Protocole de gestion de réseau simple et sécurisé

Table des matières

- Introduction
- Conditions préalables
  - Exigences
  - Composants utilisés
- Informations générales
- Stratégies de sécurisation du SNMP
  - Éviter les chaînes de communauté SNMP non sécurisées
  - Configuration de la vue SNMP
  - Configurer la communauté SNMP avec la liste de contrôle d'accès (ACL)
  - Configuration de SNMPv3
    - Étape 1 : identification de l'adresse NMS de confiance
    - Étape 2 : création d'une liste de contrôle d'accès pour le NMS approuvé
    - Étape 3. Création d'une vue SNMP
    - Étape 4. Création d'un groupe SNMPv3
    - Étape 5. Création de l'utilisateur SNMPv3
    - Étape 6. (Facultatif) Configuration des déroutements ou des informations SNMPv3
    - Étape 7. Désactivation ou prévention des communautés SNMPv1 et SNMPv2c inutiles
    - Remarques importantes
    - Vérifier
  - Configurer la liste de contrôle d'accès sur les interfaces
- Vérification des erreurs SNMP : procédure
- Informations connexes

Introduction

Ce document décrit comment sécuriser votre protocole SNMP (Simple Network Management Protocol).

Conditions préalables

Exigences

Aucune exigence spécifique n'est associée à ce document.

Composants utilisés

Les informations de ce document sont basées sur les fonctionnalités SNMP, telles que SNMP View et SNMP Version 3 (SNMPv3) qui ont été introduites dans la version du logiciel Cisco IOS®. Bien que certains exemples de configuration et la syntaxe de commande soient basés sur Cisco IOS®, les concepts de sécurité SNMP de base s'appliquent également aux plates-formes Cisco IOS XE plus récentes. La syntaxe de commande, les algorithmes d'authentification et de confidentialité pris en charge, les fonctionnalités de plate-forme et les fonctionnalités de protection du plan de gestion peuvent varier entre les versions de Cisco IOS et de Cisco IOS XE.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Informations générales

La sécurisation du protocole SNMP est importante, car un accès SNMP non autorisé peut exposer des informations sur les périphériques, autoriser des modifications de configuration lorsque l'accès en lecture/écriture est activé ou contribuer à des conditions de déni de service (DoS).

Les versions SNMP antérieures, telles que SNMPv1 et SNMPv2c, reposent sur des chaînes de communauté pour le contrôle d'accès. Ces chaînes de communauté fonctionnent de la même manière que les mots de passe partagés, mais elles sont envoyées en texte clair et ne fournissent pas d'authentification ou de chiffrement forts. Si une chaîne de communauté est réutilisée, exposée dans des fichiers de configuration ou capturée à partir du réseau, un utilisateur non autorisé peut interroger les informations du périphérique ou, dans le cas d'une communauté en lecture-écriture, modifier les paramètres du périphérique.

Voici quelques-unes des limitations de sécurité SNMPv1/v2c les plus courantes :

- Utilisation de chaînes de communauté bien connues, telles que public ou private
- Transmission en texte clair des chaînes de communauté
- Absence d'authentification par utilisateur
- Manque de cryptage pour les données utiles SNMP

Pour des déploiements sécurisés, utilisez SNMPv3 avec authentification et confidentialité, le cas

échéant. SNMPv3 fournit une authentification et un cryptage basés sur l'utilisateur, qui aident à protéger les données de contrôle d'accès et de gestion. En outre, vous pouvez limiter l'accès SNMP aux stations de gestion approuvées, éviter les accès en lecture/écriture inutiles et limiter les objets MIB accessibles avec les vues SNMP.



Remarque : Validez la configuration exacte de l'interface de ligne de commande (CLI), la prise en charge des fonctionnalités et les commandes de vérification pour la plate-forme et la version logicielle spécifiques avant le déploiement sur un réseau de production.

Stratégies de sécurisation du SNMP

Éviter les chaînes de communauté SNMP non sécurisées

N'utilisez pas de chaînes de communauté connues, telles que public ou private. Si SNMPv1 ou SNMPv2c est requis pour la compatibilité, utilisez des chaînes de communauté uniques et non évidentes, limitez-les à l'aide de listes de contrôle d'accès et évitez les communautés en lecture-écriture, sauf en cas de besoin opérationnel spécifique.



Remarque : Préférez SNMPv3 avec authPriv pour les déploiements sécurisés. Le niveau authPriv fournit à la fois l'authentification et le chiffrement. L'authentification vérifie que les messages SNMP proviennent d'un utilisateur SNMPv3 valide et la confidentialité chiffre la charge utile SNMP afin que les données de gestion ne soient pas envoyées en texte clair.

Configuration de la vue SNMP

Une vue SNMP limite l'accès à des sous-arborescences MIB spécifiques. Lorsqu'une vue est appliquée à une communauté ou à un groupe SNMPv3, seuls les objets MIB inclus sont accessibles. Les sous-arborescences MIB qui ne sont pas incluses sont implicitement refusées. Vous pouvez également exclure explicitement des sous-arborescences spécifiques d'une sous-arborescence incluse plus large.

Pour créer ou mettre à jour une entrée de vue SNMP, utilisez la commande de configuration globale snmp-server view. Pour supprimer l'entrée d'affichage du serveur SNMP spécifié, utilisez la forme no de cette commande.

```
snmp-server view
```

```
        {included | excluded}
```

```
no snmp-server view
```

Description de la syntaxe :

- myview-name — Libellé de l'enregistrement d'affichage que vous mettez à jour ou créez. Le nom est utilisé pour référencer l'enregistrement.
- oid-tree — Identificateur d'objet (OID) de la sous-arborescence de notation de syntaxe abstraite 1 (ASN.1) à inclure ou à exclure de la vue. Pour identifier la sous-arborescence, spécifiez une chaîne de texte composée de chiffres, par exemple 1.3.6.2.4, ou d'un mot, par exemple système. Remplacez un sous-identificateur unique par le caractère générique astérisque (*) pour spécifier une famille de sous-arborescence ; par exemple 1.3.*.4.
- included or excluded — Type de vue. Vous devez spécifier inclus ou exclu.

La documentation SNMP existante, y compris la RFC 1447, a introduit le concept de vues MIB pour contrôler quelles parties de l'arborescence MIB sont incluses ou exclues de l'accès SNMP. Bien que la RFC 1447 et son modèle de sécurité SNMPv2 basé sur des parties soient obsolètes, le concept de vue MIB reste pertinent dans le SNMP moderne via le modèle de contrôle d'accès basé sur des vues (VACM), défini dans la RFC 3415. Les vues Cisco SNMP utilisent ce concept pour limiter l'accès à des sous-arborescences MIB spécifiques. Une vue SNMP peut être appliquée aux communautés SNMPv1/v2c ou aux groupes SNMPv3.

Cet exemple crée une vue qui inclut tous les objets du groupe système MIB-II, à l'exception de sysServices (System 7) et de tous les objets de l'interface 1 dans le groupe d'interfaces MIB-II :

<#root>

```
snmp-server view agon system included
```

```
snmp-server view agon system.7 excluded
```

```
snmp-server view agon ifEntry.*.1 included
```

Dans cet exemple, la vue autorise l'accès aux objets MIB-II et MIB privés Cisco, mais exclut la table ARP représentée par atEntry:

<#root>

```
snmp-server view myview mib-2 included
```

```
snmp-server view myview atEntry excluded
```

```
snmp-server view myview cisco included
```

```
snmp-server community C1sc03xample view myview RO 11
```

```
snmp-server community C1sc03xample2 view myview RW 11
```

```
snmp-server contact ciscouser@cisco.com
```

Remarque : Certains de ces exemples peuvent faire référence à des objets MIB plus anciens des versions de Cisco IOS, tels que atTable ou atEntry. Sur les nouvelles plates-formes Cisco IOS XE, des données équivalentes peuvent utiliser différents objets MIB ou OID.

Remarque : Avant de déployer une vue SNMP, vérifiez que le nom de l'objet MIB ou l'OID existe sur la plate-forme cible et la version du logiciel. Utilisez SNMP Object Navigator

---

pour plus d'informations.

Configurer la communauté SNMP avec la liste de contrôle d'accès (ACL)

Si SNMPv1 ou SNMPv2c est requis, limitez chaque chaîne de communauté aux adresses NMS (Network Management System) approuvées avec une liste de contrôle d'accès. La liste de contrôle d'accès associée à la communauté SNMP contrôle quelles adresses IP source peuvent utiliser cette chaîne de communauté pour envoyer des requêtes SNMP au périphérique.

La communication SNMP inclut généralement deux types de trafic différents :

- Interrogation/requêtes : Le NMS envoie des requêtes SNMP GET, GETNEXT, GETBULK ou SET au périphérique réseau. Ces requêtes ciblent généralement le port UDP 161 sur le périphérique géré.
- Interruptions / notifications : Le périphérique réseau envoie des interruptions SNMP non sollicitées ou des messages d'information au NMS pour signaler des événements, des alarmes ou des changements d'état. Ces notifications ciblent généralement le port UDP 162 sur le NMS.

Utilisez des chaînes de communauté différentes pour les demandes d'interrogation et les notifications d'interruption. Cette séparation limite l'exposition si une chaîne de communauté est découverte. Par exemple, si un pirate apprend la chaîne de communauté de déroutement à partir d'un paquet de notification, cette chaîne ne doit pas également autoriser l'accès d'interrogation SNMP au périphérique.

<#root>

access-list 10 permit

<#root>

snmp-server community

RO 10

<#root>

snmp-server host

version 2c

Dans cet exemple :

- <RO_POLLING_COMMUNITY> est utilisé par le NMS pour interroger le périphérique.
- <TRAP_NOTIFICATION_COMMUNITY> est utilisé par le périphérique lorsqu'il envoie des déroutements ou des notifications au NMS.
- La liste de contrôle d'accès ACL 10 restreint l'accès à l'interrogation de sorte que seul <NMS_IP> peut utiliser la chaîne de communauté d'interrogation.
- La chaîne de communauté de notification de déroutement n'est pas réutilisée pour l'accès d'interrogation SNMP.

Si une chaîne de communauté de déroutements est configurée, vérifiez qu'elle n'autorise pas involontairement l'accès à l'interrogation SNMP. Sur certaines versions du logiciel Cisco IOS, une chaîne de communauté utilisée pour les déroutements peut également devenir utilisable pour l'accès SNMP, sauf si elle est explicitement restreinte ou désactivée.

Pour empêcher l'interrogation de l'accès avec la chaîne de communauté de déroutements, refusez explicitement son utilisation en tant que communauté SNMP :

<#root>

```
access-list 99 deny any
```

```
<#root>

snmp-server community

    RO 99
```

Évitez de configurer des communautés en lecture-écriture, sauf en cas de besoin opérationnel spécifique. Si un accès en lecture-écriture est requis, limitez-le à une station de gestion dédiée, utilisez une chaîne de communauté distincte et appliquez une liste de contrôle d’accès restrictive. Préférez SNMPv3 avec authentification et confidentialité pour des déploiements sécurisés.

Configuration de SNMPv3

Utilisez SNMPv3 avec authentification et confidentialité pour des déploiements SNMP sécurisés. SNMPv3 fournit une authentification et un cryptage basés sur l'utilisateur, contrairement à SNMPv1 et SNMPv2c, qui reposent sur des chaînes de communauté.

Pour les déploiements sécurisés, utilisez le niveau de sécurité authPriv SNMPv3 :

- L'authentification vérifie que le message SNMP provient d'un utilisateur SNMPv3 valide.
- La confidentialité chiffre la charge utile SNMP afin que les données de gestion ne soient pas envoyées en texte clair.
- Évitez noAuthNoPriv et authNoPriv pour les déploiements de production sécurisés.
- Évitez les algorithmes faibles ou hérités tels que MD5 et DES lorsque la plate-forme prend en charge des options plus puissantes.

Remarque : La prise en charge des algorithmes varie selon la plate-forme et la version du

---

logiciel Cisco. Utilisez les algorithmes d'authentification et de confidentialité les plus puissants pris en charge par le périphérique, tels que SHA ou SHA-2 pour l'authentification et AES pour la confidentialité.

Étapes de configuration SNMPv3

Étape 1 : identification de l’adresse NMS de confiance

Déterminez quel système de gestion de réseau est autorisé à interroger le périphérique.

Exemple de valeur :

- Adresse IP NMS : <NMS_IP>
- Adresse IP de gestion des périphériques : <DEVICE_MGMT_IP>



Remarque : Seules les stations de gestion approuvées doivent être autorisées à accéder aux services SNMP.

Étape 2 : création d’une liste de contrôle d’accès pour le NMS approuvé

Créez une ACL qui autorise l'accès SNMP uniquement à partir du NMS approuvé.

Exemple :

<#root>

access-list 10 permit

access-list 10 deny any log

Cette liste de contrôle d'accès limite les adresses IP source pouvant utiliser le groupe SNMPv3. L'entrée de journal deny any permet d'identifier les tentatives d'accès SNMP non autorisées dans syslog.

Étape 3. Création d’une vue SNMP

Créez une vue SNMP pour limiter les objets MIB auxquels l'utilisateur SNMPv3 peut accéder.

Exemple :

<#root>

snmp-server view

mib-2 included

<#root>

snmp-server view

cisco included

Cet exemple permet d'accéder à la sous-arborescence MIB-II et aux objets MIB privés Cisco. Si une vue plus restrictive est requise, excluez explicitement les sous-arborescences MIB sensibles ou inutiles.

Exemple :

<#root>

snmp-server view

excluded

Remarque : Une vue SNMP réduit l'exposition en permettant au NMS d'accéder uniquement aux objets MIB requis pour la surveillance.

Étape 4. Création d’un groupe SNMPv3

Créez un groupe SNMPv3 qui utilise le niveau de sécurité priv et référence la vue SNMP et l'ACL.

Exemple :

<#root>

snmp-server group

v3 priv read

access 10

Cette commande effectue trois actions importantes :

- v3 spécifie SNMPv3.
- priv nécessite à la fois l'authentification et le chiffrement.
- read <VIEW_NAME> limite les objets MIB lisibles avec la vue SNMP précédemment définie.
- access 10 limite l'accès SNMP à l'adresse IP source NMS approuvée avec la liste de contrôle d'accès définie.



Remarque : Pour la plupart des cas d'utilisation de la surveillance, l'accès en lecture seule est généralement suffisant. Configurez l'accès en écriture uniquement en cas de besoin opérationnel spécifique.

Étape 5. Création de l’utilisateur SNMPv3

Créez un utilisateur SNMPv3 et attribuez-le au groupe SNMPv3.

Exemple :

<#root>

snmp-server user

v3 auth sha

priv aes 256

Cette commande crée un utilisateur avec :

- authentification SNMPv3
- Authentification SHA, si prise en charge
- AES avec cryptage 256 bits, si pris en charge
- Appartenance au groupe SNMPv3 restreint



Remarque : Utilisez des mots de passe forts et uniques pour l'authentification et la confidentialité. Ne réutilisez pas le même mot de passe pour les deux valeurs.



Remarque : Si de nouvelles plates-formes prennent en charge des options plus puissantes, telles que SHA-2 ou des variantes AES plus puissantes, utilisez l'option la plus puissante prise en charge par le périphérique et NMS.

Étape 6. (Facultatif) Configuration des déroutements ou des informations SNMPv3

Si le périphérique doit envoyer des notifications au NMS, configurez l'hôte SNMP avec SNMPv3.

Exemple :

<#root>

snmp-server host

version 3 priv

Les déroutements et les informations sont des notifications envoyées par le périphérique au NMS. Elles sont différentes des requêtes d'interrogation, où le NMS envoie des requêtes SNMP au périphérique. Utilisez les notifications SNMPv3 pour intercepter ou informer le trafic et bénéficier également de l'authentification et de la confidentialité.

Si nécessaire, configurez également l'interface source du déroutement :

<#root>

snmp-server trap-source



Remarque : L’utilisation d’une source de déroutement cohérente aide le NMS à identifier le périphérique et permet aux pare-feu ou aux listes de contrôle d’accès de correspondre à des adresses sources prévisibles.

Étape 7. Désactivation ou prévention des communautés SNMPv1 et SNMPv2c inutiles

Si SNMPv1 ou SNMPv2c n'est pas requis, ne configurez pas de chaînes de communauté et ne supprimez pas les chaînes de communauté inutilisées.

Exemple :

<#root>

no snmp-server community



Remarque : Cela réduit le risque d'accès SNMP non autorisé par le biais de chaînes de communauté en texte clair.

L'extrait de configuration suivant montre un exemple qui autorise l'interrogation SNMPv3 uniquement à partir de NMS 10.189.5.161, limite les objets MIB lisibles avec une vue SNMP et requiert l'authentification et le chiffrement.

<#root>

```
Router#configure terminal
Router(config)#

access-list 10 permit 10.189.5.161

Router(config)#

access-list 10 deny any log

Router(config)#!
Router(config)#

snmp-server view ciscoview mib-2 included

Router(config)#

snmp-server view ciscoview cisco included

Router(config)#

snmp-server view ciscoview ipNetToMediaEntry.2 excluded

Router(config)#

snmp-server group myciscogroup v3 priv read ciscoview access 10


Router(config)#

snmp-server user ciscouser myciscogroup v3 auth sha C1sc03xampl3 priv aes 256 C1sc03xampl32
```

Remarques importantes

- Configurez la vue SNMP avant de l'attribuer au groupe SNMPv3.
- Si un ID de moteur SNMP local est configuré manuellement, configurez-le avant de créer des utilisateurs SNMPv3. La modification de l'ID de moteur après la création de l'utilisateur peut nécessiter la recréation des utilisateurs SNMPv3.
- Les informations utilisateur SNMPv3 n'apparaissent pas complètement dans show running-config pour des raisons de sécurité. Utilisez show snmp user pour la vérification.

- La syntaxe exacte des objets MIB et les algorithmes pris en charge varient selon les versions de Cisco IOS et de Cisco IOS XE. Validez la syntaxe de commande pour la plate-forme cible avant le déploiement.

Vérifier

Utilisez ces commandes pour vérifier la configuration SNMP locale :

show snmp user
show snmp group
show snmp view
show snmp
show ip access-lists
show running-config | section snmp

<#root>

ISP-C#

show snmp user

```
User name: ciscouser
Engine ID: 800000090300000A38EB6F800
storage-type: nonvolatile        active
Authentication Protocol:
```

SHA

```
Privacy Protocol:
```

AES256

```
Group-name: myciscogroup

ISP-C#show snmp group
groupname: ILMI                             security model:v1
contextname:




              storage-type: permanent
readview : *ilmi                            writeview: *ilmi
notifyview:
```

```
row status: active

groupname: ILMI                              security model:v2c
contextname:




                storage-type: permanent
readview : *ilmi                             writeview: *ilmi
notifyview:




row status: active

groupname: myciscogroup                      security model:v3 priv
contextname:




                  storage-type: nonvolatile
readview : ciscoview                         writeview:




notifyview:




row status: active      access-list: 10

ISP-C#
```

show snmp view

```
*ilmi system - included permanent active
```

```
*ilmi atmForumUni - included permanent active
cac_view pimMIB - included read-only active
cac_view msdpMIB - included read-only active
cac_view system - included read-only active
cac_view interfaces - included read-only active
cac_view ip - included read-only active
cac_view ospf - included read-only active
cac_view bgp - included read-only active
cac_view ifMIB - included read-only active
cac_view nhrpMIB - included read-only active
cac_view ipMRouteStdMIB - included read-only active
cac_view igmpStdMIB - included read-only active
cac_view pimStdMIB - included read-only active
cac_view mgmdStdMIB - included read-only active
cac_view ospfv3MIB - included read-only active
cac_view ipForward - included read-only active
cac_view ipTrafficStats - included read-only active
cac_view ospfTrap - included read-only active
cac_view sysUpTime.0 - included read-only active
cac_view ciscoPingMIB - included read-only active
cac_view ciscoPimMIB - included read-only active
cac_view ciscoBgp4MIB - included read-only active
cac_view ciscoIfExtensionMIB - included read-only active
cac_view ciscoEigrpMIB - included read-only active
cac_view ciscoCefMIB - included read-only active
cac_view ciscoNhrpExtMIB - included read-only active
cac_view ciscoIpMRouteMIB - included read-only active
cac_view ciscoDlcSwitchMIB - included read-only active
cac_view ciscoExperiment.101 - included read-only active
cac_view ciscoIetfIsisMIB - included read-only active
cac_view ifIndex - included read-only active
cac_view ifDescr - included read-only active
cac_view ifType - included read-only active
cac_view ifAdminStatus - included read-only active
cac_view ifOperStatus - included read-only active
cac_view snmpTraps.3 - included read-only active
cac_view snmpTraps.4 - included read-only active
cac_view snmpTrapOID.0 - included read-only active
cac_view snmpMIB.1.4.3.0 - included read-only active
cac_view lifEntry.20 - included read-only active
cac_view cciDescriptionEntry.1 - included read-only active
ciscoview mib-2 - included nonvolatile active
ciscoview cisco - included nonvolatile active
ciscoview ipNetToMediaEntry.2 - excluded nonvolatile active
v1default iso - included permanent active
v1default internet - included permanent active
v1default snmpUsmMIB - excluded permanent active
v1default snmpVacmMIB - excluded permanent active
v1default snmpCommunityMIB - excluded permanent active

ISP-C#
```

show ip access-lists

```
Standard IP access list 10
    10 permit 10.189.5.161 (26 matches)
    20 deny   any log (6 matches)
Extended IP access list meraki-fqdn-dns
```

```
ISP-C#
```

show running-config | section snmp

```
snmp-server group myciscogroup v3 priv read ciscoview access 10
snmp-server view ciscoview mib-2 included
snmp-server view ciscoview cisco included
snmp-server view ciscoview ipNetToMediaEntry.2 excluded
```

Vous pouvez également effectuer une vérification SNMP pour l'arborescence des systèmes MIB-II :

<#root>

ciscouser@Desktop %

snmpwalk -v3 -l authPriv -u ciscouser -a SHA -A 'C1sc03xampl3' -x AES -X 'C1sc03xampl32' 10.207.214.25 s

```
SNMPv2-MIB::sysDescr.0 = STRING: Cisco IOS Software [Cupertino], ASR1000 Software (X86_64_LINUX_IOSD-UNI
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2023 by Cisco Systems, Inc.
Compiled Wed 26-Jul-23 10:29 b
SNMPv2-MIB::sysObjectID.0 = OID: SNMPv2-SMI::enterprises.9.1.2348
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (107487239) 12 days, 10:34:32.39
SNMPv2-MIB::sysContact.0 = STRING:
SNMPv2-MIB::sysName.0 = STRING: ISP-C
SNMPv2-MIB::sysLocation.0 = STRING:
SNMPv2-MIB::sysServices.0 = INTEGER: 78
SNMPv2-MIB::sysORLastChange.0 = Timeticks: (0) 0:00:00.00
```

La commande et le résultat suivants montrent que vous ne pouvez pas obtenir le groupe ipNetToMediaEntry.2 :

<#root>

ciscouser@Desktop %

```
snmpwalk -v3 -l authPriv -u ciscouser -a SHA -A 'C1sc03xampl3' -x AES -X 'C1sc03xampl32' 10.207.214.25 i
```

```
IP-MIB::ipNetToMediaPhysAddress = No Such Object available on this agent at this OID
```

La commande suivante et le résultat obtenu sont pour le groupe Système local Cisco :

<#root>

ciscouser@Desktop %

```
snmpwalk -v3 -l authPriv -u ciscouser -a SHA -A 'C1sc03xampl3' -x AES -X 'C1sc03xampl32' 10.207.214.25 .
```

```
SNMPv2-SMI::enterprises.9.2.1.1.0 = STRING: "
17.15(4r)
"
SNMPv2-SMI::enterprises.9.2.1.2.0 = STRING: "LocalSoft"
SNMPv2-SMI::enterprises.9.2.1.3.0 = STRING: "ISP-C"
SNMPv2-SMI::enterprises.9.2.1.4.0 = ""
```

```
SNMPv2-SMI::enterprises.9.2.1.5.0 = IpAddress: 10.189.5.161
```

```
SNMPv2-SMI::enterprises.9.2.1.6.0 = IpAddress: 0.0.0.0
SNMPv2-SMI::enterprises.9.2.1.8.0 = INTEGER: -796648892
SNMPv2-SMI::enterprises.9.2.1.9.0 = INTEGER: 1646
SNMPv2-SMI::enterprises.9.2.1.10.0 = INTEGER: 1000
SNMPv2-SMI::enterprises.9.2.1.11.0 = INTEGER: 1557645
SNMPv2-SMI::enterprises.9.2.1.12.0 = INTEGER: 0
SNMPv2-SMI::enterprises.9.2.1.13.0 = INTEGER: 0
SNMPv2-SMI::enterprises.9.2.1.14.0 = INTEGER: 104
SNMPv2-SMI::enterprises.9.2.1.15.0 = INTEGER: 1200
SNMPv2-SMI::enterprises.9.2.1.16.0 = INTEGER: 1200
SNMPv2-SMI::enterprises.9.2.1.17.0 = INTEGER: 2500
SNMPv2-SMI::enterprises.9.2.1.18.0 = INTEGER: 2684018
SNMPv2-SMI::enterprises.9.2.1.19.0 = INTEGER: 0
SNMPv2-SMI::enterprises.9.2.1.20.0 = INTEGER: 0
SNMPv2-SMI::enterprises.9.2.1.21.0 = INTEGER: 0
SNMPv2-SMI::enterprises.9.2.1.22.0 = INTEGER: 600
SNMPv2-SMI::enterprises.9.2.1.23.0 = INTEGER: 900
SNMPv2-SMI::enterprises.9.2.1.24.0 = INTEGER: 900
SNMPv2-SMI::enterprises.9.2.1.25.0 = INTEGER: 2000
SNMPv2-SMI::enterprises.9.2.1.26.0 = INTEGER: 26757370
SNMPv2-SMI::enterprises.9.2.1.27.0 = INTEGER: 0
SNMPv2-SMI::enterprises.9.2.1.28.0 = INTEGER: 0
SNMPv2-SMI::enterprises.9.2.1.29.0 = INTEGER: 0
SNMPv2-SMI::enterprises.9.2.1.30.0 = INTEGER: 1536
SNMPv2-SMI::enterprises.9.2.1.31.0 = INTEGER: 900
SNMPv2-SMI::enterprises.9.2.1.32.0 = INTEGER: 899
SNMPv2-SMI::enterprises.9.2.1.33.0 = INTEGER: 1800
SNMPv2-SMI::enterprises.9.2.1.34.0 = INTEGER: 8891131
SNMPv2-SMI::enterprises.9.2.1.35.0 = INTEGER: 0
SNMPv2-SMI::enterprises.9.2.1.36.0 = INTEGER: 1
SNMPv2-SMI::enterprises.9.2.1.37.0 = INTEGER: 1
SNMPv2-SMI::enterprises.9.2.1.38.0 = INTEGER: 5024
```

```
SNMPv2-SMI::enterprises.9.2.1.39.0 = INTEGER: 100
SNMPv2-SMI::enterprises.9.2.1.40.0 = INTEGER: 100
SNMPv2-SMI::enterprises.9.2.1.41.0 = INTEGER: 300
SNMPv2-SMI::enterprises.9.2.1.42.0 = INTEGER: 0
SNMPv2-SMI::enterprises.9.2.1.43.0 = INTEGER: 0
SNMPv2-SMI::enterprises.9.2.1.44.0 = INTEGER: 1
SNMPv2-SMI::enterprises.9.2.1.45.0 = INTEGER: 1
SNMPv2-SMI::enterprises.9.2.1.46.0 = INTEGER: 0
SNMPv2-SMI::enterprises.9.2.1.47.0 = INTEGER: 0
SNMPv2-SMI::enterprises.9.2.1.48.0 = IpAddress: 0.0.0.0
SNMPv2-SMI::enterprises.9.2.1.49.0 = ""
SNMPv2-SMI::enterprises.9.2.1.51.0 = IpAddress: 0.0.0.0
SNMPv2-SMI::enterprises.9.2.1.52.0 = ""
SNMPv2-SMI::enterprises.9.2.1.56.0 = INTEGER: 0
SNMPv2-SMI::enterprises.9.2.1.57.0 = INTEGER: 0
SNMPv2-SMI::enterprises.9.2.1.58.0 = INTEGER: 0
SNMPv2-SMI::enterprises.9.2.1.59.0 = INTEGER: 4972
SNMPv2-SMI::enterprises.9.2.1.60.0 = INTEGER: 0
SNMPv2-SMI::enterprises.9.2.1.61.0 = STRING: "cisco Systems, Inc.
170 West Tasman Dr.
San Jose, CA  95134-1706
U.S.A.
Ph +1-408-526-4000
Customer service 1-800-553-6387 or +1-408-526-7208
24HR Emergency 1-800-553-2447 or +1-408-526-7209
Email Address tac@cisco.com
World Wide Web http://www.cisco.com"
SNMPv2-SMI::enterprises.9.2.1.62.0 = INTEGER: 18024
SNMPv2-SMI::enterprises.9.2.1.63.0 = INTEGER: 20
SNMPv2-SMI::enterprises.9.2.1.64.0 = INTEGER: 20
SNMPv2-SMI::enterprises.9.2.1.65.0 = INTEGER: 33
SNMPv2-SMI::enterprises.9.2.1.66.0 = INTEGER: 0
SNMPv2-SMI::enterprises.9.2.1.67.0 = INTEGER: 0
SNMPv2-SMI::enterprises.9.2.1.68.0 = INTEGER: 1
SNMPv2-SMI::enterprises.9.2.1.69.0 = INTEGER: 1
SNMPv2-SMI::enterprises.9.2.1.70.0 = INTEGER: 0
SNMPv2-SMI::enterprises.9.2.1.71.0 = INTEGER: 0
SNMPv2-SMI::enterprises.9.2.1.72.0 = IpAddress: 0.0.0.0
SNMPv2-SMI::enterprises.9.2.1.73.0 = STRING: "bootflash:asr1000-universalk9.17.09.04.SPA.bin"
SNMPv2-SMI::enterprises.9.2.1.74.0 = INTEGER: 3
```

Configurer la liste de contrôle d’accès sur les interfaces

Les listes de contrôle d’accès d’interface peuvent être utiles en tant que couche de protection supplémentaire pour limiter les hôtes pouvant envoyer du trafic SNMP à une interface de périphérique. Elles sont particulièrement utiles sur les plates-formes qui ne prennent pas en charge des fonctions de protection du plan de contrôle plus ciblées, telles que la CoPP (Control Plane Policing) ou les listes de contrôle d'accès du plan de gestion.

Une liste de contrôle d'accès d'interface peut bloquer les paquets SNMP non autorisés avant qu'ils ne soient traités par le périphérique, ce qui réduit l'exposition aux interrogations indésirables, aux tentatives de chaîne de communauté en force ou au trafic SNMP excessif provenant de sources non fiables.

⚠ Mise en garde : Soyez prudent lors de l’application des ACL d’interface. Une liste de contrôle d'accès appliquée avec ip access-group filtre le trafic dans la direction sélectionnée et peut affecter à la fois le trafic destiné au routeur et le trafic de transit. Incluez toujours toutes les instructions d’autorisation requises et validez la liste de contrôle d’accès dans une fenêtre de maintenance ou un laboratoire avant le déploiement en production.

<#root>

ip access-list extended SNMP-MGMT-IN permit udp host

host

eq snmp deny udp any host

eq snmp log permit ip any any

La liste de contrôle d’accès doit ensuite être appliquée à toutes les interfaces à l’aide des commandes de configuration suivantes :

<#root>

interface

ip access-group SNMP-MGMT-IN in

Dans cet exemple :

- L'interrogation SNMP du NMS approuvé vers l'adresse IP de gestion du périphérique est autorisée.
- L'interrogation SNMP à partir d'autres sources vers l'adresse IP de gestion du périphérique est refusée et consignée.
- Le reste du trafic IP est autorisé par l'instruction finale permit ip any any.



Remarque : Vous pouvez adapter cet exemple à la conception de votre réseau. Si la plate-forme prend en charge les listes CoPP, iACL ou ACL du plan de gestion, ces options peuvent fournir une protection du plan de contrôle plus ciblée. Pour les périphériques disposant de nombreuses adresses IP configurées ou de nombreux hôtes devant communiquer avec le routeur, cette solution n'est pas toujours évolutive. La protection de votre coeur : Le document Listes de contrôle d'accès de protection de l'infrastructure présente des directives et des techniques de déploiement recommandées pour les ACL.

Vérification des erreurs SNMP : procédure

Configurez les ACL de la communauté SNMP avec le mot clé log. Surveillez syslog pour les tentatives infructueuses, comme illustré.

<#root>

```
access-list 10 deny any log
snmp-server community
```

```
    RO 10
```

Lorsqu'une personne tente d'accéder au routeur avec le public de la communauté, vous voyez un message syslog similaire à celui-ci :

<#root>

```
%SEC-6-IPACCESSLOGS: list 10 denied 172.16.1.15 packet
```

Ce résultat signifie que la liste d'accès 10 a refusé cinq paquets SNMP provenant de l'hôte 172.16.1.15.

Vérifiez régulièrement les erreurs SNMP à l'aide de la commande show snmp, comme indiqué ici :

<#root>

ISP-C#

show snmp

```
Chassis: TKM21110169
186 SNMP packets input
 0 Bad SNMP version errors 58 Unknown community name
    0 Illegal operation for community name supplied
 0 Encoding errors
    115 Number of requested variables
    0 Number of altered variables
    2 Get-request PDUs
    113 Get-next PDUs
    0 Set-request PDUs
    0 Input queue packet drops (Maximum queue size 1000)
126 SNMP packets output
    0 Too big errors (Maximum packet size 1500)
    0 No such name errors
    0 Bad values errors
    0 General errors
    0 Response PDUs
    0 Trap PDUs
Packets currently in SNMP process input queue: 0
SNMP global trap: disabled

SNMP logging: disabled
```

Observez les compteurs mis en évidence pour détecter des augmentations inattendues des taux d'erreur qui peuvent indiquer une tentative d'exploitation de ces vulnérabilités. Pour signaler un problème de sécurité, reportez-vous à Réponse aux incidents de sécurité des produits Cisco.

Informations connexes

- Vulnérabilités SNMP dans les avis de sécurité Cisco
- Assistance technique de Cisco et téléchargements

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.