Implementierung von ASA SNMP Feature Enhancer

Inhalt

Einführung

Dieses Dokument beschreibt die neuen SNMP-Funktionen (Simple Network Management Protocol), die in Softwareversion 9.1.5 und Version 9.2.(1) für die Cisco Adaptive Security Appliance (ASA) Firewall der Serie 5500-X verfügbar sind.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf der Firewall der Cisco Serie ASA 5500-X, die die Cisco ASA® Softwareversion 9.1.5 und die Versionen 9.2.(1) und höher ausführt.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Hintergrundinformationen

In den ASA-Versionen 9.1.5 und 9.2.1 werden die folgenden SNMP-Erweiterungen eingeführt:

- Unterstützung für 128 SNMP-Hosts wird hinzugefügt.
- Unterstützung für cpmCPUTotal5minRev SNMP Object Identifiers (OIDs) wird hinzugefügt.
- Unterstützung für 1.472-Byte-SNMP-Nachrichten wird hinzugefügt.

Unterstützung für 128 SNMP-Hosts

Mit dieser Funktion kann die ASA mehr als die aktuellen 32 SNMP-Hosts unterstützen.

Zweck

Derzeit ist die ASA auf insgesamt 32 SNMP-Hosts begrenzt. Dies umfasst Hosts, die für Traps und für das Polling konfiguriert werden können. In den nächsten Abschnitten werden die Auswirkungen beschrieben, die dieses Feature auf Einzel- und Mehrkontextmodi hat.

Modus mit einem Kontext

- Ermöglicht die Konfiguration einer wesentlich höheren Anzahl von Einträgen (insgesamt Hosts) ab 4.096. Von diesen Einträgen können jedoch nur 128 für Traps verwendet werden.
- Für das Polling von Konfigurationen können bis zu 4.096 Polling-Hosts und 128 Trap-Hosts konfiguriert werden. Die tatsächliche Anzahl der Server, die das System abfragen, sollte jedoch auf weniger als 128 beschränkt werden, da die Auswirkungen einer höheren Anzahl von Hosts auf die Leistung unbekannt sind und nicht unterstützt werden.

Multi-Context-Modus

- Zu Konfigurationszwecken sind bis zu 4.000 Hosts pro Kontext zulässig, und es wird eine systemweite Beschränkung auf 64.000 Hosts auferlegt.
- Von den insgesamt konfigurierten Hosts können nur 128 (pro Kontext) für Traps verwendet werden, und der Gesamtsystemgrenzwert für Traps im Multi-Context-Modus beträgt 32.000.

- Obwohl Sie bis zu 4.000 Hosts pro Kontext konfigurieren können, sollte die tatsächliche Anzahl der Server, die einen beliebigen Kontext abfragen, auf 128 beschränkt sein.

Beschreibung

Sie ziehen es vor, die Netzwerkgeräte über einen großen Pool von SNMP-Hosts zu überwachen. Im Idealfall sollten Sie einen IP-Bereich und/oder ein Subnetz der IP-Adressen angeben können, die die Netzwerkgeräte überwachen dürfen. Die ASA bietet derzeit keine solche Flexibilität und beschränkt die maximalen SNMP-Hosts auf 32.

Die Unterstützung dieser Funktion umfasst zwei Aspekte:

- ASA kann bis zu 128 SNMP-Hosts verarbeiten.

- Stellen Sie die erforderlichen Konfigurationsbefehle bereit, damit Sie eine wesentlich höhere Anzahl an Hosts konfigurieren können, wie im vorherigen Abschnitt über einen einzigen Befehl beschrieben.

Das aktuelle Design auf der ASA ermöglicht die Konfiguration einzelner Hosts über die CLI. Für diese Funktion wurden folgende zusätzliche Designanforderungen berücksichtigt:

- Einführung des CLI-Befehls **snmp-server host-group** mit Befehlsspeicherung für **snmp-server host** CLI.

- Die Möglichkeit, Einträge von den Befehlen **snmp-server host-group** und **snmp-server host** CLI zu beziehen.

- Für SNMP Version 3 wird der Befehl **snmp-server userlist** CLI mit der Befehlsspeicherung für **Benutzer-SNMP-Server** eingeführt.

- Eine Konfigurationsüberschneidung muss ebenfalls unterstützt werden. Beispielsweise können die Befehle mehrerer **Hostgruppen** mit Hosts übermittelt werden, die sich in den Netzwerkobjekten überschneiden. Ebenso können Sie einen Host mit einer IP-Adresse angeben, der sich mit den aktuellen Hosts oder der Hostgruppe überschneidet. Dies stellt einen Mechanismus bereit, der verwendet werden kann, um die Parameter für einige Hosts in einer Gruppe zu überschreiben, ohne dass die gesamte Gruppe neu konfiguriert werden muss.

Zu den Softwarebeschränkungen und -einschränkungen, die mit dieser Funktion in Zusammenhang stehen, gehören:

- Als Teil des Befehls **snmp-server host-group** lautet der Standardwert **Polll**, wenn **[trap|poll]** nicht angegeben ist. Wichtig ist auch, dass für diesen Befehl sowohl Traps als auch Polling für dieselbe Hostgruppe nicht aktiviert werden können. Falls dies erforderlich ist, empfiehlt Cisco, den Befehl **snmp-server host** für die relevanten Hosts zu verwenden.

- Sie können Netzwerkobjekte angeben, die sich in verschiedenen **Hostgruppenbefehlen** überschneiden. Die Werte, die in der letzten Hostgruppe angegeben sind, werden für den allgemeinen Satz von Hosts in den verschiedenen Netzwerkobjekten wirksam.

Hier ein Beispiel:

```
object network network1
range 64.103.236.40 64.103.236.50
object network network2
range 64.103.236.35 64.103.236.55

snmp-server host-group inside network1 poll version 3 user-list SNMP-List
snmp-server host-group inside network2 poll version 3 user-list SNMP-List
```

Geben Sie den Befehl **show snmp-server host** ein, um die Hosteinträge anzuzeigen:

```
asa(config)# show snmp-server host
host ip = 64.103.236.35, interface = inside poll version 3 cisco1
host ip = 64.103.236.36, interface = inside  poll version 3 cisco1
host ip = 64.103.236.37, interface = inside  poll version 3 cisco1
host ip = 64.103.236.38, interface = inside  poll version 3 cisco1
host ip = 64.103.236.39, interface = inside  poll version 3 cisco1
host ip = 64.103.236.40, interface = inside  poll version 3 cisco1
host ip = 64.103.236.41, interface = inside  poll version 3 cisco1
host ip = 64.103.236.42, interface = inside  poll version 3 cisco1
host ip = 64.103.236.43, interface = inside  poll version 3 cisco1
host ip = 64.103.236.44, interface = inside  poll version 3 cisco1
host ip = 64.103.236.45, interface = inside  poll version 3 cisco1
host ip = 64.103.236.46, interface = inside  poll version 3 cisco1
host ip = 64.103.236.47, interface = inside  poll version 3 cisco1
host ip = 64.103.236.48, interface = inside  poll version 3 cisco1
host ip = 64.103.236.49, interface = inside  poll version 3 cisco1
host ip = 64.103.236.50, interface = inside  poll version 3 cisco1
host ip = 64.103.236.51, interface = inside  poll version 3 cisco1
host ip = 64.103.236.52, interface = inside  poll version 3 cisco1
host ip = 64.103.236.53, interface = inside  poll version 3 cisco1
host ip = 64.103.236.54, interface = inside  poll version 3 cisco1
host ip = 64.103.236.55, interface = inside  poll version 3 cisco1
```

Hier einige wichtige Hinweise zur Verwendung dieser Funktion:

- Wenn eine Hostgruppe oder ein Host, die sich mit anderen Hostgruppen überschneidet, gelöscht wird, werden die Hosts erneut mit den Werten eingerichtet, die für die konfigurierten Hostgruppen verwendet werden.
- Die Werte oder Parameter, die den Hosts zugeordnet sind, hängen von der Reihenfolge ab, in der die Befehle ausgeführt werden.
- Die konfigurierte Benutzerliste kann nicht gelöscht werden, wenn die Liste von einer bestimmten Hostgruppe verwendet wird.
- Der SNMP-Benutzer kann nicht gelöscht werden, wenn auf den Benutzer in einer bestimmten Benutzerliste verwiesen wird.
- Ein Netzwerkobjekt kann nicht gelöscht werden, wenn es vom CLI-Befehl **der Hostgruppe** verwendet wird.

Konfigurieren

Verwenden Sie die in diesem Abschnitt beschriebenen Informationen, um die ASA so zu konfigurieren, dass diese neue Funktion implementiert wird.

> **Hinweis**: Verwenden Sie das Command Lookup Tool (nur registrierte Kunden), um weitere Informationen zu den in diesem Abschnitt verwendeten Befehlen zu erhalten.

CLI-Befehle

Für SNMP Version 3 kann der Administrator verschiedene Benutzer einer angegebenen Gruppe von Hosts zuordnen. Dies ist nützlich, wenn ein Administrator möchte, dass eine Gruppe von Benutzern über eine Gruppe von Hosts auf die ASA zugreifen kann. Dieser CLI-Befehl wird verwendet, um eine Benutzerliste für mehrere Benutzer zu konfigurieren:

```
ASA(config)# [no] snmp-server user-list
```

Um die Benutzerliste einer Hostgruppe zuzuordnen, geben Sie diesen Befehl in die CLI ein:

```
[no] snmp-server host-group
```

Mit diesem Befehl können Sie ein Netzwerkobjekt angeben, um die mehreren Hosts anzugeben, die hinzugefügt werden sollen. Mit dem Netzwerkobjekt können Sie entweder eine Subnetzmaske oder den Bereich der IP-Adressen angeben, die hinzugefügt werden sollen, wobei Sie einen einzelnen Befehl verwenden. Alle IP-Adressen, die als Teil des Netzwerkobjekts aufgeführt sind, werden als SNMP-Hosteinträge hinzugefügt. Ebenso gibt es für jeden Benutzer, der in der Benutzerliste angegeben ist, einen separaten SNMP-Host-Eintrag.

Diese Befehle werden verwendet, damit Administratoren die neuen Konfigurationsoptionen für die SNMP-Server löschen und anzeigen können:

- **clear configure snmp-server user list**
- **clear configure snmp-server host-group**
- **show running-config snmp-server user-list**
- **show running-config snmp-server host-group**

Beispielkonfiguration

Gehen Sie wie folgt vor, um die neuen SNMP-Gruppenoptionen zu verwenden und eine SNMP-Server-Hostgruppe für die Abfrage von Version 2c zu erstellen:

1. Erstellen eines Netzwerkobjekts:

```
asa(config)# object network network1
asa(config-network-object)# range 64.103.236.40 64.103.236.50
```

2. Definieren Sie die SNMP-Hostgruppe:

```
asa(config)#snmp-server host-group inside network1 poll community ***** version 2c
```

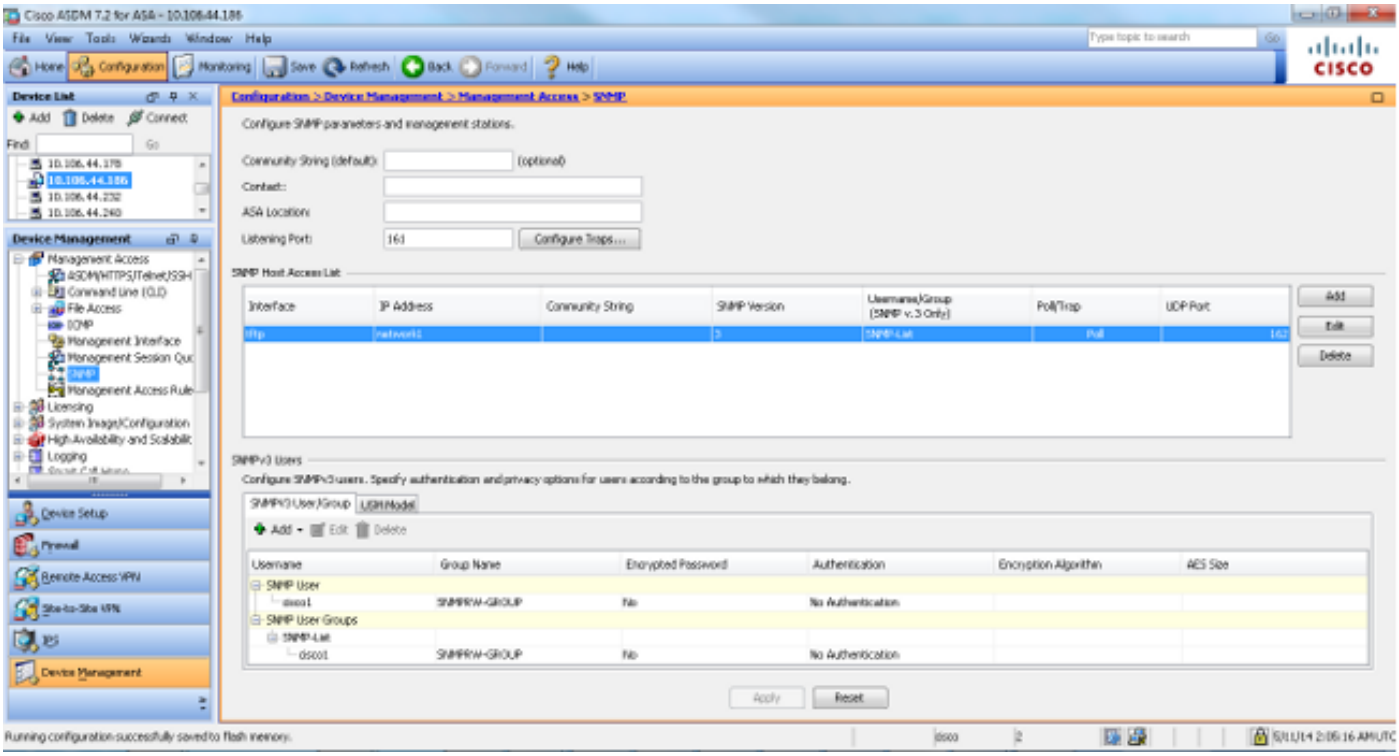
3. Definieren Sie die Gruppe SNMP Version 3:

```
asa(config)#snmp-server group SNMPRW-GROUP v3 noauth
```

4. Verbinden Sie die Gruppen mit den Benutzern:

```
asa(config)#snmp-server user cisco1 SNMPRW-GROUP v3
asa(config)#snmp-server user-list SNMP-List username cisco1
asa(config)#snmp-server host-group inside  network1 poll version 3 user-list SNMP-List
```

Dieses Bild zeigt die Änderungen, die im Cisco Adaptive Security Device Manager (ASDM) vorgenommen werden:



Unterstützung für cpmCPUTotal5minRev SNMP OIDs

Diese Funktion ermöglicht der ASA die Unterstützung von **cpmCPUTotal5minRev**-SNMP-OIDs.

Zweck

Diese Funktion bietet Unterstützung für **cpmCPUTotal5minRev** und **cpmCPUTotal1minRev** OIDs auf der ASA und setzt die derzeit unterstützten OIDs **cpmCPUTotal5min** und **cpmCPUTotal1min außer Kraft**. Diese OIDs dienen zur Überwachung der CPU-Auslastung. Die aktuell unterstützten OIDs liegen zwischen 1 und 100, während die neu unterstützten OIDs zwischen 0 und 100 liegen. Daher wurde Unterstützung für neuere OIDs hinzugefügt, da diese ein größeres Spektrum abdecken.

Da die veralteten OIDs (**cpmCPUTotal5min** und **cpmCPUTotal1min**) auf der ASA nicht mehr unterstützt werden, gibt die ASA keine Informationen für diese OIDs zurück, wenn die ASA aktualisiert wird und die veralteten OIDs abgefragt werden. Nach einem Upgrade der ASA müssen Sie nun den **cpmCPUTotal5minRev** und **cpmCPUTotal1minRev** für die CPU-Auslastung überwachen.

CLI-Befehle

Mit dieser neuen Funktion wurden keine CLI-Änderungen eingeführt.

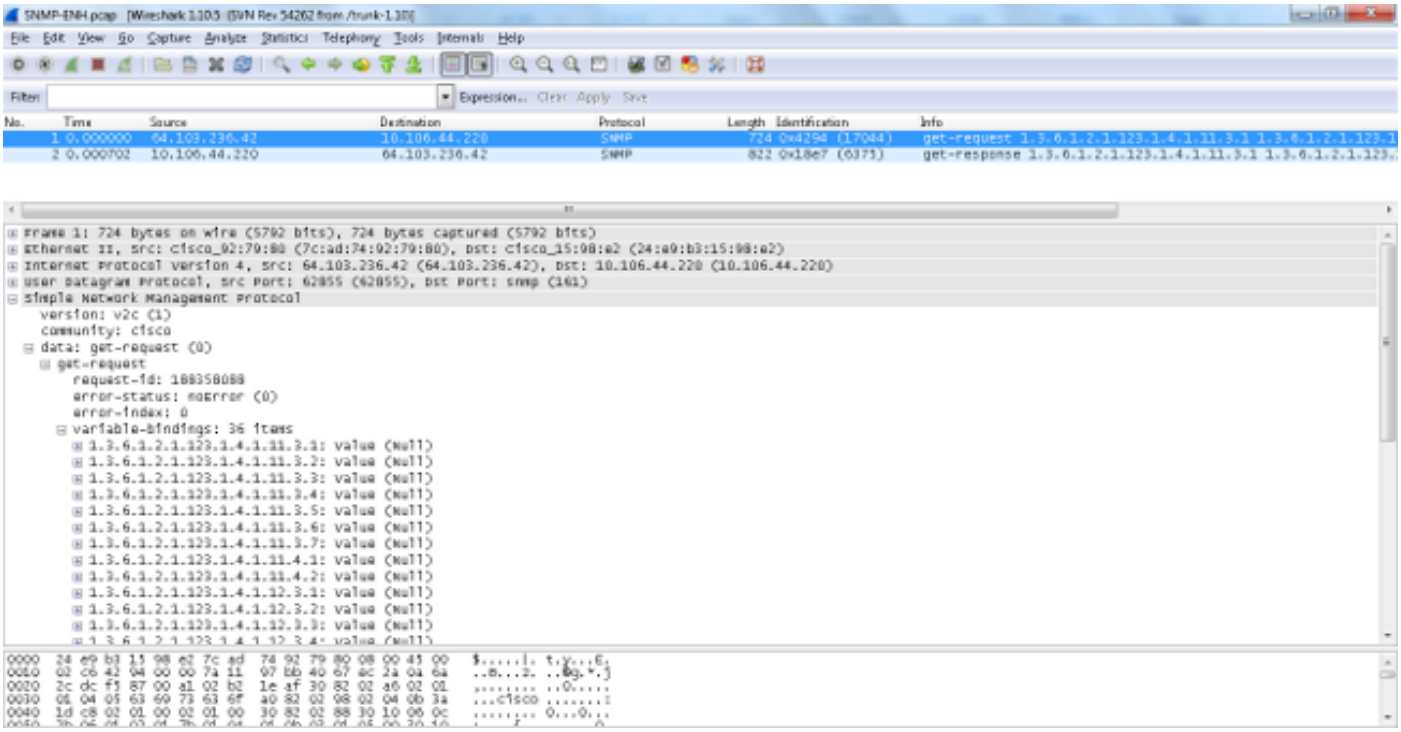
Neue OIDs

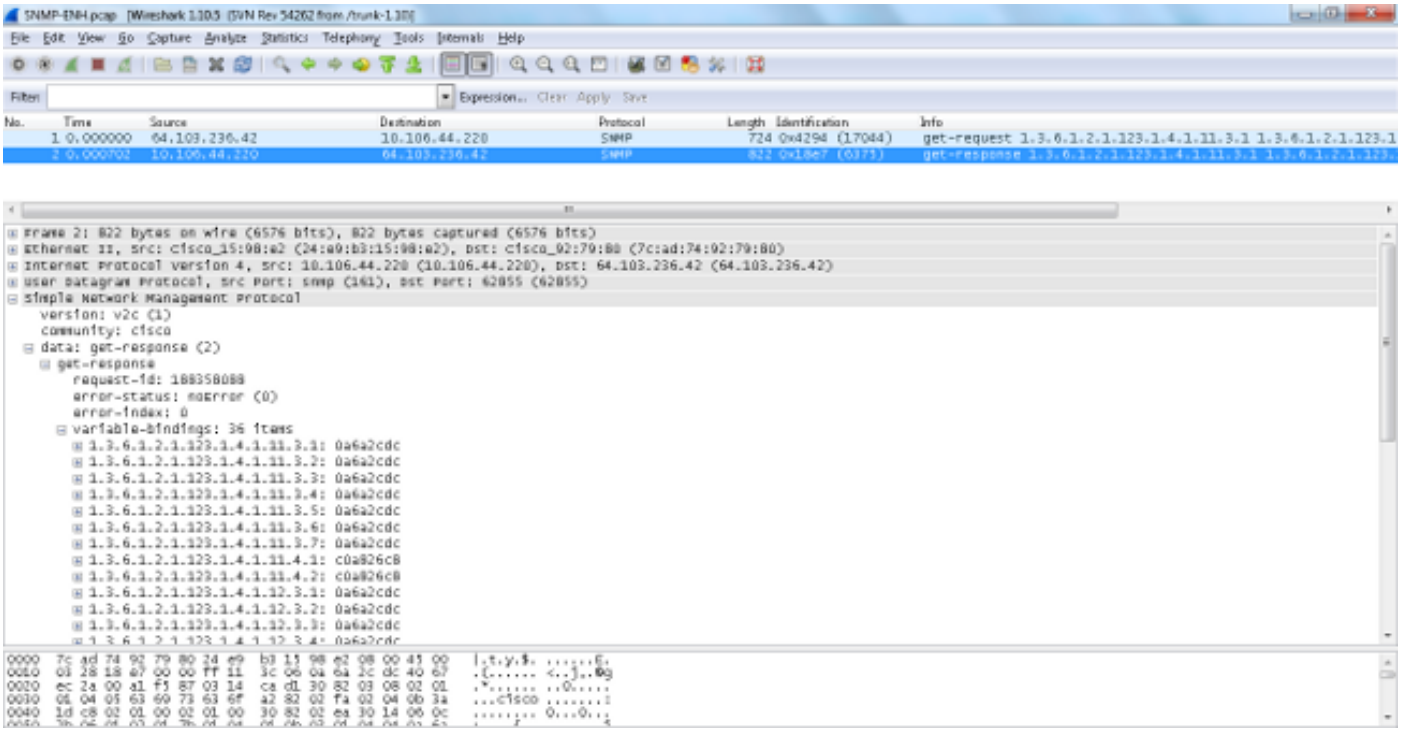
Dies sind die neuen OIDs, die mit dieser Funktion hinzugefügt werden:

- **1.3.6.1.4.1.9.9.109.1.1.1.1.7 cpmCPUTotal1minRev**
- **1.3.6.1.4.1.9.9.109.1.1.1.1.8 cpmCPUTotal5minRev**

Unterstützung für 1.472-Byte-SNMP-Nachrichten

Die ASA-Plattformen beschränken die maximale Paketgröße für SNMP-Anfragen auf 512 Byte. Wenn Sie eine Massenabfrage für eine große Anzahl von MIB-OIDs innerhalb einer einzigen SNMP-Anforderung durchführen, werden die SNMP-Verbindungszeitüberschreitung und ein Fehler-Syslog auf der ASA generiert. RFC3417 schlägt vor, dass die maximale Paketgröße für SNMP-Anforderungen 1.472 Byte betragen sollte. Dies ist die Größe der SNMP-Payload für das Paket. Darüber hinaus müssen der Ethernet-Header und die IP-Header-Größe hinzugefügt werden, um die Gesamtgröße des Pakets zu berechnen.





Hinweis: Diese Funktion unterstützt sowohl den Einzelkontext- als auch den Mehrkontext-Modus.

Fehlerbehebung

Dieser Abschnitt enthält Informationen, die Sie zur Behebung von Systemproblemen auf der ASA verwenden können.

Befehle anzeigen

Diese **show-**Befehle können nützlich sein, wenn versucht wird, Probleme mit der ASA zu beheben:

- asa# **show run snmp-server host-group**
  SNMP-server host-group in network1 polll version 3 user-list SNMP-List

- asa# **show run snmp-server user-list**
  SNMP-server user list SNMP-List username cisco1

- asa# **show snmp-server host**

Dieser CLI-Befehl zeigt die Einträge in der Adresstabelle des SNMP-Servers an, die sowohl die Host- als auch die Host-Gruppenkonfiguration enthält:

```
asa(config)#show run object network
object network network1
range 64.103.236.40 64.103.236.50
object network network2
range 64.103.236.35 64.103.236.55
object network network3
```

```
range 64.103.236.60 64.103.236.70

ciscoasa/admin(config)# show run snmp-server
snmp-server group cisco-group v3 noauth
snmp-server user user1 cisco-group v3
snmp-server user user2 cisco-group v3
snmp-server user user3 cisco-group v3
snmp-server user-list cisco username user1
snmp-server user-list cisco username user2
snmp-server user-list cisco username user3
snmp-server host-group management0/0 net2 poll version 3 user-list cisco
no snmp-server locationno snmp-server contact

ciscoasa/admin(config)# show snmp-server host
host ip = 64.103.236.35, interface = inside poll version 3 cisco1
host ip = 64.103.236.36, interface = inside  poll version 3 cisco1
host ip = 64.103.236.37, interface = inside  poll version 3 cisco1
host ip = 64.103.236.38, interface = inside  poll version 3 cisco1
host ip = 64.103.236.39, interface = inside  poll version 3 cisco1
host ip = 64.103.236.40, interface = inside  poll version 3 cisco1
host ip = 64.103.236.41, interface = inside  poll version 3 cisco1
host ip = 64.103.236.42, interface = inside  poll version 3 cisco1
```

Wie gezeigt, zeigen diese Befehle alle Hosts an, die über den Befehl **host-group** konfiguriert sind. Mit diesem Befehl können Sie überprüfen, ob alle Einträge verfügbar sind, und auch die Hostgruppen, die sich überschneiden, überprüfen.