シスコの SNMP authenticationFailure トラップの原因の調査方法

内容

概要

このドキュメントでは、authenticationFailure トラップの原因となった IP アドレスの判別方法について説明しています。authenticationFailure トラップは、送信プロトコル エンティティが、正式な認証のないプロトコル メッセージのアドレス保持者であることを表しています。このトラップが発生するのは、Network Management System（NMS; ネットワーク管理システム）が誤ったコミュニティ ストリングでデバイスをポーリングした場合です。

前提条件

要件

このドキュメントの読者は次のトピックについての専門知識を有している必要があります。

- MIB の定義
- Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）トラップ
- オブジェクト識別子（OID）

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- すべてのCisco IOS®ソフトウェアリリース11.xおよび12.x
- シスコのルータとスイッチのすべて
- Cisco-System-MIB をサポートする Catalyst OS（CatOS）6.3.1

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド

キュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

表記法

ドキュメント表記の詳細は、「シスコ テクニカル ティップスの表記法」を参照してください。

AuthenticationFailure トラップ

このトラップ自体は、一緒に取得される varbind authAddr がないと、あまり役には立ちません。varbind は、Old-Cisco-System MIB から派生する付加的な MIB オブジェクトです。authAddr には、最後に SNMP 認証が失敗した IP アドレスが示されています。次に、2 つの MIB の定義を示します。

1 番目の MIB の定義

この定義は『CISCOTRAP-MIB の定義』からの引用です。

```
.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}
```

2 番目の MIB 定義

この定義は『OLD-CISCO-SYSTEM-MIB の定義』からの引用です。

```
.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

Cisco-General-Traps MIB を NMS システムにロードして、トラップを正しく設定する必要があります。Cisco-General-Traps MIB をコンパイルする前に、Cisco-General-Trap MIB の先頭にインポートするものがすべてリストされている必要があります。それらを次にリストします。

```
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;
```

MIB の正しい定義がすべてコンパイルされると、トラップは次のようになります。

```
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
```

172.18.123.63 から 10.29.4.1 をポーリングする際に、誤ったコミュニティ ストリングが使用されていることが分かります。このシステムが 10.29.4.1 デバイスにポーリングするシステムである場合、システムによって誤ったコミュニティが使用される理由を判断するために 172.18.123.63 を調査する必要があります。次に、コミュニティを正しいコミュニティ ストリングに変更します。システムが既知の NMS ではない場合、SNMP を経由して何者かがデバイスに不法侵入を試みていることが問題である可能性があります。

関連情報

- IP アプリケーション サービス設計テクニカルノート
- テクニカル サポートとドキュメント – Cisco Systems