

Table of Contents

Table of Contents	1
Настройка сенсоров	2
Настройка сенсоров (описание)	3

Documentation: ☒

Product: SIEM

Version: 7.x

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

Сенсоры UserGate

Сенсор UserGate подключает одно устройство типа межсетевого экрана UserGate к UserGate SIEM. Для подключения сенсора UserGate необходимо выполнить следующие шаги:

1. На **NGFW** разрешить сервисы **Log Analyzer** и **SNMP** в настройках требуемой зоны:

```
Admin@ngfw-nodename# set network zone <zone-name> enabled-services [ SNMP "Log Analyzer" ]
```

2. На **NGFW** получить токен устройства:

```
Admin@ngfw-nodename# show settings general log-analyzer
```

```
state          : ready
logan-server    : 127.0.0.1
logan-version   : 7.1.0.
device-version  : 7.1.0.
device-code     : 9R4FCVET
```

3. В UserGate SIEM разрешить сервис **База данных журналов** в свойствах требуемой зоны:

```
Admin@nodename# set network zone <zone-name> enabled-services [ "Log Analyzer" ]
```

4. Создать сенсор UserGate.

Для создания сенсора UserGate используется команда:

```
Admin@ndefornaledo# create sensors ug-sensors <parameters>
```

Необходимо добавить следующие параметры:

Параметр	Описание
enabled	Включает или выключает данный сенсор UserGate.
name	Название сенсора UserGate.
description	Опциональное описание сенсора UserGate.
address	IP-адрес узла UserGate, для которого создается данный сенсор.
SIEM-address	IP-адрес сервера UserGate SIEM, который будет использоваться на узле UserGate, в качестве назначения для отсылки журналов. Для выбора отображаются только те адреса, на интерфейсах зон которых разрешен сервис Log Analyzer.
device-code	Токен, полученный на узле UserGate.

После создания сенсора, узел UserGate начинает отсылать данные в UserGate SIEM.

Для просмотра сенсоров UserGate используется команда:

```
Admin@nodename# show sensors ug-sensors
```

Сенсоры SNMP

С помощью сенсора SNMP администратор может подключить SNMP-совместимое сетевое устройство к серверу UserGate SIEM для сбора и анализа его метрик. UserGate SIEM может отображать любые счетчики, полученные по SNMP с помощью запросов SNMP. Для настройки сенсора SNMP необходимо иметь базы MIB (Management Information Base) на управляемое устройство.

Для настройки сенсора SNMP необходимо выполнить следующие шаги:

1. Загрузить базу MIB того устройства, которое требуется добавить для мониторинга.

2. Создать сенсор SNMP:

```
Admin@nodename# create sensors snmp-sensors <parameters>
```

Далее указать следующие параметры::

Наименование	Описание
enabled	Включает или выключает данный сенсор SNMP.
name	Название сенсора SNMP.
description	Опциональное описание сенсора SNMP.
ip	IP-адрес сенсора SNMP.
port	Порт сенсора SNMP. Обычно для запросов данных по протоколу SNMP используется порт TCP 161.
version	Указывает версию протокола SNMP, которая будет использоваться в данном сенсоре. Возможны варианты SNMP v2 (2) и SNMP v3 (3).
community	SNMP community — строка для идентификации сервера UserGate SIEM и сетевого устройства для версии SNMP v2. Используйте только латинские буквы и цифры.
interval	Интервал в секундах, через который сервер UserGate SIEM будет инициировать получение данных с сетевого устройства.
username	Только для SNMP v3. Имя пользователя для аутентификации сетевом устройстве.
auth-type	Выбор режима аутентификации. Возможны варианты: • Без аутентификации, без шифрования (none). • С аутентификацией, без шифрования (no-encrypt). • С аутентификацией, с шифрованием (encrypt).
auth-alg	Алгоритм, используемый для аутентификации: • md5; • sha; • sha224; • sha256; • sha284; • sha512.
auth-password	Пароль, используемый для аутентификации.
encrypt-alg	Алгоритм, используемый для шифрования. Возможно использовать DES и AES.
encrypt-password	Пароль, используемый для шифрования.
counters	Укажите здесь все требуемые данные, которые UserGate SIEM будет запрашивать на сетевом устройстве. Счетчики выбираются из баз MIB, которые загружены на устройство. Укажите в скобках [] SNMP OID счетчика.

Для просмотра сенсоров SNMP используется команда:

```
Admin@nodename# show sensors snmp-sensors
```

Сенсоры WMI

С помощью сенсора WMI администратор может подключить WMI-совместимое сетевое устройство (компьютер под управлением ОС Windows) к UserGate SIEM для сбора и анализа его метрик.

Для создания сенсора WMI используется команда:

```
Admin@nodename# create sensors wmi-sensors <parameters>
```

Далее указать следующие параметры::

Наименование	Описание
enabled	Включает или выключает данный сенсор.
name	Название сенсора.
description	Опциональное описание сенсора.
ip	IP-адрес сенсора.
login	Имя пользователя для подключения к устройству.
password	Пароль пользователя для подключения к устройству.
namespace	Пространство имен идентификаторов.
polling-interval	Интервал опроса в секундах.
counters	Указать данные, которые UserGate SIEM будет мониторить на сетевом устройстве: name — название счетчика. type — тип счетчика (windows-event-logs). filter-query — WQL запрос (например, Logfile='Security').

Для просмотра сенсоров WMI используется команда:

```
Admin@nodename# show sensors wmi-sensors
```

Конечные устройства

Конечное устройство с установленным программным обеспечением UserGate Client будет отображено при выборе на UGMC данного устройства UserGate SIEM в качестве сервера для передачи информации о событиях, при этом UserGate SIEM должен быть предварительно зарегистрирован на UGMC (подробнее читайте в разделе [Управление устройствами LogAn](#)).

Для просмотра данных конечных устройств используется команда:

```
Admin@nodename# show sensors endpoint-devices
```

Коннекторы

Коннекторы используются для возможности подключения устройства UserGate SIEM к различным средствам защиты с целью сбора информации.

Для добавления коннектора предназначена команда:

```
Admin@nodename# create sensors connectors <parameters>
```

Необходимо указать следующие данные:

Параметр	Описание
name	Название коннектора.

Параметр	Описание
description	Описание коннектора (опционально).
server-type	Выбор типа сервера: • SSH; • HTTP; • HTTPS (в текущей версии реализован только для интеграции с ГосСОПКА) .
address-format	Тип: • ip. • fqdn.
ip	IP-адрес сервера; указывается в случае выбора адреса сервера типа IP .
port	Порт сервера; указывается в случае выбора адреса сервера типа IP .
fqdn	FQDN сервера; указывается в случае выбора адреса сервера типа FQDN .
url-path	Используется при управлении устройством по API.
login	Логин пользователя для авторизации на коннекторе.
password	Пароль учётной записи пользователя, необходимый для авторизации на коннекторе.
connamd-group	Указание группы команд доступно только для SSH-сервера, подробнее читайте в разделе Команды .
headers	Указание заголовков доступно только для серверов HTTP и HTTPS.

Для редактирования созданного ранее коннектора используется команда:

```
Admin@nodename# create sensors connectors <connector-name> <parameters>
```

Для просмотра параметров созданных ранее коннекторов используется команда:

```
Admin@nodename# show sensors connectors <connector-name>
```

Для удаления созданных ранее коннекторов используется команда:

```
Admin@nodename# delete sensors connectors <connector-name>
```

