Table of Contents

Table of Contents 1
Настройка раздела журналы и отчеты 2
- Настройка экспорта журналов 3
- Настройка отчетов 5

Настройка раздела журналы и отчеты

Настройка экспорта журналов

Product: SWG
Version: 7.5.x

Функция экспорта журналов позволяет выгружать информацию на внешние серверы для последующего анализа или обработки.

Для создания нового правила экспорта журналов используется команда:

Admin@nodename# create logs logs-export <parameters>

Параметры правила экспорта журналов.

Параметр	**Описание**
enabled	Включение или отключение правила: • on; • off
name	Название правила
description	Описание правила
server-type	Тип сервера: • ssh; • ftp; • syslog. При выборе типа сервера доступны следующие дополнительные настройки: • port — порт сервера, на который следует отправлять данные. • login — имя учетной записи для подключения к удаленному серверу (не применяется к методу отправки syslog). • password — пароль учетной записи для подключения к удаленному серверу (не применяется к методу отправки syslog). • path — каталог на сервере для копирования файлов журналов (не применяется к методу отправки syslog). • passive — пассивный режим ftp. • transport — только для типа серверов syslog. TCP или UDP. • protocol — только для типа серверов syslog. RFC5424 или BSD syslog RFC 3164. Выберите протокол, совместимый с используемой у вас системой SIEM. • severity — только для типа серверов syslog. Критичность. Возможны следующие значения: alert, critical, error, warning, notice, info. • facility — только для типа серверов syslog. Объект. Возможны следующие значения: user-level, system-daemons, security-auth, log-audit, log-alert, local- (0-7). • hostname — 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
target	IP-адрес или доменное имя сервера.

Параметр	Описание
logs	Журналы для экспорта: • dns — журнал DNS; • events — журнал событий; • webaccess — журнал веб-доступа; • traffic — журнал трафика; • userid — журнал UserID. Для каждого журнала можно выбрать синтаксис выгрузки: • cef; • cef-compact; • json; • cee-json; • off.
schedule	Выбор расписания для отправки логов. Не применяется к методу отправки Syslog. Crontab-формат: <минуты: 0-59> <часы: 0-23> <дни месяца: 1-31> <месяцы: 1-12> <дни недели: 0-6, где 0 — воскресенье>. Каждое из полей может быть задано следующим образом: • Звездочка (*) — для выбора всех значений. • Дефис (-) — для указания диапазона значений. • Запятая (,) — в качестве разделителя значений. • Косая черта (/) — для указания шага между значениями

Команда для редактирования ранее созданных правил:

Admin@nodename# set logs logs-export <log-export-rule-name>

Параметры, доступные для редактирования, аналогичны параметрам создания правил экспорта.

Команды для просмотра параметров созданных ранее правил экспорта:

Admin@nodename# show logs logs-export
Admin@nodename# show logs logs-export <log-export-rule-name>

Команда для удаления созданных ранее правил экспорта:

Admin@nodename# delete logs logs-export <log-export-rule-name>

Команда для настройки параметров разового экспорта журналов:

Admin@nodename# execute logs send-once <log-export-rule-name> <parameters>

Параметр	Описание
fresh	Экспортировать свежие логи
range	Указать интервал для экспорта: • start-export-range — начало интервала в формате: 2022-12-31T23:59:59; • end-export-range — конец интервала в формате: 2022-12-31T23:59:59

Product: SWG
Version: 7.5.x

Настройка отчетов в интерфейсе командной строки выполняется в режиме конфигурации на уровне reports.

С помощью команд этого раздела можно просматривать имеющиеся на устройстве шаблоны отчетов, создавать и редактировать правила отчетов, просматривать ранее созданные отчеты.

Шаблоны отчетов

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

Для просмотра имеющихся шаблонов отчетов используется команда:

Admin@nodename# show reports report-templates

Правила отчетов

Правила отчетов задают параметры создаваемого отчета, а также расписание запуска отчетов и способы их доставки пользователям.

Для создания нового правила отчетов используется команда:

Admin@nodename# create reports report-rules <parameters>

Параметры правила отчетов.

Параметр	Описание
enabled	Включение/отключение правила: • on; • off
name	Название правила
description	Описание правила
language	Выбор языка создания отчета: • ru; • en
time-range	Диапазон времени в секундах, за который необходимо подготовить отчет
format	Выбор формата, в котором будет создан отчет: • pdf; • html
query-limit	Задание ограничения числа записей, которые будут выводиться в отчетах с ограничением по количеству записей, например, топ 20 пользователей с ошибочной авторизацией в веб-консоль
query-limit-by	Задание ограничения числа записей, которые будут выводиться в отчетах с ограничением 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
templates	Список шаблонов, которые будут использоваться для построения отчета. Обязательно необходимо добавить хотя бы один шаблон
email-sender	Отправитель письма с созданным отчетом

Параметр	Описание
email-recipients	Список получателей письма с отчетом. Получатели должны быть добавлены в списки библиотеки «Почтовые адреса» (email-list)
email-subject	Тема письма с отчетом
email-body	Содержимое письма с отчетом
smtp-profile	Профиль SMTP, который будет использован для отправки отчетов.
schedule	Расписание для отправки отчетов. Crontab-формат: <минуты: 0-59> <часы: 0-23> <дни месяца: 1-31> <месяцы: 1-12> <дни недели: 0-6, где 0 — воскресенье>. Каждое из полей может быть задано следующим образом: • Звездочка (*) — для выбора всех значений. • Дефис (-) — для указания диапазона значений. • Запятая (,) — в качестве разделителя значений. • Косая черта (/) — для указания шага между значениями

Команда для редактирования ранее созданных правил:

Admin@nodename# set reports report-rules <report-rule-name> <parameters>

Параметры, доступные для редактирования, аналогичны параметрам создания правил отчетов.

Команды для просмотра параметров созданных ранее правил отчетов:

Admin@nodename# show reports report-rules
Admin@nodename# show reports report-rules <report-rule-name>

Команда для удаления созданных ранее правил отчетов:

Admin@nodename# delete reports report-rules <report-rule-name>

Созданные отчеты

Для просмотра информации о созданных отчетах используется команда:

Admin@nodename# show reports generated-reports
Admin@nodename# show reports generated-reports <generated-report-name>