Sécurisez votre protocole de gestion de réseau simple

Table des matières

[Introduction](#)
[Conditions préalables](#)
[Exigences](#)
[Composants utilisés](#)
[Conventions](#)
[Informations générales](#)
[Stratégies de sécurisation du SNMP](#)
[Choisir une chaîne de communauté SNMP correcte](#)
[Configuration de la vue SNMP](#)
[Configuration de la communauté SNMP avec la liste d'accès](#)
[Configuration de SNMP version 3](#)
[Configurer ACL sur les interfaces](#)
[rACL](#)
[Les ACL d´infrastructure](#)
[Fonctionnalité de sécurité du commutateur LAN Cisco Catalyst](#)
[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 contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- SNMP View : logiciel Cisco IOS® version 10.3 ou ultérieure.
- SNMP version 3 — Introduit dans le logiciel Cisco IOS version 12.0(3)T.

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.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Informations générales

Il est important de sécuriser votre SNMP, en particulier lorsque les vulnérabilités de SNMP peuvent être exploitées à plusieurs reprises pour produire un déni de service (DoS).

Stratégies de sécurisation du SNMP

Choisir une chaîne de communauté SNMP correcte

Il n'est pas recommandé d'utiliser **public** en lecture seule et **private** en tant que chaînes de communauté en lecture-écriture.

Configuration de la vue SNMP

Les Setup SNMP view peut bloquer l'utilisateur avec un accès limité à la base d'informations de gestion (MIB). Par défaut, il n'y a SNMP view entry exists . Cette commande est configurée en mode de configuration globale et introduite pour la première fois dans le logiciel Cisco IOS version 10.3. Il fonctionne de la même manière que **access-list** si vous avez des SNMP View sur certaines arborescences MIB, toutes les autres arborescences sont refusées inexplicablement. Cependant, la séquence n'est pas importante et elle parcourt toute la liste pour une correspondance avant de s'arrêter.

Pour créer ou mettre à jour une entrée de vue, utilisez la **snmp-server view global configuration** erasecat4000_flash:. Pour supprimer l'entrée d'affichage du serveur SNMP spécifié, utilisez la commande **no** de cette commande.

Syntaxe:

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

no snmp-server view view-name
```

Description de la syntaxe:

- view-name: étiquette de l'enregistrement de vue que vous mettez à jour ou créez. Le nom est utilisé pour référencer l'enregistrement.
- oid-tree : identificateur d'objet du sous-arbre 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 nombres, par exemple 1.3.6.2.4, ou d'un mot, par exemple system. Remplacez un sous-identificateur unique par le caractère générique astérisque (*) pour spécifier une famille de sous-arborescences ; par exemple 1.3.*.4.
- included | excluded: type de vue. Vous devez spécifier inclus ou exclu.

Deux vues prédéfinies standard peuvent être utilisées lorsqu'une vue est requise au lieu d'une vue qui doit être définie. Tout d'abord, ce qui indique que l'utilisateur peut voir tous les objets. L'autre est *restreint*, ce qui indique que l'utilisateur peut voir trois groupes : system, snmpStats,et snmpParties. Les vues prédéfinies sont décrites dans la RFC 1447.

Remarque : la première snmp-server que vous entrez active les deux versions de SNMP.

Cet exemple montre comment créer une vue qui inclut tous les objets du groupe système MIB-II, à l'exception de sysServices (Système 7) et tous les objets pour l'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
```

Ceci est un exemple complet de la façon d'appliquer la MIB avec une chaîne de communauté et le résultat de la commande snmpwalk avec view en place. Cette configuration définit une vue refusant l'accès SNMP pour la table ARP (Address Resolution Protocol) (atEntry) et l'autorise pour les MIB-II et les MIB privées 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
```

Voici la commande et le résultat pour le groupe Système MIB-II :

```
NMSPrompt 82 % snmpwalk cough system
system.sysDescr.0 : DISPLAY STRING- (ascii):Cisco Internetwork Operating System Software
Cisco 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 %
```

Voici la commande et le résultat pour le groupe système Cisco local :

```
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
```

Voici la commande et le résultat de la table ARP MIB-II :

```
NMSPrompt 84 % snmpwalk cough atTable

no MIB objects contained under subtree.

NMSPrompt 85 %
```

Configuration de la communauté SNMP avec la liste d'accès

Les meilleures pratiques actuelles recommandent d'appliquer des listes de contrôle d'accès (ACL) aux chaînes de communauté et de s'assurer que les chaînes de communauté des requêtes ne sont pas identiques aux chaînes de communauté des notifications. Les listes d'accès fournissent une protection supplémentaire lorsqu'elles sont utilisées en combinaison avec d'autres mesures de protection.

Cet exemple configure une ACL sur une chaîne de communauté :

```
access-list 1 permit 10.1.1.1

snmp-server community string1 ro 1
```

Lorsque vous utilisez différentes chaînes de communauté pour les requêtes et les messages d'interruption, cela réduit la probabilité d'attaques ou de compromissions supplémentaires si la chaîne de communauté est découverte par un pirate. Sinon, un pirate peut compromettre un périphérique distant ou détecter un message de déroutement du réseau sans autorisation.

Une fois que vous avez activé le déroutement avec une chaîne de communauté, la chaîne peut être activée pour l'accès SNMP dans certains logiciels Cisco IOS. Vous devez désactiver explicitement cette communauté. Exemple :

```
access-list 10 deny any
snmp-server host 10.1.1.1 mystring1
snmp-server community mystring1 RO 10
```

Configuration de SNMP version 3

SNMP version 3 a été introduit pour la première fois dans le logiciel Cisco IOS version 12.0, mais n'est pas encore couramment utilisé dans la gestion de réseau. Procédez comme suit pour configurer SNMP version 3 :

1. Attribuez un ID de moteur à l'entité SNMP (facultatif).
2. Définissez un utilisateur, **userone**, qui appartient au groupe **groupone** et appliquez **noAuthentication** (no password) et **noPrivacy** (no encryption) à cet utilisateur.
3. Définissez un utilisateur, **usertwo ;** qui appartient au groupe **grouptwo** et appliquez **noAuthentication** (pas de mot de passe) et **noPrivacy** (pas de chiffrement) à cet utilisateur.
4. Définissez un utilisateur, **userthree,** qui appartient au groupe **groupthree** et appliquez **Authentication** (le mot de passe est user3passwd) et **noPrivacy** (pas de cryptage) à cet utilisateur.
5. Définissez un utilisateur, **userfour**, qui appartient au groupe **groupfour** et appliquez l'**authentification** (le mot de passe est user4passwd) et la **confidentialité** (chiffrement des56) à cet utilisateur.
6. Définissez un groupe, **groupone**, à l'aide de User Security Model (USM) V3 et activez l'accès en lecture sur la vue **v1 par défaut** (la vue par défaut).
7. Définissez un groupe, **grouptwo**, au moyen de USM V3 et activez l'accès en lecture sur la vue **myview** .
8. Définissez un groupe, **groupthree**, au moyen de USM V3, et activez l'accès en lecture sur la vue **v1 par défaut** (la vue par défaut), au moyen de l'**authentification** .
9. Définissez un groupe, **groupfour**, au moyen de USM V3, et activez l'accès en lecture sur la vue **v1 par défaut** (la vue par défaut), au moyen de l'**authentification** et de la **confidentialité** .
10. Définissez une vue, **myview**, qui fournit un accès en lecture sur la MIB-II et refuse l'accès en lecture sur la MIB Cisco privée.Les **show running** fournit des lignes supplémentaires pour le groupe **public**, en raison du fait qu'il y a une chaîne de communauté Read-Only **public** qui a été définie.Les **show running** le résultat n'affiche pas **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
```

Voici la commande et le résultat pour le groupe Système MIB-II avec l'utilisateur **userone** :

```
NMSPrompt 94 % snmpwalk -v3 -n "" -u userone -l noAuthNoPriv clumsy system
Module SNMPV2-TC not found
system.sysDescr.0 = Cisco Internetwork Operating System Software
Cisco 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 %
```

Voici la commande et le résultat pour le groupe Système MIB-II avec l'utilisateur **usertwo** :

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

Module SNMPV2-TC not found
system.sysDescr.0 = Cisco Internetwork Operating System Software
Cisco 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
```

Voici la commande et le résultat pour le groupe Système local Cisco avec l'utilisateur **userone** :

```
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"
```

Voici la commande et le résultat qui montre que vous ne pouvez pas obtenir le groupe Système local Cisco avec l'utilisateur **usertwo** :

```
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 commande et le résultat obtenu correspondent à une commande personnalisée tcpdump (correctif pour la prise en charge de SNMP version 3 et ajout de 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
```

Configurer ACL sur les interfaces

La fonctionnalité ACL fournit des mesures de sécurité qui empêchent les attaques telles que l'usurpation d'adresse IP. La liste de contrôle d'accès peut être appliquée aux interfaces entrantes ou sortantes sur les routeurs.

Sur les plates-formes qui n'ont pas la possibilité d'utiliser des listes de contrôle d'accès de réception (rACL), il est possible d'autoriser le trafic UDP (User Datagram Protocol) vers le routeur à partir d'adresses IP approuvées avec des listes de contrôle d'accès d'interface.

La liste de contrôle d'accès étendue suivante peut être adaptée à votre réseau. Cet exemple suppose que le routeur a les adresses IP 192.168.10.1 et 172.16.1.1 configurées sur ses interfaces, que tout accès SNMP doit être limité à une station de gestion avec l'adresse IP 10.1.1.1, et que la station de gestion doit seulement communiquer avec l'adresse IP 192.168.10.1 :

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

Les access-list doit ensuite être appliqué à toutes les interfaces avec 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 doivent être spécifiquement répertoriés dans la liste d'accès précédente. La plate-forme logicielle Cisco IOS utilise des ports compris entre 49152 et 65535 comme ports source pour les sessions sortantes telles que les requêtes DNS (Domain Name System).

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.

rACL

Pour les plates-formes distribuées, les rACL peuvent être une option qui démarre dans le logiciel Cisco IOS Version 12.0(21)S2 pour le routeur de commutation Gigabit (GSR) de la gamme Cisco 12000 et Version 12.0(24)S pour la gamme Cisco 7500. Les listes d'accès de réception protègent le périphérique du trafic nuisible avant que le trafic n'ait un impact sur le processeur de routage. Les listes de contrôle d'accès de chemin de réception sont également considérées comme une meilleure pratique en matière de sécurité réseau et doivent être considérées comme un ajout à long terme à une bonne sécurité réseau, ainsi qu'une solution de contournement pour cette

vulnérabilité spécifique. La charge du processeur est distribuée aux processeurs de la carte de ligne et permet de réduire la charge sur le processeur de la route principale. Le livre blanc intitulé GSR : Receive Access Control Lists permet d'identifier le trafic légitime. Utilisez ce livre blanc pour comprendre comment envoyer du trafic légitime à votre périphérique et refuser tous les paquets indésirables.

Les ACL d´infrastructure

Bien qu'il soit souvent difficile de bloquer le trafic qui transite par votre réseau, il est possible d'identifier le trafic qui ne doit jamais être autorisé à cibler vos périphériques d'infrastructure et de bloquer ce trafic à la périphérie de votre réseau. Les listes de contrôle d'accès d'infrastructure (iACL) sont considérées comme une meilleure pratique en matière de sécurité réseau et doivent être considérées comme un ajout à long terme à une bonne sécurité réseau, ainsi qu'une solution de contournement pour cette vulnérabilité spécifique. Le livre blanc Protecting Your Core : Infrastructure Protection Access Control Lists présente des directives et des techniques de déploiement recommandées pour les listes de contrôle d'accès iACL.

Fonctionnalité de sécurité du commutateur LAN Cisco Catalyst

La fonctionnalité de liste d'autorisation d'adresses IP limite les accès entrants au commutateur par Telnet et SNMP à partir d'adresses IP source non autorisées. Les messages de journal système et les interruptions SNMP sont pris en charge pour aviser un système de gestion lorsqu'il y a une violation ou un accès non autorisé.

Une combinaison des fonctions de sécurité du logiciel Cisco IOS peut être utilisée pour gérer les routeurs et les commutateurs Cisco Catalyst. Il est nécessaire d'établir une stratégie de sécurité qui limite le nombre de stations de gestion pouvant accéder aux commutateurs et aux routeurs.

Pour plus d'informations sur la façon d'augmenter la sécurité sur les réseaux IP, référez-vous à Augmenter la sécurité sur les réseaux IP.

Vérification des erreurs SNMP : procédure

Configurez les listes de contrôle d'accès SNMP avec **log** mot clé. Monitor **syslog** pour les tentatives infructueuses, comme indiqué ci-dessous.

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

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

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

Ce résultat signifie que la liste d'accès 10 a refusé cinq paquets SNMP provenant de l'hôte 172.16.1.1.

Vérifiez régulièrement que le protocole SNMP ne comporte pas d'erreurs show snmp , comme illustré ci-dessous :

```
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 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 la section Cisco Product Security Incident Response.

Informations connexes

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

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.