

Table of Contents

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

Настройка экспорта журналов

Documentation: ☒

Product: NGFW

Version: 7.x

Функция экспортирования журналов позволяет выгружать информацию на внешние серверы для последующего анализа или для обработки в системах SIEM.

Для создания нового правила экспорта журналов используется команда:

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

Доступные параметры:

Параметр	Описание
enabled	Включение/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. • idps — Журнал COB. • mailsecurity — Журнал почтового трафика. • ssh — Журнал инспектирования SSH. • 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. rontab-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: 1-31) (месяц: 1-12) (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".

Для редактирования ранее созданных правил используется команда:

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

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

Для просмотра параметров созданных ранее правил экспорта используется команда:

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

Для удаления созданных ранее правил экспорта используется команда:

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

Для настройки параметров разового экспорта журналов используется команда:

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

Параметр	Описание
fresh	Экспортировать свежие логи.
range	Указать диапазон экспорта: • start-export-range — начало диапазона в формате: 2022-12-31T23:59:59 • end-export-range — конец диапазона в формате: 2022-12-31T23:59:59

Product: NGFW
Version: 7.x

Настройка отчетов в интерфейсе командной строки CLI (доступно в версии 7.4.0 и выше) происходит 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 отчётов 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>

Доступные параметры:

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 отчётов, которые содержат группирование.
templates	Список шаблонов, которые будут использоваться для построения отчёта. Обязательно необходимо добавить хотя бы один шаблон.
email-sender	Отправитель письма с созданным отчётом.

Параметр	Описание
email-recipients	Список получателей письма с отчётом. 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	Выбор расписания для отправки отчетов. Crontab-подобный формат, при котором строка выглядит как шесть полей, разделённых пробелами. Поля задают время в следующем виде: (минуты: 0-59) (часы: 0-23) (дни месяца: 1-31) (месяц: 1-12) (день недели: 0-6, 0 — воскресенье). Каждое из первых пяти полей может быть задано следующим образом: - Звёздочка (*) — 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), разделённые запятыми. Например, 1,5,10,11 или 1-11,19-23. - Звёздочка или диапазон с шагом. Используется для пропусков в диапазонах. Шаг указывается после косой черты. Например, выражение «2-10/2» будет значить: «2,4,6,8,10», а выражение: «*/2» в поле «часы» будет означать каждые два часа.

Для редактирования ранее созданных правил используется команда:

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

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

Для просмотра параметров созданных ранее правил отчетов используется команда:

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

Для удаления созданных ранее правил отчетов используется команда:

```
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>
```

