступ в Интернет.

Для работы UserGate LogAn достаточно одного настроенного интерфейса. Разделение функций управления устройством и сбора данных на разные сетевые интерфейсы рекомендовано для обеспечения безопасности, но не является жестким требованием.

Администраторы UserGate LogAn могут изменять настройки зон, созданных по умолчанию, а также создавать дополнительные зоны.

Примечание

Можно создать не более 255 зон.

Для создания зоны необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Создать зону	Нажать на кнопку **Добавить** и дать название зоне.
Шаг 2. Настроить параметры защиты зоны от DoS (опционально)	Указать параметры защиты зоны от сетевого флуда для протоколов TCP (SYN-flood), UDP, ICMP: • **Порог уведомления** - при превышении количества запросов с одного IP-адреса над указанным значением происходит запись события в системный журнал. • **Порог отбрасывания пакетов** - при превышении количества запросов с одного IP-адреса над указанным значением UserGate LogAn начинает

	отбрасывать пакеты, поступившие с этого IP-адреса, и записывает данное событие в системный журнал. Рекомендованные значения для порога уведомления - 300 запросов в секунду, для порога отбрасывания пакетов - 600 запросов в секунду. **Исключения защиты от DoS** - позволяет указать список IP-адресов серверов, которые необходимо исключить из защиты. Это может быть полезно, например, для шлюзов UserGate, которые могут слать большой объем данных на сервера LogAn.
Шаг 3. Настроить параметры контроля доступа зоны (опционально)	Указать предоставляемые UserGate LogAn сервисы, которые будут доступны клиентам, подключенным к данной зоне. Для зон, подключенных к неконтролируемым сетям, таким, как интернет, рекомендуется отключить все сервисы. Сервисы: • **Ping** - позволяет пинговать UserGate LogAn. • **SNMP** – доступ UserGate Log Analyzer по протоколу SNMP (UDP 161). • **XML-RPC для управления** – позволяет управлять продуктом по API (TCP 4040). • **Консоль администрирования** - доступ к веб-консоли управления (TCP 8010). • **CLI по SSH** – доступ к серверу для управления им с помощью CLI (command line interface), порт TCP 2200. • **Log Analyzer** – сервис анализатора журналов Log Analyzer. Необходимо разрешить на зонах, с которых LogAn будет получать данные от серверов UserGate (TCP 1269). Подробнее о требованиях сетевой доступности читайте в Приложение 1. Требования к сетевому окружению.
Шаг 4. Настроить параметры защиты от IP-спуфинг атак (опционально)	Атаки на основе IP-спуфинга позволяют передать пакет из одной сети, например, из **Trusted**, в другую, например, в **Management**. Для этого атакующий подменяет IP-адрес источника на предполагаемый адрес необходимой сети. В таком случае ответы на этот пакет будут пересылаться на внутренний адрес. Для защиты от подобных атак администратор может указать диапазоны IP-адресов, адреса источников которых допустимы в выбранной зоне. Сетевые пакеты с адресами источников отличных от указанных будут отброшены. С помощью чекбокса **Инвертировать** администратор может указать адреса источников, которые не могут быть получены на интерфейсах данной зоны. В этом случае будут отброшены пакеты с указанными диапазонами IP-адресов источников. Например, можно указать диапазоны "серых" IP-адресов 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0./16 и включить опцию **Инвертировать**.

6.2 Настройка интерфейсов

Раздел **Интерфейсы** отображает все физические и виртуальные интерфейсы, имеющиеся в системе, позволяет менять их настройки и добавлять VLAN и бонд-интерфейсы.

Кнопка **Редактировать** позволяет изменять параметры сетевого интерфейса:

- Включить или отключить интерфейс.

- Указать тип интерфейса - Layer 3.
- Назначить зону интерфейсу.
- Изменить физические параметры интерфейса - MAC-адрес и размер MTU.
- Выбрать тип присвоения IP-адреса - без адреса, статический IP-адрес или динамический IP-адрес, полученный по DHCP.

Кнопка **Добавить** позволяет добавить следующие типы логических интерфейсов:

- VLAN.
- Бонд.

6.2.1 Объединение интерфейсов в бонд

С помощью кнопки **Добавить бонд-интерфейс** администратор может объединить несколько физических интерфейсов в один логический агрегированный интерфейс для повышения пропускной способности или для отказоустойчивости канала. При создании бонда необходимо указать следующие параметры:

Наименование	Описание
Вкл	Включает бонд.
Название	Название бонда.
Зона	Зона, к которой принадлежит бонд.
Интерфейсы	Один или более интерфейсов, которые будут использованы для построения бонда.
Режим	Режим работы бонда должен совпадать с режимом работы на том устройстве, куда подключается бонд. Может быть: • **Round robin**. Пакеты отправляются последовательно, начиная с первого доступного интерфейса и заканчивая последним. Эта политика применяется для балансировки нагрузки и отказоустойчивости. • **Active backup**. Только один сетевой интерфейс из объединенных будет активным. Другой интерфейс может стать активным только в том случае, когда упадет текущий активный интерфейс. При такой политике MAC-адрес бонд-интерфейса виден снаружи только через один сетевой порт, во избежание появления проблем с коммутатором. Эта политика применяется для отказоустойчивости. • **XOR**. Передача распределяется между сетевыми картами используя формулу: [(«MAC-адрес источника» XOR «MAC-адрес назначения») по модулю «число интерфейсов»]. Получается, одна и та же сетевая карта передает пакеты одним и тем же получателям. Опционально распределение передачи может быть основано и на политике «xmit_hash». Политика XOR применяется для балансировки нагрузки и отказоустойчивости. • **Broadcast**. Передает все на все сетевые интерфейсы. Эта политика применяется для отказоустойчивости. • **IEEE 802.3ad** - режим работы, установленный по умолчанию, поддерживается большинством сетевых коммутаторов. Создаются агрегированные группы сетевых карт с одинаковой скоростью и дуплексом. При таком объединении передача задействует все каналы в активной агрегации согласно стандарту IEEE 802.3ad. Выбор, через какой интерфейс отправлять пакет, определяется политикой; по умолчанию используется XOR-политика, можно также использовать «xmit_hash» политику.

	• **Adaptive transmit load balancing**. Исходящий трафик распределяется в зависимости от загруженности каждой сетевой карты (определяется скоростью загрузки). Не требует дополнительной настройки на коммутаторе. Входящий трафик приходит на текущую сетевую карту. Если она выходит из строя, то другая сетевая карта берет себе MAC-адрес вышедшей из строя карты. • **Adaptive load balancing**. Включает в себя предыдущую политику плюс осуществляет балансировку входящего трафика. Не требует дополнительной настройки на коммутаторе. Балансировка входящего трафика достигается путем ARP-переговоров. Драйвер перехватывает ARP-ответы, отправляемые с локальных сетевых карт наружу, и переписывает MAC-адрес источника на один из уникальных MAC-адресов сетевой карты, участвующей в объединении. Таким образом, различные пиры используют различные MAC-адреса сервера. Балансировка входящего трафика распределяется последовательно (round-robin) между интерфейсами.
MII monitoring period (мсек)	Устанавливает периодичность MII-мониторинга в миллисекундах. Определяет, как часто будет проверяться состояние линии на наличие отказов. Значение по умолчанию - 0 - отключает MII-мониторинг.
Down delay (мсек)	Определяет время (в миллисекундах) задержки перед отключением интерфейса, если произошел сбой соединения. Эта опция действительна только для мониторинга MII (miimon). Значение параметра должно быть кратным значениям miimon. Если оно не кратно, то округлится до ближайшего кратного значения. Значение по умолчанию 0.
Up delay (мсек)	Задает время задержки в миллисекундах, перед тем как поднять канал при обнаружении его восстановления. Этот параметр возможен только при MII-мониторинге (miimon). Значение параметра должно быть кратным значениям miimon. Если оно не кратно, то округлится до ближайшего кратного значения. Значение по умолчанию 0.
LACP rate	Определяет, с каким интервалом будут передаваться партнером LACPDU-пакеты в режиме 802.3ad. Возможные значения: • **Slow** - запрос партнера на передачу LACPDU-пакетов каждые 30 секунд. • **Fast** - запрос партнера на передачу LACPDU-пакетов каждую 1 секунду.
Failover MAC	Определяет, как будут прописываться MAC-адреса на объединенных интерфейсах в режиме active-backup при переключении интерфейсов. Обычным поведением является одинаковый MAC-адрес на всех интерфейсах. Возможные значения: • **Отключено** - устанавливает одинаковый MAC-адрес на всех интерфейсах во время переключения. • **Active** - MAC-адрес на бонд-интерфейсе будет всегда таким же, как на текущем активном интерфейсе. MAC-адреса на резервных интерфейсах не изменяются. MAC-адрес на бонд-интерфейсе меняется во время обработки отказа. • **Follow** - MAC-адрес на бонд-интерфейсе будет таким же, как на первом интерфейсе, добавленном в объединение. На втором и последующем интерфейсе этот MAC не устанавливается, пока они в резервном режиме. MAC-адрес прописывается во время обработки отказа, когда резервный интерфейс становится активным, он принимает новый MAC (тот, что на бонд-интерфейсе), а старому активному интерфейсу прописывается MAC, который был на текущем активном.
Xmit hash policy	Определяет хэш-политику передачи пакетов через объединенные интерфейсы в режиме XOR или

	IEEE 802.3ad. Возможные значения: • **Layer 2** - использует только MAC-адреса для генерации хэша. При этом алгоритме трафик для конкретного сетевого хоста будет отправляться всегда через один и тот же интерфейс. Алгоритм совместим с IEEE 802.3ad. • **Layer 2+3** - использует как MAC-адреса, так и IP-адреса для генерации хэша. Алгоритм совместим с IEEE 802.3ad. • **Layer 3+4** - используются IP-адреса и протоколы транспортного уровня (TCP или UDP) для генерации хэша. Алгоритм не всегда совместим с IEEE 802.3ad, так как в пределах одного и того же TCP- или UDP-взаимодействия могут передаваться как фрагментированные, так и нефрагментированные пакеты. Во фрагментированных пакетах порт источника и порт назначения отсутствуют. В результате в рамках одной сессии пакеты могут дойти до получателя не в том порядке, так как отправляются через разные интерфейсы.
Сеть	Способ присвоения IP-адреса - без адреса, статический IP-адрес или динамический IP-адрес, полученный по DHCP.

6.3 Настройка шлюзов

Для подключения UserGate LogAn к интернету необходимо указать IP-адрес одного или нескольких шлюзов.

Можно указать несколько шлюзов, если для подключения к интернету используется несколько провайдеров. Пример настройки сети с двумя провайдерами:

- Интерфейс port1 с IP-адресом 192.168.11.2 подключен к интернет-провайдеру 1. Для выхода в интернет с этого провайдера необходимо добавить шлюз с IP-адресом 192.168.11.1
- Интерфейс port2 с IP-адресом 192.168.12.2 подключен к интернет-провайдеру 2. Для выхода в интернет с этого провайдера необходимо добавить шлюз с IP-адресом 192.168.12.1

При наличии двух или более шлюзов возможны 2 варианта работы:

Наименование	Описание
Балансировка трафика между шлюзами	Установить флажок **Балансировка** и указать **Вес** каждого шлюза. В этом случае весь трафик в интернет будет распределен между шлюзами в соответствии с указанными весами (чем больше вес, тем большая доля трафика идет через шлюз).
Основной шлюз с переключением на запасной	Выбрать один из шлюзов в качестве основного и настроить **Проверку сети**, нажав на одноименную кнопку в интерфейсе. Проверка сети проверяет доступность хоста в интернет с указанной в настройках периодичностью, и в случае, если хост перестает быть доступен, переводит весь трафик на запасные шлюзы в порядке их расположения в консоли.

По умолчанию проверка доступности сети настроена на работу с публичным DNS-сервером Google (8.8.8.8), но может быть изменена на любой другой хост по желанию администратора.

6.4 Маршруты

Данный раздел позволяет указать маршрут в сеть, доступную за определенным маршрутизатором. Например, в локальной сети может быть маршрутизатор, который объединяет несколько IP-подсетей.

Для добавления маршрута необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Задать название и описание данного маршрута	В разделе **Сеть** выберите в меню **Маршруты**, нажмите кнопку **Добавить**. Укажите имя для данного маршрута. Опционально можно задать описание маршрута.
Шаг 2. Указать адрес назначения	Задайте подсеть, куда будет указывать маршрут, например, 172.16.20.0/24 или 172.16.20.5/32.
Шаг 3. Указать шлюз	Задайте IP-адрес шлюза, через который указанная подсеть будет доступна. Этот IP-адрес должен быть доступен с сервера UserGate LogAn.
Шаг 4. Указать интерфейс	Выберите интерфейс, через который будет добавлен маршрут. Если оставить значение **Автоматически**, то UserGate LogAn сам определит интерфейс, исходя из настроек IP-адресации сетевых интерфейсов.
Шаг 5. Указать метрику	Задайте метрику маршрута. Чем меньше метрика, тем приоритетней маршрут, если маршрутов несколько в данную сеть несколько.

7 ИНТЕРФЕЙС КОМАНДНОЙ СТРОКИ (CLI)

UserGate LogAn позволяет создавать базовые настройки устройства с помощью интерфейса командной строки, или CLI (command line interface). С помощью CLI администратор может выполнить ряд диагностирующих команд, таких, как ping, nslookup, traceroute, осуществить настройку сетевых интерфейсов и зон, а также перезагрузить или выключить устройство.

CLI полезно использовать для диагностики сетевых проблем или в случае, когда доступ к веб-консоли утерян, например, некорректно указан IP-адрес интерфейса или ошибочно установлены параметры контроля доступа для зоны, запрещающие подключение к веб-интерфейсу.

Подключение к CLI можно выполнить через стандартные порты VGA/клавиатуры (при наличии таких портов на оборудовании UserGate LogAn), через последовательный порт или с помощью SSH по сети.

Для подключения к CLI с использованием монитора и клавиатуры необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Подключить монитор и клавиатуру к UserGate LogAn	Подключить монитор к разъему VGA(HDMI), клавиатуру к разъему USB.
Шаг 2. Войти в CLI	Войти в CLI, используя имя и пароль пользователя с правами Full administrator (по умолчанию Admin). Если устройство UserGate LogAn не прошло первоначальную инициализацию, то для доступа к CLI необходимо использовать в качестве имени пользователя Admin, в качестве пароля - utm.

Для подключения к CLI с использованием последовательного порта необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Подключиться к UserGate LogAn	Используя специальный кабель для последовательного порта или переходник USB-Serial, подключить свой компьютер к UserGate LogAn.
Шаг 2. Запустить терминал	Запустить терминал, позволяющий подключение через последовательный порт, например, Putty для Windows или minicom для Linux. Установить подключение через последовательный порт, указав параметры подключения 115200 8n1.
Шаг 3. Войти в CLI	Войти в CLI, используя имя и пароль пользователя с правами Full administrator (по умолчанию Admin). Если устройство UserGate LogAn не прошло первоначальную инициализацию, то для доступа к CLI необходимо использовать в качестве имени пользователя Admin, в качестве пароля - utm.

Для подключения к CLI по сети с использованием протокола SSH необходимо выполнить следующие шаги:

Наименование	Описание

Шаг 1. Разрешить доступ к CLI (SSH) для выбранной зоны	Разрешить доступ для протокола CLI по SSH в настройках зоны, к которой вы собираетесь подключаться для управления с помощью CLI. Будет открыт порт TCP 2200.
Шаг 2. Запустить SSH-терминал	Запустить у себя на компьютере SSH-терминал, например, SSH для Linux или Putty для Windows. Указать в качестве адреса адрес UserGate LogAn, в качестве порта подключения - 2200, в качестве имени пользователя - имя пользователя с правами Full administrator (по умолчанию Admin). Для Linux команда на подключение должна выглядеть так: *ssh Admin@IPUserGateLogAn -p 2200*
Шаг 3. Войти в CLI	Войти в CLI, используя пароль пользователя, указанного на предыдущем шаге. Если устройство UserGate LogAn не прошло первоначальную инициализацию, то для доступа к CLI необходимо использовать в качестве имени пользователя Admin, в качестве пароля - utm.

После успешного входа в CLI можно посмотреть список возможных команд с помощью команды **help**. Для подробного описания любой команды необходимо использовать синтаксис
help commandНапример, для получения подробной справки по использованию команды настройки сетевого интерфейса iface необходимо выполнить
help Iface

Полный список команд:

Наименование	Описание
help	Показывает список доступных команд.
exit quit Ctrl+D	Выйти из CLI.
date	Посмотреть текущее время на сервере.
gateway	Посмотреть или задать значения шлюза. Смотрите gateway help для детальной информации.
iface	Набор команд для просмотра и настройки параметров сетевого интерфейса. Смотрите iface help для детальной информации.
license	Посмотреть информацию о лицензии.
netcheck	Проверить доступность стороннего HTTP/HTTPS-сервера. **netcheck [-t TIMEOUT] [-d] URL** Опции: -t – максимальный таймаут ожидания ответа от веб-сервера -d – запросить содержание сайта. По умолчанию запрашиваются только заголовки.

nslookup	Выполнить определение IP-адреса по имени хоста.
ping	Выполнить ping определенного хоста.
radmin	Включить или отключить удаленный доступ к серверу для технической поддержки UserGate LogAn.
radmin_e	Включить или отключить удаленный доступ к серверу для технической поддержки UserGate LogAn, в случаях, когда сервер UserGate LogAn завис.
reboot	Перезагрузить сервер UserGate LogAn.
route	Создать, изменить, удалить маршрут.
shutdown	Выключить сервер UserGate LogAn.
traceroute	Выполнить трассировку соединения до определенного хоста.
zone	Набор команд для просмотра и настройки параметров зоны. Смотрите zone help для детальной информации.

8 СЕНСОРЫ

Для сбора информации с различных устройств и последующего ее анализа UserGate LogAn использует сенсоры. Сенсор - это совместимое с LogAn устройство, которое может передавать определенные данные на сервер LogAn. Сенсорами могут выступать шлюзы UserGate, а также любые другие сетевые устройства, способные передавать данные по протоколу SNMP.

8.1 Сенсоры UserGate

Сенсор UserGate подключает одно устройство типа шлюз безопасности UserGate к серверу LogAn. Для подключения сенсора UserGate необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. На сервере UserGate разрешить сервисы Log Analyzer и SNMP на требуемой зоне	На сервере UserGate, который вы хотите добавить в качестве сенсора, в разделе **Сеть --> Зоны** выберите зону, через интерфейсы которой будет происходить сетевой обмен с сервером LogAn, и разрешите сервисы Log Analyzer и SNMP.
Шаг 2. На сервере UserGate скопируйте токен в буфер обмена	На сервере UserGate, который вы хотите добавить в качестве сенсора, в разделе **Настройки --> Log Analyzer** скопируйте значение токена в буфер обмена. Он понадобится на шаге 4.
Шаг 3. На сервере LogAn разрешить сервис Log Analyzer на требуемой зоне	На сервере LogAn в разделе **Сеть --> Зоны** выберите зону, через интерфейсы которой будет происходить сетевой обмен с сервером UserGate, и разрешите сервис **Log Analyzer**.
Шаг 4. Создайте сенсор UserGate	На сервере LogAn в разделе **Сенсоры --> Сенсоры UserGate** нажмите кнопку **Добавить** и заполните необходимые поля.

При создании сенсора UserGate необходимо заполнить следующие поля:

Наименование	Описание
Включено	Включает или выключает данный сенсор UserGate.
Название	Название сенсора UserGate.
Описание	Опциональное описание сенсора UserGate.
Адрес сервера	IP-адрес сервера UserGate, для которого создается данный сенсор.
Log Analyzer адрес	IP-адрес сервера LogAn, который будет использоваться на сервере UserGate, в качестве назначения для отсылки журналов. Для выбора отображаются только те адреса, на интерфейсах зон которых разрешен сервис Log Analyzer.

Токен	Токен, полученный на сервере UserGate.

После создания сенсора, сервер UserGate начинает отсылать данные на сервер LogAn.

Примечание

После подключения Log Analyzer обработка и экспорт журналов, создание отчётов и обработка других статистических данных сенсора UserGate производятся сервером LogAn.

На сервере UserGate произошли следующие изменения конфигурации:

- В разделе **Настройки --> Log Analyzer** изменился адрес сервера Log Analyzer на адрес, указанный при создании сенсора UserGate.
- В разделе **Диагностика и мониторинг --> SNMP** добавилось правило SNMP, разрешающее серверу Log Analyzer получать информацию по протоколу SNMP.

На сервере LogAn добавились следующие элементы:

- В разделе **Журналы и отчеты --> Журналы** появились записи с созданного UserGate сенсора.
- В **Дашборде** появилась возможность добавить новый виджет - **График сенсора UserGate**, содержащий информацию, полученную с сенсора UserGate.

Примечание

В случае изменения администратором правила SNMP на сервере UserGate, LogAn вернет настройки или пересоздаст правило при включении/отключении сенсора на сервере LogAn.

8.2 Сенсоры SNMP

С помощью сенсора SNMP администратор может подключить SNMP-совместимое сетевое устройство к серверу UserGate LogAn для сбора и анализа его метрик. UserGate LogAn может отображать любые счетчики, полученные по SNMP с помощью запросов SNMP. Для настройки сенсора SNMP необходимо иметь базы MIB (Management Information Base) на управляемое устройство. Подробнее об управлении базами MIB смотрите раздел данного руководства Управление SNMP MIB.

Для настройки сенсора SNMP необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Загрузите базу MIB того устройства, которое хотите добавить для мониторинга.	На сервере LogAn в разделе **Сенсоры --> Управление SNMP MIB** загрузите файл с MIB.
Шаг 2. Создайте сенсор SNMP	На сервере LogAn в разделе **Сенсоры --> Сенсоры SNMP** нажмите кнопку **Добавить** и заполните необходимые поля.

При создании сенсора SNMP необходимо заполнить следующие поля:

Наименование	Описание
Включено	Включает или выключает данный сенсор SNMP.
Название	Название сенсора SNMP.
Описание	Опциональное описание сенсора SNMP.
Адрес сервера	IP-адрес сенсора SNMP.
Порт	Порт сенсора SNMP. Обычно для запросов данных по протоколу SNMP используется порт TCP 161.
Версия	Указывает версию протокола SNMP, которая будет использоваться в данном сенсоре. Возможны варианты SNMP v2c и SNMP v3.
Community	SNMP community - строка для идентификации сервера LogAn и сетевого устройства для версии SNMP v2c. Используйте только латинские буквы и цифры.
Интервал опроса (сек)	Интервал, через который сервер LogAn будет инициировать получение данных с сетевого устройства.
Пользователь	Только для SNMP v3. Имя пользователя для аутентификации на сетевом устройстве.
Тип аутентификации	Выбор режима аутентификации. Возможны варианты: • Без аутентификации, без шифрования (noAuthNoPriv). • С аутентификацией, без шифрования (authNoPriv). • С аутентификацией, с шифрованием (authPriv). Наиболее безопасным считается режим работы authPriv.
Алгоритм аутентификации	Алгоритм, используемый для аутентификации.
Пароль аутентификации	Пароль, используемый для аутентификации.
Алгоритм шифрования	Алгоритм, используемый для шифрования. Возможно использовать DES и AES.
Пароль шифрования	Пароль, используемый для шифрования.
Счетчики	Укажите здесь все требуемые данные, которые LogAn будет запрашивать на сетевом устройстве. Счетчики выбираются из баз MIB, которые загружены на устройство. Выберите в дереве SNMP необходимый раздел и добавьте соответствующий счетчик либо укажите в строке SNMP OID счетчика и его тип.

После успешного добавления сенсора во вкладке **Дашборд** появилась возможность добавить виджет с графиками данных SNMP, полученными с данного сенсора.

8.3 Управление SNMP MIB

В данном разделе администратор может добавлять и удалять базы MIB (Management Information Base) на сервере UserGate LogAn.

Для получения специфических MIB обратитесь к производителю вашего устройства. UserGate LogAn уже содержит наиболее популярные базы сетевых устройств.

9 ДАШБОРД

Данный раздел позволяет посмотреть текущее состояние сервера и серверов, которые подключены к нему для отправки логов, их загрузку, статус лицензии и так далее.

Отчеты предоставлены в виде виджетов, которые могут быть настроены администратором системы в соответствии с его требованиями. Виджеты можно добавлять, удалять, изменять расположение и размер на странице **Дашборд**. По умолчанию созданы страницы с виджетами Log Analyzer (отображение состояния сервера Log Analyzer), NOC (Network Operation Center) и SOC (Security Operation Center).

Некоторые виджеты позволяют настроить отображение, указать фильтрацию данных и настроить прочие параметры. Для настройки виджета необходимо кликнуть по символу шестеренки в правом верхнем углу. Не все параметры, перечисленные ниже, доступны для каждого типа виджетов.

Наименование	Описание
Название	Название виджета, которое будет отображаться в Дашборд.
Описание	Опциональное описание виджета.
Количество записей	Максимальное количество записей для отображения.
Группировать по	Поле данных, по которому будут сгруппированы данные в виджете.
Диаграмма	Выбор типа представления данных. Доступны значения: • Число • Круговая диаграмма • Вертикальная гистограмма • Горизонтальная гистограмма • Таблица • График • Карта мира
Запрос фильтра	SQL-подобная строка запроса, позволяющая ограничить объем информации, используемой при построении виджета. Для формирования запросов используются названия полей, значения полей, ключевые слова и операторы. Ключевые слова и операторы, а так же примеры их использования можно посмотреть в разделе документации Поиск и фильтрация данных.
Сенсор	Сенсор, данные с которого используются для данного виджета.

10 ЖУРНАЛЫ И ОТЧЕТЫ

10.1 Журналы

UserGate LogAn журналирует все события, которые происходят во время его работы и работы подключенных к нему серверов, и записывает их в следующие журналы:

- **Журнал событий** – события, связанные с изменением настроек сервера UserGate LogAn, авторизацией пользователей, администраторов, обновлениями различных списков и т.п.
- **Журнал веб-доступа** – подробный журнал всех веб-запросов, обработанных UserGate LogAn.
- **Журнал трафика** – подробный журнал срабатывания правил межсетевого экрана, NAT, DNAT, Port forwarding, Policy based routing.
- **Журнал СОВ** – события, регистрируемые системой обнаружения и предотвращения событий.
- **Журнал АСУ ТП** – события, регистрируемые правилами контроля систем АСУ ТП.
- **Журнал инспектирования SSH** – журнал срабатывания правил инспектирования SSH.
- **История поиска** – поисковые запросы пользователей в популярных поисковых системах.

10.1.1 Журнал событий

Журнал событий отображает события, связанные с изменением настроек сервера UserGate LogAn, например, добавление/удаление/изменение данных учетной записи, правила или любого другого элемента. Здесь же отображаются все события входа в веб-консоль, авторизации пользователей через Captive-портал и другие.

Для удобства поиска необходимых событий записи могут быть отфильтрованы по различным критериям, например таким, как диапазон дат, компоненте, важности, типу события.

Администратор может выбрать только те столбцы для показа, которые ему необходимы. Для этого следует кликнуть указателем мыши на любой из столбцов, и в появившемся контекстном меню оставить галочки только для тех столбцов, которые необходимо отображать.

С помощью кнопки **Экспортировать в CSV** администратор может скачать отфильтрованные данные журнала в csv-файл для дальнейшего анализа.

10.1.2 Журнал веб-доступа

Журнал веб-доступа отображает все запросы пользователей в интернет по протоколам HTTP и HTTPS. Отображается следующая информация:

- Узел UserGate, на котором произошло событие.
- Время события.
- Пользователь.
- Действия.
- Правило.
- Причины (при блокировке сайта).
- URL назначения.
- Зона источника.
- IP-адрес источника.
- Порт источника.
- IP назначения.
- Порт назначения.

- Категории.
- Протокол (HTTP).
- Метод (HTTP).
- Код ответа (HTTP).
- MIME (если присутствует).
- Байт передано/получено.
- Пакетов отправлено.
- Реферер (при наличии).
- Операционная система.
- Браузер.

Администратор может выбрать только те столбцы для показа, которые ему необходимы. Для этого следует кликнуть указателем мыши на любой из столбцов, и в появившемся контекстном меню оставить галочки только для тех столбцов, которые необходимо отображать.

Для удобства поиска необходимых событий записи могут быть отфильтрованы по различным критериям, например таким, как учетная запись пользователя, правило, действие и т.д.

С помощью кнопки **Экспортировать в CSV** администратор может скачать отфильтрованные данные журнала в csv-файл для дальнейшего анализа.

10.1.3 Журнал трафика

Журнал трафика отображает события срабатывания правил межсетевого экрана или правил NAT, в настройках которых включено логирование пакетов. Отображается следующая информация:

- Узел UserGate, на котором произошло событие.
- Время события.
- Пользователь.
- Действие.
- Правило.
- Приложение.
- Протокол.
- Зона источника.
- Адрес источника.
- Порт источника.
- IP-назначения.
- Порт назначения.
- NAT IP-источника (если это правило NAT).
- NAT порт источника (если это правило NAT).
- NAT IP назначения (если это правило NAT).
- NAT порт назначения (если это правило NAT).
- Байт отправлено/получено.
- Пакетов.

Администратор может выбрать только те столбцы для показа, которые ему необходимы. Для этого следует кликнуть указателем мыши на любой из столбцов, и в появившемся контекстном меню оставить галочки только для тех столбцов, которые необходимо отображать.

Для удобства поиска необходимых событий записи могут быть отфильтрованы по различным критериям, например таким, как учетная запись пользователя, правило, действие и т.д.

С помощью кнопки **Экспортировать в CSV** администратор может скачать отфильтрованные данные журнала в csv-файл для дальнейшего анализа.

10.1.4 Журнал СОВ

Журнал системы обнаружения вторжений отображает сработавшие сигнатуры СОВ, для которых установлено действие журналировать или блокировать. Отображается следующая информация:

- Узел UserGate, на котором произошло событие.
- Время.
- Действие.
- Сигнатура.
- Класс - класс сигнатуры.
- CVE - номер уязвимости по базе CVE.
- Bugtrack - номер уязвимости по базе Bugtrack.
- Nessus - номер уязвимости по базе Nessus.
- Протокол.
- IP источника.
- Порт источника.
- IP назначения.
- Порт назначения.
- Подробности срабатывания сигнатуры.

Администратор может выбрать только те столбцы для показа, которые ему необходимы. Для этого следует кликнуть указателем мыши на любой из столбцов, и в появившемся контекстном меню оставить галочки только для тех столбцов, которые необходимо отображать.

Для удобства поиска необходимых событий записи могут быть отфильтрованы по различным критериям, например таким, как протокол, диапазон дат, действие и т.д.

С помощью кнопки **Экспортировать в CSV** администратор может скачать отфильтрованные данные журнала в csv-файл для дальнейшего анализа.

10.1.5 Журнал АСУ ТП

Журнал АСУ ТП отображает сработавшие правила АСУ ТП, для которых установлено действие журналировать или блокировать. Отображается следующая информация:

- Узел UserGate, на котором произошло событие.
- Время.
- Правило.
- Зона источника.
- IP источника.
- IP назначения.
- Порт назначения.
- Протокол.
- Команда АСУ ТП.
- Адрес регистра.

Администратор может выбрать только те столбцы для показа, которые ему необходимы. Для этого следует кликнуть указателем мыши на любой из столбцов, и в появившемся контекстном меню оставить галочки только для тех столбцов, которые необходимо отображать.

Для удобства поиска необходимых событий записи могут быть отфильтрованы по различным критериям, например таким, как протокол, диапазон дат, действие и т.д.

С помощью кнопки **Экспортировать в CSV** администратор может скачать отфильтрованные данные журнала в csv-файл для дальнейшего анализа.

10.1.6 Журнал инспектирования SSH

Журнал инспектирования SSH отображает сработавшие правила инспектирования SSH. Отображается следующая информация:

- Узел UserGate, на котором произошло событие.
- Время.
- Пользователь.
- Действие.
- Правило.
- Команда.
- Зона источника.
- IP-адрес источника.
- Порт источника.
- MAC-адрес источника.
- Зона назначения.
- IP-адрес назначения.
- Порт назначения.

Администратор может выбрать только те столбцы для показа, которые ему необходимы. Для этого следует кликнуть указателем мыши на любой из столбцов и в появившемся контекстном меню оставить отмеченными только те столбцы, которые необходимо отображать.

Для удобства поиска необходимых событий записи могут быть отфильтрованы по различным критериям, например таким, как протокол, диапазон дат, действие и т.д.

С помощью кнопки **Экспортировать в CSV** администратор может скачать отфильтрованные данные журнала в csv-файл для дальнейшего анализа.

Нажатие на кнопку **Показать** выведет окно с подробным описанием события.

10.1.7 История поиска

В разделе **История поиска** отображаются все поисковые запросы пользователей, для которых настроено журналирование в политиках веб-безопасности. Администратор может выбрать только те столбцы для показа, которые ему необходимы. Для этого следует кликнуть указателем мыши на любой из столбцов, и в появившемся контекстном меню оставить галочки только для тех столбцов, которые необходимо отображать.

Для удобства поиска необходимых событий записи могут быть отфильтрованы по различным критериям, например таким, как пользователи, диапазон дат, поисковые системы и т.д.

С помощью кнопки **Экспортировать в CSV** администратор может скачать отфильтрованные данные журнала в csv-файл для дальнейшего анализа.

10.1.8 Поиск и фильтрация данных

Количество записей, регистрируемых в журналах, как правило, очень велико, и UserGate LogAn предоставляет удобные способы поиска и фильтрации необходимой информации. Администратор может использовать простой и расширенный поиск по содержимому журналов.

При использовании простого поиска администратор использует графический интерфейс, чтобы задать фильтрацию по значениям требуемых полей журналов, отфильтровывая таким образом ненужную информацию. Например, администратор может задать интересующий его диапазон времени, список пользователей, категорий и т.п. Задание критериев поиска интуитивно понятно и не требует специальных знаний.

Построение более сложных фильтров возможно в режиме расширенного поиска с использованием специального языка запросов. В режиме расширенного поиска можно строить запросы с использованием полей журналов, которые недоступны в базовом режиме. Для формирования запросов используются названия полей, значения полей, ключевые слова и операторы. Значения полей могут быть введены с использованием одинарных или двойных кавычек, или без них, если значения не содержат пробелов. Для группировки нескольких условий можно использовать круглые скобки.

Ключевые слова отделяются пробелами и могут быть следующими:

Наименование	Описание
AND или and	Логическое И, требует выполнения всех условий, заданных в запросе.
OR или or	Логическое ИЛИ, достаточно выполнения одного из условий запроса.

Операторы определяют условия фильтра и могут быть следующими:

Наименование	Описание
=	Равно. Требует полного совпадения значения поля указанному значению, например, *ip=172.16.31.1* будут отображены все записи журнала, в котором поле IP будет точно соответствовать значению 172.16.31.1.
!=	Не равно. Значение указанного поля не должно совпадать с указанным значением, например, *ip!=172.16.31* будут отображены все записи журнала, в котором поле IP не будет равно значению 172.16.31.1.
<=	Меньше либо равно. Значение поля должно быть меньше либо равны указанному в запросе значению. Может быть применимо только для полей, поддерживающих сравнения, например, поля даты, portSource, portDest, statusCode и т.п., например, *date <= '2019-03-28T20:59:59' AND statusCode=303*.
>=	Больше либо равно. Значение поля должно быть больше либо равны указанному в запросе значению. Может быть применимо только для полей, поддерживающих сравнения, например, поля даты, portSource, portDest, statusCode и т.п., например, *date >= "2019-03-13T21:00:00" AND statusCode=200*.
<	Меньше. Значение поля должно быть меньше указанного в запросе значения. Может быть

	применимо только для полей, поддерживающих сравнения, например, поля даты, portSource, portDest, statusCode и т.п., например, *date < '2019-03-28T20:59:59' AND statusCode=404*.
>	Больше. Значение поля должно быть больше указанного в запросе значения. Может быть применимо только для полей, поддерживающих сравнения, например, поля даты, portSource, portDest, statusCode и т.п., например, *(statusCode>200 AND statusCode <300) OR (statusCode=404)*.
IN	Позволяет указать несколько значений поля в запросе. Список значений необходимо указывать в круглых скобках, например, например, *category IN (botnets, compromised, 'illegal software', 'phishing and fraud','reputation high risk','unknown category')*.
NOT IN	Позволяет указать несколько значений поля в запросе; будут отображены записи, несодержащие указанные значения. Список значений необходимо указывать в круглых скобках, например, *category NOT IN (botnets, compromised, 'illegal software', 'phishing and fraud','reputation high risk','unknown category')*.
~	Содержит. Позволяет указать подстроку, которая должна находиться в указанном поле, например, *browser ~ "Mozilla/5.0"* Данный оператор может быть применен только к полям, в которых хранятся строковые данные.
!~	Не содержит. Позволяет указать подстроку, которая не должна присутствовать в указанном поле, например, *browser !~ "Mozilla/5.0"* Данный оператор может быть применен только к полям, в которых хранятся строковые данные.

При составлении расширенного запроса UserGate LogAn показывает возможные варианты названия полей, применимых к ним операторов и возможных значений, облегчая оператору системы формирование сложных запросов. При переключении режима поиска с основного на расширенный UserGate LogAn автоматически формирует строку с поисковым запросом, которая соответствует фильтру, указанному в основном режиме поиска.

10.1.9 Экспорт журналов

Функция экспортирования журналов UserGate LogAn позволяет выгружать информацию на внешние серверы для последующего анализа или для обработки в системах SIEM (Security information and event management).

UserGate LogAn поддерживает выгрузку следующих журналов:

- Журнал событий.
- Журнал веб-доступа.
- Журнал СОВ.
- Журнал АСУ ТП.
- Журнал трафика.
- Журнал инспектирования SSH.

Поддерживается отправка журналов на серверы SSH (SFTP), FTP и Syslog. Отправка на серверы SSH и FTP проводится по указанному в конфигурации расписанию. Отправка на серверы Syslog происходит сразу же при добавлении записи в журнал.

Для отправки журналов необходимо создать конфигурации экспорта журналов в разделе **Экспорт журналов**.

При создании конфигурации требуется указать следующие параметры:

Наименование	Описание
Название правила	Название правила экспорта журналов.
Описание	Опциональное поле для описания правила.
Журналы для экспорта	Выбор файлов журналов, которые необходимо экспортировать: • Журнал событий. • Журнал веб-доступа. • Журнал трафика. • Журнал СОВ. • Журнал АСУ ТП. • Журнал инспектирования SSH. Для каждого из журналов возможно указать синтаксис выгрузки: • CEF – Common Event Format (ArcSight). • JSON – JSON format. • @CEE: JSON - CEE Log Syntax (CLS) Encoding JSON. Обратитесь к документации на используемую у вас систему SIEM для выбора необходимого формата выгрузки журналов. Подробное описание форматов журналов читайте в Приложение 2. Описание форматов журналов.
Тип сервера	SSH (SFTP), FTP, Syslog.
Адрес сервера	IP-адрес или доменное имя сервера.
Транспорт	Только для типа серверов Syslog - TCP или UDP.
Порт	Порт сервера, на который следует отправлять данные.
Протокол	Только для типа серверов Syslog – RFC5424 или BSD syslog RFC 3164. Выберите протокол, совместимый с используемой у вас системой SIEM.
Критичность	Только для типа серверов Syslog. Необязательное поле, проконсультируйтесь с документацией на используемую у вас систему SIEM. Возможны следующие значения: • **Тревога**: состояние, требующее незамедлительного вмешательства. • **Критическая**: состояние, требующее незамедлительного вмешательства либо предупреждающее о сбое в системе. • **Ошибки**: в системе возникли ошибки. • **Предупреждения**: предупреждения о возможном возникновении ошибок, если не будут предприняты никакие действия. • **Уведомительная**: события, которые относятся к необычному поведению системы, но не являются ошибками. • **Информативная**: информационные сообщения.

Facility	Только для типа серверов Syslog. Необязательное поле, проконсультируйтесь с документацией на используемую у вас систему SIEM. Возможны следующие значения: • **Сообщения пользовательские**. • **Системный сервис**. • **Безопасность/аутентификация**. • **Аудит**. • **Тревога**. • **Local 0**. • **Local 1**. • **Local 2**. • **Local 3**. • **Local 4**. • **Local 5**. • **Local 6**. • **Local 7**.
Имя хоста	Только для типа серверов Syslog. Уникальное имя хоста, идентифицирующее сервер, отправляющий данные на сервер syslog, в формате Fully Qualified Domain Name (FQDN).
App-Name	Только для типа серверов Syslog. Уникальное имя приложения, которое отправляет данные на сервер Syslog.
Логин	Имя учетной записи для подключения к удаленному серверу. Не применяется к методу отправки Syslog.
Пароль	Пароль учетной записи для подключения к удаленному серверу. Не применяется к методу отправки Syslog.
Повторите пароль	Подтверждение пароля учетной записи для подключения к удаленному серверу. Не применяется к методу отправки Syslog.
Путь на сервере	Каталог на сервере для копирования файлов журналов. Не применяется к методу отправки Syslog.
Расписание	Выбор расписания для отправки логов. Не применяется к методу отправки Syslog. Возможны варианты: • Ежедневно. • Еженедельно. • Ежемесячно • Каждые … часов. • Каждые … минут. • Задать вручную. При задании вручную необходимо использовать crontab-подобный формат, при котором строка выглядит как шесть полей, разделенных пробелами. Поля задают время в следующем виде: (минуты: 0-59) (часы: 0-23) (дни месяца: 0-31) (месяц: 0-12) (день недели: 0-6, 0-воскресенье). Каждое из первых пяти полей может быть задано следующим образом: • Звездочка (*) - обозначает весь диапазон (от первого до последнего). • Дефис (-) - обозначает диапазон чисел. Например, "5-7" будет означать 5,6 и 7. • Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или

	"1-11,19-23". • Звездочка или диапазон с шагом. Используется для пропусков в диапазонах. Шаг указывается после косой черты. Например, "2-10/2" будет значить "2,4,6,8,10", а выражение "*/2" в поле "часы" будет означать "каждые два часа".

10.2 Отчеты

С помощью отчетов администратор может предоставить различные срезы данных о событиях безопасности, конфигурирования или действиях пользователей. Отчеты могут создаваться по созданным ранее правилам и шаблонам в автоматическом режиме и отправляться адресатам по электронной почте.

Раздел отчеты состоит из трех подразделов - шаблоны, правила и созданные отчеты. Что бы создать отчет необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Создать правило создания отчета	Создать правило создания отчета, в котором указать необходимые параметры создания отчета.
Шаг 2. Запустить отчет	Запустить отчет в ручном режиме или дождаться времени, когда он запустится в автоматическом режиме по указанному в правиле расписанию.
Шаг 3. Получить отчет	Получить отчет по почте, если в правиле была настроена отправка отчета по почте, или скачать полученный отчет в разделе **Созданные отчеты.**

Примечание

Процесс создания отчета может продолжаться достаточно длительное время и может потреблять большое количество вычислительных ресурсов.

10.2.1 Шаблоны

Шаблон определяет внешний вид и поля, которые будут использоваться в отчете. Шаблоны отчетов предоставляются компанией разработчиком UserGate.

Список возможных шаблонов отчетов, сгруппированных по категориям:

- **Captive-портал** - группа шаблонов по событиям, авторизации пользователей с помощью Captive-портала.
- **События** - группа шаблонов по событиям, регистрируемым в журнале событий.
- **СОВ** - группа шаблонов по событиям, регистрируемым в журнале СОВ.
- **Сетевая активность** - группа шаблонов по событиям, регистрируемым в журнале трафика.
- **Веб-портал** - группа шаблонов авторизации через SSL VPN.
- **Трафик** - группа шаблонов по событиям, регистрируемым в журнале трафика и относящимся к объему потребленного трафика пользователями, приложениями и т.п.

- **VPN** – группа шаблонов по событиям, относящимся к VPN.
- **Веб-активность** - группа шаблонов по событиям, регистрируемым в журнале веб-доступа.

Каждый шаблон содержит название, описание отчета и тип отображения отчета (таблица, гистограмма, пирог).

10.2.2 Пользовательские шаблоны

В отличии от обычных шаблонов, предоставляемых производителем решения, пользовательские шаблоны позволяют создать отчет по тем критериям, которые необходимо пользователю. Администратор может выбрать необходимые поля для отображения, задать условия и возможные группировки. Созданные пользовательские отчеты могут быть использованы в правилах построения отчетов наряду с обычными предопределенными отчетами. Для создания пользовательского шаблона необходимо в разделе **Отчеты--Пользовательские отчеты** нажать на кнопку **Добавить** и заполнить следующие параметры:

Наименование	Описание
Название	Название пользовательского шаблона.
Описание	Опциональное поле для описания пользовательского шаблона.
Категория	Выбор источника данных для данного шаблона. Доступны значения: • Журнал событий. • Журнал веб-доступа. • Журнал трафика. • Журнал СОВ. • Журнал инспектирования SSH.
Запрос фильтра	SQL-подобная строка запроса, позволяющая ограничить объем информации, используемой при построении отчета по данному шаблону. Для формирования запросов используются названия полей, значения полей, ключевые слова и операторы. В качестве полей данных можно использовать столбцы, перечисленные ниже в поле **Столбцы.** Ключевые слова и операторы, а также примеры их использования можно посмотреть в разделе документации Поиск и фильтрация данных.
Сортировать по	Укажите поле данных, по которому будут отсортированы данные в отчете. Сортировку можно указать по возрастанию и по убыванию.
Группировать по	Укажите поле данных, по которому будут сгруппированы данные в отчете.
Столбцы	Список столбцов, доступных для конкретного источника данных.
Выбранные	Список столбцов, выбранных для отображения в отчете.

10.2.3 Правила отчетов

Правило отчета задает параметры создаваемого отчета, а также расписание запуска отчетов и способы доставки отчета пользователям. При создании правила отчета администратор указывает следующие параметры:

Наименование	Описание
Включено	Включение/отключения отчета.
Название	Название правила.
Описание	Опциональное поле для описания правила.
Язык отчета	Выбор языка, который будет использован в отчете.
Диапазон	Диапазон времени, за который необходимо подготовить отчет.
Формат отчета	Формат отчета (PDF, HTML, XML, CSV), в котором будет создаваться данный отчет. В ажно! Создание отчета в формате PDF создает высокую нагрузку на процессор и память. Чем объемнее отчет, тем более высокая нагрузка. Не используйте формат отчета PDF для пользовательских шаблонов. Для шаблонов **Подробный список всех посещенных URL** и **Подробный список всех посещенных сайтов** автоматически используется формат CSV, независимо от выбранного формата.
Количество записей	Задание ограничения числа записей, которые будут выводиться в отчетах, в которых присутствует ограничение по количеству топ записей, например, топ 20 пользователей с ошибочной авторизацией в веб-консоль.
Количество в группировке (если применимо)	Задание ограничения числа записей, которые будут выводиться в отчетах, в которых присутствует ограничение по количеству сгруппированных записей, например, топ 10 пользователей по категориям - для каждой категории будет указано не более 10 пользователей. Данное ограничение применимо только для тех шаблонов отчетов, которые содержат группирование.
Пользователи	Задает пользователей или группы пользователей, для которых будет создаваться отчет. Если оставить поле пустым, то отчет будет создаваться для всех пользователей.
Шаблоны	Список шаблонов, которые будут использоваться для построения отчета. Обязательно необходимо добавить хотя бы один шаблон.
Расписание	Выбор расписания для создания отчетов. Возможны варианты: • Ежедневно. • Еженедельно. • Ежемесячно. • Каждые ... часов. • Каждые ... минут. • Задать вручную. При задании вручную необходимо использовать crontab-подобный формат, при котором

	строка выглядит как шесть полей, разделенных пробелами. Поля задают время в следующем виде: (минуты: 0-59) (часы: 0-23) (дни месяца: 0-31) (месяц: 0-12) (день недели: 0-6, 0-воскресенье). Каждое из первых пяти полей может быть задано следующим образом: • Звездочка (*) - обозначает весь диапазон (от первого до последнего). • Дефис (-) - обозначает диапазон чисел. Например, "5-7" будет означать 5,6 и 7 • Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23" Звездочка или диапазон с шагом. Используется для пропусков в диапазонах. Шаг указывается после косой черты. Например, "2-10/2" будет значить "2,4,6,8,10", а выражение "*/2" в поле "часы" будет означать "каждые два часа.
Доставка	Возможность задать опциональную отправку созданного отчета получателям по протоколу SMTP. Необходимо задать: • Профиль SMTP, который будет использован для отправки отчетов. Подробно о настройке профилей SMTP смотрите в главе Профили оповещений**.** • От - имя отправителя письма. • Тема письма - тема письма (subject). • Тело письма - содержимое письма. • Получатели - список получателей письма. Получатели должны быть добавлены в списки библиотеки **Почтовые адреса.**

Примечание

Процесс создания отчета может продолжаться достаточно длительное время и может потреблять большое количество вычислительных ресурсов. Особенно важно учитывать загрузку ресурсов при запуске отчетов за большой диапазон времени.

Примечание

Для того, чтобы запустить правило отчета не обязательно включать его и указывать время запуска правила. В ручном режиме можно запустить любой, в том числе отключенный отчет, для этого в списке правил необходимо выбрать требуемое правило и нажать на кнопку **Запустить сейчас**. Готовый отчет после создания будет доступен в разделе **Созданные отчеты.**

10.2.4 Созданные отчеты

В разделе **Созданные отчеты** хранятся все полученные отчеты. Отчеты создаются в формате pdf или csv. Для каждого отчета указывается название отчета, которое совпадает с названием правила отчета, которое было использовано для создания данного отчета, время создания отчета и размер отчета.

Для скачивания отчета необходимо использовать кнопку **Скачать**, для удаления - **Удалить**.

Время хранения готовых отчетов (ротация) настраивается по нажатию на кнопку **Настроить**. Значение по умолчанию - 60 дней.

11 ТЕХНИЧЕСКАЯ ПОДДЕРЖКА

Раздел технической поддержки на сайте компании https://www.usergate.com/ru/support содержит дополнительную информацию по настройке UserGate LogAn. Кроме этого, здесь же вы можете оставить заявку на решение вашей проблемы.

12 ПРИЛОЖЕНИЕ 1. ТРЕБОВАНИЯ К СЕТЕВОМУ ОКРУЖЕНИЮ

Сервис	Протокол	Порт	Исходящий/Входящий	Функция
Веб-консоль	TCP	8010	Входящий (к веб-консоли UserGate LogAn)	Доступ к веб-интерфейсу управления устройством.
CLI по SSH	TCP	2200	Входящий (к CLI по SSH)	Доступ к интерфейсу командной строки (CLI) UserGate по протоколу SSH.
XML-RPC	TCP	4041	Входящий (к UserGate по API)	Управление устройством UserGate по API.
Удалённый помощник	TCP	22	Исходящий (до серверов технической поддержки)	Удалённый доступ к серверу технической поддержки. Доступ к серверам: • 93.91.171.46; • 178.154.221.222; • ra.entensys.com.
NTP	UDP	123	Исходящий (до сервера точного времени)	Синхронизация времени.
DNS	UDP	53	Исходящий (до DNS-серверов)	Сервис получения информации (IP-адрес) о доменах.
Регистрация сервера UserGate	TCP	443	Исходящий (до сервера регистрации)	Доступ до сервера регистрации продуктов UserGate reg2.entensys.com.
Обновление ПО и библиотек	TCP	443	Исходящий (до серверов обновления)	Обновление программного обеспечения и элементов библиотек: доступ до серверов static.entensys.com.
Связь с UserGate Management Center	TCP	9712	Исходящий (от LogAn к UGMC)	Первоначальная установка связи и обмен ключами шифрования с сервером UserGate Management Center.
		2022	Исходящий (от LogAn к UGMC)	Построение SSH-туннеля для обмена данными с помощью полученных ключей.
Сервис UserGate Log Analyzer	TCP	9713	Исходящий (от LogAn к UG NGFW)	Первоначальная установка связи и обмен ключами шифрования с сервером UserGate NGFW.
		2023	Исходящий (от LogAn к UG NGFW)	Построение SSH-туннеля для обмена данными с помощью полученных ключей.

	TCP	1269 (приём данных от NGFW 6.x.x)	Входящий (от UG NGFW к LogAn)	Сервис сбора журналов Log Analyzer.
SNMP	UDP	161	Входящий (до UG LogAn)	Доступ к серверу UserGate по протоколу SNMP.
LDAP	TCP	389, 636	Исходящий (на LDAP-коннектор)	Выполнение запросов LDAP (389 – для LDAP и 636 - для LDAP over SSL).
SMTP	TCP	25	Исходящий (до постового сервера)	Отправка уведомлений на электронную почту.
DHCP	UDP	67, 68	Исходящий (запрос на получение адреса от UserGate на сервер DHCP)	Сервис службы DHCP.
FTP (экпорт журналов)	TCP	21	Исходящий (до сервера FTP)	Экспорт журналов на сервер FTP.
SSH (экпорт журналов)	TCP	22	Исходящий (до сервера SSH)	Экспорт журналов на сервер SSH.
Syslog (экпорт журналов)	TCP/UDP	514	Исходящий (до сервера Syslog)	Экспорт журналов на сервер Syslog.

13 ПРИЛОЖЕНИЕ 2. ОПИСАНИЕ ФОРМАТОВ ЖУРНАЛОВ

13.1 Экспорт журналов в формате CEF

13.1.1 Формат журнала событий

Тип поля	Название поля	Описание	Пример значения
CEF заголовок	**CEF:Version**	Версия CEF.	CEF:0
	Device Vendor	Производитель продукта.	Usergate
	Device Product	Тип продукта.	UTM
	Device Version	Версия продукта.	6
	Source	Тип журнала.	events
	Origin	Модуль, в котором произошло событие.	admin_console
	Severity	Важность события.	Может принимать значения: • 1 – информационные. • 4 – предупреждения. • 7 – ошибки. • 10 – критичные.
CEF [расширение]	**rt**	Время, когда было получено событие: миллисекунды с 1 января 1970 года.	1652344423822
	deviceExternalId	Имя, которое однозначно идентифицирует устройство, генерирующее это событие.	utmcore@ersthetatica
	suser	Имя пользователя.	Admin
	cat	Компонент, в котором произошло событие.	console_auth
	act	Тип события.	login_successful
	src	IPv4-адрес источника.	192.168.117.254
	cs1Label	Поле используется для указания деталей события.	Attributes

	cs1	Детали события в формате JSON.	{"name":"MIME_BUILTIN_COMPOSITE","module":"nlist_import"}

13.1.2 Формат журнала веб-доступа

Тип поля	Название поля	Описание	Пример значения
CEF заголовок	**CEF:Version**	Версия CEF.	CEF:0
	Device Vendor	Производитель продукта.	Usergate
	Device Product	Тип продукта.	UTM
	Device Version	Версия продукта.	6
	Source	Название журнала.	webaccess
	Name	Тип источника.	log
	Threat Level	Уровень угрозы категории URL.	Может принимать значения 2, 4, 6, 8, 10 (установленный уровень угрозы, умноженный на 2); Unknown, если категория не определена.
CEF [расширение]	**rt**	Время, когда было получено событие: миллисекунды с 1 января 1970 года.	1652344423822
	deviceExternalId	Имя, которое однозначно идентифицирует устройство, генерирующее это событие.	utmcore@ersthetatica
	act	Действие, принятое устройством в соответствии с настроенными политиками.	captive
	reason	Причина, по которой было создано событие, например, причина блокировки сайта.	{"id":39,"name":"Social Networking","threat_level":3}
	suser	Имя пользователя.	user_example (Unknown, если пользователь неизвестен)
	cs1Label	Поле используется для указания срабатывания правила.	Rule

	cs1	Название правила, срабатывание которого вызвало событие.	Default Allow
	src	IPv4 источника трафика.	10.10.10.10
	spt	Порт источника.	Может принимать значения от 0 до 65535.
	cs2Label	Поле используется для индикации зоны источника.	Source Zone
	cs2	Название зоны источника.	Trusted
	cs3Label	Поле используется для указания страны источника.	Source Country
	cs3	Название страны источника.	RU (отображается двухбуквенный код страны)
	dst	IPv4 адрес назначения трафика.	194.226.127.130
	dpt	Порт назначения.	Может принимать значения от 0 до 65535.
	cs4Label	Поле используется для индикации зоны назначения.	Destination Zone
	cs4	Название зоны назначения.	Untrusted
	cs5Label	Поле используется для указания страны назначения.	Destination Country
	cs5	Название страны назначения.	RU (отображается двухбуквенный код страны)
	cs6Label	Поле указывает было ли содержимое расшифровано.	Decrypted
	cs6	Расшифровано или нет.	true, false
	app	Протокол прикладного уровня и его версия.	HTTP/1.1
	requestMethod	Метод, используемый для доступа к URL-адресу (POST, GET и т.п.).	GET

	request	В случае HTTP-запроса поле содержит URL-адрес запрашиваемого ресурса с указанием используемого протокола.	http://www.secure.com
	requestContext	URL источника запроса (реферер HTTP).	https://www.google.com/
	requestClientApplication	Useragent пользовательского браузера.	Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:96.0) Gecko/20100101 Firefox/96.0
	cn3Label	Поле указывает исходный ответ сервера.	Response
	cn3	Код ответа HTTP.	302
	flexString1Label	Поле указывает на тип контента.	Media type
	flexString1	Тип контента.	text/html
	flexString2Label	Поле указывает на категорию запрашиваемого URL-адреса.	URL Categories
	flexString2	Категория URL.	Computers & Technology
	in	Количество переданных входящих байтов; данные передаются в направлении источник – назначение.	231
	out	Количество переданных исходящих байтов; данные передаются в направлении назначение – источник.	40
	cn1Label	Поле используется для указания количества переданных пакетов в направлении источник - назначение.	Packets sent
	cn1	Количество переданных пакетов в направлении источник - назначение.	3
	cn2Label	Поле используется для указания количества	Packets received

		переданных пакетов в направлении назначение - источник.	
	cn2	Количество переданных пакетов в направлении назначение - источник.	1

13.1.3 Формат журнала трафика

Тип поля	Название поля	Описание	Пример значения
CEF заголовок	**CEF:Version**	Версия CEF.	CEF:0
	Device Vendor	Производитель продукта.	Usergate
	Device Product	Тип продукта.	UTM
	Device Version	Версия продукта.	6
	Source	Тип журнала.	traffic
	Rule Type	Тип правила, срабатывание которого вызвало событие.	firewall
	Threat Level	Уровень угрозы приложения.	Может принимать значения от 1 (если приложения нет) до 10 (указанный уровень угрозы, умноженный на 2).
CEF [расширение]	**rt**	Время, когда было получено событие: миллисекунды с 1 января 1970 года.	1652344423822
	deviceExternalId	Имя, которое однозначно идентифицирует устройство, генерирующее это событие.	utmcore@ersthetatica
	suser	Имя пользователя.	user_example (Unknown, если пользователь неизвестен)
	act	Действие, принятое устройством в соответствии с настроенными политиками.	accept
	cs1Label	Поле используется для указания срабатывания правила.	Rule

	cs1	Название правила, срабатывание которого вызвало событие.	Allow trusted to untrusted
	src	IPv4 источника трафика.	10.10.10.10
	spt	Порт источника.	Может принимать значения от 0 до 65535.
	cs2Label	Поле используется для индикации зоны источника.	Source Zone
	cs2	Название зоны источника.	Trusted
	cs3Label	Поле используется для указания страны источника.	Source Country
	cs3	Название страны источника.	RU (отображается двухбуквенный код страны)
	proto	Используемый протокол 4-го уровня.	TCP или UDP
	dst	IPv4 адрес назначения трафика.	194.226.127.130
	dpt	Порт назначения.	Может принимать значения от 0 до 65535.
	cs4Label	Поле используется для индикации зоны назначения.	Destination Zone
	cs4	Название зоны назначения.	Untrusted
	cs5Label	Поле используется для указания страны назначения.	Destination Country
	cs5	Название страны назначения.	RU (отображается двухбуквенный код страны)
	sourceTranslatedAddress	Адрес источника после переназначения (если настроены правила NAT).	192.168.174.134 (0.0.0.0 – если нет)
	sourceTranslatedPort	Порт источника после переназначения (если настроены правила NAT).	Может принимать значения от 0 до 65535 (0 – если нет)
	destinationTranslatedAddress	Адрес назначения после переназначения (если	192.226.127.130 (0.0.0.0 –

		настроены правила NAT).	если нет)
	destinationTranslatedPort	Порт назначения после переназначения (если настроены правила NAT).	Может принимать значения от 0 до 65535 (0 – если нет)
	in	Количество переданных входящих байтов; данные передаются в направлении источник – назначение.	231
	out	Количество переданных исходящих байтов; данные передаются в направлении назначение – источник.	40
	cn1Label	Поле используется для указания количества переданных пакетов в направлении источник - назначение.	Packets sent
	cn1	Количество переданных пакетов в направлении источник - назначение.	3
	cn2Label	Поле используется для указания количества пакетов, переданных в направлении назначение - источник.	Packets received
	cn2	Количество пакетов, переданных в направлении назначение - источник.	1

13.1.4 Формат журнала СОВ

Тип поля	Название поля	Описание	Пример значения
CEF заголовок	**CEF:Version**	Версия CEF.	CEF:0
	Device Vendor	Производитель продукта.	Usergate
	Device Product	Тип продукта.	UTM
	Device Version	Версия продукта.	6

	Source	Тип журнала.	idps
	Signature	Название сработавшей сигнатуры СОВ.	BlackSun Test
	Threat Level	Уровень угрозы сигнатуры.	Может принимать значения от 2 до 10 (указанный уровень угрозы, умноженный на 2).
CEF [расширение]	**rt**	Время, когда было получено событие: миллисекунды с 1 января 1970 года.	1652344423822
	deviceExternalId	Имя, которое однозначно идентифицирует устройство, генерирующее это событие.	utmcore@ersthetatica
	suser	Имя пользователя.	user_example (Unknown, если пользователь неизвестен)
	act	Действие, принятое устройством в соответствии с настроенными политиками.	accept
	cs1Label	Поле используется для указания срабатывания правила.	Rule
	cs1	Название правила, срабатывание которого вызвало событие.	IDPS Rule Example
	msg	Уровень угрозы сигнатуры и её название.	[2] BlackSun
	app	Протокол прикладного уровня.	HTTP
	proto	Используемый протокол 4-го уровня.	TCP или UDP
	src	IPv4 источника трафика.	10.10.10.10
	spt	Порт источника.	Может принимать значения от 0 до 65535.
	cs2Label	Поле используется для индикации зоны источника.	Source Zone
	cs2	Название зоны источника.	Trusted

	cs3Label	Поле используется для указания страны источника.	Source Country
	cs3	Название страны источника.	RU (отображается двухбуквенный код страны)
	dst	IPv4 адрес назначения трафика.	194.226.127.130
	dpt	Порт назначения.	Может принимать значения от 0 до 65535.
	cs4Label	Поле используется для индикации зоны назначения.	Destination Zone
	cs4	Название зоны назначения.	Untrusted
	cs5Label	Поле используется для указания страны назначения.	Destination Country
	cs5	Название страны назначения.	RU (отображается двухбуквенный код страны)
	in	Количество переданных входящих байтов; данные передаются в направлении источник – назначение.	231
	out	Количество переданных исходящих байтов; данные передаются в направлении назначение – источник.	40

13.1.5 Формат журнала АСУ ТП

Тип поля	Название поля	Описание	Пример значения
CEF заголовок	**CEF:Version**	Версия CEF.	CEF:0
	Device Vendor	Производитель продукта.	Usergate
	Device Product	Тип продукта.	UTM
	Device Version	Версия продукта.	6
	Source	Название журнала.	scada

	Name	Тип источника.	log
	PDU Severity	Критичность АСУ ТП.	1
CEF [расширение]	**rt**	Время, когда было получено событие: миллисекунды с 1 января 1970 года.	1652344423822
	deviceExternalId	Имя, которое однозначно идентифицирует устройство, генерирующее это событие.	utmcore@ersthetatica
	act	Действие, принятое устройством в соответствии с настроенными политиками.	accept
	cs1Label	Поле используется для указания срабатывания правила.	Rule
	cs1	Название правила, срабатывание которого вызвало событие.	Scada Rule Example
	src	IPv4 источника трафика.	10.10.10.10
	spt	Порт источника.	Может принимать значения от 0 до 65535.
	cs2Label	Поле используется для индикации зоны источника.	Source Zone
	cs2	Название зоны источника.	Trusted
	cs3Label	Поле используется для указания страны источника.	Source Country
	cs3	Название страны источника.	RU (отображается двухбуквенный код страны)
	dst	IPv4 адрес назначения трафика.	194.226.127.130
	dpt	Порт назначения.	Может принимать значения от 0 до 65535.
	cs4Label	Поле используется для индикации зоны назначения.	Destination Zone

	cs4	Название зоны назначения.	Untrusted
	cs5Label	Поле используется для указания страны назначения.	Destination Country
	cs5	Название страны назначения.	RU (отображается двухбуквенный код страны)
	app	Протокол прикладного уровня.	Modbus
	cs6Label	Поле указывает на информацию об устройстве.	PDU Details
	cs6	Информация об устройстве в формате JSON.	{"protocol":"modbus","pdu_severity":0,"pdu_func":"3","pdu_address":0,"mb_value":0,"mb_quantity":0,"mb_payload":"AAIAAA==","mb_message":"response","mb_addr":0}

13.1.6 Формат журнала инспектирования SSH

Тип поля	Название поля	Описание	Пример значения
CEF заголовок	**CEF:Version**	Версия CEF.	CEF:0
	Device Vendor	Производитель продукта.	Usergate
	Device Product	Тип продукта.	UTM
	Device Version	Версия продукта.	6
	Source	Название журнала.	ssh
	Name	Тип источника.	log
	Threat Level	Уровень угрозы приложения.	Может принимать значения от 1 (если приложения нет) до 10 (указанный уровень угрозы, умноженный на 2).
CEF [расширение]	**rt**	Время, когда было получено событие: миллисекунды с 1 января 1970 года.	1652344423822
	deviceExternalId	Имя, которое однозначно идентифицирует устройство,	utmcore@ersthetatica

		генерирующее это событие.	
	act	Действие, принятое устройством в соответствии с настроенными политиками.	accept
	app	Протокол прикладного уровня.	SSH или SFTP
	suser	Имя пользователя.	user_example (Unknown, если пользователь неизвестен)
	cs1Label	Поле используется для указания срабатывания правила.	Rule
	cs1	Название правила, срабатывание которого вызвало событие.	SSH inspection rule
	src	IPv4 источника трафика.	10.10.10.10
	spt	Порт источника.	Может принимать значения от 0 до 65535.
	smac	MAC-адрес источника.	FA:16:3E:65:1C:B4
	cs2Label	Поле используется для индикации зоны источника.	Source Zone
	cs2	Название зоны источника.	Trusted
	cs3Label	Поле используется для указания страны источника.	Source Country
	cs3	Название страны источника.	RU (отображается двухбуквенный код страны)
	dst	IPv4 адрес назначения трафика.	194.226.127.130
	dpt	Порт назначения.	Может принимать значения от 0 до 65535.
	cs4Label	Поле используется для индикации зоны назначения.	Destination Zone
	cs4	Название зоны назначения.	Untrusted
	cs5Label	Поле используется для указания страны назначения.	Destination Country

	cs5	Название страны назначения.	RU (отображается двухбуквенный код страны)
	cs6Label	Указание на команду, передаваемую по SSH.	Command
	cs6	Команда, передаваемая по SSH, в формате JSON.	whoami

13.2 Экспорт журналов в формате JSON

13.2.1 Описание журнала событий

Название поля	Описание	Пример значения
user	Имя пользователя.	Admin
timestamp	Время получения события в формате: yyyy-mm-ddThh:mm:ssZ.	2022-05-12T08:11:46.15869Z
ip_address	IPv4-адрес источника события.	192.168.174.134
node	Имя, которое однозначно идентифицирует устройство, генерирующее это событие.	utmcore@ersthetatica
attributes	Детали события в формате JSON.	{"rule":{"logrotate":12,"attributes":{"timezone":"Asia/Novosibirsk"},"id":"66f9de9f-d698-4bec-b3b0-ba65b46d3608","name":"Example log export ftp"}
event_type	Тип события.	logexport_rule_updated
event_severity	Важность события.	info (информационные), warning (предупреждения), error (ошибки), critical (критичные).
event_origin	Модуль, в котором произошло событие.	core
event_component	Компонент, в котором произошло событие.	console_auth

13.2.2 Описание журнала веб-доступа

Название поля		Описание	Пример значения
timestamp		Время получения события в формате: yyyy-mm-ddThh:mm:ssZ.	2022-05-12T08:11:46.15869Z
url_categories	**id**	Идентификатор категории, к которой относится URL.	39
	threat_level	Уровень угрозы категории URL.	Может принимать значения: • 1 – очень низкий. • 2 – низкий. • 3 – средний. • 4 – высокий. • 5 – очень высокий.
	name	Название категории, к которой относится URL.	Social Networking
bytes_sent		Количество байтов, переданных в направлении источник – назначение.	52
node		Имя, которое однозначно идентифицирует устройство, генерирующее это событие.	utmcore@ersthetatica
packets_recv		Количество байтов, переданных в направлении назначение – источник.	5
request_method		Метод, используемый для доступа к URL-адресу (POST, GET и т.п.).	GET
url		Поле содержит URL-адрес запрашиваемого ресурса с указанием используемого протокола.	http://www.secure.com
packets_sent		Количество пакетов, переданных в направлении источник – назначение.	2
action		Действие, принятое устройством в соответствии с настроенными политиками.	block
media_type		Тип контента.	application/json
host		Имя хоста.	www.google.com
session		Идентификатор сессии.	a7a3cd49-8232-4f1a-962a-3659af89e96f (если System:

				00000000-0000-0000-0000-000000000000)
app_protocol			Протокол прикладного уровня и его версия.	HTTP/1.1
status_code			Код ответа HTTP.	302
bytes_recv			Количество пакетов, переданных в направлении назначение – источник.	100
http_referer			URL источника запроса (реферер HTTP).	https://www.google.com/
decrypted			Поле указывает было ли содержимое расшифровано.	true, false
reasons			Причина, по которой было создано событие, например, причина блокировки сайта.	"url_cats":[{"id":39,"name":"Social Networking","threat_level":3}]
useragent			Useragent пользовательского браузера.	Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:96.0) Gecko/20100101 Firefox/96.0
source	**zone**	**guid**	Уникальный идентификатор зоны источника трафика.	d0038912-0d8a-4583-a525-e63950b1da47
		name	Название зоны источника.	Trusted
	country		Страна источника трафика.	RU (отображается двухбуквенный код страны)
	ip		IPv4-адрес источника.	10.10.10.10
	port		Порт источника.	Может принимать значения от 0 до 65535.
destination	**zone**	**guid**	Уникальный идентификатор зоны назначения трафика.	3c0b1253-f069-4060-903b-5fec4f465db0
		name	Название зоны назначения трафика.	Untrusted
	country		Страна назначения.	RU (отображается двухбуквенный код страны)
	ip		IPv4-адрес назначения.	192.168.174.134
	port		Порт назначения.	Может принимать значения от 0 до 65535.

rule	**guid**		Уникальный идентификатор правила, срабатывание которого вызвало создание события.	f93da24d-74f9-4f8c-9e9b-8e6d02346fb4
	name		Название правила.	Default allow
user	**guid**		Уникальный идентификатор пользователя.	a7a3cd49-8232-4f1a-962a-3659af89e96f
	name		Имя пользователя	user_name
	groups	**guid**	Уникальный идентификатор группы, в которой состоит пользователь.	919878b2-e882-49ed-3331-8ec72c3c79cb
		name	Название группы, в которой состоит пользователь.	Default Group

13.2.3 Описание журнала трафика

Название поля	Описание	Пример значения
timestamp	Время получения события в формате: yyyy-mm-ddThh:mm:ssZ.	2022-05-12T08:11:46.15869Z
bytes_sent	Количество байтов, переданных в направлении источник - назначение.	100
node	Имя, которое однозначно идентифицирует устройство, генерирующее это событие.	utmcore@ersthetatica
packets_recv	Количество пакетов, переданных в направлении назначение - источник.	1
proto	Используемый протокол 4-го уровня.	TCP или UDP
packets_sent	Количество пакетов, переданных в направлении источник - назначение.	1
action	Действие, принятое устройством в соответствии с настроенными политиками.	accept
session	Идентификатор сессии.	a7a3cd49-8232-4f1a-962a-3659af89e96f (если System: 00000000-0000-0000-0000-000000000000)

bytes_recv			Количество байтов, переданных в направлении назначение – источник.	6
signatures	**id**		Идентификатор сработавшей сигнатуры.	999999
	threat_level		Уровень угрозы сработавшей сигнатуры.	Может принимать значения: • 1 – очень низкий. • 2 – низкий. • 3 – средний. • 4 – высокий. • 5 – очень высокий.
	name		Название сработавшей сигнатуры.	BlackSun Test
application	**id**		Идентификатор приложения.	195
	threat_level		Уровень угрозы приложения.	Может принимать значения: • 1 – очень низкий. • 2 – низкий. • 3 – средний. • 4 – высокий. • 5 – очень высокий.
	name		Название приложения.	Youtube
source	**zone**	**guid**	Уникальный идентификатор зоны источника трафика.	d0038912-0d8a-4583-a525-e63950b1da47
		name	Название зоны источника трафика.	Trusted
	country		Название страны источника.	RU (отображается двухбуквенный код страны)
	ip		IPv4-адрес источника трафика.	10.10.10.10
	port		Порт источника.	Может принимать значения от 0 до 65535.
destination	**zone**	**guid**	Уникальный идентификатор зоны назначения трафика.	3c0b1253-f069-4060-903b-5fec4f465db0
		name	Название зоны назначения трафика.	Untrusted
	country		Название страны назначения.	RU (отображается двухбуквенный код страны)
	ip		IPv4-адрес назначения трафика.	104.19.197.151

	port		Порт назначения	Может принимать значения от 0 до 65535.
nat	**source**	**ip**	Адрес источника после переназначения (если настроены правила NAT).	192.168.117.85 (если NAT не настроен, то: **"nat":null**)
		port	Порт источника после переназначения (если настроены правила NAT).	Может принимать значения от 0 до 65535 (если NAT не настроен, то: **"nat":null**)
	destination	**ip**	Адрес назначения после переназначения (если настроены правила NAT).	64.233.164.198 (если NAT не настроен, то: **"nat":null**)
		port	Порт источника после переназначения (если настроены правила NAT).	Может принимать значения от 0 до 65535 (если NAT не настроен, то: **"nat":null**)
rule	**guid**		Уникальный идентификатор правила, срабатывание которого создало событие.	59e38e06-533a-4771-9664-031c3e8b2e1f
	type		Тип правила.	firewall
	name		Название правила, срабатывание которого вызвало событие.	Allow trusted to untrusted
user	**guid**		Уникальный идентификатор пользователя. Если пользователь типа Unknown, то идентификатор: 00000000-0000-0000-0000-000000000000.	a7a3cd49-8232-4f1a-962a-3659af89e96f
	name		Имя пользователя.	Admin
	groups	**guid**	Уникальный идентификатор группы, в которых состоит пользователь.	919878b2-e882-49ed-3331-8ec72c3c79cb
		name	Название группы, в которой состоит пользователь.	Default Group

13.2.4 Описание журнала СОВ

Название поля	Описание	Пример значения
timestamp	Время получения события в формате: yyyy-mm-ddThh:mm:ssZ.	2022-05-12T08:11:46.15869Z

session			Идентификатор сессии.	a7a3cd49-8232-4f1a-962a-3659af89e96f (если System: 00000000-0000-0000-0000-000000000000)
packets_sent			Количество пакетов, переданных в направлении источник - назначение.	1
packets_recv			Количество пакетов, переданных в направлении назначение - источник.	1
node			Имя, которое однозначно идентифицирует устройство, генерирующее это событие.	utmcore@ersthetatica
proto			Используемый протокол 4-го уровня.	TCP или UDP
bytes_sent			Количество байтов, переданных в направлении источник - назначение.	100
bytes_recv			Количество байтов, переданных в направлении назначение – источник.	6
action			Действие, принятое устройством в соответствии с настроенными политиками.	accept
application	**id**		Идентификатор приложения.	195
	threat_level		Уровень угрозы приложения.	Может принимать значения: • 1 – очень низкий. • 2 – низкий. • 3 – средний. • 4 – высокий. • 5 – очень высокий.
	name		Название приложения.	Youtube
user	**guid**		Уникальный идентификатор пользователя. Если пользователь типа Unknown, то идентификатор: 00000000-0000-0000-0000-000000000000.	a7a3cd49-8232-4f1a-962a-3659af89e96f
	name		Имя пользователя.	Admin
	groups	**guid**	Уникальный идентификатор группы, в которых состоит пользователь.	919878b2-e882-49ed-3331-8ec72c3c79cb

		name	Название группы, в которой состоит пользователь.	Default Group
rule	**guid**		Уникальный идентификатор правила, срабатывание которого создало событие.	59e38e06-533a-4771-9664-031c3e8b2e1f
	name		Название правила, срабатывание которого вызвало событие.	Allow trusted to untrusted
signatures	**id**		Идентификатор сработавшей сигнатуры.	999999
	threat_level		Уровень угрозы сработавшей сигнатуры.	Может принимать значения: • 1 – очень низкий. • 2 – низкий. • 3 – средний. • 4 – высокий. • 5 – очень высокий.
	name		Название сработавшей сигнатуры.	BlackSun Test
source	**zone**	**guid**	Уникальный идентификатор зоны источника трафика.	d0038912-0d8a-4583-a525-e63950b1da47
		name	Название зоны источника трафика.	Trusted
	country		Название страны источника.	RU (отображается двухбуквенный код страны)
	ip		IPv4-адрес источника трафика.	10.10.10.10
	port		Порт источника.	Может принимать значения от 0 до 65535.
destination	**zone**	**guid**	Уникальный идентификатор зоны назначения трафика.	3c0b1253-f069-4060-903b-5fec4f465db0
		name	Название зоны назначения трафика.	Untrusted
	country		Название страны назначения.	RU (отображается двухбуквенный код страны)
	ip		IPv4-адрес назначения трафика.	104.19.197.151
	port		Порт назначения	Может принимать значения от 0 до 65535.

13.2.5 Описание журнала АСУ ТП

Название поля		Описание	Пример значения
timestamp		Время получения события в формате: yyyy-mm-ddThh:mm:ssZ.	2022-05-12T08:11:46.15869Z
pdu_severity		Критичность АСУ ТП.	1
pdu_func		Код функции (говорит ведомому устройству, какие данные или выполнение какого действия требует от него ведущее устройство).	12
pdu_address		Адрес регистра, с которым необходимо провести операцию.	3154
node		Имя, которое однозначно идентифицирует устройство, генерирующее это событие.	utmcore@ersthetatica
details	**pdu_varname**	Имя переменной. Параметр, в основном, используется для обмена данными в режиме реального времени. Параметр относится к протоколу MMS.	VAR
	pdu_device	Адрес устройства, используемый в протоколах MMS и OPCUA.	DEV
	mb_write_quantity	Количество значений для записи (команда Read Write Register).	998
	mb_write_addr	Начальный адрес регистра для записи (команда Read Write Register).	776
	mb_value	Записываемое значение (для команд Write Single Coil, Write Single Register).	322
	mb_unit_id	Адрес устройства.	186
	mb_read_quantity	Количество значений для чтения (команда Read Write Register).	658
	mb_read_addr	Начальный адрес регистра для чтения (команда Read Write Register).	122
	mb_quantity	Количество значений для чтения.	875
	mb_payload	Значения регистров (для команд Read	75be5ecdc24f9883

			Coil, Read Holding Registers, Read Input Registers, Read/Write Multiple registers, Write Multiple Coil).	
	mb_or_mask		Значение маски OR команды Mask Write Register.	1024
	mb_message		Сообщение Modbus.	exception
	mb_exception_code		Код ошибки. Актуален для типа сообщения error_response.	255
	mb_and_mask		Значение маски AND команды Mask Write Register.	121
	mb_addr		Адрес регистра.	3154
	iec104_msgtype		Тип запроса.	request, response, error_response
	iec104_ioa		Адрес объекта информации, который позволяет однозначно идентифицировать приёмной стороной тип события.	23
	iec104_cot		Причина передачи протокольного блока данных прикладного уровня (Application Protocol Data Unit, APDU).	6
	iec104_asdu		Адрес ASDU (COA – Common Object Address). Параметр относится к протоколу IEC-104.	123
app_protocol			Протокол прикладного уровня.	Modbus
action			Действие, принятое устройством в соответствии с настроенными политиками.	pass
source	**zone**	**guid**	Уникальный идентификатор зоны источника трафика.	d0038912-0d8a-4583-a525-e63950b1da47
		name	Название зоны источника трафика.	Trusted
	country		Название страны источника.	RU (отображается двухбуквенный код страны)
	ip		IPv4-адрес источника трафика.	10.10.10.10
	port		Порт источника.	Может принимать значения от 0 до 65535.

destination	**zone**	**guid**	Уникальный идентификатор зоны назначения трафика.	3c0b1253-f069-4060-903b-5fec4f465db0
		name	Название зоны назначения трафика.	Untrusted
	country		Название страны назначения.	RU (отображается двухбуквенный код страны)
	ip		IPv4-адрес назначения трафика.	104.19.197.151
	port		Порт назначения	Может принимать значения от 0 до 65535.
rule	**guid**		Уникальный идентификатор правила, срабатывание которого создало событие.	59e38e06-533a-4771-9664-031c3e8b2e1f
	name		Название правила, срабатывание которого вызвало событие.	SCADA Sample Rule

13.2.6 Описание журнала инспектирования SSH

Название поля			Описание	Пример значения
timestamp			Время получения события в формате: yyyy-mm-ddThh:mm:ssZ.	2022-05-12T08:11:46.15869Z
node			Имя, которое однозначно идентифицирует устройство, генерирующее это событие.	utmcore@ersthetatica
command			Команда, передаваемая по SSH.	whoami
app_threat			Уровень угрозы приложения.	Может принимать значения от 2 до 10 (установленный уровень угрозы приложения, умноженный на 2)
app_protocol			Протокол прикладного уровня.	SSH или SFTP
app_id			Идентификатор приложения.	195
action			Действие, принятое устройством в соответствии с настроенными политиками.	block
source	**zone**	**guid**	Уникальный идентификатор зоны источника трафика.	d0038912-0d8a-4583-a525-e63950b1da47

		name	Название зоны источника трафика.	Trusted
	country		Название страны источника.	RU (отображается двухбуквенный код страны)
	ip		IPv4-адрес источника трафика.	10.10.10.10
	port		Порт источника.	Может принимать значения от 0 до 65535.
	mac		MAC-адрес источника.	FA:16:3E:65:1C:B4
destination	**zone**	**guid**	Уникальный идентификатор зоны назначения трафика.	3c0b1253-f069-4060-903b-5fec4f465db0
		name	Название зоны назначения трафика.	Untrusted
	country		Название страны назначения.	RU (отображается двухбуквенный код страны)
	ip		IPv4-адрес назначения трафика.	104.19.197.151
	port		Порт назначения	Может принимать значения от 0 до 65535.
rule	**guid**		Уникальный идентификатор правила, срабатывание которого создало событие.	59e38e06-533a-4771-9664-031c3e8b2e1f
	name		Название правила, срабатывание которого вызвало событие.	SSH Rule Example
user	**guid**		Уникальный идентификатор пользователя. Если пользователь типа Unknown, то идентификатор: 00000000-0000-0000-0000-000000000000.	a7a3cd49-8232-4f1a-962a-3659af89e96f
	name		Имя пользователя.	Admin
	groups	**guid**	Уникальный идентификатор группы, в которых состоит пользователь.	919878b2-e882-49ed-3331-8ec72c3c79cb
		name	Название группы, в которой состоит пользователь.	Default Group