

# SNMP trap para monitorear el cambio de la adyacencia del EIGRP en el nexa 7000

## Contenido

[Información general](#)

[Ejemplo:](#)

## Información general

El nexa soporta solamente dos desvíos para EIGRP-MIB, cEigrpAuthFailureEvent y cEigrpRouteStuckInActive, pero ningún SNMP traps para los vecinos EIGRP arriba/abajos (cEigrpNbrDownEvent).

Una solución alternativa viable para generar el SNMP traps para monitorear los cambios de la adyacencia del EIGRP sería configurar dos scripts EEM - uno para el vecino para arriba y uno para el vecino abajo - accionados basado en el modelo del Syslog.

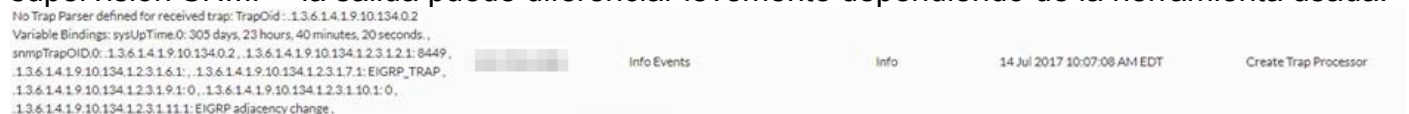
## Ejemplo:

```
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"
```

Usted puede entonces probar agitando una interfaz de la capa 3 (usted puede crear una prueba SVI para verificar en cuanto a para no interrumpir la Conectividad):

```
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 el nexa está mandando éstos correctamente marcando su herramienta de supervisión SNMP - la salida puede diferenciar levemente dependiendo de la herramienta usada:



The screenshot shows a network device's command-line interface displaying an SNMP trap. The text is as follows:

```
No Trap Parser defined for received trap: TrapOid:1.3.6.1.4.1.9.10.134.0.2
Variable Bindings: sysUpTime:0:305 days, 23 hours, 40 minutes, 20 seconds,
snmpTrapOID:0:1.3.6.1.4.1.9.10.134.0.2,1.3.6.1.4.1.9.10.134.1.2.3.1.2.1:8449,
1.3.6.1.4.1.9.10.134.1.2.3.1.6.1:,1.3.6.1.4.1.9.10.134.1.2.3.1.7.1:EIGRP_TRAP,
1.3.6.1.4.1.9.10.134.1.2.3.1.9.1:0,1.3.6.1.4.1.9.10.134.1.2.3.1.10.1:0,
1.3.6.1.4.1.9.10.134.1.2.3.1.11.1:EIGRP adjacency change,
```

Usted puede también revisar este SNMP traps vía una captura de Wireshark:

*Nota: Dependiendo de la versión de Wireshark, la cadena no estará en el texto legible sino se puede filtrar vía "snmp.value.octets contiene "el "" del 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: 45494752502061646a6163656e6379206368616e6765

Usted puede también verificar que el nexa esté enviando éstos sobre el EEM que acciona con Ethalyzer - ejemplo:

```
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 no nos da la opción de configurar “el **Syslog de los desvíos del permiso del SNMP-servidor**” que a su vez permitiría que usted monitoreara el registro entero sí mismo del registro entonces filtra para los mensajes del EIGRP. Esta característica fue agregada en versiones posteriores, 7.x y posterior.