# Sécurisation du protocole simple de gestion de réseau

## Contenu



# Introduction

Ce document fournit des informations sur la sécurisation de votre protocole de gestion de réseau simple (SNMP). Sécuriser votre SNMP est important, particulièrement quand les vulnérabilités du SNMP peuvent être exploitées à plusieurs reprises pour produire un déni de service (DoS).

# Conditions préalables

## Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

## Composants utilisés

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

- Vue SNMP — Version de logiciel 10.3 ou ultérieures de Cisco IOS®.
- SNMP version 3 — Introduit dans le Logiciel Cisco IOS version 12.0(3)T.

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.

## Stratégies pour sécuriser le SNMP

### Choisissez une bonne chaîne de caractères de la communauté SNMP

Il n'est pas dans une bonne pratique d'utiliser le **public** aussi en lecture seule et **privé** que des chaînes de caractères de la communauté en lecture-écriture.

### Vue SNMP d'installation

La commande de **vue SNMP d'installation** peut bloquer l'utilisateur avec seulement l'accès au Management Information Base limité (MIB). Par défaut, il n'y a aucune **entrée de vue SNMP existe**. Cette commande est configurée au mode de configuration globale et d'abord introduite dans la version de logiciel 10.3 de Cisco IOS. Cela fonctionne semblable à la **liste d'accès** dans cela si vous avez n'importe quel **point de vue SNMP** sur certaines arborescences MIB, chaque autre arborescence est refusé inexplicablement. Cependant, l'ordre n'est pas important et il passe par la liste entière pour une correspondance avant qu'il arrête.

Pour créer ou mettre à jour une entrée de vue, utilisez la commande de **configuration globale de snmp-server view**. Pour retirer l'entrée spécifiée de vue de serveur SNMP, utilisez le **forme no de** cette commande.

Syntaxe :

```
snmp-server view view-name oid-tree {included | excluded}

no snmp-server view view-name
```

Description de syntaxe :

- **vue-nom** — Étiquette pour l'enregistrement de vue que vous mettez à jour ou créez. Le nom est utilisé pour mettre en référence l'enregistrement.
- **oid-arborescence** — Objectez l'identifiant du sous-arbre de l'Abstract Syntax Notation One (ASN.1) à inclure ou être exclu de la vue. Pour identifier le sous-arbre, spécifiez une chaîne de texte se composant des nombres, tels que 1.3.6.2.4, ou un mot, tel que le **système**. Remplacez un sous-titre-identifiant simple par le masque d'astérisque (*) pour spécifier une famille de sous-arbre ; par exemple 1.3.*.4.
- **inclus | exclu** — Type de vue. Vous devez spécifier inclus ou exclu.

Deux vues standard de prédéfinis peuvent être utilisées quand une vue est exigée, au lieu de définir une vue. On est tout, qui indique que l'utilisateur peut voir tous les objets. L'autre *est limité*, qui indique que l'utilisateur peut voir trois groupes : **système**, **snmpStats**, et **snmpParties**. Les vues de prédéfinis sont décrites dans RFC 1447.

**Note**: Le premier ordre de **serveur SNMP** que vous écrivez des enables les deux versions de SNMP.

Cet exemple crée une vue qui inclut tous les objets au groupe système MIB-II excepté les **sysServices** (système 7) et tous les objets pour interface 1 dans le groupe d'interfaces MIB-II :

```
snmp-server view agon system included

snmp-server view agon system.7 excluded

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

C'est un exemple complet pour que la façon applique le MIB avec la chaîne de la communauté et la sortie du **snmpwalk** avec la **vue** en place. Cette configuration définit une vue qui refuse l'accès SNMP pour la table de Protocole ARP (Address Resolution Protocol) (**atEntry**) et le permet pour MIB-II et MIB privé de Cisco :

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


snmp-server view myview atEntry excluded


snmp-server view myview cisco included


snmp-server community public view myview RO 11


snmp-server community private view myview RW 11


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

C'est la commande et la sortie pour le groupe système MIB-II :

```
NMSPrompt 82 % snmpwalk cough system
system.sysDescr.0 : DISPLAY STRING- (ascii):Cisco Internetwork Operating System Software
IOS (tm) 2500 Software (C2500-JS-L), Version 12.0(1)T,RELEASE SOFTWARE (fc2)
Copyright (c) 1986-1998 by cisco Systems, Inc.
Compiled Wed 04-Nov-98 20:37 by dschwart
system.sysObjectID.0 : OBJECT IDENTIFIER:
   .iso.org.dod.internet.private.enterprises.cisco.ciscoProducts.cisco2520
system.sysUpTime.0 : Timeticks: (306588588) 35 days, 11:38:05.88
system.sysContact.0 : DISPLAY STRING- (ASCII):pvanderv@cisco.com
system.sysName.0 : DISPLAY STRING- (ASCII):cough
system.sysLocation.0 : DISPLAY STRING- (ASCII):
```

```
system.sysServices.0 : INTEGER: 78
system.sysORLastChange.0 : Timeticks: (0) 0:00:00.00

NMSPrompt 83 %
```

C'est la commande et la sortie pour le groupe système local de Cisco :

```
NMSPrompt 83 % snmpwalk cough lsystem

cisco.local.lsystem.romId.0 : DISPLAY STRING- (ASCII):
System Bootstrap, Version 11.0(10c), SOFTWARE
Copyright (c) 1986-1996 by cisco Systems

cisco.local.lsystem.whyReload.0 : DISPLAY STRING- (ASCII):power-on
cisco.local.lsystem.hostName.0 : DISPLAY STRING- (ASCII):cough
```

C'est la commande et la sortie pour la table ARP MIB-II :

```
NMSPrompt 84 % snmpwalk cough atTable

no MIB objects contained under subtree.

NMSPrompt 85 %
```

## La Communauté SNMP d'installation avec la liste d'accès

Les meilleures activités actuelles recommandent s'appliquer le Listes de contrôle d'accès (ACL) aux chaînes de la communauté et s'assurer que les chaînes de la communauté de demandes ne sont pas identiques aux chaînes de la communauté de notifications. Les Listes d'accès assurent davantage de protection une fois utilisées en combination avec d'autres mesures de sauvegarde.

Cet exemple a installé l'ACL à la chaîne de la communauté :

```
access-list 1 permit 1.1.1.1

snmp-server community string1 ro 1
```

Utilisant la communauté différente les chaînes pour des demandes et des messages déroutés réduit la probabilité des futures attaques ou compromet si la chaîne de la communauté est découverte par un attaquant, par compromettre un périphérique distant ou en reniflant un message dérouté du réseau sans autorisation.

Une fois que vous activez le déroutement avec une chaîne de la communauté, la chaîne peut être activée pour l'accès SNMP en du logiciel de Cisco IOS. Vous devez explicitement désactiver cette communauté.

Exemple :

```
access-list 10 deny any
snmp-server host 1.1.1.1 mystring1
snmp-server community mystring1 RO 10
```

## SNMP version 3 d'installation

Le SNMP version 3 a été introduit la première fois dans la version de logiciel 12.0 de Cisco IOS, mais n'est pas utilisé généralement en Gestion de réseau encore. Pour configurer le SNMP version 3, terminez-vous ces étapes :

1. Assignez un ID du moteur pour l'entité SNMP (facultative).
2. Définissez un utilisateur, **userone**, en appartenant au **groupone de** groupe et appliquez-vous le **noAuthentication** (aucun mot de passe) et le **noPrivacy** (aucun cryptage) à cet utilisateur.
3. Définissez un utilisateur, **usertwo**, en appartenant au **grouptwo de** groupe et appliquez-vous le **noAuthentication** (aucun mot de passe) et le **noPrivacy** (aucun cryptage) à cet utilisateur.
4. Définissez un utilisateur, **userthree**, en appartenant au **groupthree de** groupe et appliquez-vous l'**authentification** (le mot de passe est user3passwd) et le **noPrivacy** (aucun cryptage) à cet utilisateur.
5. Définissez un utilisateur, **userfour**, en appartenant au **groupfour de** groupe et appliquez-vous l'**authentification** (le mot de passe est user4passwd) et l'**intimité** (cryptage des56) à cet utilisateur.
6. Définissez un groupe, **groupone**, utilisant le modèle de Sécurité d'utilisateur (USM) accès en lecture V3 et de avoir sur la vue **v1default** (le par défaut).
7. Définissez un groupe, **grouptwo**, utilisant USM V3 et accès en lecture de avoir sur le **myview de** vue.
8. Définissez un groupe, **groupthree**, utilisant USM V3, en ayant l'accès en lecture sur la vue **v1default** (le par défaut), et en utilisant l'**authentification**.
9. Définissez un groupe, **groupfour**, utilisant USM V3, en ayant l'accès en lecture sur la vue **v1default** (le par défaut), et en utilisant l'**authentification** et l'**intimité**.
10. Définissez une vue, le **myview**, qui fournit l'accès en lecture sur le MIB-II et refuse l'accès en lecture sur le MIB privé de Cisco.La sortie **courante d'exposition** donne des lignes supplémentaires pour le **public de** groupe, étant donné qu'il y a un **public** en lecture seule de chaîne de la communauté qui a été défini.La sortie **courante d'exposition** n'affiche pas l'**userthree**.Exemple :

```
snmp-server engineID local 1111000000000000000000000
snmp-server user userone groupone v3
snmp-server user usertwo grouptwo v3
snmp-server user userthree groupthree v3 auth md5 user3passwd
snmp-server user userfour groupfour v3 auth md5 user4passwd priv des56
  user4priv
snmp-server group groupone v3 noauth
snmp-server group grouptwo v3 noauth read myview
snmp-server group groupthree v3 auth
snmp-server group groupfour v3 priv
snmp-server view myview mib-2 included
snmp-server view myview cisco excluded
snmp-server community public RO
```

C'est la commande et la sortie pour le groupe système MIB-II utilisant l'**userone d'**utilisateur :

```
NMSPrompt 94 % snmpwalk -v3 -n "" -u userone -l noAuthNoPriv clumsy system
Module SNMPV2-TC not found
system.sysDescr.0 = Cisco Internetwork Operating System Software
IOS (TM) 4500 Software (C4500-IS-M), Version 12.0(3)T,RELEASE SOFTWARE (fc1)
Copyright (c) 1986-1999 by cisco Systems, Inc.
Compiled Tue 23-Feb-99 03:59 by ccai
system.sysObjectID.0 = OID: enterprises.9.1.14
system.sysUpTime.0 = Timeticks: (28208096) 3 days, 6:21:20.96
system.sysContact.0 =
system.sysName.0 = clumsy.cisco.com
system.sysLocation.0 =
system.sysServices.0 = 78
system.sysORLastChange.0 = Timeticks: (0) 0:00:00.00
NMSPrompt 95 %
```

C'est la commande et la sortie pour le groupe système MIB-II utilisant l'**usertwo d'**utilisateur :

```
NMSPrompt 95 % snmpwalk -v3 -n "" -u usertwo -l noAuthNoPriv clumsy system

Module SNMPV2-TC not found
system.sysDescr.0 = Cisco Internetwork Operating System Software
IOS (TM) 4500 Software (C4500-IS-M), Version 12.0(3)T,RELEASE SOFTWARE (fc1)
Copyright (c) 1986-1999 by cisco Systems, Inc.
Compiled Tue 23-Feb-99 03:59 by ccai
system.sysObjectID.0 = OID: enterprises.9.1.14
system.sysUpTime.0 = Timeticks: (28214761) 3 days, 6:22:27.61
system.sysContact.0 =
system.sysName.0 = clumsy.cisco.com
system.sysLocation.0 =
system.sysServices.0 = 78
system.sysORLastChange.0 = Timeticks: (0) 0:00:00.00
```

C'est la commande et la sortie pour le groupe de système local de Cisco utilisant l'**userone d'**utilisateur :

```
NMSPrompt 98 % snmpwalk -v3 -n "" -u userone -l noAuthNoPriv clumsy .1.3.6.1.4.1.9.2.1

Module SNMPV2-TC not found
enterprises.9.2.1.1.0 = "..System Bootstrap, Version 5.2(7b) [mkamson 7b],
   RELEASE SOFTWARE (fc1)..Copyright (c) 1995 by cisco Systems,
Inc..."
enterprises.9.2.1.2.0 = "reload"
enterprises.9.2.1.3.0 = "clumsy"
enterprises.9.2.1.4.0 = "cisco.com"
```

C'est la commande et la sortie vous affichant ne peut pas obtenir le groupe de système local de Cisco utilisant l'**usertwo d'**utilisateur :

```
NMSPrompt 99 % snmpwalk -v3 -n "" -u usertwo -l noAuthNoPriv clumsy .1.3.6.1.4.1.9.2.1

Module SNMPV2-TC not found
enterprises.9.2.1 = No more variables left in this MIB View

NMSPrompt 100 %
```

Cette sortie de commande et de résulter est pour un **tcpdump** personnalisé (correctif pour le support de SNMP version 3 et le supplément du printf) :

```
NMSPrompt 102 % snmpget -v3 -n "" -u userone -l noAuthNoPriv clumsy system.sysName.0

Module SNMPV2-TC not found
system.sysName.0 = clumsy.cisco.com
```

## ACL d'installation sur des interfaces

La fonctionnalité d'ACL fournit des mesures de sécurité en empêchant des attaques telles que l'usurpation d'adresse IP. L'ACL peut être appliqué sur des interfaces en entrée ou en sortie sur des Routeurs.

Sur les Plateformes qui n'ont pas l'option de utiliser recevez ACLs (rACLs), il est possible pour permettre le trafic de Protocole UDP (User Datagram Protocol) au routeur des adresses IP de confiance avec l'interface ACLs.

La liste d'accès étendue suivante peut être adaptée à votre réseau. Cet exemple suppose que le routeur a des adresses IP 192.168.10.1 et 172.16.1.1 configurés sur ses interfaces, que tout l'accès SNMP doit être limité à une station de Gestion avec l'adresse IP de 10.1.1.1, et que le besoin de station de Gestion communiquent seulement avec l'adresse IP 192.168.10.1 :

```
access-list 101 permit udp host 10.1.1.1 host 192.168.10.1
```

**La liste d'accès** doit alors être appliquée à toutes les interfaces utilisant ces commandes de configuration :

```
interface ethernet 0/0

ip access-group 101 in
```

Tous les périphériques qui communiquent directement avec le routeur sur des ports UDP devront être spécifiquement répertoriés dans la liste d'accès ci-dessus. Le logiciel de Cisco IOS utilise des ports entre 49152 et 65535 comme port de source pour des sessions en partance telles que des requêtes de Système de noms de domaine (DNS).

Pour les périphériques qui ont beaucoup d'adresses IP configurées, ou beaucoup d'hôtes qui doivent communiquer avec le routeur, ceci peut ne pas être une solution évolutive.

## rACLs

Pour les Plateformes distribuées, les rACLs peuvent être une option commençant dans le Logiciel Cisco IOS version 12.0(21)S2 pour le routeur de commutateur de gigabit de gamme Cisco 12000 (GSR) et relâcher 12.0(24)S pour la gamme Cisco 7500. Les Listes d'accès de réception protègent le périphérique contre le trafic néfaste avant que le trafic puisse affecter le processeur d'artère. Recevez le chemin ACLs également sont considérés une pratique recommandée de sécurité des réseaux, et devraient être considérés comme ajout à long terme à la bonne sécurité des réseaux, aussi bien que contournement pour cette vulnérabilité spécifique. Le chargement CPU est distribué aux processeurs de carte de ligne et les aides atténuent le chargement sur le processeur d'artère principale. Le livre blanc autorisé GSR : Recevez les listes de contrôle d'accès aidera à identifier et permettre le trafic légitime à votre périphérique et à refuser tous les paquets non désirés.

### Les ACL d´infrastructure

Bien qu'il soit souvent difficile de bloquer le trafic transitant votre réseau, il est possible d'identifier le trafic qui devrait ne jamais être permis pour viser vos périphériques d'infrastructure et pour bloquer ce trafic au cadre de votre réseau. L'infrastructure ACLs (iACLs) sont considérées une pratique recommandée de sécurité des réseaux et devraient être considérées comme ajout à long terme à la bonne sécurité des réseaux aussi bien que contournement pour cette vulnérabilité spécifique. Le livre blanc autorisé protégeant votre noyau : Les listes de contrôle d'accès de protection d'infrastructure présente des instructions et des techniques recommandées de déploiement pour des iACLs.

### Caractéristique de sécurité du commutateur de RÉSEAU LOCAL de Cisco Catalyst

La caractéristique de liste d'autorisation IP limite le telnet d'arrivée et l'accès SNMP au commutateur des adresses IP non autorisées de source. Des messages de Syslog et les déroutements SNMP sont pris en charge pour informer un système de gestion quand une violation ou un accès non autorisé se produit.

Une combinaison des caractéristiques de cisco IOS software security peut être utilisée pour gérer des Routeurs et des commutateurs Cisco Catalyst. Une stratégie de sécurité doit être établie qui limite le nombre de stations de Gestion capables d'accéder aux Commutateurs et les Routeurs.

Pour plus d'informations sur la façon augmenter la Sécurité sur des réseaux IP, référez-vous à la Sécurité croissante sur des réseaux IP.

## Comment vérifier des erreurs SNMP

Configurez la communauté ACLs SNMP avec le **mot clé de journal**. Surveillez le **Syslog** pour des essais ratés, en tant qu'exposition ci-dessous.

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

Quand quelqu'un des essais pour accéder au routeur avec le public de la communauté, vous voient un **Syslog** semblable à ce qui suit :

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

Cette sortie signifie que la liste d'accès 10 a refusé cinq paquets SNMP de l'hôte 172.16.1.1.

Vérifiez périodiquement le SNMP pour des erreurs en exécutant une commande de **show snmp**, comme affiché ici :

```
router#show snmp Chassis: 21350479 17005 SNMP packets input

37 Bad SNMP version errors**
15420 Unknown community name**
0 Illegal operation for community name supplied
1548 Encoding errors**
0 Number of requested variables
0 Number of altered variables
0 Get-request PDUs
0 Get-next PDUs
0 Set-request PDUs 0 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
```

Observez les compteurs marqués ** pour des augmentations inattendues des taux d'erreur qui peuvent indiquer l'exploitation tentée de ces vulnérabilités. Pour signaler n'importe quel problème de sécurité, référez-vous au résolution d'incidents de sécurité des produits Cisco.

# Informations connexes

- Vulnérabilités SNMP d'avis de sécurité Cisco
- SNMP v3 d'installation avec IOS 12.0
- Protocole de gestion de réseau simple (SNMP)
- Configurer le SNMP
- Support technique - Cisco Systems