## Table of Contents

**How to Find the Source of Cisco SNMP AuthenticationFailure Traps** ................................................................. 1

- **Introduction** .................................................................................................................................................... 1
- **Prerequisites** ................................................................................................................................................... 1
- **Hardware and Software Versions** .................................................................................................................. 1
- **AuthenticationFailure Traps** ....................................................................................................................... 1
  - MIB Definition #1 ........................................................................................................................................ 2
  - MIB Definition #2 ........................................................................................................................................ 2
- **Cisco−General−Traps MIB** .......................................................................................................................... 2
- **Related Information** ....................................................................................................................................... 3
How to Find the Source of Cisco SNMP AuthenticationFailure Traps

Introduction

Prerequisites

Hardware and Software Versions AuthenticationFailure Traps

MIB Definition #1
MIB Definition #2
Cisco−General−Traps MIB
Related Information

Related Topics
Additional Documentation

Introduction

This document can be used to determine the IP address that has caused the authenticationFailure trap. An authenticationFailure trap signifies that the sending protocol entity is the addressee of a protocol message that is not properly authenticated. You get this trap if a Network Management System (NMS) is polling the device with the wrong community string.

Prerequisites

Readers of this document should be knowledgeable of the following:

- MIB Definitions
- SNMP Traps
- OIDs

Hardware and Software Versions

The information in this document is based on the software and hardware versions below.

- All Native IOS versions 11.x and 12.x
- All Cisco routers and switches
- CATOS 6.3.1 for Cisco−System−MIB support

AuthenticationFailure Traps

The trap itself is not much help without the varbind (additional MIB Object) authAddr that is also sent with the trap. This object comes from the Old−Cisco−System MIB. authAddr tells us the last SNMP authorization failure IP address. Here are both MIB definitions below.
MIB Definition #1


.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 Definition #2

From ftp://ftp.cisco.com/pub/mibs/v1/OLD−CISCO−SYSTEM−MIB.my

.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−General−Traps MIB

You must have the Cisco−General−Traps MIB loaded in you NMS system to properly format the trap. You must also have all of the imports listed at the top of the Cisco−General−Trap MIB before you can compile the Cisco−General−Traps MIB. Here is the list below:

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;

This is what the trap should look like when all the correct MIB definitions are compiled:

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.1system.authAddr.0 = IpAddress: 172.18.123.63

Cisco − How to Find the Source of Cisco SNMP authenticationFailure Traps
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

From this we can see that 172.18.123.63 is polling 10.29.4.1 with the wrong community string. We would have to investigate 172.18.123.63 and see why the wrong community is being used and change it to the correct community string if it is a system that should be polling the 10.29.4.1 device. If it is not a known NMS system we may have something trying to hack into the device via SNMP.

Related Information

• IP Application Services Technical Tips

All contents are Copyright © 1992—2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.