

Table of Contents

Table of Contents	1
Режим конфигурации	2
Режим конфигурации (описание)	3

Режим конфигурации (описание)

Documentation: ☒
Product: SIEM
Version: 7.1.x

Для перехода в режим конфигурации используется команда:

```
Admin@nodename> configure
```

После перехода в режим конфигурации командная строка будет выглядеть следующим образом:

```
Admin@nodename#
```

Для просмотра подсказки о текущих возможных значениях или для автодополнения команд необходимо нажать клавишу **Tab**. В подсказке могут использоваться следующие вспомогательные символы:

- * — обязательное поле в командах create и ряде других команд;
- + — необязательное/вариативное поле;
- > — вложенное поле, после его введения предыдущий список полей становится недоступным, появляется новый список полей, которые можно ввести.

Например:

```
Admin/system@nodename# set network zone Trusted
* name          Name
+ antispoof-enable  Enable/Disable IP spoofing protection
+ antispoof-negate  Enable/Disable Negate ip-spoof addresses
+ description      Description
+ enabled-services  Services list to enable
+ geoip            IP spoofing protection by geo IP code
+ ip-list           IP spoofing protection by IP list
> dos-protection-icmp  Confugure DoS protection per IP for ICMP packets
> dos-protection-syn   Confugure DoS protection per IP for SYN packets
> dos-protection-udp   Confugure DoS protection per IP for UDP packets
> service-addresses   Access control service addresses
```

Общая структура команд в режиме конфигурации

Команды интерфейса командной строки имеют следующую структуру:

```
<action> <level> <filter> <configuration_info>
```

где:

- <action> — действие, которое необходимо выполнить.
- <level> — уровень конфигурации; уровни соответствуют разделам веб-интерфейса LogAn.
- <filter> — идентификатор объекта, к которому происходит обращение.
- <configuration_info> — значение параметров, которые необходимо применить к объекту <filter>.

Наименование	Описание

Наименование	Описание
<action>	В режиме конфигурации доступны следующие действия: • execute — выполнение команд, которые не относятся к конфигурации UserGate (ping, date, traceroute и т.п.) Команда доступна независимо от уровня конфигурации (<level>). • set — редактирование всех объектов, а также включение различных параметров, например, radmin. • end — переход на один уровень выше. • show — отображение текущих значений. Можно использовать на любом уровне конфигурации — будет отображено всё, что находится глубже текущего уровня. • edit — переход на какой-либо уровень конфигурации. Уровень конфигурации будет отображён под командной строкой. • top — возврат на самый верхний уровень конфигурации. • exit — выход из режима конфигурации. • export — экспорт конфигурации. • import — импорт конфигурации. • create — создание новых объектов. • delete — удаление объекта или параметра из списка параметров. Например, для просмотра информации о всех интерфейсах необходимо выполнить команду: <pre>Admin@nodename# show network interface</pre> С использованием следующей команды производится переход на уровень network interface. Текущий уровень будет отображён под командной строкой: <pre>Admin@nodename# edit network interface Admin@nodename# Level: network interface</pre> После перехода на уровень network interface для отображения всех интерфейсов используется команда show без указания уровня: <pre>Admin@nodename# show</pre> <pre>adapter: port0 type : adapter interface-name : port0 node-name : node zone : Management enabled : on ip-addresses : 192.168.56.3/24 iface-mode : dhcp Level: network interface</pre> Для возвращения с уровня network interface обратно на общий уровень режима конфигурации необходимо набрать команду end: <pre>Admin@nodename# end Level: network interface Admin@nodename# end Level: network Admin@nodename#</pre>

Наименование	Описание
<level>	Уровни в командной строке повторяют веб-интерфейс системной консоли LogAn: • network — соответствует разделу веб-интерфейса Сеть. • settings — соответствует разделу веб-интерфейса UserGate. • users — соответствует разделу веб-интерфейса Пользователи и устройства. • libraries — соответствует разделу веб-интерфейса Библиотеки. • monitoring — соответствует разделу веб-интерфейса Диагностика и мониторинг. • sensors — соответствует разделу веб-интерфейса Сенсоры. • analytics — соответствует разделу веб-интерфейса Аналитика. • incident — соответствует разделу веб-интерфейса Инциденты.
<filter>	Идентификатор объекта, к которому происходит обращение. Идентификация происходит по имени объекта. Если имеются объекты с одинаковыми именами или удобнее идентифицировать объект по другому параметру, то используются круглые скобки, в которых необходимо указать <configuration_info>. В результате будет найден объект, для которого совпали все поля, указанные в круглых скобках.
<configuration_info>	Набор пар: параметр-аргумент. Параметр — имя поля, для которого нужно установить аргумент. Аргумент может быть одиночным или множественным. Одиночный аргумент — значение, соответствующее параметру. Если строка содержит пробелы, то необходимо использовать кавычки. Например, необходимо создать профиль аутентификации с именем New profile: <pre>Admin@nodename# create users auth-profile name "New profile"</pre> Множественные аргументы используются для установки множества значений какого-либо параметра; записываются в квадратных скобках и разделяются пробелами. Например, необходимо создать список IP-адресов в библиотеке элементов и добавить в него два IP-адреса 10.10.0.1 и 10.10.0.2: <pre>Admin@nodename# create libraries ip-list name testlist ips [10.10.0.1 10.10.0.2]</pre> Важно! Квадратные скобки должны быть отделены пробелами с обеих сторон.

Команды execute

Команды имеет следующую структуру:

Admin@nodename# execute <command-name>

Доступны следующие команды:

Параметр	Описание
traceroute	Трассировка соединения до определённого хоста. Доступны параметры: • hostname <ip-or-domain> — IP-адрес или имя домена, для которого производится трассировка. • interface <iface-name> — интерфейс, с которого будут отправляться пакеты. • not-map-ip — не искать hostname для IP-адреса при отображении. • use-icmp-echo — использовать ICMP echo. • port — указать порт вместо порта по умолчанию (1 — 65535). • min-interval — минимальный интервал между пакетами. <pre>Admin@nodename# execute traceroute hostname <hostname></pre>
termination	Закрытие сессий администраторов. Подробнее читайте в разделе Управление сессиями администраторов.

Параметр	Описание
ping	Выполнение ping определенного хоста. Можно задать следующие параметры: • hostname — IP-адрес или доменное имя хоста. • count — количество отправляемых echo-запросов. Если параметр не задан, то отправка пакетов будет происходить, пока соединение не будет прервано пользователем (чтобы прервать отправку: Ctrl+C). • numeric — не резолвить имена. • timestamp — отображение временных меток. • interval — интервал времени, через который будет производиться отправка пакетов; указывается в секундах. • ttl — время жизни пакета. • interface — адрес выбранного интерфейса будет использоваться в качестве адреса источника для выполнения ping. • mtu — размер mtu отправляемых пакетов. • virtual-router — имя виртуального маршрутизатора. Admin@nodename# execute ping hostname <hostname> count <number>
reboot	Перезагрузка устройства.
date	Просмотр текущих даты и времени на сервере.
shutdown	Выключение устройства.
netcheck	Проверка доступности стороннего HTTP/HTTPS-сервера. Могут быть использованы следующие параметры: • address — доменное имя хоста для проверки доступности по TCP или URL для HTTP. • dns-ip — IP-адрес сервера DNS. • dns-tcp — использование TCP вместо UDP для DNS-запроса. • check-cert — проверка SSL-сертификата • type — проверка доступности по: ◦ http. ◦ tcp (если порт не указан, то используется порт 80). • data — запрос содержимого сайта. По умолчанию запрашиваются только заголовки. • timeout — максимальный таймаут ожидания ответа от веб-сервера. • user-agent — параметр для указания типа браузера (useragent). На некоторых сайтах может быть разрешен доступ только с определенных браузеров. Значение параметра указывается в двойных кавычках. Admin@nodename# execute netcheck type tcp address <host-domain-name> data on Admin@nodename# execute netcheck address <host-domain-name>
dig	Проверка записи DNS домена. • hostname — доменное имя хоста или IP-адрес для реверсивного поиска. • reverse-lookup — получение хоста по IP-адресу. • dns — указание IP-адреса DNS-сервера. • tcp — использование протокола TCP вместо UDP. Admin@nodename# execute dig hostname <host-domain-name> Admin@nodename# execute dig hostname <IP-address> reverse-lookup on
license	Команда регистрации продукта имеет следующую структуру: Admin@nodename# execute license activate <pin-code> Укажите код активации продукта вместо <pin-code>.

Часть представленных выше команд также доступны в режиме диагностики и мониторинга. Для их выполнения используется команда:

Admin@nodename> <command-name>

