# Trouver la source des dérivateurs AuthenticationFailure de Cisco SNMP

## Contenu


Introduction
Conditions préalables
Conditions requises
Components Used
Conventions
Interruptions AuthenticationFailure
Numéro de définition MIB 1
Numéro de définition MIB 2
MIB de trappes générales Cisco
Informations connexes


## Introduction

Ce document vous permet de déterminer l'adresse IP qui a entraîné le déroutement authenticationFailure. Le déroutement authenticationFailure signifie que l'entité ayant envoyé le protocole est le destinataire d'un message de gestion de protocole qui n'est pas correctement authentifié. Ce déroutement survient si un système d'administration de réseaux (NMS) connecte l'appareil à la mauvaise chaîne de communauté.

## Conditions préalables

### Conditions requises

Les lecteurs de ce document devraient avoir connaissance des sujets suivants :

- Définitions MIB
- Interruptions SNMP (Simple Network Management Protocol)
- Identificateurs d'objet (OID)

### Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Toutes les versions du logiciel Cisco IOS® 11.x et 12.x
- Tous les routeurs et commutateurs Cisco
- Catalyst OS (CatOS) 6.3.1 pour la prise en charge de 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.

### Conventions

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

## Interruptions AuthenticationFailure

Le piège lui-même n'est pas beaucoup d'aide sans le **varbind** `authAddr` qui vient avec le piège. Le **varbind** est un objet MIB supplémentaire qui provient de l'ancienne MIB du système Cisco. L'adresse `authAddr` vous indique la dernière adresse IP d'échec d'autorisation SNMP. Voici les deux définitions MIB :

### Numéro de définition MIB 1

Cette définition provient de CISCOTRAP-MIB Definitions :

```
.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}
```

### Numéro de définition MIB 2

Cette définition provient des anciennes définitions 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 trappes générales Cisco

Vous devez charger la base MIB Cisco-General-Traps dans votre système NMS afin de formater correctement le déroutement. En outre, toutes les importations doivent figurer en haut de la MIB de déroutement Cisco-General-Trap avant de pouvoir compiler la MIB de déroutement Cisco-General-Traps. Voici la liste :

```
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;
```

Après avoir compilé toutes les définitions MIB correctes, le déroutement ressemble à ceci :

```
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
```

Vous pouvez voir que 172.18.123.63 effectue une interrogation sur 10.29.4.1 avec la mauvaise chaîne de communauté. Si ce système doit interroger le périphérique 10.29.4.1, vous devez examiner 172.18.123.63 afin de déterminer pourquoi le système utilise la mauvaise communauté. Ensuite, changez la communauté en chaîne de communauté correcte . Si le système n'est pas un système de gestion de réseau connu, le problème peut être que quelque chose essaie de pirater le périphérique via SNMP.

## Informations connexes

- Notes techniques de conception des services d'applications IP
- Support et documentation techniques - Cisco Systems