

# Armadilha de SNMP para monitorar a mudança da adjacência EIGRP no nexo 7000

## Índice

[Visão geral](#)

[Exemplo](#)

## Visão geral

O nexa apoia somente duas armadilhas para EIGRP-MIB, cEigrpAuthFailureEvent e cEigrpRouteStuckInActive, mas nenhum SNMP traps para os vizinhos EIGRP up/down (cEigrpNbrDownEvent).

Uma ação alternativa viável para gerar o SNMP traps para monitorar mudanças da adjacência EIGRP seria configurar dois scripts EEM - um para o vizinho acima e um para o vizinho para baixo - provocados baseado no teste padrão do Syslog.

## Exemplo

```
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"
```

Você pode então testar batendo uma relação da camada 3 (você pode criar um teste SVI para verificar a respeito de para não interromper a Conectividade):

```
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"
```

Confirme que o nexa está enviando estes para fora corretamente verificando sua ferramenta de monitoramento SNMP - a saída pode diferir levemente segundo a ferramenta usada:



Você pode igualmente rever este SNMP traps através de uma captura de Wireshark:

*Nota: Segundo a versão de Wireshark, a corda não estará no texto compreensível para o utilizador mas pode ser filtrada através de "snmp.value.octets contém "o "" 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

Você pode igualmente verificar que o nexa está enviando estes em cima do EEM que provoca com Ethalyzer - exemplo:

```
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
```

Nota: Pre NX-OS 7.x não nos dá que a opção de configurar o “servidor snmp permite o Syslog das armadilhas” que permitiria por sua vez que você monitorasse o log de registro inteiro próprio filtra então para as mensagens EIGRP. Esta característica foi adicionada em umas liberações mais atrasadas, 7.x e mais tarde.