

Interceptação SNMP para monitorar a alteração de adjacência do EIGRP no Nexus 7000

Contents

[Introduction](#)

[Exemplo](#)

Introduction

Este documento descreve a armadilha do Protocolo de Gerenciamento de Rede Simples (SNMP - Simple Network Management Protocol) para monitorar a alteração de adjacência do Protocolo de Roteamento de Gateway Interior Avançado (EIGRP - Enhanced Interior Gateway Routing Protocol) no Nexus 7000. O Nexus suporta apenas duas armadilhas para EIGRP-MIB, cEigrpAuthFailureEvent e cEigrpRouteStuckInActive, mas nenhuma armadilha SNMP para vizinhos EIGRP up/down (cEigrpNbrDownEvent).

Uma solução viável para gerar armadilhas SNMP para monitorar alterações de adjacência EIGRP seria configurar dois scripts EEM - um para Neighbor Up e outro para Neighbor Down - disparado com base no padrão 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"
```

Em seguida, você pode testar a sincronização de uma interface de Camada 3 (você pode criar uma Interface Virtual do Switch (SVI) para verificar se não interrompe a conectividade):

```
2017 Jul 12 15:51:06 N7K-AGG2 %EIGRP-5-NBRCHANGE_DUAL: eigrp-10 [4049] (default-base) IP-
EIGRP(0) 10: Neighbor 10.10.10.84
(Vlan1064) is down: holding time expired 2017 Jul 12 15:51:10 N7K-AGG2 %EIGRP-5-NBRCHANGE_DUAL:
eigrp-10 [4049] (default-base) IP-EIGRP(0) 10: Neighbor 10.10.10.84
(Vlan1064) is up: new adjacency
```

Confirme se o Nexus os envia corretamente e verifique sua ferramenta de monitoramento SNMP - a saída pode ser um pouco diferente e depende da ferramenta usada:



Você também pode revisar essas interceptações SNMP por meio de uma captura Wireshark:

Note: Depende da versão do Wireshark, a string não estará em texto legível por humanos, mas pode ser filtrada por "snmp.value.octets contém "EIGRP".

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

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: `snmp.value.octets contains "EIGRP"` Expression... Clear Apply Save

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: 45494752502061646a6a6163656e6379206368616e6765

Você também pode verificar se o Nexus envia esses dados sobre o desencadeamento do Embedded Event Manager (EEM) com o Ethalyzer. Veja o 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
```

Note: O Pre NX-OS 7.x não nos dá a opção de configurar o `snmp-server enable traps syslog`, que, por sua vez, permitirá que você monitore todo o log de log em si e filtre as mensagens do EIGRP. Este recurso foi adicionado em versões 7.x e posteriores.