

SNMP Trap to monitor EIGRP Adjacency change in Nexus 7000

Contents

[Overview](#)

[Example](#)

Overview

The Nexus only supports two traps for EIGRP-MIB, cEigrpAuthFailureEvent and cEigrpRouteStuckInActive, but no SNMP traps for EIGRP neighbors up/down (cEigrpNbrDownEvent).

A viable workaround to generate SNMP traps to monitor EIGRP adjacency changes would be to configure two EEM scripts - one for Neighbor Up and one for Neighbor Down - triggered based on the syslog pattern.

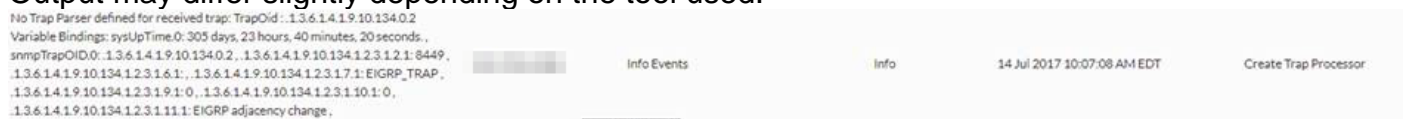
Example

```
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"
```

You can then test by flapping a Layer 3 interface (you may create a test SVI to verify as to not disrupt connectivity):

```
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
```

Confirm that the Nexus is sending these out correctly by checking your SNMP Monitoring tool - Output may differ slightly depending on the tool used:



You may also review these SNMP traps via a Wireshark capture:

Note: Depending on the version of Wireshark, the string will not be in human readable text but can be filtered via "snmp.value.octets contains "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

You can also verify that the Nexus is sending these upon the EEM triggering with Ethalyzer - Example:

```
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: Pre NX-OS 7.x does not give us the option of configuring “**snmp-server enable traps syslog**” which would in turn allow you to monitor the entire logging log itself then filter for the EIGRP messages. This feature was added in later releases, 7.x and later.