# Hoe de bron van Cisco SNMP-verificatietraps te vinden

## Inhoud



## Inleiding

Dit document stelt u in staat het IP-adres te bepalen dat de val `van` de `authenticatiefout` heeft veroorzaakt. Een `authenticatieFalen` betekent dat de verzendende protocol entiteit de adressaat is van een protocol bericht dat geen goede authenticatie heeft. Je krijgt deze val als een netwerk Management System (NMS) het apparaat polls met de verkeerde community string.

## Voorwaarden

### Vereisten

Lezers van dit document zouden kennis moeten hebben van deze onderwerpen:

- MIB - definities
- Simple Network Management Protocol (SNMP)-traps
- Objectidentificatoren (OID's)

### Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Alle Cisco IOS® softwarereleases 11.x en 12.x
- Alle Cisco-routers en -switches
- Catalyst OS (CatOS) 6.3.1 voor Cisco-System-MIB ondersteuning

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een

opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

### Conventies

Raadpleeg Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

## Detectietraps

De val zelf is niet veel hulp zonder de **varodieke** `auth`Addr die met de val komt. De **varbind** is een extra MIB object dat uit het Old-Cisco-System MIB komt. De `authAdressaten` vertellen u het laatste IP adres van de de van SNMP vergunning mislukte. Hier zijn beide MIB definities:

### MIB Definitie nummer 1

Deze definitie is afkomstig van CISCOTRAP-MIB Definities:

```
.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}
```

### MIB Definitie nummer 2

Deze definitie is afkomstig van OUD-CISCO-SYSTEM-MIB Definities:

```
.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 }
```

## Cisco MIB-tranches

U moet de Cisco-General-Traps MIB in uw NMS-systeem laden om de val naar behoren te kunnen opmaken. Bovendien moet u alle import bovenaan de Cisco-General-Trap MIB hebben staan voordat u de Cisco-General-Trap MIB kunt compileren. Dit is de lijst:

```
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;
```

Na de samenstelling van alle correcte MIB - definities ziet de val er zo uit:

```
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
```

Je kunt zien dat 172.18.123.63 10.29.4.1 is met de verkeerde gemeenschapsstring. Als dit systeem er één is die het 10.29.4.1 apparaat moet inleiden, moet je 172.18.123.63 onderzoeken om te bepalen waarom het systeem de verkeerde gemeenschap gebruikt. Verander dan de gemeenschap in de juiste gemeenschapsstring. Als het systeem geen bekende NMS is, kan het probleem zijn dat iets via SNMP in het apparaat probeert te hacken.

## Gerelateerde informatie

- TechNotes voor IP-toepassingsservices
- Technische ondersteuning en documentatie – Cisco Systems