如何查詢Cisco SNMP身份驗證失敗陷阱的來源

目錄

[簡介](#)
[必要條件](#)
[需求](#)
[採用元件](#)
[慣例](#)
[AuthenticationFailure陷阱](#)
[MIB定義編號1](#)
[MIB定義數字2](#)
[Cisco-General-Traps MIB](#)
[相關資訊](#)

簡介

本文檔用於確定導致authenticationFailure陷阱的IP地址。authenticationFailure陷阱表示傳送協定實體是不具有正確身份驗證的協定消息的地址。如果網路管理系統(NMS)使用錯誤的社群字串輪詢裝置，便會收到此陷阱。

必要條件

需求

本文檔的讀者應瞭解以下主題：

- MIB定義
- 簡單網路管理協定(SNMP)陷阱
- 對象識別符號(OID)

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 所有Cisco IOS®軟體版本11.x和12.x
- 所有思科路由器和交換機
- 適用於Cisco-System-MIB支援的Catalyst OS(CatOS)6.3.1

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

AuthenticationFailure陷阱

如果沒有陷阱附帶的**varbind** `authAddr`，陷阱本身就幫不上大忙。**varbind**是來自舊思科系統MIB的附加MIB對象。`authAddr`會告訴您最後一個SNMP授權失敗IP位址。以下兩個MIB定義：

MIB定義編號1

此定義來自CISCOTRAP-MIB定義:

```
.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定義數字2

此定義來自舊的CISCO-SYSTEM-MIB定義:

```
.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

您必須在NMS系統中載入Cisco-General-Traps MIB，才能正確格式化陷阱。此外，在編譯Cisco-General-Traps MIB之前，必須在Cisco-General-Traps MIB的頂部列出所有匯入。以下是清單：

```
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;
```

編譯所有正確的MIB定義後，陷阱如下所示：

```
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
```

您可以看到172.18.123.63正在使用錯誤的社群字串輪詢10.29.4.1。如果此系統應該輪詢10.29.4.1裝置，則需要調查172.18.123.63以確定系統使用錯誤社群的原因。然後，將團體更改為正確的團體字串。如果系統不是已知的NMS，則問題可能是某些裝置試圖通過SNMP侵入裝置。

相關資訊

- IP應用程式服務設計技術說明
- 技術支援與文件 - Cisco Systems