Schützen Sie Ihr Simple Network Management Protocol

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie Sie das Simple Network Management Protocol (SNMP) schützen.

Voraussetzungen

Anforderungen

Es gibt keine spezifischen Anforderungen für dieses Dokument.

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- SNMP View - Cisco IOS® Software Version 10.3 oder höher
- SNMP-Version 3 - Einführung in Version 12.0(3)T der Cisco IOS-Software.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher,

dass Sie die möglichen Auswirkungen aller Befehle verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions (Technische Tipps von Cisco zu Konventionen).

Hintergrundinformationen

Es ist wichtig, Ihr SNMP zu schützen, insbesondere wenn die Schwachstellen von SNMP wiederholt ausgenutzt werden können, um einen Denial of Service (DoS) zu erzeugen.

Strategien zur Sicherung von SNMP

Wählen Sie eine gute SNMP-Community-Zeichenfolge.

Es ist nicht empfehlenswert, **public** als schreibgeschützte und **private** als Community-Strings mit Lese- und Schreibzugriff zu verwenden.

SNMP-Ansicht einrichten

Die Fehlermeldung Setup SNMP view kann den Benutzer nur mit Zugriff auf die Management Information Base (MIB) blockieren. Standardmäßig gibt es keine SNMP view entry exists . Dieser Befehl wird im globalen Konfigurationsmodus konfiguriert und zuerst in Version 10.3 der Cisco IOS-Software eingeführt. Es funktioniert ähnlich wie **access-list** in diesem Fall SNMP View auf bestimmten MIB-Trees wird jeder andere Tree unerklärlicherweise abgelehnt. Die Sequenz ist jedoch nicht wichtig, und sie durchläuft die gesamte Liste für eine Übereinstimmung, bevor sie beendet wird.

Um einen Ansichtseintrag zu erstellen oder zu aktualisieren, verwenden Sie den **snmp-server view global configuration** aus. Um den angegebenen Eintrag für die SNMP-Serveransicht zu entfernen, verwenden Sie den **no** dieses Befehls.

Syntax:

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

no snmp-server view view-name
```

Syntaxbeschreibung:

- view-name- Beschriftung für den Ansichtsdatensatz, den Sie aktualisieren oder erstellen. Der Name wird für den Verweis auf den Datensatz verwendet.
- oid-tree - Objekt-ID des ASN.1-Unterbaums (Abstract Syntax Notation One), der in die Ansicht eingeschlossen oder aus ihr ausgeschlossen werden soll. Geben Sie zum Identifizieren der Unterstruktur eine Textzeichenfolge an, die aus Zahlen besteht, z. B. 1.3.6.2.4, oder ein Wort wie system. Ersetzen Sie einen einzelnen Unterbezeichner durch das Sternchen (*), um eine Unterbaumfamilie anzugeben, z. B. 1.3.*.4.

- included | excluded- Ansichtstyp. Sie müssen entweder eingeschlossen oder ausgeschlossen angeben.

Wenn eine Ansicht erforderlich ist, können anstelle einer Ansicht, die definiert werden muss, zwei vordefinierte Standardansichten verwendet werden. Eins ist alles, was anzeigt, dass der Benutzer alle Objekte sehen kann. Die andere ist *eingeschränkt*, was bedeutet, dass der Benutzer drei Gruppen sehen kann: system, snmpStatsund snmpParties. Die vordefinierten Ansichten werden in RFC 1447 beschrieben.

Hinweis: Die erste snmp-server aktiviert beide Versionen von SNMP.

In diesem Beispiel wird eine Ansicht erstellt, die alle Objekte in der MIB-II-Systemgruppe mit Ausnahme von **sysServices** (System 7) und alle Objekte für Schnittstelle 1 in der MIB-II-Schnittstellengruppe:

```
snmp-server view agon system included

snmp-server view agon system.7 excluded

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

Dies ist ein vollständiges Beispiel für die Anwendung der MIB mit Community-String und der Ausgabe der snmpwalk mit view eingerichtet. Diese Konfiguration definiert eine Ansicht, die den SNMP-Zugriff für die ARP-Tabelle (Address Resolution Protocol) verweigert (atEntry) und ermöglicht MIB-II und Cisco Private MIB:

```
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
```

Dies ist der Befehl und die Ausgabe für die MIB-II-Systemgruppe:

```
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 %
```

Dies ist der Befehl und die Ausgabe für die lokale Cisco System-Gruppe:

```
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
```

Dies ist der Befehl und die Ausgabe für die MIB-II-ARP-Tabelle:

```
NMSPrompt 84 % snmpwalk cough atTable

no MIB objects contained under subtree.

NMSPrompt 85 %
```

Einrichtung der SNMP-Community mit Zugriffsliste

Nach den aktuellen Best Practices sollten Sie Zugriffskontrolllisten (ACLs) auf Community-Strings anwenden und sicherstellen, dass die Anforderungen-Community-Strings nicht mit den Benachrichtigungen-Community-Strings identisch sind. Zugriffslisten bieten zusätzlichen Schutz, wenn sie in Kombination mit anderen Schutzmaßnahmen verwendet werden.

In diesem Beispiel wird die ACL auf einen Community-String eingerichtet:

```
access-list 1 permit 10.1.1.1

snmp-server community string1 ro 1
```

Wenn Sie verschiedene Community-Strings für Anfragen und Trap-Nachrichten verwenden, verringert dies die Wahrscheinlichkeit weiterer Angriffe oder Kompromisse, wenn der Community-String von einem Angreifer entdeckt wird. Andernfalls könnte ein Angreifer ein Remote-Gerät kompromittieren oder ohne Autorisierung eine Trap-Nachricht aus dem Netzwerk abhören.

Wenn Sie Trap mit einem Community-String aktivieren, kann dieser String in einigen Cisco IOS-Programmen für den SNMP-Zugriff aktiviert werden. Sie müssen diese Community explizit deaktivieren. Beispiele:

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

SNMP-Version 3 einrichten

Die SNMP-Version 3 wurde zuerst in Version 12.0 der Cisco IOS-Software eingeführt, wird jedoch noch nicht häufig für die Netzwerkverwaltung verwendet. Gehen Sie folgendermaßen vor, um die SNMP-Version 3 zu konfigurieren:

1. Weisen Sie der SNMP-Einheit eine Modul-ID zu (optional).
2. Definieren Sie einen Benutzer, einen **Benutzer,** der zur **Gruppe** gehört, und wenden Sie **noAuthentication (**kein Kennwort) und **noPrivacy (keine Verschlüsselung) auf diesen Benutzer an.**
3. Definieren Sie einen Benutzer, **userTwo ;**der zur Gruppe **groupTwo** gehört, und wenden Sie **noAuthentication (**kein Kennwort) und **noPrivacy (keine Verschlüsselung) auf diesen Benutzer an.**
4. Definieren Sie einen Benutzer, **BenutzerDrei,** der zur Gruppe **GruppeDrei** gehört, und wenden Sie **Authentication (**password is user3passwd) und **noPrivacy (no encryption) auf diesen Benutzer an.**
5. Definieren Sie einen Benutzer, **userFour,** der zur Gruppe **group** gehört, und wenden Sie **Authentication (**password is user4passwd) und **Privacy (**des56 encryption) auf diesen Benutzer an.
6. Definieren Sie mithilfe des Benutzersicherheitsmodells (USM) V3 eine Gruppe (**group),** und aktivieren Sie den Lesezugriff in der **v1-**Standardansicht (der Standardansicht).
7. Definieren Sie eine Gruppe**, groupTwo**, mithilfe von USM V3 und aktivieren Sie den Lesezugriff in der Ansicht **myview** .
8. Definieren Sie eine Gruppe (**Gruppe drei)** mithilfe von USM V3, und aktivieren Sie den Lesezugriff in der **v1-**Standardansicht (der Standardansicht) mittels **Authentifizierung**.
9. Definieren Sie eine Gruppe**, eine Gruppe** mithilfe von USM V3, und aktivieren Sie den Lesezugriff in der **v1default-**Ansicht (die Standardansicht) mithilfe von **Authentifizierung** und **Datenschutz** .
10. Definieren Sie eine Ansicht (**myview**), die Lesezugriff auf die MIB-II gewährt und Lesezugriff auf die private Cisco MIB verweigert.Die Fehlermeldung **show running** gibt zusätzliche Zeilen für die Gruppe **public** aus, da ein Community String Read-Only **public** definiert wurde.Die Fehlermeldung **show running** Ausgabe zeigt den **Benutzer** nicht **an**.

Beispiel:

```
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
```

Dies ist der Befehl und die Ausgabe für die MIB-II-Systemgruppe mit dem Benutzer **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 %
```

Dies ist der Befehl und die Ausgabe für die MIB-II-Systemgruppe mit Benutzer**2**:

```
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
```

Dies ist der Befehl und die Ausgabe für die Cisco Local System-Gruppe mit dem Benutzer **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"
```

Mit diesem Befehl und dieser Ausgabe wird angezeigt, dass Sie die Cisco Local System-Gruppe mit Benutzer**2** nicht abrufen können:

```
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 %
```

Dieser Befehl und das Ausgabeergebnis sind für eine benutzerdefinierte tcpdump (Patch für SNMP-Unterstützung der Version 3 und Addendum von 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
```

Einrichten von ACL auf Schnittstellen

Die ACL-Funktion stellt Sicherheitsmaßnahmen bereit, die Angriffe wie IP-Spoofing verhindern. Die ACL kann auf eingehende oder ausgehende Schnittstellen auf Routern angewendet werden.

Auf Plattformen, die keine Empfangszugriffskontrolllisten (rACLs) verwenden können, ist es möglich, UDP-Datenverkehr (User Datagram Protocol) von vertrauenswürdigen IP-Adressen mit Schnittstellenzugriffskontrolllisten zum Router zuzulassen.

Die nächste erweiterte Zugriffsliste kann an Ihr Netzwerk angepasst werden. In diesem Beispiel wird davon ausgegangen, dass für die Schnittstellen des Routers die IP-Adressen 192.168.10.1 und 172.16.1.1 konfiguriert sind, dass der gesamte SNMP-Zugriff auf eine Verwaltungsstation mit der IP-Adresse 10.1.1.1 beschränkt sein muss und dass die Verwaltungsstation nur mit der IP-Adresse 192.168.10.1 kommunizieren muss :

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

Die Fehlermeldung access-list muss dann mit den folgenden Konfigurationsbefehlen auf alle Schnittstellen angewendet werden:

```
interface ethernet 0/0

ip access-group 101 in
```

Alle Geräte, die über UDP-Ports direkt mit dem Router kommunizieren, müssen in der vorherigen Zugriffsliste speziell aufgeführt werden. Die Cisco IOS-Software verwendet Ports zwischen 49152 und 65535 als Quellport für ausgehende Sitzungen wie DNS-Abfragen (Domain Name System).

Bei Geräten mit vielen konfigurierten IP-Adressen oder vielen Hosts, die mit dem Router kommunizieren müssen, ist dies nicht immer eine skalierbare Lösung.

Zugriffskontrolllisten

Für verteilte Plattformen können rACLs eine Option sein, die in der Cisco IOS Software-Version 12.0(21)S2 für den Cisco Gigabit Switch Router der Serie 12000 (GSR) und in der Version

12.0(24)S für die Cisco Serie 7500 beginnt. Die Empfangs-Zugriffslisten schützen das Gerät vor schädlichem Datenverkehr, bevor dieser den Routing-Prozessor beeinträchtigen kann. Empfangspfad-ACLs gelten ebenfalls als Best Practice in Bezug auf die Netzwerksicherheit und müssen als langfristige Ergänzung zu guter Netzwerksicherheit sowie als Problemumgehung für diese spezifische Schwachstelle angesehen werden. Die CPU-Last wird auf die Linecard-Prozessoren verteilt und trägt dazu bei, die Last auf dem Hauptroutenprozessor zu reduzieren. Das Whitepaper GSR: Receive Access Control Lists unterstützt Sie bei der Identifizierung von legitimem Datenverkehr. In diesem Whitepaper erfahren Sie, wie Sie legitimen Datenverkehr an Ihr Gerät senden und unerwünschte Pakete blockieren können.

Infrastruktur ACLs

Obwohl es oft schwierig ist, Datenverkehr zu blockieren, der durch Ihr Netzwerk fließt, ist es möglich, Datenverkehr zu identifizieren, der niemals Ihre Infrastrukturgeräte erreichen darf, und diesen Datenverkehr an der Grenze Ihres Netzwerks zu blockieren. Infrastruktur-ACLs (iACLs) gelten als Best Practice für die Netzwerksicherheit und müssen als langfristige Ergänzung zu guter Netzwerksicherheit sowie als Workaround für diese spezifische Schwachstelle betrachtet werden. Das Whitepaper "Protecting Your Core: Infrastructure Protection Access Control Lists" enthält Richtlinien und empfohlene Implementierungsverfahren für iACLs.

Sicherheitsfunktion für Cisco Catalyst LAN-Switches

Die Funktion "IP Permit List" (IP-Genehmigungsliste) schränkt den eingehenden Telnet- und SNMP-Zugriff von nicht autorisierten Quell-IP-Adressen auf den Switch ein. Syslog-Meldungen und SNMP-Traps werden unterstützt, um ein Managementsystem zu benachrichtigen, wenn eine Verletzung oder ein nicht autorisierter Zugriff auftritt.

Eine Kombination der Sicherheitsfunktionen der Cisco IOS Software kann zur Verwaltung von Routern und Cisco Catalyst Switches verwendet werden. Es muss eine Sicherheitsrichtlinie erstellt werden, die die Anzahl der Verwaltungsstationen begrenzt, die auf die Switches und Router zugreifen können.

Weitere Informationen zur Erhöhung der Sicherheit in IP-Netzwerken finden Sie unter Erhöhte Sicherheit in IP-Netzwerken.

Überprüfen von SNMP-Fehlern

Konfigurieren Sie die Zugriffskontrolllisten der SNMP-Community mit dem **log** Schlüsselwort. Überwachen **syslog** für fehlgeschlagene Versuche, wie unten gezeigt.

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

Wenn jemand versucht, über die Community auf den Router zuzugreifen, wird ein syslog ähnlich wie hier:

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

Diese Ausgabe bedeutet, dass Zugriffsliste 10 fünf SNMP-Pakete vom Host 172.16.1.1 verweigert hat.

Regelmäßige Überprüfung des SNMP auf Fehler mit dem show snmp Befehl, wie hier gezeigt:

```
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
```

Achten Sie auf die mit ** gekennzeichneten Zähler auf unerwartete Erhöhungen der Fehlerquoten, die auf eine versuchte Ausnutzung dieser Schwachstellen hinweisen können. Informationen zum Melden von Sicherheitsproblemen finden Sie unter Cisco Product Security Incident Response.

Zugehörige Informationen

- SNMP-Sicherheitslücken in Cisco Security Advisors
- Technischer Support und Downloads von Cisco

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.