Управление и мониторинг по протоколу SNMP

ECSS-10, версия 3.14.15

Содержание

1 Отправка алармов ECSS-10 через SNMP трапы

Система ECSS-10 позволяет настроить отправку алармов системы через SNMP сообщения.

Подсистема SNMP в рамках ECSS-10 в силу особенностей библиотеки Erlang по работе с SNMP настраивается через набор файлов, располагающихся по пути:

```
/etc/ecss/snmp/agent
```

Для того чтобы ECSS-10 мог отправлять трапы на сторонний сервер, необходимо в файле `target_addr.conf` описать конфигурационную строку:

```
% В данной конфигурации указана транспортная информация, куда необходимо пересылать
трапы
% {TargetName, Ip, Udp, Timeout, RetryCount, TagList, ParamsName, EngineId, TMask,
MaxMessageSize}.
```

- TargetName — уникальное имя для направления отправки трапов
- Ip, Udp — адрес и порт для отправки трапаTimeout — тайм-аут на доставку сообщения
- RetryCount — количество повторных посылок сообщения
- TagList — имя тега, указанного в notify.conf
- EngineId — имя target-a, который будет указан в target_params.conf

Пример:

```
{"Eltex EMS v2", [172,16,0,22], 162, 1500, 3, "std_trap", "target_v2", "", [], 2048}.
```

Для того чтобы с SSW можно было повторно запросить список аварий, которые он оправляет через SNMP трапы (повторно запросить отправку трапов), в файле необходимо `/etc/ecss/snmp/agent/community.conf` прописать *community* с именем *private* (comminuty должно совпадать с тем, что используется на стороне клиента) с правами на изменения:

```
{"private", "private", "all-rights", "", ""}.
```

После этого необходимо перезапустить ecss-mediator:

```
sudo systemctl restart ecss-mediator.service
```

Активировать snmpAgent в системе ECSS-10 через терминал управления Cocon:

```
ssw@[bus@ecss1]:/$ cluster/mediator/md1/properties/rpss/set * snmpAgentEnable true

Property "snmpAgentEnable" successfully changed from:
false
   to
true.
```

Выполнив эти действия, ECSS-10 на запрос по SNMP set по OID `1.3.6.1.4.1.35265.4.4` со значением 1 повторно вышлет все аварии через SNMP трапы. Так же в случаи возникновения других аварий в системе, они будут отправлены на указанный хост в SNMP трапах.

2 Настройка SNMP агента

SNMP агент ECSS по умолчанию использует порт udp/1610. Изменить его можно, отредактировав в конфигурационном файле /etc/ecss/snmp/agent/agent.conf опцию intAgentUDPPort.

Например:

```
{intAgentUDPPort, 3161}.
```

После этого нужно перезапустить ecss-mediator:

```
sudo systemctl restart ecss-mediator
```

Убедитесь, что данный порт не конфликтует с портом snmpd (по умолчанию udp/161, подробнее Настройка snmpd).

3 Доступ к активным вызовам в SNMP-таблице доменов

Мониторинг доменов осуществляется через SNMP таблицу по фиксированные Oid, при этом конкретный домен определяется или с помощью контекста (SNMP v.3), или с помощью community (SNMP v.2c). Права доступа выставляются непосредственно на строку таблицы. Вместо утилиты *snmpwalk*, которая использует SNMP-запрос *get-next*, необходимо использовать *snmpget*. Для того чтобы получить доступ по протоколу SNMPv2c необходимо выбрать для домена секретную строчку *community*. Затем, используя утилиту *snmpget* и данную строчку *community*, можно получить значения интересующих нас параметров.

3.1 Пример настройки SNMPv2c

Для избежания конфликтов community в разных доменах, community-строка префиксируется именем домена. Таким образом результирующая строка community должна иметь вид:
`<имя домена>:<community>`
Настройка *community* через интерфейс командной строки:

```
ssw@[bus@ecss1]:/$ domain/test.domain/snmp/agent/properties/set snmp_v2c_community
test.domain:aaa111
Property "snmp_v2c_community" successfully changed from:
"none"
to
"test.domain:aaa111".
```

По умолчанию сразу после создания домена доступ по snmp v.2 выключен. Для того чтобы включить доступ, необходимо задать community-строку, и выставить значение свойства snmp_v2c_enabled = true:

```
admin@[mycelium1@ecss1]:/$ domain/test.domain/snmp/agent/properties/set
snmp_v2c_enabled true
Property "snmp_v2c_enabled" successfully changed from:
false
   to
true.
```

При переходе с более ранней версии, старые community, которые не удовлетворяют новой политике доступа, станут невалидными, и доступ по snmp v.2c будет закрыт. Чтобы открыть доступ, необходимо задать корректные в рамках новой политики community.

3.2 Пример настройки SNMPv3

Для SNMPv3 необходимо сконфигурировать *authentication* и *privacy* ключи. Имя пользователя в данном случае = <имя домена>.

Настройка *authentication* и *privacy* ключей через интерфейс командной строки:

```
ssw@[bus@ecss1]:/$ domain/test.domain/snmp/agent/properties/set snmp_v3_auth_priv
sample_auth_key sample_priv_key
Property "snmp_v3_auth_priv" successfully changed from:
{none}
to
{"sample_auth_key","sample_priv_key"}.
```

По умолчанию сразу после создания домена доступ по snmp 3 выключен. Для того чтобы включить доступ, необходимо задать authentication и privacy ключи, и выставить значение свойства snmp_v3_enabled = true:

```
admin@[mycelium1@ecss1]:/$ domain/test.domain/snmp/agent/properties/set
snmp_v3_enabled true
Property "snmp_v3_enabled" successfully changed from:
false
   to
true.
```

3.3 Доступ к данным домена

Чтобы прочитать значение ячейки в SNMP-таблице доменов можно использовать *snmpget* .
Свойства домена имеют следующий абсолютный Oid:

`1.3.6.1.4.1.35265.2.10.11.2.<Oid свойства>`

Где Oid свойства может иметь следующие значения:

- "1" — Имя домена;
- "2" — Количество активных вызовов.

3.3.1 Доступ к данным домена для SNMP v2c:

Получение всех свойств домена с помощью snmpwalk:
`snmpwalk -c <Community> -v 2c <Host>:<Port> .1.3.6.1.4.1.35265.2.10.11.2`

Получение конкретного свойства домена с помощью snmpget:
`snmpget -c <Community> -v 2c <Host>:<Port> .1.3.6.1.4.1.35265.2.10.11.2.<Oid свойства>.0`

Пример:
Все свойства домена:

```
snmpwalk -c test.domain:aaa111 -v 2c 192.168.23.114:1610 .1.3.6.1.4.1.35265.2.10.11.2
-l noAuthNoPriv
iso.3.6.1.4.1.35265.2.10.11.2.1.0 = STRING: "test.domain"
iso.3.6.1.4.1.35265.2.10.11.2.2.0 = Gauge32: 5
iso.3.6.1.4.1.35265.2.10.11.2.2.0 = No more variables left in this MIB View (It is
past the end of the MIB tree),
```

Имя домена:

> *davidqo@ubuntu:~$ snmpget -c test.domain:aaa111 2c 192.168.23.114:1610 .1.3.6.1.4.1.35265.2.10.11.2.1.1.2.2*
> *iso.3.6.1.4.1.35265.1.2.1.1.2.2 = STRING: "domain2"*

Количество активных вызовов:

> *davidqo@ubuntu:~$ snmpget -c test.domain:aaa111 -v 2c 192.168.23.114:1610 .1.3.6.1.4.1.35265.2.10.11.2.1.1.3.2*
> *iso.3.6.1.4.1.35265.1.2.1.1.3.2 = Gauge32: 22*

Где

- *STRING: "test.domain"* — имя домена;
- *Gauge32: 5* — количество активных вызовов.

3.3.2 Для версии SNMPv3

Команда для получения всех свойств домена с помощью snmpwalk имеет следующий вид:
`snmpwalk -u <DomainName> -A <AuthKey> -X <PrivKey> -v 3 <Host>:<Port> . 1.3.6.1.4.1.35265.2.10.11.2 -l authPriv -n <DomainName>`

Получение конкретного свойства домена с помощью snmpget:

`snmpget -u <DomainName> -A <AuthKey> -X <PrivKey> -v 3 <Host>:<Port> . 1.3.6.1.4.1.35265.2.10.11.2.<Oid свойства>.0 -l authPriv -n <DomainName>`

Где

- *<AuthKey>* и *<PrivKey>* — Это соответственно authentication и privacy ключи (см. Команды SNMP)
- Флаг *-u* — Имя пользователя (Равно имени домена)
- Флаг *-n* — Context (Равно имени домена)

Пример

```
snmpwalk -u test.domain -A sample_auth -X sample_priv -v 3 192.168.23.114:1610 .
1.3.6.1.4.1.35265.2.10.11.2 -l authPriv -n test.domain
iso.3.6.1.4.1.35265.2.10.11.2.1.0 = STRING: "test.domain"
iso.3.6.1.4.1.35265.2.10.11.2.2.0 = Gauge32: 5
iso.3.6.1.4.1.35265.2.10.11.2.2.0 = No more variables left in this MIB View (It is
past the end of the MIB tree)
```

Имя домена:

```
snmpwalk -u test.domain -A sample_auth_key -X sample_priv_key -v 3 192.168.118.29:1610
 .1.3.6.1.4.1.35265.2.10.11.2.1 -l authPriv -n test.domain
iso.3.6.1.4.1.35265.2.10.11.2.1.0 = STRING: "test.domain"
```

Количество активных вызовов:

```
snmpwalk -u test.domain -A sample_auth_key -X sample_priv_key -v 3
192.168.118.29:1610 .1.3.6.1.4.1.35265.2.10.11.2.2 -l authPriv -n test.domain
iso.3.6.1.4.1.35265.2.10.11.2.2.0 = Gauge32: 5
```

Где

- *STRING: "test.domain"* — имя домена;
- *Gauge32: 5* — количество активных вызовов.

Для каждого домена ECSS-10 создаётся один SNMP пользователь. Значение *community* по умолчанию отсутствуют. Значения по умолчанию для SNMPv3 AuthKey и PrivKey также отсутствуют. После создания домена необходимо задать безопасные значения.

3.4 Включение и отключение мониторинга по SNMP

Чтобы отключить доступ по SNMPv3 необходимо выставить свойства SNMP _v3_enabled в значение false:

```
ssw@[bus@ecss1]:/$ domain/test.domain/snmp/agent/properties/set snmp_v3_enabled false
Property "snmp_v3_enabled" successfully changed from:
true
to
false
```

Аналогично для версии SNMP2c свойства *snmp_v2c_enabled* нужно выставить в значение true для включения и false для выключения.

4 Доступ к активным вызовам системы

Команды по изменению параметров доступа по SNMPv2c и SNMPv3 уровня ECSS-10:

```
/cluster/mediator/<NAME>/snmp/agent/properties/
```

Параметры доступа по протоколу SNMP для информации уровня ECSS-10, аналогичны параметрам уровня домена:

```
ssw@[bus@ecss1]:/$ cluster/mediator/md1/snmp/agent/properties/info

┌──────────────────┬──────────────────────────┐
│     Property     │          Value           │
├──────────────────┼──────────────────────────┤
│snmp_v2c_community│12345678                  │
│snmp_v2c_enabled  │true                      │
│snmp_v3_auth_priv │{"12345678","23456789"}   │
│snmp_v3_enabled   │true                      │
└──────────────────┴──────────────────────────┘
```

Имя пользователя для аутентификации по SNMPv3 *"ssw"*.

Для дополнительной информации о настройке доступа по SNMP v2c и v3 см. настройку доступа по SNMP уровня домена.

4.1 Получение списка активных вызовов в ECSS-10 через протокол SNMPv3

`snmpget -u ssw -A <AuthKey> -X <PrivKey> -v 3 <Host>:<Port> -l authPriv . 1.3.6.1.4.1.35265.2.10.11.3.1.0`

Пример:

```
snmpget -u ssw -A 12345678 -X 23456789 -v 3 192.168.23.38:1610 -l authPriv .
1.3.6.1.4.1.35265.2.10.11.3.1.0
iso.3.6.1.4.1.35265.1.3.1.0 = Gauge32: 17
```

17 — число активных вызовов

4.2 Получение списка активных вызовов в ECSS-10 через протокол SNMPv2c

`snmpget -c <Community> -v 2c <Host>:<Port> .1.3.6.1.4.1.35265.2.10.11.3.1.0`

Пример:

```
snmpget -c 12345678 -v 2c 192.168.23.38:1610 .1.3.6.1.4.1.35265.2.10.11.3.1.0
iso.3.6.1.4.1.35265.1.3.1.0 = Gauge32: 17
```

17 — число активных вызовов