

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

## Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenciones](#)

[Notificaciones de trampa de AuthenticationFailure](#)

[Definición de MIB número 1](#)

[Definición de MIB número 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.

## [prerrequisitos](#)

### [Requisitos](#)

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

- Definiciones de MIB
- Desvíos del Simple Network Management Protocol (SNMP)
- Identificadores de objeto (OID)

### [Componentes Utilizados](#)

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

- Todos los Software Release 11.x y 12.x de Cisco IOS®
- Todos los switches y routers Cisco
- Catalyst OS (CatOS) 6.3.1 para el soporte Cisco-Sistema-MIB

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

## Convenciones

Para obtener más información sobre las convenciones del documento, consulte las [Convenciones de Consejos Técnicos de Cisco](#).

## Notificaciones de trampa de AuthenticationFailure

El desvío sí mismo no es mucha ayuda sin el `authAddr` del **varbind** que viene con el desvío. El **varbind** es un objeto del MIB adicional que viene del Viejo-Cisco-sistema MIB. El `authAddr` le dice la dirección IP de la falla de autorización del último SNMP. Aquí están ambas Definiciones de MIB:

### Definición de MIB número 1

Esta definición es de las [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 }
```

### Definición de MIB número 2

Esta definición es de las [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

Usted debe cargar los Cisco-General-desvíos MIB en su sistema NMS para formatear correctamente el desvío. También, usted debe tener todas las importaciones enumeradas en la cima del Cisco-General-desvío MIB antes de que usted pueda compilar los Cisco-General-

desvíos MIB. Aquí está 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 de MIB correctas, el desvío parece esto:

```
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
```

Usted 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 de 10.29.4.1, usted necesita investigar 172.18.123.63 para determinar porqué el sistema utiliza la comunidad incorrecta. Entonces, cambie a la comunidad a la cadena de comunidad correcta. Si el sistema no es un NMS sabido, el problema puede ser que algo está intentando cortar en el dispositivo vía el SNMP.

## [Información Relacionada](#)

- [Notas técnicas de diseño de los Servicios de aplicación IP](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)