Cómo encontrar la fuente de las trampas de falla de autenticación SNMP de Cisco

Contenido

Introducción
Prerequisites
Requirements
Componentes Utilizados
Convenciones
Notificaciones de trampa de AuthenticationFailure
Número de definición de MIB 1
Número de definición MIB 2
MIB de trampas generales de Cisco
Información Relacionada

Introducción

Este documento permite determinar la dirección IP que generó la trampa authenticationFailure. Una trampa authenticationFailure significa que la entidad de protocolo de envío es la destinataria de un mensaje de protocolo que carece de autenticación correcta. Obtendrá esta trampa si un sistema de administración de red (NMS) sondea el dispositivo con una cadena de comunidad incorrecta.

Prerequisites

Requirements

Quienes lean este documento deben tener conocimiento de los siguientes temas:

- Definiciones de MIB
- Capturas de protocolo simple de administración de red (SNMP)
- Identificadores de objetos (OID)

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Todas las versiones 11.x y 12.x del software Cisco IOS®
- Todos los switches y routers Cisco
- Catalyst OS (CatOS) 6.3.1 para compatibilidad con Cisco-System-MIB

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Convenciones

For more information on document conventions, refer to the Cisco Technical Tips Conventions.

Notificaciones de trampa de AuthenticationFailure

La propia trampa no es de mucha ayuda sin el **varbind** `authAddr` que viene con la trampa. **varbind** es un objeto MIB adicional que viene de la MIB del sistema antiguo de Cisco. La `authAddr` le indica la última dirección IP de falla de autorización SNMP. Estas son ambas definiciones de MIB:

Número de definición de MIB 1

Esta definición es de Definiciones CISCOTRAP-MIB:

```
.1.3.6.1.2.1.11.0.4
authenticationFailure OBJECT-TYPE
-- FROM CISCOTRAP-MIB
TRAP
VARBINDS { authAddr }
DESCRIPTION "An authenticationFailure trap signifies that the sending protocol
entity is the addressee of a protocol message that is not properly authenticated.
While implementations of the SNMP must be capable of generating this trap, they
must also be capable of suppressing the emission of such traps via an implementation-
specific mechanism."
::= { iso(1) org(3) dod(6) internet(1) mgmt(2) mib-2(1) snmp(11) snmp#(0) 4}
```

Número de definición MIB 2

Esta definición es de Definiciones OLD-CISCO-SYSTEM-MIB:

```
.1.3.6.1.4.1.9.2.1.5
authAddr OBJECT-TYPE
-- FROM OLD-CISCO-SYSTEM-MIB
SYNTAX IpAddress
MAX-ACCESS read-only
STATUS Mandatory
DESCRIPTION "This variable contains the last SNMP
authorization failure IP address."
::= { ISO(1) org(3) DOD(6) Internet(1) private(4) enterprises(1) cisco(9) local(2)
  lsystem(1) 5 }
```

MIB de trampas generales de Cisco

Debe cargar Cisco-General-Traps MIB en su sistema NMS para formatear correctamente la trampa. Además, debe tener todas las importaciones listadas en la parte superior de Cisco-General-Trap MIB antes de poder compilar Cisco-General-Traps MIB. Esta es la lista:

```
IMPORTS
```

```
  sysUpTime, ifIndex, ifDescr, ifType, egpNeighAddr,
  tcpConnState
  FROM RFC1213-MIB
  cisco
  FROM CISCO-SMI
  whyReload, authAddr
  FROM OLD-CISCO-SYSTEM-MIB
  locIfReason
  FROM OLD-CISCO-INTERFACES-MIB
  tslineSesType, tsLineUser
  FROM OLD-CISCO-TS-MIB
  loctcpConnElapsed, loctcpConnInBytes, loctcpConnOutBytes
  FROM OLD-CISCO-TCP-MIB
  TRAP-TYPE
  FROM RFC-1215;
```

Después de la compilación de todas las definiciones MIB correctas, la trampa tiene el siguiente aspecto:

```
Oct 18 16:54:04 nms-server2 snmptrapd[415]: 10.29.4.1: Authentication Failure
  Trap (0) Uptime: 148 days, 19:19:06.60,

enterprises.cisco.local.lsystem.authAddr.0 = IpAddress: 172.18.123.63

Oct 18 16:54:05 nms-server2 snmptrapd[415]: 10.29.4.1: Authentication Failure
  Trap (0) Uptime: 148 days, 19:19:07.61,

enterprises.cisco.local.lsystem.authAddr.0 = IpAddress: 172.18.123.63
```

Puede ver que 172.18.123.63 está sondeando 10.29.4.1 con la cadena de comunidad incorrecta. Si este sistema es uno que debe sondear el dispositivo 10.29.4.1, debe investigar 172.18.123.63 para determinar por qué el sistema utiliza la comunidad incorrecta. Luego, cambie la comunidad a la cadena de comunidad correcta . Si el sistema no es un NMS conocido, el problema puede ser que algo está tratando de acceder al dispositivo a través de SNMP.

Información Relacionada

- Notas técnicas de diseño de servicios de aplicaciones IP
- Soporte Técnico y Documentación - Cisco Systems