

Table of Contents

Table of Contents	1
Настройка библиотек	2
Настройка библиотек (Описание)	3

Documentation: 
Product: NGFW
Version: 7.x

Настройка морфологии

Для создания списка морфологии используется следующая команда:

Admin@nodename# create libraries morphology <parameter>

Далее необходимо указать:

Параметр	Описание
name	Название морфологического списка.
description	Описание списка.
threat-lvl	Уровень угрозы: • very-low — очень низкий уровень угрозы. • low — низкий уровень угрозы. • medium — средний уровень угрозы. • high — высокий уровень угрозы. • very-high — высокий уровень угрозы.
threshold	Вес морфологической категории, при превышении которого сработает правило.
type	Тип списка: • local — локальный. • updatable — если список является обновляемым, то необходимо указать адрес, с которого загружаются обновления (url). Периодичность обновления списка указывается параметром shedule в формате crontab. Crontab-формат: (минуты: 0-59) (часы: 0-23) (дни месяца: 1-31) (месяц: 1-12) (день недели: 0-6; 0 — вс). Каждое из поле 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".
words	Слова и фразы, которые необходимо добавить в список. • word — слова и фразы. При добавлении слова в морфологический словарь можно использовать модификатор «!» перед словом, например, «!bassterd». В данном случае жаргонное слово не будет преобразовываться в словоформы, что может серьезно уменьшить вероятность ложной блокировки. • weight — вес слова или фразы. Если вес не задан, то автоматический устанавливается значение 100. Для добавления слов и фраз: Admin@nodename# create libraries morphology ... words new word "word or phrase" weight <weight>

Чтобы редактировать список, необходимо использовать следующую команду:

Admin@nodename# set libraries morphology <morphology-list-name> <parameter>

Далее указываются параметры, значения которых необходимо обновить (список параметров представлен в таблице выше). Для добавления в список новых слов или фраз необходимо использовать команду:

Admin@nodename# set libraries morphology <morphology-list-name> words new word "word or phrase" weight <weight>

Чтобы заменить слово в списке:

Admin@nodename# set libraries morphology <morphology-list-name> words (word "old word or phrase" weight <weight>) word "new word or phrase" weight <weight>

Следующие команды используются для удаления всего морфологического списка или отдельных слов, содержащихся в нём:

Admin@nodename# delete libraries morphology <morphology-list-name>

Admin@nodename# delete libraries morphology <morphology-list-name> words (word "word or phrase" weight <weight>)

Команды отображения информации о всех имеющихся морфологических списках:

Admin@nodename# show libraries morphology

Чтобы отобразить информацию об определённом списке, далее необходимо указать название интересующего морфологического списка. Чтобы просмотреть содержание определённого морфологического списка:

Admin@nodename# show libraries morphology <morphology-list-name> words

Настройка сервисов

Данный раздел настраиается на уровне **libraries services**.

Для добавления нового сервиса используется следующая команда:

Admin@nodename# create libraries services <parameter>

Далее необходимо задать следующие параметры:

Параметр	Описание
name	Название сервиса.
description	Описание сервиса.
protocols	Указание сетевого протокола и портов источника/назначения: • protocol — сетевой протокол. • alg — L7 шлюз, только для TCP или UDP (поддерживается SIP, H323, FTP, TFTP — для протокола UDP). • dest-ports — порт(ы) назначения (указывается номер порта или диапазон портов). • source-ports — порт(ы) источника (указывается номер порта или диапазон портов).

Для редактирования существующего сервиса:

Admin@nodename# set libraries services <service-name> <parameter>

Для обновления сетевого протокола и портов источника/назначения сервиса:

Admin@nodename# set libraries services <service-name> protocols (<protocol-filter>)

<protocol-filter> — фильтр, настроенный с использованием значений параметра protocols.

Далее указываются новые значения параметра **protocols**.

Для добавления сетевого протокола и портов источника/назначения в существующий сервис:

```
Admin@nodename# set libraries services <service-name> protocols new <parameter>
```

Далее необходимо указать **protocol, dest-ports, source-ports**.

Чтобы удалить сервис используется следующая команда:

```
Admin@nodename# delete libraries services <service-name>
```

Также возможно удаления из сервиса заданных сетевых протоколов:

```
Admin@nodename# delete libraries services <service-name> protocols ( <protocol-filter> )
```

Следующие команды предназначены для отображения информации о всех сервисах или об определённом сервисе:

```
Admin@nodename# show libraries services
Admin@nodename# show libraries services <service-name>
```

Настройка групп сервисов

Данный раздел находится на уровне **libraries service-groups**. Для создания группы сервисов предназначена следующая команда:

```
Admin@nodename# create libraries service-groups <parameter>
```

Далее указываются параметры:

Параметр	Описание
name	Название группы сервисов.
description	Описание группы.
services	Сервисы, которые необходимо добавить в группу.

Для редактирования группы сервисов (список параметров, доступных для обновления, аналогичен списку параметров команды создания группы):

```
Admin@nodename# set libraries service-groups <service-group-name> <parameter>
```

Чтобы добавить в группу сервисы:

```
Admin@nodename# set libraries service-groups <service-group-name> [ <service1> < service2> ... ]
```

Следующие команды используются для удаления группы сервисов или отдельных сервисов, содержащихся в ней:

```
Admin@nodename# delete libraries service-groups <service-group-name>
Admin@nodename# delete libraries service-groups <service-group-name> services [ <service> ... ]
```

Команды отображения информации о всех имеющихся списках:

```
Admin@nodename# show libraries service-groups
```

об определённом списке:

```
Admin@nodename# show libraries service-groups <service-group-name>
```

или списка сервисов, добавленных в группу:

```
Admin@nodename# show libraries service-groups <service-group-name> services
```

Настройка IP-адресов

Данный раздел находится на уровне **libraries ip-list**.

Для создания группы IP-адресов используется следующая команда:

```
Admin@nodename# create libraries ip-list <parameter>
```

Далее необходимо задать следующие параметры:

Параметр	Описание
name	Название списка адресов.
description	Описание списка.
threat-lvl	Уровень угрозы: • very-low — очень низкий уровень угрозы. • low — низкий уровень угрозы. • medium — средний уровень угрозы. • high — высокий уровень угрозы. • very-high — высокий уровень угрозы.
type	Тип списка: • local — локальный. • updatable — если список является обновляемым, то необходимо указать адрес, с которого загружаются обновления (url). Периодичность обновления списка указывается параметром shedule в формате crontab. Crontab-формат: (минуты: 0-59) (часы: 0-23) (дни месяца: 1-31) (месяц: 1-12) (день недели: 0-6; 0 — вс). Каждое из поле 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".
lists	Выбор существующих IP-листов для добавления в создаваемый лист.
ips	IP-адреса или диапазон IP-адресов, которые необходимо включить в список. Указывается в формате: <ip>, <ip/mask> или <ip_range_start-ip_range_end>.

Для редактирования списка (список параметров, доступных для обновления, аналогичен списку параметров команды создания списка):

```
Admin@nodename# set libraries ip-list <ip-list-name> <parameter>
```

Чтобы добавить в список новые адреса:

```
Admin@nodename# set libraries ip-list <ip-list-name> ips [ <ip1> <ip2> ... ]
```

Следующие команды используются для удаления всего списка адресов или IP-адресов, содержащихся в нём:

```
Admin@nodename# delete libraries ip-list <ip-list-name>
Admin@nodename# delete libraries ip-list <ip-list-name> ips [ <ip1> <ip2>... ]
```

Команда отображения информации о всех имеющихся списках:

```
Admin@nodename# show libraries ip-list
```

Чтобы отобразить информацию об определённом списке, необходимо указать название интересующего списка IP-адресов:

```
Admin@nodename# show libraries ip-list <ip-list-name>
```

Также доступен просмотр содержимого списка IP-адресов:

```
Admin@nodename# show libraries ip-list <ip-list-name> items
```

Настройка Useragent браузеров

Раздел настраивается на уровне **libraries useragents**.

Следующая команда используется для добавления нового списка Useragent браузеров:

```
Admin@nodename# create libraries useragents <parameter>
```

Далее указываются следующие данные:

Параметр	Описание
name	Название списка Useragent.
description	Описание списка.
type	Тип списка: local — локальный. updatable — если список является обновляемым, то необходимо указать адрес, с которого загружаются обновления (url). Периодичность обновления списка указывается параметром shedule в формате crontab. Crontab-формат: (минуты: 0-59) (часы: 0-23) (дни месяца: 1-31) (месяц: 1-12) (день недели: 0-6; 0 — вс). Каждое из поле 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".
patterns	Шаблоны Useragent. Список Useragent браузеров доступен по ссылке: http://www.useragentstring.com/pages/useragentstring.php .

Для редактирования существующего списка:

```
Admin@nodename# set libraries useragents <useragent-list-name> <parameter>
```

Далее указываются параметры, которые необходимо обновить. Параметры представлены в таблице выше. Чтобы добавить новые Useragent браузеров:

```
Admin@nodename# set libraries useragents <useragent-list-name> [ <useragent1> <useragent2> ... ]
```

Следующие команды используются для удаления всего списка или отдельных Useragent браузеров, содержащихся в нём:

```
Admin@nodename# delete libraries useragents <useragent-list-name>
Admin@nodename# delete libraries useragents <useragent-list-name> patterns [ <useragent> ... ]
```

Команда отображения информации о всех имеющихся списках:

```
Admin@nodename# show libraries useragents
```

Чтобы отобразить информацию об определённом списке, необходимо указать название списка Useragent браузеров. Чтобы просмотреть содержание списка Useragent браузеров:

```
Admin@nodename# show libraries useragents <useragent-list-name> patterns
```

Настройка типов контента

Раздел **Типы контента** находится на уровне **libraries content-types**.

Добавление нового списка типов контента доступно с использованием следующей команды:

```
Admin@nodename# create libraries content-types <parameter>
```

Далее указывается следующая информация:

Параметр	Описание
name	Название списка типов контента.
description	Описание списка.
type	Тип списка: local — локальный. updatable — если список является обновляемым, то необходимо указать адрес, с которого загружаются обновления (url). Периодичность обновления списка указывается параметром shedule в формате crontab. Crontab-формат: (минуты: 0-59) (часы: 0-23) (дни месяца: 1-31) (месяц: 1-12) (день недели: 0-6; 0 — вс). Каждое из поле 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".
mime	Типы контента, которые необходимо добавить в список. Различные типы контента и их описание доступны по ссылке https://www.iana.org/assignments/media-types/media-types.xhtml .

Для редактирования списка используется следующая команда:

```
Admin@nodename# set libraries content-types <content-types-list-name> <parameter>
```

Параметры, доступные для обновления, представлены в таблице выше.

Следующая команда используется для удаления списка с типами контента:

```
Admin@nodename# delete libraries content-types <content-types-list-name>
```

Также доступно удаление отдельных типов контента из списка:

```
Admin@nodename# delete libraries content-types <content-types-list-name> mime [ <mime-type> ... ]
```

Следующие команды используются для отображения информации о списках типов контента:

```
Admin@nodename# show libraries content-types
Admin@nodename# show libraries content-types <content-types-list-name>
```

Для отображения типов контента, содержащихся в списке, используется команда:

```
Admin@nodename# show libraries content-types <content-types-list-name> mime
```

Настройка списков URL

Настройка списков URL производится на уровне **libraries url-list**.

Для добавления нового списка URL предназначена следующая команда:

```
Admin@nodename# create libraries url-list <parameter>
```

Далее указывается следующая информация:

Параметр	Описание
name	Название списка URL.
description	Описание списка URL.
type	Тип списка: local — локальный. updatable — если список является обновляемым, то необходимо указать адрес, с которого загружаются обновления (url). Периодичность обновления списка указывается параметром schedule в формате crontab. Crontab-формат: (минуты: 0-59) (часы: 0-23) (дни месяца: 1-31) (месяц: 1-12) (день недели: 0-6; 0 -вс). Каждое из поле 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".
urls	URL, которые необходимо добавить в список.
case-sensitivity	Чувствительность к регистру в написании адреса URL: - sensitive — чувствительно к регистру букв в адресе. - insensitive — нечувствительно к регистру букв в адресе. - domain — список адресов доменов.

Для редактирования списка URL:

```
Admin@nodename# set libraries url-list <url-list-name> <parameter>
```

Параметры, значения которых можно обновить, представлены в таблицы выше.

Далее представлены команды, с использованием которых доступно удаление всего списка URL или отдельных адресов URL:

```
Admin@nodename# delete libraries url-list <url-list-name>
```

```
Admin@hostname# delete libraries uri-list <uri-list-name> uris [ <uri> ... ]
```

Для просмотра информации о всех списках URL, об определённом списке URL или об адресах, входящих в определённый список, используются команды:

```
Admin@nodename# show libraries url-list
```

```
Admin@nodename# show libraries url-list <url-list-name>
```

```
Admin@nodename# show libraries url-list <url-list-name> urls
```

Настройка календарей

Данный раздел находится на уровне **libraries time-sets**.

Для создания группы используется следующая команда:

```
Admin@nodename# create libraries time-sets <parameter>
```

Далее необходимо задать следующие параметры:

Параметр	Описание
name	Название группы.
description	Описание группы.

Параметр	Описание
time-set	interval-name — название интервала повторения. type — тип интервала повторения: daily — ежедневно: time-from — время начала (указывается в формате HH:MM). time-to — время окончания (указывается в формате HH:MM). all-day on — весь день. weekly — каждую неделю: time-from — время начала (указывается в формате HH:MM). time-to — время окончания (указывается в формате HH:MM). all-day on — весь день. days [Mon Tue Wed Thu Fri Sat Sun] — дни недели. monthly — каждый месяц: time-from — время начала (указывается в формате HH:MM). time-to — время окончания (указывается в формате HH:MM). all-day on — весь день. days — числа месяца (от 1 до 31). fixed — одновременно: time-from — время начала (указывается в формате HH:MM). time-to — время окончания (указывается в формате HH:MM). all-day on — весь день. fixed-date — нужная дата (указывается в формате YYYY-MM-DD). span — повторяющиеся события: time-from — время начала (указывается в формате HH:MM). time-to — время окончания (указывается в формате HH:MM). all-day on — весь день. fixed-date-from — дата начала (указывается в формате YYYY-MM-DD). fixed-date-to — дата окончания (указывается в формате YYYY-MM-DD). range — диапазон дат: time-from-enabled <on off> — включение/отключение указания даты начала интервала. fixed-date-from — дата начала (указывается в формате YYYY-MM-DD). time-from — время начала (указывается в формате HH:MM). time-to-enabled <on off> — включение/отключение указания даты окончания интервала. fixed-date-to — дата окончания (указывается в формате YYYY-MM-DD). time-to — время окончания (указывается в формате HH:MM).

Для редактирования календаря:

```
Admin@nodename# set libraries time-sets <time-sets-name> <parameter>
```

Параметры, доступные для обновления, представлены в таблице выше.

Для редактирования интервала, заданного в календаре:

```
Admin@nodename# set libraries time-sets <time-sets-name> ... time-set <time-set-type> ( <time-set-filter> )
```

Далее указываются новые значения; <time-set-filter> — фильтр из текущих значений интервала.

Добавление нового элемента в существующую группу:

```
Admin@nodename# create libraries time-sets <time-sets-name> ... time-set <time-set-type> new
```

Команда для удаления группы элементов:

```
Admin@nodename# delete libraries time-sets <time-sets-name>
```

Для удаления элемента календаря:

```
Admin@nodename# delete libraries time-sets <time-sets-name> <time-set-type> ( <time-set-filter> )
```

Для отображения информации о всех календарях:

```
Admin@nodename# show libraries time-sets
```

Для отображения информации об определённом календаре:

```
Admin@nodename# show libraries time-sets <time-sets-name>
```

Для отображения информации об элементах группы с одинаковым типом повторения:

```
Admin@nodename# show libraries time-sets <time-sets-name> <time-set-type>
```

Настройка полос пропускания

Раздел находится на уровне **libraries bandwidth-pools**.

Для добавления новой полосы пропускания используется следующая команда:

```
Admin@nodename# create libraries bandwidth-pools <parameter>
```

Далее необходимо задать следующие параметры:

Параметр	Описание
name	Название полосы пропускания.
description	Описание полосы пропускания.
rate	Скорость передачи данных; указывается в Кбит/с.
dscp	Значение DSCP QoS (при указании будет прописываться в каждый IP-пакет; принимает значения от 0 до 63).

Для редактирования параметров полосы пропускания:

```
Admin@nodename# set libraries bandwidth-pools <bandwidth-name> <parameter>
```

Параметры, доступные для изменения такие же, как и для команды создания полосы пропускания.

Чтобы удалить полосу пропускания:

```
Admin@nodename# delete libraries bandwidth-pools <bandwidth-name>
```

С использованием **show** можно отобразить информацию о всех полосах пропускания:

```
Admin@nodename# show libraries bandwidth-pools
```

или об определённой полосе:

```
Admin@nodename# show libraries bandwidth-pools <bandwidth-name>
```

Настройка шаблонов страниц

Раздел находится на уровне **libraries response-pages**. Доступно создание следующих типов шаблонов страниц (<response-page-type>):

- **blockpage** — шаблоны страниц блокировки;
- **captiveportal-user-auth** — шаблоны страниц авторизации captive-портала;
- **captiveportal-user-session** — шаблоны страниц captive-портала, сессия пользователя;
- **content-warning** — шаблоны страниц предупреждения;
- **ftp-client** — шаблоны страниц отображения FTP поверх HTTP;
- **proxy-portal** — шаблоны страниц веб-портала;
- **pp-login-ssh** — шаблоны страниц SSH-логина веб-портала;
- **pp-login-rdp** — шаблоны страниц RDP-логина веб-портала;
- **totp-init-page** — шаблоны страниц инициализации TOTP;
- **network-error-page** — шаблоны страниц сетевых ошибок от прокси-сервера (доступно в версии ПО 7.4.0 и выше).

Команда, используемая для создания шаблона страницы:

```
Admin@nodename# create libraries response-pages <response-page-type> <parameter>
```

Необходимо указать параметры:

Параметр	Описание
name	Название шаблона страницы.
description	Описание шаблона.

Параметр	Описание
original-template	Выбор базового шаблона. Базовые шаблоны для страницы блокировки (blockpage): blockpage-en — шаблон страницы блокировки на английском языке; blockpage-ru — шаблон страницы блокировки на русском языке. Базовые шаблоны для страницы авторизации captive-портала (captiveportal-user-auth): captiveportal_user_auth-en — шаблон страницы авторизации пользователя с помощью captive-портала на английском языке; captiveportal_user_auth-ru — шаблон страницы авторизации пользователя с помощью captive-портала на русском языке; captiveportal-user-auth-policy-en — шаблон страницы авторизации пользователя с помощью captive-портала на английском языке. Шаблон, помимо формы авторизации, выводит правила пользования сетью (соглашение об использовании) и требует принятия пользователем правил политики доступа; captiveportal-user-auth-policy-ru — шаблон страницы авторизации пользователя с помощью captive-портала на русском языке. Шаблон, помимо формы авторизации, выводит правила пользования сетью (соглашение об использовании) и требует принятия пользователем правил политики доступа; captiveportal-user-auth-email-en — шаблон страницы авторизации пользователя с помощью captive-портала на английском языке, позволяющий пользователю самостоятельно зарегистрироваться в системе с подтверждением пользователя по email; captiveportal-user-auth-email-ru — шаблон страницы авторизации пользователя с помощью captive-портала на русском языке, позволяющий пользователю самостоятельно зарегистрироваться в системе с подтверждением пользователя по email; captiveportal-user-auth-sms-en — шаблон страницы авторизации пользователя с помощью captive-портала на английском языке, позволяющий пользователю самостоятельно зарегистрироваться в системе с подтверждением пользователя по SMS; captiveportal-user-auth-sms-ru — шаблон страницы авторизации пользователя с помощью captive-портала на русском языке, позволяющий пользователю самостоятельно зарегистрироваться в системе с подтверждением пользователя по SMS; captiveportal-user-policy-en — шаблон страницы авторизации пользователя с помощью captive-портала на английском языке. Шаблон не требует ввода имени и пароля пользователя, а выводит правила пользования сетью (соглашение об использовании) и требует принятия пользователем правил политики доступа. Для работы данного шаблона требуется установить метод Принять политику в качестве метода аутентификации в профиле авторизации; captiveportal-user-policy-ru — шаблон страницы авторизации пользователя с помощью captive-портала на русском языке. Шаблон не требует ввода имени и пароля пользователя, а выводит правила пользования сетью (соглашение об использовании) и требует принятия пользователем правил политики доступа. Для работы данного шаблона требуется установить метод Принять политику в качестве метода аутентификации в профиле авторизации. Базовые шаблоны для страницы captive-портал, сессия пользователя (captiveportal-user-session): captiveportal-user-session-en — шаблон на английском языке, с помощью которого пользователь может завершить свою авторизованную сессию, перейдя на страницу http://USERGATE_IP/cps: captiveportal-user-session-ru — шаблон на русском языке, с помощью которого пользователь может завершить свою авторизованную сессию, перейдя на страницу http://logout.captive или http://USERGATE_IP/cps. Базовые шаблоны для страницы предупреждения (content-warning): content-warning-en — шаблон страницы предупреждения на английском языке, отображаемый при срабатывании правила контентной фильтрации с действием Предупредить; content-warning-ru — шаблон страницы предупреждения на русском языке, отображаемый при срабатывании правила контентной фильтрации с действием Предупредить. Базовые шаблоны для страницы отображения FTP поверх HTTP (ftp-client): ftp-client-en — шаблон на английском языке для отображения контента FTP-серверов поверх HTTP; ftp-client-ru — шаблон на русском языке для отображения контента FTP-серверов поверх HTTP. Базовые шаблоны для страницы веб-портала (proxy-portal): proxy-portal-en — шаблон на английском языке для отображения страницы веб-портала; proxy-portal-ru — шаблон на русском языке для отображения страницы веб-портала. Базовые шаблоны для страницы SSH-логина веб-портала (pp-login-ssh): pp-login-ssh-en — шаблон на английском языке для отображения страницы аутентификации при подключении к ресурсам SSH через веб-портал; pp-login-ssh-ru — шаблон на русском языке для отображения страницы аутентификации при подключении к ресурсам SSH через веб-портал. Базовые шаблоны для страницы RDP-логина веб-портала (pp-login-rdp): pp-login-rdp-en — шаблон на английском языке для отображения страницы аутентификации при подключении к ресурсам RDP через веб-портал; pp-login-rdp-ru — шаблон на русском языке для отображения страницы аутентификации при подключении к ресурсам RDP через веб-портал. Базовые шаблоны для страницы инициализации TOTP (totp-init-page): totp-init-page-en — шаблон на английском языке для отображения страницы инициализации устройства TOTP для VPN-пользователей; totp-init-page-ru — шаблон на русском языке для отображения страницы инициализации устройства TOTP для VPN-пользователей. Базовые шаблоны для страницы сетевых ошибок от прокси-сервера (network-error-page). Доступно в версии ПО 7.4.0 и выше: network-error-page-en — шаблон на английском языке для отображения страницы сетевых ошибок от прокси-сервера; network-error-page-ru — шаблон на русском языке для отображения страницы сетевых ошибок от прокси-сервера.
default	Использовать шаблон по умолчанию: on; off.

```
Для редактирования значений шаблона:
Admin@nodename# set libraries response-pages <response-page-type> <response-page-name> <parameters>

Далее необходимо указать значения параметров; параметры представлены в таблице выше.

Чтобы удалить шаблон страницы, используется следующая команда:
Admin@nodename# delete libraries response-pages <response-page-type> <response-page-name>

Для просмотра информации о всех имеющихся шаблонах страниц:
Admin@nodename# show libraries response-pages

Для просмотра информации об отдельном типе шаблонов страниц:
Admin@nodename# show libraries response-pages <response-page-type>

Для просмотра информации об отдельном шаблоне страницы:
Admin@nodename# show libraries response-pages type <response-page-type> <response-page-name>
```

Настройка категорий URL

Раздел находится на уровне **libraries url-categories**.

Для создания группы категорий URL используется следующая команда:

```
Admin@nodename# create libraries url-categories <parameter>
```

Параметры, которые необходимо указать:

Параметр	Описание

Параметр	Описание
name	Название группы URL-категорий.
description	Описание группы.
categories	Категории URL, которые необходимо добавить в группу.

Команда для редактирования параметров группы:

Admin@nodename# set libraries url-categories <list-name> <parameter>

Для добавления категорий URL в существующую группу:

Admin@nodename# set libraries url-categories <list-name> categories [<url-category> ...]

Команды для удаления группы URL-категорий:

Admin@nodename# delete libraries url-categories <list-name>

или отдельных категорий из группы:

Admin@nodename# delete libraries url-categories <list-name> categories [<url-category> ...]

Команды для просмотра информации о всех группах URL-категорий:

Admin@nodename# show libraries url-categories

об определённой группе:

Admin@nodename# show libraries url-categories <list-name>

Чтобы отобразить список категорий URL, входящих в группу:

Admin@nodename# show libraries url-categories <list-name> categories

Настройка изменённых категорий URL

Настройка раздела **Изменённые категории URL** производится на уровне **overridden-url-categories**.

Для добавления новой изменённой категории URL:

Admin@nodename# create libraries overridden-url-categories <parameter>

Далее необходимо указать параметры:

Параметр	Описание
domain	Доменное имя проверяемого ресурса.
description	Описание изменяемого домена.
categories	Новые категории сайта (можно указать не более 2-х категорий).

Для редактирования параметров:

Admin@nodename# set libraries overridden-url-categories <domain> <parameter>

Для удаления сайта с изменёнными категориями:

Admin@nodename# delete libraries overridden-url-categories <domain>

Для отображения всего списка сайтов с изменёнными категориями:

Admin@nodename# show libraries overridden-url-categories

Для отображения информации об определённом сайте с изменёнными категориями URL:

Admin@nodename# show libraries overridden-url-categories <domain>

Настройка групп приложений

Данный раздел настраивается на уровне **libraries application-groups**.

Для создания группы приложений используется команда:

Admin@nodename# create libraries application-groups

Далее указываются параметры:

Параметр	Описание
name	Название группы приложений.
description	Описание группы приложений.
apps	Приложения, которые необходимо добавить в группу.

Для редактирования параметров:

Admin@nodename# set libraries application-groups <app-group-name>

Чтобы добавить новые приложения в существующую группу, используется команда:

Admin@nodename# set libraries application-groups <app-group-name> apps [<application> ...]

Для удаления группы приложений полностью или отдельных приложений в ней используются команды:

Admin@nodename# delete libraries application-groups <app-group-name>

Admin@nodename# delete libraries application-groups <app-group-name> apps [<application> ...]

Следующие команды предназначены для отображения информации о всех созданных группах приложений:

Admin@nodename# show libraries application-groups

или об определённой группе:

Admin@nodename# show libraries application-groups <app-group-name>

Также доступно отображение приложений, входящих в определённый список:

Admin@nodename# show libraries application-groups <app-group-name> apps

Настройка профилей приложений

Настройка профилей приложений производится на уровне **libraries application-profile**.

Для создания профиля приложений используется команда:

Admin@nodename# create libraries application-profile <parameter>

Необходимо указание следующих параметров:

Параметр	Описание
name	Название профиля приложений.
description	Описание профиля приложений.
filters	Фильтр для выбора релевантных сигнатур из библиотеки сигнатур приложений.
unknown-application-settings	Параметры сигнатуры для неизвестных приложений.

Представленная ниже команда предназначена для редактирования существующего профиля приложений:

```
Admin@nodename# set libraries application-profile <application-profile-name> <parameter>
```

Параметры, доступные для обновления, аналогичны параметрам, доступным при создании профиля.

С использованием следующих команда возможен просмотр информации о всех профилях приложений:

```
Admin@nodename# show libraries application-profile
```

или об одном профиле:

```
Admin@nodename# show libraries application-profile <application-profile-name>
```

Пример создания профиля приложений:

```
Admin@nodename# create libraries application-profile name "Test app profile 1" description "Test app profile 1 description" filters new action drop value "category = Games" enabled on
Admin@nodename# show libraries application-profile "Test app profile 1"
```

```
name      : Test app profile 1
description : Test app profile 1 description
filters   :
  enabled  : on
  value    : category = Games
  enable-setting : on
  action   : drop
  pcap    : off
  track-by : src
  duration : 0 days 0 hours 5 minutes
```

Для удаления профиля приложений используется команда:

```
Admin@nodename# delete libraries application-profile <application-profile-name>
```

Подробнее о профилях приложений читайте в статье [Профили приложений](#) Руководства администратора.

Настройка сигнатур приложений

На уровне **libraries application-signature** возможно создание и настройка пользовательских кастомизированных сигнатур приложений.

Для создания пользовательской сигнатуры приложений используется команда:

```
Admin@nodename# create libraries application-signature <parameters>
```

Необходимо указание следующих параметров:

Параметр	Описание
name	Название сигнатуры. Не может быть изменено для сигнатур, созданных UserGate.
description	Описание сигнатуры. Не может быть изменено для сигнатур, созданных UserGate.
signature-id	Идентификатор группы сигнатур. Не может быть изменен для сигнатур, созданных UserGate.
enabled	Индикатор включения сигнатуры. - on -включить. - off — отключить.
categories	Категория сигнатуры приложений — группа сигнатур, объединенных общими параметрами. Список категорий приложений может быть пополнен. - Media streaming - Email - Coin Miners - TunnelingGames - Remote access - Conferencing - Trojan Horses - Business - Mobile - Proxies and anonymizers - Standard networks - VOIP - Web posting - Software update - File storage and backup - Web browsing - File sharing P2P - Instant messaging - Social networking

Параметр	Описание
threat	Уровень угрозы, определяемый сигнатурой. Определены следующие значения: • very-low — очень низкий. • low — низкий. • medium — средний. • high — высокий. • very-high — очень высокий.
technology	Технология приложения. • browser-based — браузерное веб-приложение. • client-server — клиент-серверное приложение. • network-protocol — сетевой протокол. • peer-to-peer — приложение точка-точка.
type	Тип сигнатуры: • app — сигнатура приложения. • proto — сигнатура протокола. • support — вспомогательная сигнатура.
uasl	Описание сигнатуры приложений с помощью синтаксиса UASL.

Представленная ниже команда предназначена для редактирования ранее созданной сигнатуры приложений:

```
Admin@nodename# set libraries application-signature <application-signature-name> <parameters>
```

Параметры, доступные для обновления, аналогичны параметрам, доступным при создании сигнатуры.

С использованием следующих команда возможен просмотр информации о всех сигнатурах приложений:

```
Admin@nodename# show libraries application-signature
```

или об одной сигнатуре:

```
Admin@nodename# show libraries application-signature <application-signature-name>
```

Пример создания сигнатуры приложений:

```
Admin@nodename# create libraries application-signature name "Test app signature 2" description "Test app signature 2 description" categories [ "Web browsing" ] signature-id 2 technology browser-based threat low type app uasl "UASL(.dst_addr=
Admin@nodename# show libraries application-signature "Test app signature 2"
```

```
signature-id : 2
name         : Test app signature 2
threat       : low
technology   : browser-based
categories   : Web browsing
uasl         : UASL(.dst_addr=192.168.10.1;)
owner        : You
type         : custom
description  : Test app signature 2 description
```

Для удаления созданной ранее сигнатуры приложений используется команда:

```
Admin@nodename# delete libraries application-signature <application-signature-name>
```

Подробнее о сигнатурах приложений читайте в статье [Приложения](#) Руководства администратора.

Настройка тайм-аутов приложений

Значение пользовательского тайм-аута бездействия для приложения настраивается в интерфейсе командной строки (CLI) на уровне libraries application-signature.

Для проприетарных сигнатур приложений (сигнатур, созданных UserGate) значение тайм-аута бездействия устанавливается с помощью команды:

```
Admin@nodename# set libraries application-signature <"signature-name"> idle-timeout <num>
```

Значение тайм-аута указывается в секундах в диапазоне от 60 до 604 800.

Посмотреть установленное значение тайм-аута можно с помощью команды:

```
Admin@nodename# show libraries application-signature <"signature-name">
```

Пример:

```
Admin@nodename# set libraries application-signature "1C" idle-timeout 400
Admin@nodename# show libraries application-signature "1C"

signature-id : 188
name         : 1C
type         : app
description  : 1C is a Russian company specializing in the distribution, support and development of computer programs
              and databases for business and home use.
threat       : very-low
technology   : Client-server
categories   : Business
idle-timeout : 400
```

Вернуть значение тайм-аута по умолчанию можно с помощью команды:

```
Admin@nodename# set libraries application-signature <"signature-name"> idle-timeout default
```

Примеч:

```
Admin@oulmetioeth# set libraries application-signature "1C" idle-timeout default
Admin@oulmetioeth# show libraries application-signature "1C"
```

```
signature-id : 188
name         : 1C
type         : app
description  : 1C is a Russian company specializing in the distribution, support and development of computer programs
              and databases for business and home use.
threat       : very-low
technology   : Client-server
categories   : Business
idle-timeout : default
```

В пользовательских сигнатурах (сигнатурах, созданных самими пользователями) значение тайм-аута бездействия можно указать при создании сигнатуры:

```
Admin@nodename# create libraries application-signature name <signature-name> uasl <"uasl-code"> idle-timeout <num>
```

Значение тайм-аута указывается в секундах.

Посмотреть установленное значение тайм-аута можно с помощью команды:

```
Admin@nodename# show libraries application-signature <"signature-name">
```

Пример создания пользовательской сигнатуры с указанием тайм-аута бездействия:

```
Admin@nodename# create libraries application-signature name test_sig1 uasl "UASL(.name=\"EXAMPLE2\")" idle-timeout 500
Admin@nodename# show libraries application-signature "test_sig1"
```

```
signature-id : 1050002
name : test_sig1
type : app
threat : very-low
idle-timeout : 500
uasl : UASL(.name="EXAMPLE2");
```

В ранее созданных пользовательских сигнатурах можно менять значение тайм-аута с помощью команды:

```
Admin@nodename# set libraries application-signature <"signature-name"> idle-timeout <num>
```

Пример:

```
Admin@oulmetioeth# set libraries application-signature "test_sig1" idle-timeout 700
Admin@oulmetioeth# show libraries application-signature "test_sig1"
```

```
signature-id : 1050002
name : test_sig1
type : app
threat : very-low
idle-timeout : 700
uasl : UASL(.name="EXAMPLE2");
```

Установить значение тайм-аута по умолчанию (в зависимости от протокола транспортного уровня) можно с помощью команды:

```
Admin@nodename# set libraries application-signature <"signature-name"> idle-timeout default
```

Настройка почтовых адресов

Раздел находится на уровне **libraries email-list**.

Чтобы добавить новую группу почтовых адресов используется следующая команда:

```
Admin@nodename# create libraries email-list <parameter>
```

Далее указываются параметры:

Параметр	Описание
name	Название группы почтовых адресов.
description	Описание группы почтовых адресов.
type	Тип списка: • local — локальный. • updatable — если список является обновляемым, то необходимо указать адрес, с которого загружаются обновления (url). Периодичность обновления списка указывается параметром schedule в формате crontab. Crontab-формат: (минуты: 0-59) (часы: 0-23) (дни месяца: 1-31) (месяц: 1-12) (день недели: 0-6; 0 — вс). Каждое из поле 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".
emails	Почтовые адреса, которые необходимо добавить в данную группу.

Команда, предназначенная для редактирования информации о группе почтовых адресов:

```
Admin@nodename# set libraries email-list <email-list-name> <parameter>
```

Параметры, доступные для обновления, аналогичны параметрам, доступным при создании группы почтовых адресов.

Для удаления группы или почтовых адресов из неё используются следующие команды:

```
Admin@nodename# delete libraries email-list <email-list-name>
Admin@nodename# delete libraries email-list <email-list-name> emails [ <email> ... ]
```

Следующие команды используются для просмотра информации о всех созданных группах, об определённых группах или для просмотра почтовых адресов, входящих в группу:

```
Admin@nodename# show libraries email-list
Admin@nodename# show libraries email-list <email-list-name>
Admin@nodename# show libraries email-list <email-list-name> emails
```

Настройка номеров телефонов

Настройка раздела **Номера телефонов** производится на уровне **libraries phone-list**.

Для создания группы телефонных номеров:

```
Admin@nodename# create libraries phone-list <parameter>
```

Далее необходимо указать следующие данные:

Параметр	Описание
name	Название группы телефонных номеров.
description	Описание группы телефонных номеров.
type	Тип списка: • local — локальный. • updatable — если список является обновляемым, то необходимо указать адрес, с которого загружаются обновления (url). Периодичность обновления списка указывается параметром schedule в формате crontab. Crontab-формат: (минуты: 0-59) (часы: 0-23) (дни месяца: 1-31) (месяц: 1-12) (день недели: 0-6; 0 — вс). Каждое из поле 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".
phones	Номера телефонов, которые необходимо добавить в данную группу.

Для редактирования информации о группе телефонных номеров используется команда:

```
Admin@nodename# set libraries phone-list <phone-list-name> <parameter>
```

Параметры, доступные для обновления, представлены в таблице выше.

Для удаления группы или номеров телефонов из неё используются следующие команды:

```
Admin@nodename# delete libraries phone-list <phone-list-name>
Admin@nodename# delete libraries phone-list <phone-list-name> phones [ <phone> ... ]
```

Следующие команды используются для просмотра информации о всех созданных группах:

```
Admin@nodename# show libraries phone-list
```

или об определённых группах телефонных номеров:

```
Admin@nodename# show libraries phone-list <phone-list-name>
```

Для просмотра номеров, содержащихся в группе, используется команда:

```
Admin@nodename# show libraries phone-list <phone-list-name> phones
```

Настройка сигнатур COB

На уровне **libraries ips-signature** возможно создание и настройка пользовательских кастомизированных сигнатур системы обнаружения вторжения (COB).

Для создания пользовательской сигнатуры COB используется команда:

```
Admin@nodename# create libraries ips-signature <parameters>
```

Необходимо указание следующих параметров:

Параметр	Описание
name	Название сигнатуры COB. Не может быть изменено для сигнатур, созданных UserGate.
description	Описание сигнатуры COB. Не может быть изменено для сигнатур, созданных UserGate.
signature-id	Идентификатор группы сигнатур. Не может быть изменен для сигнатур, созданных UserGate.
enabled	Индикатор включения сигнатуры. - on — включить. - off — отключить.
threat	Уровень угрозы, определяемый сигнатурой. Определены следующие значения: - very-low — очень низкий. - low — низкий. - medium — средний. - high — высокий. - very-high — очень высокий. Не может быть изменен для сигнатур, созданных UserGate.
action	Действие на срабатывание сигнатуры. Определены следующие значения: - none — действие не определено. - pass — пропустить пакет. - drop — отбросить пакет. - rst — отбросить пакет с разрывом TCP соединения (отправка TCP reset). - block — блокировать IP-адрес источника и/или назначения.
log	Журналирование: - on — включить запись в журнал. - off — отключить запись в журнал.
os	Тип операционной системы, для которой определена сигнатура: - windows - linux - bsd - macos - solaris - cisco - ios - android - other Не может быть изменено для сигнатур, созданных UserGate.
pcap	Трассировка срабатывания сигнатуры с записью в файл формата pcap. - on — включить. - off — отключить.
track-by	Применимость действий типа block или rst на срабатыване сигнатуры: - src — действия block или rst применяются к адресу источника отправления пакетов. - dst — действия block или rst применяются к адресу назначения отправления пакетов. - both — действия block или rst применяются и к источнику, и к назначению.
duration	Длительность блокировки для действия block .
uasl	Описание сигнатуры с помощью синтаксиса UASL. Не может быть изменено для сигнатур, созданных UserGate.
cve	Идентификатор уязвимостей по реестру CVE.

Параметр	Описание
bdu	Идентификатор уязвимостей по реестру BDU.
uri	Опциональная ссылка на ресурс с описанием уязвимости.
category	Категория сигнатуры — группа сигнатур, объединенных общими параметрами. Список категорий может быть пополнен. • adware pup. • attack_response — сигнатуры, определяющие ответы на известные сетевые атаки. • coinminer — скачивание, установка, деятельность известных майнеров. • dns — известные уязвимости DNS. • dos — сигнатуры известных Denial of services атак. • exploit — сигнатуры известных exploits. • ftp — известные FTP-уязвимости. • imap — известные IMAP-уязвимости. • info — потенциальная утечка информации. • ldap — известные LDAP-уязвимости. • malware — скачивание, установка, деятельность известных malware. • misc — другие известные сигнатуры. • netbios — известные уязвимости протокола NETBIOS. • phishing — сигнатуры известных phishing атак. • pop3 — известные уязвимости протокола POP3. • rpc — известные уязвимости протокола RPC. • scada — известные уязвимости протокола SCADA. • scan — сигнатуры, определяющие попытки сканирования сети на известные приложения. • shellcode — сигнатуры, определяющие известные попытки запуска программных оболочек. • smtp — известные уязвимости протокола SMTP. • snmp — известные уязвимости протокола SNMP. • sql — известные уязвимости SQL. • telnet — известные попытки взлома по протоколу telnet. • tftp — известные уязвимости протокола TFTP. • user_agents — сигнатуры подозрительных Useragent. • voip — известные уязвимости протокола VoIP. • web_client — сигнатуры, определяющие известные попытки взлома различных веб-клиентов, например, Adobe Flash Player. • web_server — сигнатуры, определяющие известные попытки взлома различных веб-серверов. • web_specific_apps — сигнатуры, определяющие известные попытки взлома различных веб приложений. • worm — сигнатуры, определяющие сетевую активность известных сетевых червей. Не может быть изменена для сигнатур, созданных UserGate.
classtype	Класс сигнатуры определяет тип атаки, которая детектируется данной сигнатурой. Определяются также общие события, которые не относятся к атаке, но могут быть интересны в определенных случаях, например, обнаружение установления сессии TCP. Список классов может быть пополнен. • arbitrary-code-execution — попытка запуска произвольного кода. • attempted-admin — попытка получения административных привилегий. • attempted-dos — попытка совершения атаки Denial of Service. • attempted-recon — попытка атаки, направленной на утечку данных. • attempted-user — попытка получения пользовательских привилегий. • bad-unknown — потенциально плохой трафик. • command-and-control — попытка общения с C&C центром • default-login-attempt — попытка логина с именем/паролем по умолчанию. • denial-of-service — обнаружена атака Denial of Service. • exploit-kit — обнаружен exploit kit • misc-activity — прочая активность. • misc-attack — обнаружена атака. • shellcode-detect — обнаружен исполняемый код. • string-detect — обнаружена подозрительная строка. • suspicious-login — попытка логина с использованием подозрительного имени пользователя. • trojan-activity — обнаружен сетевой троян. • web-application-attack — обнаружена атака на веб-приложение. Не может быть изменен для сигнатур, созданных UserGate.

Представленная ниже команда предназначена для редактирования ранее созданной сигнатуры COB:

```
Admin@nodename# set libraries ips-signature <ips-signature-name> <parameters>
```

Параметры, доступные для обновления, аналогичны параметрам, доступным при создании сигнатуры.

С использованием следующих команд возможен просмотр информации о сигнатурах COB:

```
Admin@nodename# show libraries ips-signature
```

или об определенной сигнатуре:

```
Admin@nodename# show libraries ips-signature <ips-signature-name>
```

Пример создания сигнатуры COB:

```
Admin@nodename# create libraries ips-signature name "Test signature" action none threat low description "Test signature description" log on pcap on url example.org uasl "UASL(.name="EXAMPLE");" enabled off
Admin@nodename# show libraries ips-signature "Test signature"
```

```
signature-id : 5
name         : Test signature
enabled      : off
description  : Test signature description
threat       : low
action       : none
log          : on
```

pcap : on
track-by : src
duration : 0 days 0 hours 5 minutes
uasl : UASL(.name="EXAMPLE";)
url : example.org
owner : You
type : custom

Для удаления созданной ранее сигнатуры COB используется команда:

Admin@nodename# delete libraries ips-signature <ips-signature-name>

Подробнее о сигнатурах COB читайте в статье [Сигнатуры COB](#) Руководства администратора.

Настройка профилей COB

Настройка профилей COB производится на уровне **libraries ips-profile**.

Для создания профиля системы обнаружения вторжения используется команда:

Admin@nodename# create libraries ips-profile <parameter>

Необходимо указание следующих параметров:

Параметр	Описание
name	Название профиля COB.
description	Описание профиля COB.
filters	Фильтр для выбора релевантных сигнатур из библиотеки сигнатур COB. new — создание нового фильтра в профиле; value — SQL-подобное выражение для выбора сигнатур из библиотеки; enabled — активация фильтра в профиле; settings — задание свойств отобранных фильтром сигнатур: action — предпринимаемое действие, если сигнатура сработала, т.е. была найдена в трафике. Действия могут быть следующие: пропустить пакет (pass), отбросить пакет (drop), сбросить пакет с разрывом TCP соединения (reset), блокировать IP-адрес источника и/или назначения (block-ip). Значение default (по умолчанию) оставляет для всех сигнатур то действие, которое было определено в самих сигнатурах по умолчанию. enabled — возможность включить/отключить сигнатуры. log — включение/отключение журналирования срабатывания сигнатуры. pcap-file — включение/отключение записи в PCAP-файл, если сигнатура сработала.

Пример создания профиля COB:

Admin@nodename# create libraries ips-profile name 222 filters new value "protocol = 'http' AND (category = 'exploit') AND (os = 'Linux')\" settings action drop log on pcap-file on enabled on

Команда для редактирования существующего профиля COB:

Admin@nodename# set libraries ips-profile <ips-profile-name> <parameter>

Список настраиваемых параметров аналогичен списку параметров, используемых при создании профиля (таблица выше).

Пример редактирования созданного ранее профиля COB:

Admin@nodename# set libraries ips-profile 222 filters 1 settings action reset

С помощью следующей команды можно перенастроить параметры системных сигнатур COB, входящих в правило:

Admin@nodename# set libraries ips-profile <ips-profile-name> override signature <signature-name> <parameters>

Следующая команда позволяет вернуть перенастроенные ранее параметры системной сигнатуры COB в первоначальное значение:

Admin@nodename# set libraries ips-profile <ips-profile-name> override signature <signature-name> restore-default

С использованием следующих команд возможен просмотр информации о профилях COB:

Admin@nodename# show libraries ips-profile

или об определенном профиле:

Admin@nodename# show libraries ips-profile <ips-profile-name>

Пример просмотра определенного фильтра в ранее созданном профиле COB:

Admin@nodename# show libraries ips-profile 222 filters 1

enabled : on
value : protocol = 'http' AND (category = 'exploit') AND (os = 'Linux')
settings :
enabled : on
action : reset
pcap-file : on
duration : 5
track-by : both
log : on

Для удаления профиля COB используется команда:

Admin@nodename# delete libraries ips-profile <ips-profile-name>

Для удаления определенного фильтра в ранее созданном профиле COB используется команда:

Admin@nodename# delete libraries ips-profile <ips-profile-name> filters <filter-number>

Подробнее о профилях COB читайте в статье [Профили COB](#) Руководства администратора.

Настройка профилей оповещений

Профили оповещений SMTP (по email) и SMPP (по SMS) настраиваются на уровне **libraries notification-profiles**.

Для добавления нового профиля оповещения SMTP:

Admin@nodename# create libraries notification-profiles smtp <parameter>

Далее необходимо указать:

Параметр	Описание
name	Название профиля.
description	Описание профиля.
host	IP-адрес или FQDN сервера SMTP, который будет использоваться для отсылки почтовых сообщений.
port	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.

Параметр	Описание
connection-security	Варианты безопасности отправки почты; возможны варианты: • none. • starttls. • ssl.
authentication	Включение/отключение авторизации при подключении к серверу SMTP: • on. • off.
login	Имя учётной записи для подключения к SMTP-серверу.
password	Пароль учётной записи для подключения к SMTP-серверу.

Для создания профиля оповещения по SMS (SMPP):

Admin@nodename# create libraries notification-profiles smpp <parameter>

Далее необходимо указать значения следующих параметров:

Параметр	Описание
name	Название профиля.
description	Описание профиля.
host	IP-адрес или FQDN сервера SMPP, который будет использоваться для отсылки SMS.
port	Порт TCP, который используется для подключения к серверу SMPP. Обычно для протокола SMPP используется порт 2775; при использовании SSL — 3550.
ssl	Включение/отключение шифрования SSL: • on. • off.
login	Имя учётной записи для подключения к SMPP-серверу.
password	Пароль учётной записи для подключения к SMPP-серверу.
phone-translation-rules	Правила трансляции телефонных номеров. Правила используются для соответствия требованиям провайдера. Например, если необходимо заменить все номера, начинающиеся на +7, на 8: Admin@nodename# set libraries notification-profiles smpp <profile-name> phone-translation-rules + [+7/8]
source-ton	Тип номера (Type of Number) для источника сообщения: • 0 — Unknown (Неизвестный). • 1 — International (Международный). • 2 — National (Государственный). • 3 — Network Specific (Сетевой Специальный). • 4 — Subscriber Number (Номер абонента). • 5 — Alphanumeric (Алфавитно-цифровой). • 6 — Abbreviated (Сокращённый).
dest-ton	Тип номера (Type of Number) для адресата: • 0 — Unknown (Неизвестный). • 1 — International (Международный). • 2 — National (Государственный). • 3 — Network Specific (Сетевой Специальный). • 4 — Subscriber Number (Номер абонента). • 5 — Alphanumeric (Алфавитно-цифровой). • 6 — Abbreviated (Сокращённый).
source-npi	Индикатор схемы присвоения номеров (Numbering Plan Indicator) для источника: • 0 — Unknown. • 1 — ISDN/telephone numbering plan (E.163/E.164). • 3 — Data numbering plan (X.121). • 4 — Telex numbering plan (F.69). • 6 — Land Mobile (E.212). • 8 — National numbering plan. • 9 — Private numbering plan. • 10 — ERMES numbering plan (ETSI DE/PS 3 01-3). • 13 — Internet (IP). • 18 — WAP Client Id (to be defined by WAP Forum).

Параметр	Описание
dest-npi	Индикатор схемы присвоения номеров (Numbering Plan Indicator) для адресата: 0 — Unknown. 1 — ISDN/telephone numbering plan (E.163/E.164). 3 — Data numbering plan (X.121). 4 — Telex numbering plan (F.69). 6 — Land Mobile (E.212). 8 — National numbering plan. 9 — Private numbering plan. 10 — ERMES numbering plan (ETSI DE/PS 3 01-3). 13 — Internet (IP). 18 — WAP Client Id (to be defined by WAP Forum).

Для редактирования профиля оповещения используется команда:

```
Admin@nodename# set libraries notification-profiles <smtp | smpp> <profile-name> <parameter>
```

Параметры профилей SMTP и SMPP, доступные для изменения, представлены в соответствующих таблицах выше.

Для удаления профиля:

```
Admin@nodename# delete libraries notification-profiles <smtp | smpp> <profile-name>
```

Также для профилей оповещений SMPP доступно удаления правил трансляции номеров:

```
Admin@nodename# delete libraries notification-profiles smpp <profile-name> phone-translation-rules [ phone1|phone2 ]
```

Следующие команды предназначены для отображения информации о всех имеющихся профилях оповещений:

```
Admin@nodename# show libraries notification-profiles
```

о всех профилях одного типа:

```
Admin@nodename# show libraries notification-profiles <smtp | smpp>
```

об определённом профиле оповещения:

```
Admin@nodename# show libraries notification-profiles <smtp | smpp> <profile-name>
```

Настройка профилей Netflow

Раздел находится на уровне **libraries netflow-profiles**.

Команда для создания профиля NetFlow:

```
Admin@nodename# create libraries netflow-profiles <parameter>
```

Далее необходимо указать параметры профиля:

Параметр	Описание
name	Название профиля NetFlow.
description	Описание профиля.
ip	IP-адрес NetFlow коллектора, куда сенсор будет отправлять статистику.
port	UDP порт, на котором NetFlow коллектор будет принимать статистику.
protocol	Версия протокола NetFlow, которую необходимо использовать (должна совпадать на сенсоре и коллекторе): 5 — Netflow версии 5. 9 — Netflow версии 9. 10 — Netflow версии 10.
active-timeout	Время, через которое будет отправляться статистика на коллектор, не дожидаясь завершения потока (например, передача большого файла через сеть). Задаётся в секундах; значение по умолчанию: 1800 секунд, максимальное значение — 3600 секунд.
inactive-timeout	Время, резервируемое на завершение неактивного потока; указывается в секундах. Значение по умолчанию — 15 секунд; максимальное значение — 3600 секунд.
max-flows	Максимальное количество учитываемых потоков, с которых собирается и отправляется статистика. После достижения указанного количества все последующие потоки не будут учитываться (ограничение необходимо для защиты от DoS-атак); значение по умолчанию — 2000000; для снятия ограничения установить 0.
nat-events	Включить/отключить отправку информации о NAT преобразованиях в статистику NetFlow: on. off.
refresh-rate	Количество пакетов, после которого шаблон отправляется на принимающий хост (только для версий протокола NetFlow 9/10). Шаблон содержит информацию о настройке самого устройства и различную статистическую информацию. Значение по умолчанию — 20 пакетов.
timeout-rate	Время, через которое старый шаблон отправляется на принимающий хост (только для версий протокола NetFlow 9/10). Шаблон содержит информацию о настройке самого устройства и различную статистическую информацию. Значение по умолчанию — 1800 секунд.

Чтобы редактировать существующий профиль:

```
Admin@nodename# set libraries netflow-profiles <profile-name>
```

Параметры, значения которых можно изменить, представлены в таблице выше.

Следующая команда предназначена для удаления профиля NetFlow:

```
Admin@nodename# delete libraries netflow-profiles <profile-name>
```

Для отображения информации о всех профилях NetFlow или об отдельном профиле используются следующие команды:

```
Admin@nodename# show libraries netflow-profiles
Admin@nodename# show libraries netflow-profiles <profile-name>
```

Настройка профилей LLDP

Создание и настройка профилей LLDP (Link Layer Discovery Protocol) производятся на уровне **libraries lldp-profiles**.

Команда для создания профиля LLDP:

Admin@nodename# create libraries lldp-profiles <parameter>

Далее представлены параметры, которые необходимо указать:

Параметр	Описание
name	Название профиля LLDP.
description	Описание профиля.
port-status	Режимы: - rx — только приём данных LLDP — UserGate не будет посылать информацию LLDP, но будет анализировать информацию LLDP от соседей. - tx — только передача данных LLDP — UserGate будет посылать информацию LLDP, но будет отбрасывать информацию LLDP, полученную от соседей. - rx-tx — приём и передача данных LLDP — UserGate будет посылать информацию LLDP и будет анализировать информацию LLDP, полученную от соседей.

Следующая команда предназначена для редактирования информации о профиле:

Admin@nodename# set libraries lldp-profiles <profile-name> <parameter>

Параметры, доступные для обновления, аналогичны параметрам, указываемым при создании профиля.

Пользователь может удалить профиль LLDP, используя следующую команду:

Admin@nodename# delete libraries lldp-profiles <profile-name>

Чтобы отобразить информацию о профилях:

Admin@nodename# show libraries lldp-profiles
Admin@nodename# show libraries lldp-profiles <profile-name>

Настройка профилей SSL

Создание и настройка профилей SSL производятся на уровне **libraries ssl-profiles**.

Команда для создания профиля SSL:

Admin@nodename# create libraries ssl-profiles <parameter>

Далее представлены параметры, которые необходимо указать:

Параметр	Описание
name	Название профиля SSL.
description	Описание профиля.
min-tls-version	Минимальная версия TLS, которая может быть использована в данном профиле: - tls1. - tls1.1. - tls1.2.
max-tls-version	Максимальная версия TLS, которая может быть использована в данном профиле: - tls1. - tls1.1. - tls1.2. - tls1.3.
ssl-ciphers	Выбор необходимых алгоритмов шифрования и цифровой подписи.
ssl-ciphers-suite	Установка алгоритмов шифрования для стандартных протоколов. Параметр предназначен для облегчения выбора необходимых алгоритмов шифрования и подписи для стандартных протоколов TLS; необходимо указать версию: - tls1. - tls1.1. - tls1.2. - tls1.3.

Следующая команда предназначена для редактирования информации о профиле:

Admin@nodename# set libraries ssl-profiles <profile-name> <parameter>

Параметры, доступные для обновления, аналогичны параметрам, указываемым при создании профиля.

Пользователь может удалить профиль SSL полностью или удалить отдельные алгоритмы шифрования и цифровой подписи, заданные в нём:

Admin@nodename# delete libraries ssl-profiles <profile-name>
Admin@nodename# delete libraries ssl-profiles <profile-name> ssl-ciphers [cipher ...]

Чтобы отобразить информацию о профилях SSL:

Admin@nodename# show libraries ssl-profiles
Admin@nodename# show libraries ssl-profiles <profile-name>

Настройка профилей пересылки SSL

Данный раздел находится на уровне **libraries ssl-forwarding-profiles**.

Для создания профиля пересылки используется команда:

Admin@nodename# create libraries ssl-forwarding-profiles <parameter>

Далее необходимо указать:

Параметр	Описание
name	Название профиля пересылки SSL.
description	Описание профиля пересылки.
type	Тип пересылки: - I2. При настройке необходимо указать MAC-адрес устройства и название интерфейса, на который необходимо переслать копию трафика. - I3. Копия расшифрованного трафика передаётся по GRE-туннелю. При настройке необходимо указать GRE IP-адреса источника и назначения.

Параметр	Описание
mac	MAC-адрес назначения (указывается при использовании типа пересылки L2).
iface	Интерфейс UserGate, с которого будет производиться пересылка (указывается при использовании типа пересылки L2).
source-ip	GRE IP-адрес источника (указывается при использовании типа пересылки L3).
dest-ip	GRE IP-адрес назначения (указывается при использовании типа пересылки L3).

Следующая команда предназначена для обновления параметров профилей пересылки:

```
Admin@nodename# set libraries ssl-forwarding-profiles <profile-name> <parameter>
```

Для удаления профиля:

```
Admin@nodename# delete libraries ssl-forwarding-profiles <profile-name>
```

Чтобы отобразить информацию о всех имеющихся профилях или об определённом профиле пересылки, используются следующие команды:

```
Admin@nodename# show libraries ssl-forwarding-profiles
Admin@nodename# show libraries ssl-forwarding-profiles <profile-name>
```

Настройка объектов HIP

Данный раздел находится на уровне **libraries hip-object**

Для создания объекта HIP используется команда:

```
Admin@nodename# create libraries hip-object <parameters>
```

Далее необходимо указать:

Параметр	Описание
name	Название объекта HIP.
description	Описание объекта HIP.
process	Проверка процессов, запущенных на конечном устройстве.
running-services	Проверка служб, запущенных на конечном устройстве.
installed-updates	Проверка наличия указанного обновления на конечном устройстве. Необходимо указать номер статьи базы знаний Microsoft (KB), например, KB5013624.
os-version	Версия операционной системы устройства пользователя.
products	Проверка на соответствие статуса: • antimalware — антивирусное ПО на конечном устройстве. ◦ products — название продукта. ◦ vendor — производитель продукта. • firewall — межсетевой экран на конечном устройстве. ◦ products — название продукта. ◦ vendor — производитель продукта. • backup — ПО для резервного копирования ◦ products — название продукта. ◦ vendor — производитель продукта. • disk-encryption — ПО шифрования диска на конечном устройстве. ◦ products — название продукта. ◦ vendor — производитель продукта. • dlp — система предотвращения утечек информации на конечном устройстве. ◦ products — название продукта. ◦ vendor — производитель продукта. • patch-management — ПО для установки обновлений на конечном устройстве. ◦ products — название продукта ◦ vendor — производитель продукта.
registry-keys	Ключ реестра Microsoft Windows — каталог, в котором хранятся настройки и параметры операционной системы. Поддерживаются следующие типы параметров реестра: • REG_SZ: строка Unicode или ANSI с нулевым символом в конце. • REG_BINARY: двоичные данные в любой форме. • REG_DWORD: 32-разрядное число. Доступна проверка ключей следующих разделов реестра: • HKEY_LOCAL_MACHINE • HKEY_USERS Важно! Путь указывается с использованием обратного слэша (\), например, \HKEY_LOCAL_MACHINE, после которых через (\) указывается полный путь к параметру. Описание ключей реестра читайте в документации Microsoft .
security	Проверка активных компонентов: • firewall — межсетевой экран (да, нет, не проверять). • virus-protection — антивирусное ПО (да, нет, не проверять). • automatic-update — автоматическая установка обновлений (да, нет, не проверять). • bitlocker — шифрование дисков (да, нет, не проверять).
ug-client-version	Версия ПО UserGate Client.

Команда для редактирования параметров объектов HIP:

Admin@nodename# set libraries hip-object <hip-object-name> <parameters>

Для удаления объекта:

Admin@nodename# delete libraries hip-object <hip-object-name>

Чтобы отобразить информацию о всех имеющихся объектах или об определённом объекте, используются следующие команды:

Admin@nodename# show libraries hip-object
Admin@nodename# show libraries hip-object <hip-object-name>

Настройка профилей HIP

Данный раздел находится на уровне **libraries hip-profile**

Для создания профиля HIP используется команда:

Admin@nodename# create libraries hip-profile <parameters>

Далее необходимо указать:

Параметр	Описание
name	Название профиля HIP.
description	Описание профиля HIP.
enabled	Включение/отключение использования профиля..
hip-objects	Выбор логического элемента (И, ИЛИ, И НЕ, ИЛИ НЕ) и объектов HIP. Подробнее о создании объектов HIP читайте в разделе Настройка объектов HIP .

Следующая команда предназначена для обновления параметров HIPprofiles:

Admin@nodename# set libraries hip-profile <hip-profile-name> <parameters>

Для удаления профиля:

Admin@nodename# delete libraries hip-profile <profile-name>

Чтобы отобразить информацию о всех имеющихся профилях или об определённом HIP profiles, используются следующие команды:

Admin@nodename# show libraries hip-profile
Admin@nodename# show libraries hip-profile <hip-profile-name>

Настройка профилей BFD

Данный раздел находится на уровне **libraries bfd-profile**

Для создания профиля BFD используется команда:

Admin@nodename# create libraries bfd-profile

Далее необходимо указать:

Параметр	Описание
name	Название профиля BFD.
description	Описание профиля.
detect-multiplier	Множитель времени обнаружения; влияет на время обнаружения неисправностей соединения.
receive-interval	Интервал приема управляющих пакетов BFD (минимальное время, которое требуется между пакетами); указывается в миллисекундах.
transmit-interval	Интервал передачи управляющих пакетов BFD; интервал должен быть согласован между узлами; указывается в миллисекундах.
echo-receive-interval	Минимальный интервал, через который данная система способна принимать echo-пакеты; указывается в миллисекундах.
echo-transmit-interval	Минимальный интервал, через который система будет способна отправлять echo-пакетов BFD; указывается в миллисекундах.
echo-mode	Включить или выключить режим передачи Echo mode .
passive-mode	Включить или выключить режим Passive .
ttl	Минимальное ожидаемое TTL для входящего управляющего пакета BFD. Может принимать значения от 1 до 254.

Следующая команда предназначена для обновления параметров BFD profiles:

Admin@nodename# set libraries bfd-profile <profile-name> <parameter>

Для удаления профиля:

Admin@nodename# delete libraries bfd-profile <profile-name>

Чтобы отобразить информацию о всех имеющихся профилях или об определённом BFD profiles, используются следующие команды:

Admin@nodename# show libraries bfd-profile
Admin@nodename# show libraries bfd-profile <profile-name>

Настройка Syslog фильтров UserID агента

Создание и настройка syslog-фильтров производится на уровне **libraries syslog-filters**.

Команда для создания syslog-фильтра:

Admin@nodename# create libraries syslog-filters <parameters>

Далее необходимо указать:

Параметр	Описание
name	Название фильтра.
description	Описание фильтра.
login-address	Строка для поиска IP-адреса пользователя в syslog-сообщении.
login-event	Строка для поиска события входа пользователя в syslog-сообщении.

Параметр	Описание
login-username	Строка для поиска имени пользователя в syslog-сообщении.
logout-address	Строка для поиска IP-адреса пользователя в syslog-сообщении.
logout-event	Строка для поиска события выхода пользователя в syslog-сообщении.
logout-username	Строка для поиска имени пользователя в syslog-сообщении.

Следующая команда предназначена для редактирования информации о syslog-фильтре:

```
Admin@nodename# set libraries syslog-filters <filter-name> <parameters>
```

Параметры, доступные для обновления, аналогичны параметрам, указываемым при создании фильтра.

Чтобы отобразить информацию о syslog-фильтрах:

```
Admin@nodename# show libraries syslog-filters <filter-name>
```

Пользователь может удалить syslog-фильтр, используя следующую команду:

```
Admin@nodename# delete libraries syslog-filters <filter-name>
```

Настройка сценариев

Общие правила создания сценариев

Настройка сценариев происходит на уровне **libraries scenarios** с использованием UPL (подробнее о написании правил с помощью UserGate Policy Language читайте в разделе [Типы правил](#)).

Для задания условий сценариев и их объединения используются определения (definitions). Каждому определению присваивается уникальное пользовательское имя, по которому к нему можно будет обратиться. Условия сценария могут быть написаны в одной строке или разбиты с помощью обратного слэша (как при использовании многострочного ввода).

Для создания/изменения условий сценариев используется функция **def scenario_cond**, которая в общем виде имеет следующую структуру:

```
def scenario_cond <scenario_condition_name>
<scenario_conditions>
end
```

Параметры, использующиеся для задания разных типов условий, будут рассмотрены в следующих разделах.

Далее, после указания условий, указываются общие свойства сценария, представленные в таблице ниже:

Наименование	Описание
OK	Действие для создания сценария.
scenario_cond	Пользовательское имя определения, содержащего список условий сценария: scenario_cond = condition_example .
enabled	Включить/отключить использование сценария: enabled(true); enabled(false).
name	Задать имя сценария: name("Example scenario name") .
desc	Задать описание сценария: desc("Description for scenario created as an example") .
trigger	Применение: trigger(one_user) — при срабатывании сценария, правило, в котором используется сценарий, будет применено только к тому пользователю, для которого сработал сценарий; trigger(all_users) — при срабатывании сценария, правило в котором используется сценарий, будет применено ко всем пользователям, указанным в свойствах правила.
duration	Задать период активности сценария; указывается в минутах.
operation_mode	Задать режим активации сценария: operation_mode(all) — сценарий сработает, если выполнятся все условия; operation_mode(any) — сценарий сработает, если выполнится хотя бы одно из условий.

Примечание!При обновлении сценария необходимо указывать все условия: текущие условия сценария будут заменены на условия, указанные при изменении.

В качестве примера приведена настройка сценария с условием **Объём трафика**. Сценарий будет применён ко всем пользователям в течение минуты; ограничение объёма трафика: 1 ГБ/день:

```
Admin@nodename# create libraries scenarios 1 upl-rule \
... def scenario_cond scenario_cond_test
... traffic_limit(1GB) \
... period(day) \
... scond_type(traffic)
... end
... OK \
... scenario_cond = scenario_cond_test
... name(test) \
... trigger(all_users) \
... duration (1)
...
```

Для изменения, например, объёма трафика:

```
Admin@nodename# set libraries scenarios 3 upl-rule \
...def scenario_cond scenario_cond_test
...traffic_limit(2GB) \
...period(day) \
...scond_type(traffic)
...end
...OK \
...scenario_cond = scenario_cond_test
```

Типы условий, используемых при создании сценариев

Условие типа Категория URL

Для создания/обновления условия типа **Категория URL** укажите:

Наименование	Описание
scond_type	Тип условия: scond_type(url_category) .

Наименование	Описание
category	Категории или группы категорий сайтов: <code>category = (lib.category(URL_CATEGORY_GROUP), URL_CATEGORY_NAME)</code> .
count_interval	Интервал времени, за которое должно произойти заданное число срабатываний (указывается в минутах): <code>count_interval()</code> .
max_event_count	Количество срабатываний: <code>max_event_count()</code> .

Условие типа Обнаружен вирус

При настройке условия типа **Обнаружен вирус** укажите следующее:

Наименование	Описание
scond_type	Тип условия: <code>scond_type(virus_detection)</code> .

Условие типа Приложение

Для создания/редактирования условия типа **Приложение** используются параметры, представленные в таблице ниже:

Наименование	Описание
scond_type	Тип условия: <code>scond_type(app)</code> .
application	Категории приложений или группы приложений: <code>application = lib.applicationgroup(APP_GROUP)</code> или <code>application = lib.applicationgroup(all)</code>; <code>application = lib.category(APPS_CATEGORY_NAME)</code>.
count_interval	Интервал времени, за которое должно произойти заданное число срабатываний (указывается в минутах): <code>count_interval()</code> .
max_event_count	Количество срабатываний: <code>max_event_count()</code> .

Условие типа COB

Параметры условия типа **COB**:

Наименование	Описание
scond_type	Тип условия: <code>scond_type(ips)</code> .
ips_tl	Уровень угрозы: <code>ips_tl(very_low)</code> - очень низкий; <code>ips_tl(low)</code> - низкий; <code>ips_tl(medium)</code> - средний; <code>ips_tl(high)</code> - высокий; <code>ips_tl(very_high)</code> - очень высокий.

Условие типа Типы контента

Параметры условием типа **Типы контента**:

Наименование	Описание
scond_type	Тип условия: <code>scond_type(mime_type)</code> .
response.header.Content-Type	Тип контента: <code>response.header.Content-Type = lib.mime(MIME_CATEGORIES_LIST)</code> .
count_interval	Интервал времени, за которое должно произойти заданное число срабатываний (указывается в минутах): <code>count_interval()</code> .
max_event_count	Количество срабатываний: <code>max_event_count()</code> .

Условие типа Объём трафика

Чтобы задать или настроить условие типа **Объём трафика** используются следующие параметры:

Наименование	Описание
scond_type	Тип условия: <code>scond_type(traffic)</code> .
traffic_limit	Ограничение объёма трафика: <code>traffic_limit(1)</code> - 1 байт трафика; <code>traffic_limit(1KB)</code> - 1 Кбайт трафика; <code>traffic_limit(1MB)</code> - 1 Мбайт трафика; <code>traffic_limit(1GB)</code> - 1 Гбайт трафика.
period	Период времени: <code>period(minute)</code> - минута; <code>period(hour)</code> - час; <code>period(day)</code> - день; <code>period(week)</code> - неделя; <code>period(month)</code> - месяц.

Условие типа Проверка состояния

Для настройки условия типа **Проверка состояния** предназначены параметры:

Наименование	Описание
scond_type	Тип условия: scond_type(health_check) .
health_check_method	Метод проверки: health_check_method(ping) - ping; health_check_method(dns) - DNS-запрос; health_check_method(get) - HTTP-метод GET.
url.address	Адрес, на который будут выполняться ping и DNS-запрос: url.address = "1.1.1.1" .
url.domain	FQDN для проверки состояния путём выполнения DNS-запроса или URL для метода HTTP GET: url.domain = "example.ru" .
gateway	Название используемого шлюза: gateway() . Важно! Шлюз должен быть предварительно создан.
health_result	Результат выполнения проверки: health_result(positive) - положительный; health_result(negative) - отрицательный.
health_request_timeout	Тайм-аут подключения (в секундах): health_request_timeout() .
health_answer_timeout	Время ожидания ответа на запрос HTTP GET (в секундах): health_answer_timeout() .
health_type_request	Тип DNS-запроса: health_type_request(a). health_type_request(aaaa). health_type_request(cname). health_type_request(ns). health_type_request(ptr).
count_interval	Интервал времени, за которое должно произойти заданное число срабатываний (указывается в минутах): count_interval() .
max_event_count	Количество срабатываний: max_event_count() .

Настройка тегов

Использование тегов доступно в версии ПО 7.3.0 и выше.

Создание и настройка тегов производятся на уровне **libraries tags**.

Команда для создания тегов:

Admin@nodename# create libraries tags <parameters>

Далее необходимо указать:

Параметр	Описание
name	Название тега.
description	Описание тега.
color	Выбор цветовой маркировки тега для отображения в веб-интерфейсе: no-color (Значение по умолчанию); red; orange; yellow; green; aqua; blue; violet; pink; purple; light-gray; light-green; light-blue; black; rose; magenta; wood;

Команда для редактирования информации о теге:

Admin@nodename# set libraries tags <tag-name> <parameters>

Параметры, доступные для обновления, аналогичны параметрам, указываемым при создании тега.

Чтобы отобразить информацию о тэгах:

Admin@nodename# show libraries tags <tag-name>

Пользователь может удалить тег, используя следующую команду:

Admin@nodename# delete libraries tags <tag-name>

Примеры работы с тэгами в библиотеке:

Admin@nodename# create libraries tags name "Test tag 6" description "Tag made with CLI" color magenta

Admin@nodename# show libraries tags

Test tag 6
name : Test tag 6
description : Tag made with CLI
color : magenta

Tag 5
name : Tag 5
description : Test tag #5
color : green

Tag 1
name : Tag 1
description : Test tag #1
color : no-color

Admin@nodename# show libraries tags "Test tag 6"

name : Test tag 6
description : Tag made with CLI
color : magenta

Admin@nodename# set libraries tags "Test tag 6" description "Update tag from cli"
Admin@nodename# show libraries tags "Test tag 6"

name : Test tag 6
description : Update tag from cli
color : magenta

Admin@nodename# delete libraries tags "Test tag 6"

