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 a la izquierda muestra un sistema de administración de red que sondee la información y consiga una respuesta. La configuración a la derecha muestra un agente que envíe un desvío no solicitado o asíncrono al sistema de administración de la red (NMS).

prerrequisitos

Requisitos

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.

Utilice el SNMP traps

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 de trampa directa es que si un administrador es responsable de un gran número de dispositivos, y cada dispositivo tiene un gran número de objetos, es poco práctico que el administrador sondear o pida la información de cada objeto en cada dispositivo. La solución está para cada agente en el dispositivo administrado para notificar al administrador sin la solicitación. Hace esto enviando un mensaje conocido como desvío del evento.

Después de que el administrador reciba el evento, el administrador lo visualiza y puede elegir tomar medidas basadas en el evento. Por ejemplo, el administrador puede sondear el agente directamente, o sondee otros agentes de dispositivo asociados para conseguir una mejor comprensión del 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 dispositivo administrado no puede enviar un desvío, si el dispositivo ha tenido una interrupción catastrófica.

Los desvíos del SNMPv1 se definen en el RFC 1157, con estos campos:

- *Empresa* — Identifica el tipo de objeto administrado que genere el desvío.
- *Dirección del agente* — Proporciona el direccionamiento del objeto administrado que genera el desvío.
- *Tipo de trampa genérica* — Indica uno de varios Tipos de trampa genérica.
- Specific trap code: indica uno de varios códigos específicos de captura.
- Sello de fecha y hora - Informa cuánto tiempo transcurrió entre la última vez que la red se volvió a iniciar y el momento en que se generó la trampa.
- *Vinculaciones de variable* — El campo de datos del desvío que contiene el PDU. Cada vinculación de variable asocia un caso determinado del objeto de MIB a su valor actual.

Los desvíos genéricos estándar son: coldStart, warmStart, linkDown, linkUp, authenticationFailure, egpNeighborLoss. Para los desvíos genéricos del SNMPv1, el campo de la *empresa* contiene el valor del sysObjectID del dispositivo que envía el desvío. Para los desvíos específicos del vendedor, el *campo del Tipo de trampa genérica* se fija a enterpriseSpecific(6). Cisco implementó sus propios desvíos específicos de una manera no convencional. En vez el tener el campo de la *empresa del* desvío aún el sysObjectID y del tener el *desvío específico cifra* para identificar todos los desvíos específicos soportados por todos los dispositivos de Cisco, el identificador de trampas implementado por Cisco usando la diversa empresa del desvío y los campos específicos del código del desvío. Usted puede ver los valores reales del SNMP Object Navigator . También, Cisco redefinió algunos desvíos genéricos en CISCO-GENERAL-TRAPS MIB con la adición de variables limitadas. Para estos desvíos, mantienen lo mismo y no se fijan al *Tipo de trampa genérica a* enterpriseSpecific(6).

En el SNMPv2C el desvío se define como NOTIFICACIÓN y se formata comparado diferentemente al SNMPv1. Tiene estos parámetros:

- *sysUpTime* — Éste es lo mismo que el sello de fecha/hora en el desvío del SNMPv1.
- *snmpTrapOID* — Campo de identificación del desvío. Para los desvíos genéricos, los valores

se definen en el RFC 1907, porque el *snmpTrapOID* específico de los desvíos del vendedor es esencialmente una concatenación del *parámetro Enterprise del* SNMPv1 y dos sub-identificadores adicionales, '0', y el *parámetro del código específico del desvío del* SNMPv1.
- *VarBindList* — Ésta es una lista de vinculaciones de variable.

Para que un sistema de administración entienda un desvío enviado a él por un agente, el sistema de administración debe conocer lo que define el identificador de objeto (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 los desvíos que son soportados por los dispositivos de Cisco en el MIB específico, refiera al SNMP Object Navigator de Cisco . Esto enumera los desvíos disponibles para un MIB específico. Para recibir uno de estos desvíos, su versión de software de Cisco IOS® debe soportar el MIB enumerado. Para descubrir que el MIB se soporta en su dispositivo de Cisco, visita 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. Vea su guía del usuario del sistema de administración de red (por ejemplo, HP OpenView o Netview) sobre la compilación de MIB en su plataforma NMS. También refiera al SNMP: Preguntas frecuentes sobre el MIB y los compiladores MIB y el MIB del cargamento.

Además, un dispositivo no envía un desvío a un sistema de administración de red a menos que se configure para hacer tan. Un dispositivo debe saber que debe enviar un desvío. 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 del Cisco IOS Software posteriores, los administradores de dispositivo pueden elegir que los desvíos que quisieran envían. Para la información sobre cómo configurar un dispositivo de Cisco para el SNMP, y cómo enviar los desvíos, refiera a las guías de configuración del dispositivo y al guía de instrumentación correspondientes del marcado básico NMS, los Cisco IOS SNMP Traps soportados y cómo configurar los y el soporte del Cómo y configurar el SNMP traps del CatalystOS de Cisco.

Nota: El administrador recibe típicamente las notificaciones SNMP (los desvíos e informan) en el número del puerto 162 UDP.

Ejemplos de capturas enviadas por Cisco IOS

Esta sección contiene algunos ejemplos de los desvíos enviados por el Cisco IOS, tomado con el **paquete snmp del debug**.

Desvío genérico del SNMPv1, redefinido 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 el desvío redefinido Cisco de la conexión de CISCO-GENERAL-TRAPS MIB con cuatro variables encuadernadas. Tiene estos campos:

- *Empresa* = products.45 (sysObjectID del dispositivo que envía el desvío, en este ejemplo, es

el router c7507)

- *Tipo de trampa genérica* = 3 (conexión)
- *Código específico del desvío* = 0

Desvío específico de Cisco del 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 a Cisco el desvío específico del clogMessageGenerated del CISCO-SYSLOG-MIB con cinco variables encuadernadas. Tiene estos campos:

- Valor de la *empresa* = de la empresa del desvío del clogMessageGenerated
- *Tipo de trampa genérica* = 6 (enterpriseSpecific)
- Código específico de trampa = 1 (código específico de trampa clogMessageGenerated)

Desvío específico SNMPv2C Cisco:

```
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 a Cisco la notificación ciscoConfigManEvent específica SNMPv2C del CISCO-CONFIG-MAN-MIB con tres variables encuadernadas:

- ccmHistoryEventCommandSource
- ccmHistoryEventConfigSource
- ccmHistoryEventConfigDestination

Este desvío puede ser utilizado si ha habido algunos cambios hechos a la configuración de dispositivo. Los valores de los componentes del último dos determinan si publicaron un **comando show** o si la configuración fue tocada.

```
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