Trouver la source des dérivateurs AuthenticationFailure de Cisco SNMP

Contenu

Introduction

Ce document vous permet de déterminer l'adresse IP qui a entraîné le déroutement authenticationFailure. Le déroutement authenticationFailure signifie que l'entité ayant envoyé le protocole est le destinataire d'un message de gestion de protocole qui n'est pas correctement authentifié. Ce déroutement survient si un système d'administration de réseaux (NMS) connecte l'appareil à la mauvaise chaîne de communauté.

Conditions préalables

Conditions requises

Les lecteurs de ce document devraient avoir connaissance des sujets suivants :

- Définitions MIB
- Déroutements de Protocole SNMP (Simple Network Management Protocol)
- Identifiants d'objet (OID)

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Toutes les versions de logiciel 11.x et 12.x de Cisco IOS®
- Tous les Routeurs et Commutateurs de Cisco
- SYSTÈME D'EXPLOITATION de Catalyst (CatOS) 6.3.1 pour le support Cisco-Système-MIB

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Conventions

Pour plus d'informations sur les conventions de documents, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Déroutements d'AuthenticationFailure

Le déroutement lui-même n'est pas beaucoup d'aide sans `authAddr de` **varbind** qui est livré avec le déroutement. **Le varbind** est un objet supplémentaire MIB qui provient le MIB de Vieux-Cisco-système. `L'authAddr` t'indique la dernière adresse IP de panne d'autorisation SNMP. Voici les deux définitions MIB :

Définition numéro 1 MIB

Cette définition est des définitions 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}
```

Définition numéro 2 MIB

Cette définition est des définitions OLD-CISCO-SYSTEM-MIB :

```
.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 de Cisco-Général-déroutements

Vous devez charger le MIB de Cisco-Général-déroutements dans votre système NMS afin de formater correctement le déroutement. En outre, vous devez avoir toutes les importations répertoriées en haut du MIB de Cisco-Général-déroutement avant que vous puissiez compiler le

MIB de Cisco-Général-déroutements. Voici la liste :

```
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;
```

Après la compilation de toutes les définitions correctes MIB, le déroutement ressemble à ceci :

```
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
```

Vous pouvez voir que 172.18.123.63 vote 10.29.4.1 avec la chaîne fausse de la communauté. Si ce système est un qui devrait voter le périphérique de 10.29.4.1, vous devez étudier 172.18.123.63 afin de déterminer pourquoi le système utilise la communauté fausse. Puis, changez la communauté à la chaîne correcte de la communauté. Si le système n'est pas des NMS connus, le problème peut être que quelque chose essaye d'entailler dans le périphérique par l'intermédiaire du SNMP.

Informations connexes

- Conception TechNotes de Services d'applications IP
- Support et documentation techniques - Cisco Systems