

TRAP-СООБЩЕНИЕ SNMP для наблюдения изменения Смежности EIGRP в Nexus 7000

Содержание

[Обзор](#)

[Пример](#)

Обзор

Nexus только поддерживает два trap-сообщения для MIB EIGRP, сEigrpAuthFailureEvent и сEigrpRouteStuckInActive, но никаких trap-сообщений SNMP для Соседних eigrp/вниз (сEigrpNbrDownEvent).

Жизнеспособный обходной путь для генерации trap-сообщений SNMP для наблюдения изменений смежности EIGRP должен был бы настроить два сценария EEM - один для Соседнего узла и один для Выключенного Соседнего узла - инициированный на основе образца системного журнала.

Пример

```
event manager applet EIGRP_TRAP_nbr_dwn
  event syslog pattern "EIGRP-5-NBRCHANGE_DUAL.*down"
  action 1.1 snmp-trap strdata "EIGRP Neighbor Down"
event manager applet EIGRP_TRAP_nbr_up
  event syslog pattern "EIGRP-5-NBRCHANGE_DUAL.*up"
  action 1.1 snmp-trap strdata "EIGRP Neighbor Up"
```

Можно тогда протестировать путем переброски Интерфейсом уровня 3 (можно создать тестовый SVI для проверки относительно не, разрешают подключение):

```
event manager applet EIGRP_TRAP_nbr_dwn
  event syslog pattern "EIGRP-5-NBRCHANGE_DUAL.*down"
  action 1.1 snmp-trap strdata "EIGRP Neighbor Down"
event manager applet EIGRP_TRAP_nbr_up
  event syslog pattern "EIGRP-5-NBRCHANGE_DUAL.*up"
  action 1.1 snmp-trap strdata "EIGRP Neighbor Up"
```

Подтвердите, что Nexus отправляет их правильно путем проверки Средства мониторинга SNMP - Выходные данные могут отличаться немного в зависимости от используемого программного средства:



Можно также рассмотреть эти trap-сообщения SNMP через перехват Wireshark:

Примечание: В зависимости от версии Wireshark строка не будет в читаемом пользователем тексте, но может фильтроваться через "snmp.value.octets, содержит "EIGRP""

Capturing from 3 interfaces [Wireshark 1.10.3-Spirent-2 (SVN Rev Unkn...]

Filter: `snmp.value.octets contains "EIGRP"`

No.	Time	Source	Destination	Protocol	Length	Info
14	10.5091510	10.122.140.96	172.18.121.3	SNMP	278	snmpv2-trap 1.3.6.1.2.1.1.3.0 1.

Frame 14: 278 bytes on wire (2224 bits), 278 bytes captured (2224 bits) on interface 1

- Ethernet II, Src: Cisco_66:8a:c4 (00:13:80:66:8a:c4), Dst: Vmware_be:56:b8 (00:50:56:be:56:b8)
- Internet Protocol Version 4, Src: 10.122.140.96 (10.122.140.96), Dst: 172.18.121.3 (172.18.121.3)
- User Datagram Protocol, Src Port: 37782 (37782), Dst Port: snmptrap (162)
- Simple Network Management Protocol
 - version: v2c (1)
 - community: public
 - data: snmpv2-trap (7)
 - snmpv2-trap
 - request-id: 121
 - error-status: noError (0)
 - error-index: 0
 - variable-bindings: 8 items
 - 1.3.6.1.2.1.1.3.0: 52260863
 - 1.3.6.1.6.3.1.1.4.1.0: 1.3.6.1.4.1.9.10.134.0.2 (iso.3.6.1.4.1.9.10.134.0.2)
 - 1.3.6.1.4.1.9.10.134.1.2.3.1.2.1: 8449
 - 1.3.6.1.4.1.9.10.134.1.2.3.1.6.1: <MISSING>
 - 1.3.6.1.4.1.9.10.134.1.2.3.1.7.1: 45494752505f54455354
 - 1.3.6.1.4.1.9.10.134.1.2.3.1.9.1:
 - 1.3.6.1.4.1.9.10.134.1.2.3.1.10.1:
 - 1.3.6.1.4.1.9.10.134.1.2.3.1.11.1: 45494752502061646a6163656e6379206368616e6765

Можно также проверить, что Nexus передает их на EEM, инициирующий с Ethalyzer -
Пример:

```
N7K-A-Admin# ethalyzer local interface mgmt display-filter snmp limit-c 0
```

Capturing on mgmt0

```
2017-07-12 15:43:37.431067 10.122.140.96 -> 172.18.121.3 SNMP 278 snmpv2-trap 1.3.6.1.2.1.1.3.0
1.3.6.1.6.3.1.1.4.1.0 1.3.6.1.4.1.9.10.134.1.2.3.1.2.1 1.3.6.1.4.1.9.10.134.1.2.3.1.6.1
1.3.6.1.4.1.
9.10.134.1.2.3.1.7.1 1.3.6.1.4.1.9.10.134.1.2.3.1.9.1 1.3.6.1.4.1.9.10.134.1.2.3.1.10.1
1.3.6.1.4.1.9.10.134.1.2.3.1.11.1
```

Примечание: Пред NX-OS 7.x не дает нам опцию настройки “**snmp-server enable traps syslog**”, который в свою очередь позволил бы, что вы для мониторинга самого всего журнала регистрации тогда фильтруете для сообщений EIGRP. Эта опция была добавлена в более поздних версиях, 7.x и позже.