Comprensión de las trampas del Protocolo de administración de red simple (SNMP)

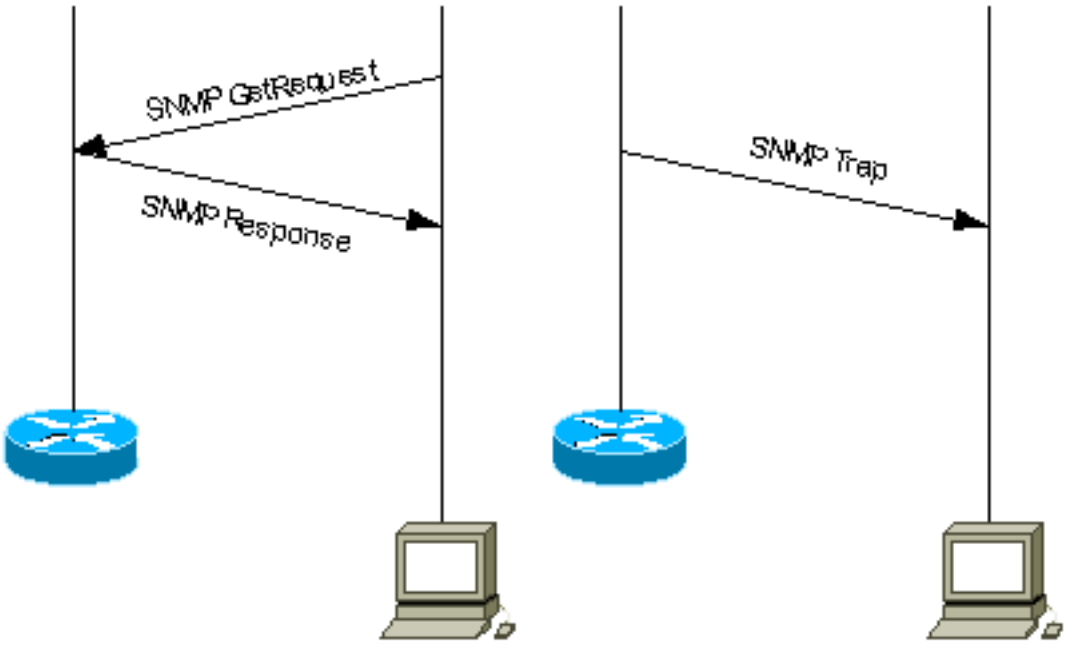
Contenido

Introducción

Este documento brinda una introducción a las trampas SNMP. Muestra cómo se utilizan SNMP traps y el papel que desempeñan en la administración de una red de datos.

Los mensajes de trampa SNMP habilitan un agente para notificar a la estación de administración de acerca de eventos significativos a través de un mensaje SNMP no solicitado.

En este diagrama, la configuración de la izquierda muestra un sistema de administración de red que consulta información y obtiene una respuesta. La configuración de la derecha muestra un agente que envía una trampa no solicitada o asincrónica al sistema de administración de red (NMS).



Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

Convenciones

Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

Usar trampas SNMP

SNMPv1 (Protocolo de administración de red simple) y SNMPv2c, junto con la Base de información para la administración (MIB) asociada, motiva la notificación de trampa directa.

La idea detrás de la notificación dirigida por trampa es que si un administrador es responsable de un gran número de dispositivos y cada dispositivo tiene un gran número de objetos, no es práctico que el administrador sondee o solicite información de cada objeto en cada dispositivo. La solución es que cada agente del dispositivo administrado notifique al administrador sin solicitarlo. Para ello, envía un mensaje conocido como trampa del evento.

Una vez que el administrador recibe el evento, éste lo muestra y puede optar por realizar una acción basada en el evento. Por ejemplo, el administrador puede sondear al agente directamente o bien consultar a otros agentes de dispositivos asociados para comprender mejor el evento.

La notificación de trampa directa puede ahorrar una gran cantidad de recursos de la red y agentes al eliminar la necesidad de pedidos SNMP frívolos. No obstante, no es posible eliminar la consulta SNMP en su totalidad. Las solicitudes SNMP son necesarias para cambios de detección y de topología. Además, un agente de dispositivo administrado no puede enviar una trampa si el dispositivo ha sufrido una interrupción catastrófica.

Las trampas SNMPv1 se definen en RFC 1157, con estos campos:

- *Empresa*: identifica el tipo de objeto administrado que genera la trampa.
- *Dirección de agente*: proporciona la dirección del objeto administrado que genera la trampa.
- *Tipo de trampa genérico*: indica uno de varios tipos de trampa genéricos.
- *Código de trampa específico*: indica uno de varios códigos de trampa específicos.
- *Marca de tiempo*: proporciona la cantidad de tiempo que ha transcurrido entre la última reinicialización de la red y la generación de la trampa.
- *Vinculaciones variables*: el campo de datos de la trampa que contiene PDU. Cada enlace de variable asocia una instancia de objeto MIB determinada con su valor actual.

Las trampas genéricas estándar son: coldStart, warmStart, linkDown, linkUp, authenticationFailure, egpNeighborLoss. Para las trampas genéricas SNMPv1, el campo

Enterprise contiene el valor sysObjectID del dispositivo que envía la trampa. Para las trampas específicas del proveedor, el campo *Tipo de trampa genérico* se establece en enterpriseSpecific(6). Cisco implementó sus propias trampas específicas de una manera no convencional. En lugar de que el campo *de* trampa *Enterprise* siga siendo sysObjectID y tenga el *código de trampa específico* para identificar todas las trampas específicas soportadas por todos los dispositivos Cisco, Cisco implementó la identificación de trampa usando varios campos de trampa Enterprise y de código de trampa específico. Puede ver los valores reales desde el SNMP Object Navigator . Además, Cisco redefinió algunas trampas genéricas en CISCO-GENERAL-TRAPS MIB con la adición de más variables enlazadas. Para estas trampas, el *tipo de trampa genérico* se mantiene igual y no se establece en enterpriseSpecific(6).

En SNMPv2c, la trampa se define como NOTIFICACIÓN y tiene un formato diferente al SNMPv1. Tiene estos parámetros:

- *sysUpTime*: es lo mismo que la marca de tiempo en la trampa SNMPv1.
- *snmpTrapOID* —Campo de identificación de trampa. Para las trampas genéricas, los valores se definen en RFC 1907, para las trampas específicas del proveedor *snmpTrapOID* es esencialmente una concatenación del parámetro *Enterprise* SNMPv1 y dos sub-identificadores adicionales, '0', y el *código de trampa específico* SNMPv1.
- *VarBindList*: es una lista de vinculaciones variables.

Para que un sistema de administración comprenda una trampa que le envía un agente, el sistema de administración debe saber qué define el identificador de objetos (OID). Por lo tanto, debe tener la MIB para esa captura cargada. Esto brinda la información del OID correcta para que el sistema de administración de la red pueda entender las notificaciones de trampa que le son enviados.

Para las trampas que son soportadas por los dispositivos Cisco en MIBs específicas, refiérase al Navegador de Objetos SNMP de Cisco . Esto enumera las trampas disponibles para una MIB específica. Para recibir una de estas trampas, su versión de software del IOS® de Cisco debe soportar la MIB enumerada. Para averiguar qué MIB se soportan en su dispositivo Cisco, visite www.cisco.com/go/mibs . La base MIB debe ser cargada en su sistema de administración de red. Esto comúnmente se refiere a una compilación. Consulte la guía del usuario de Network Management System (por ejemplo, HP OpenView o NetView) sobre la compilación de MIB en su plataforma NMS. También consulte SNMP: Preguntas frecuentes sobre MIBs y Compiladores MIB y MIBs de Carga.

Además, un dispositivo no envía una trampa a un sistema de administración de red a menos que esté configurado para hacerlo. Un dispositivo debe saber que debe enviar una trampa. El destino de la trampa a menudo está definido por una dirección IP, pero puede ser un nombre de host, si el dispositivo está configurado para consultar a un servidor del Sistema de nombre de dominio (DNS). En versiones posteriores del software Cisco IOS, los administradores de dispositivos pueden elegir qué trampas desean enviar. Para obtener información sobre cómo configurar un dispositivo Cisco para SNMP, y cómo enviar trampas, refiérase a las guías de configuración de dispositivo correspondientes y a la Guía de Implementación de NMS de Marcado Básico, Trampas SNMP Soportadas de Cisco IOS y Cómo Configurarlas y Cómo Soportar y Configurar Trampas SNMP de Cisco CatalystOS.

Nota: El administrador recibe normalmente notificaciones SNMP (TRAP e INFORM) en el puerto UDP número 162.

Ejemplos de trampas enviadas por el IOS de Cisco

Esta sección contiene algunos ejemplos de trampas enviadas por Cisco IOS, tomadas con **debug snmp packet**.

Captura genérica SNMPv1, redefinida por Cisco:

```
Nov 21 07:44:17: %LINK-3-UPDOWN: Interface Loopback1, changed state to up
4d23h: SNMP: Queuing packet to 172.17.246.162
4d23h: SNMP: V1 Trap, ent products.45, addr 172.17.246.9, gentrap 3, spectrap 0
 ifEntry.1.23 = 23
 ifEntry.2.23 = Loopback1
 ifEntry.3.23 = 24
 lifEntry.20.23 = up
```

Esta salida muestra la trampa linkUp redefinida de Cisco de MIB CISCO-GENERAL-TRAPS con cuatro variables enlazadas. Tiene estos campos:

- *Empresa* = productos.45 (sysObjectID de la trampa de envío del dispositivo, en este ejemplo, es el router c7507)
- *Tipo de trampa genérico* = 3 (linkUp)
- *Código de trampa específico* = 0

Trampa específica de Cisco SNMPv1:

```
4d23h: SNMP: Queuing packet to 172.17.246.162
4d23h: SNMP: V1 Trap, ent ciscoSyslogMIB.2, addr 172.17.246.9, gentrap 6, spectrap 1
 clogHistoryEntry.2.954 = LINK
 clogHistoryEntry.3.954 = 4
 clogHistoryEntry.4.954 = UPDOWN
 clogHistoryEntry.5.954 = Interface Loopback1, changed state to up
 clogHistoryEntry.6.954 = 43021184
```

Esta salida muestra la trampa específica de Cisco clogMessageGenerated de CISCO-SYSLOG-MIB con cinco variables enlazadas. Tiene estos campos:

- *Empresa* = Valor empresarial de la trampa clogMessageGenerated
- *Tipo de trampa genérico* = 6 (enterpriseSpecific)
- *Código específico de trampa = 1 (código específico de trampa clogMessageGenerated)*

Trampa específica de Cisco SNMPv2c:

```
4d23h: SNMP: Queuing packet to 172.17.246.162
4d23h: SNMP: V2 Trap, reqid 2, errstat 0, erridx 0
 sysUpTime.0 = 43053404
 snmpTrapOID.0 =
 clogHistoryEntry.2.958 = SYS
 clogHistoryEntry.3.958 = 6
 clogHistoryEntry.4.958 = CONFIG_I
 clogHistoryEntry.5.958 = Configured from console by vty0 (10.10.10.10)
 clogHistoryEntry.6.958 = 43053403
```

Esta salida muestra la notificación SNMPv2c específica de CiscoConfigManEvent de CISCO-CONFIG-MAN-MIB con tres variables enlazadas:

- ccmHistoryEventCommandSource
- ccmHistoryEventConfigSource
- ccmHistoryEventConfigDestination

Esta trampa se puede utilizar si se han realizado cambios en la configuración del dispositivo. Los

valores de los dos últimos componentes determinan si se ejecutó un comando **show** o si se tocó la configuración.

```
6506E#term mon
6506E#debug snmp packet
SNMP packet debugging is on

6506E#sh run
Building configuration...
...
6506E#
19:24:18: SNMP: Queuing packet to 10.198.28.80
19:24:18: SNMP: V2 Trap, reqid 2, errstat 0, erridx 0
sysUpTime.0 = 6981747
snmpTrapOID.0 = ciscoConfigManMIB.2.0.1
ccmHistoryEventEntry.3.100 = 1
!--- 1 -> commandLine. Executed via CLI. ccmHistoryEventEntry.4.100 = 3 !--- 3 -> running
ccmHistoryEventEntry.5.100 = 2 !--- 2 -> commandSource. Show command was executed.

6506E#term mon
6506E#debug snmp packet
SNMP packet debugging is on

6506E#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
6506E(config)#exit

22:57:37: SNMP: Queuing packet to 10.198.28.80
22:57:37: SNMP: V2 Trap, reqid 2, errstat 0, erridx 0
 sysUpTime.0 = 8261709
 snmpTrapOID.0 = ciscoConfigManMIB.2.0.1
 ccmHistoryEventEntry.3.108 = 1
!--- 1 -> commandLine. Executed via CLI. ccmHistoryEventEntry.4.108 = 2 !--- 2 -> commandSource
ccmHistoryEventEntry.5.108 = 3 !--- 3 -> running. Change was destined to the running
configuration.
```

Información Relacionada

- Soporte Técnico y Documentación - Cisco Systems