Come trovare l'origine dei trap degli errori di autenticazione SNMP Cisco

Sommario

[Introduzione](#)
[Prerequisiti](#)
[Requisiti](#)
[Componenti usati](#)
[Convenzioni](#)
[Trap autenticazione non riuscita](#)
[Numero definizione MIB 1](#)
[Numero definizione MIB 2](#)
[MIB Cisco-General-Traps](#)
[Informazioni correlate](#)

Introduzione

Questo documento consente di determinare l'indirizzo IP che ha causato la trap `authenticationFailure`. Un trap `authenticationFailure` indica che l'entità del protocollo di invio è il destinatario di un messaggio di protocollo per il quale non è disponibile l'autenticazione corretta. Questa trap si verifica se un sistema di gestione di rete (NMS) esegue il polling del dispositivo con la stringa della community errata.

Prerequisiti

Requisiti

Questo documento è utile per conoscere i seguenti argomenti:

- definizioni MIB
- Trap SNMP (Simple Network Management Protocol)
- OID (Object Identifier)

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Tutti i software Cisco IOS® versioni 11.x e 12.x
- Tutti i router e gli switch Cisco
- Catalyst OS (CatOS) 6.3.1 per supporto Cisco-System-MIB

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Trap autenticazione non riuscita

La trap in sé non è di grande aiuto senza il **varbind** `authAddr` fornito con la trap. Il **varbind** è un oggetto MIB aggiuntivo proveniente dal MIB del vecchio sistema Cisco. Il comando `authAddr` indica l'ultimo indirizzo IP di autorizzazione SNMP non riuscita. Di seguito sono riportate entrambe le definizioni MIB:

Numero definizione MIB 1

Questa definizione deriva dalle definizioni CISCOTRAP-MIB:

```
.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}
```

Numero definizione MIB 2

Questa definizione viene da 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 }
```

MIB Cisco-General-Traps

Per formattare correttamente la trap, è necessario caricare il MIB Cisco-General-Traps nel sistema NMS. Inoltre, per poter compilare il MIB Cisco-General-Trap, è necessario che tutte le importazioni siano elencate nella parte superiore del MIB Cisco-General-Trap. Ecco l'elenco:

```
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;
```

Dopo la compilazione di tutte le definizioni MIB corrette, la trap avrà il seguente aspetto:

```
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
```

Come si può vedere, 172.18.123.63 sta eseguendo il polling di 10.29.4.1 con la stringa della community errata. Se il sistema in uso deve eseguire il polling del dispositivo 10.29.4.1, è necessario esaminare 172.18.123.63 per stabilire perché il sistema utilizza la community errata. Quindi, modificare la community con la stringa della community corretta. Se il sistema non è un NMS noto, il problema può essere che un utente sta tentando di accedere al dispositivo tramite SNMP.

Informazioni correlate

- Note tecniche per la progettazione di servizi applicativi IP
- Documentazione e supporto tecnico – Cisco Systems