So finden Sie die Quelle für Cisco SNMP AuthenticationFailure-Traps

Inhalt

[Einführung](#)
[Voraussetzungen](#)
[Anforderungen](#)
[Verwendete Komponenten](#)
[Konventionen](#)
[Authentifizierungsfehler-Traps](#)
[MIB-Definition Nummer 1](#)
[MIB-Definition Nummer 2](#)
[Cisco General Traps MIB](#)
[Zugehörige Informationen](#)

Einführung

In diesem Dokument können Sie die IP-Adresse bestimmen, die das `authenticationFailure`-Trap verursacht hat. Ein `authenticationFailure`-Trap bedeutet, dass die sendende Protokolleinheit der Empfänger einer Protokollnachricht ist, die nicht über eine ordnungsgemäße Authentifizierung verfügt. Sie erhalten dieses Trap, wenn ein Netzwerkmanagementsystem (NMS) das Gerät mit dem falschen Community String abfragt.

Voraussetzungen

Anforderungen

Die Leser dieses Dokuments sollten folgende Themen kennen:

- MIB-Definitionen
- Simple Network Management Protocol (SNMP)-Traps
- Objekt-IDs (OIDs)

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Alle Cisco IOS® Software-Versionen 11.x und 12.x
- Alle Cisco Router und Switches
- Catalyst OS (CatOS) 6.3.1 für Cisco System-MIB-Unterstützung

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den Cisco Technical Tips Conventions.

Authentifizierungsfehler-Traps

Die Trap selbst ist ohne die **varbind**`authAddr`, die mit der Trap geliefert wird, nicht viel hilfreich. Die **varbind** ist ein zusätzliches MIB-Objekt, das von der alten Cisco-System-MIB stammt. Die `authAddr` teilt Ihnen die letzte IP-Adresse mit, an der der SNMP-Autorisierungsfehler aufgetreten ist. Im Folgenden werden beide MIB-Definitionen aufgeführt:

MIB-Definition Nummer 1

Diese Definition stammt aus CISCOTRAP-MIB-Definitionen:

```
.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 Nummer 2

Diese Definition stammt aus OLD-CISCO-SYSTEM-MIB-Definitionen:

```
.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

Sie müssen die Cisco General Traps MIB in Ihr NMS-System laden, um das Trap korrekt formatieren zu können. Außerdem müssen alle oben in der Cisco-General-Trap-MIB aufgeführten Importe aufgeführt sein, bevor Sie die Cisco-General-Traps-MIB kompilieren können. Die Liste ist

wie folgt:

```
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;
```

Nach der Kompilierung aller richtigen MIB-Definitionen sieht das Trap wie folgt aus:

```
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
```

Wie Sie sehen, fragt 172.18.123.63 10.29.4.1 mit dem falschen Community-String ab. Wenn es sich bei diesem System um ein System handelt, das das 10.29.4.1-Gerät abfragen soll, müssen Sie die Datei 172.18.123.63 untersuchen, um zu ermitteln, warum das System die falsche Community verwendet. Ändern Sie dann die Community in den korrekten Community String . Wenn es sich bei dem System nicht um ein bekanntes NMS handelt, kann das Problem darin bestehen, dass über SNMP versucht wird, in das Gerät einzudringen.

Zugehörige Informationen

- IP Application Services Design TechNotes
- Technischer Support und Dokumentation - Cisco Systems