

How to Find the Source of Cisco SNMP AuthenticationFailure Traps

Document ID: 19003

Introduction

Prerequisites

Requirements

Components Used

Conventions

AuthenticationFailure Traps

MIB Definition Number 1

MIB Definition Number 2

Cisco-General-Traps MIB

Related Information

Introduction

This document enables you 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 does not have proper authentication. You get this trap if a network management system (NMS) polls the device with the wrong community string.

Prerequisites

Requirements

Readers of this document should have knowledge of these topics:

- MIB definitions
- Simple Network Management Protocol (SNMP) traps
- Object identifiers (OIDs)

Components Used

The information in this document is based on these software and hardware versions:

- All Cisco IOS® Software Releases 11.x and 12.x
- All Cisco routers and switches
- Catalyst OS (CatOS) 6.3.1 for Cisco-System-MIB support

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.

AuthenticationFailure Traps

The trap itself is not much help without the **varbind** `authAddr` that comes with the trap. The **varbind** is an additional MIB object that comes from the Old-Cisco-System MIB. The `authAddr` tells you the last SNMP authorization failure IP address. Here are both MIB definitions:

MIB Definition Number 1

This definition is from 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}
```

MIB Definition Number 2

This definition is from OLD-CISCO-SYSTEM-MIB Definitions:

```
.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 load the Cisco-General-Traps MIB in your NMS system in order to properly format the trap. Also, you must have all 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:

```
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;
```

After the compilation of all the correct MIB definitions, the trap looks like this:

```
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
```

You can see that 172.18.123.63 is polling 10.29.4.1 with the wrong community string. If this system is one that should poll the 10.29.4.1 device, you need to investigate 172.18.123.63 in order to determine why the system uses the wrong community. Then, change the community to the correct community string . If the system is not a known NMS, the problem can be that something is trying to hack into the device via SNMP.

Related Information

- [IP Application Services Design TechNotes](#)
- [Technical Support & Documentation – Cisco Systems](#)

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2008 – 2009 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Nov 01, 2005

Document ID: 19003
