Implementación de la Función ASA SNMP Enhancement

Contenido

Introducción

Este documento describe las nuevas funciones del protocolo simple de administración de red (SNMP) disponibles para el firewall Cisco Adaptive Security Appliance (ASA) serie 5500-X en la versión de software 9.1.5 y las versiones 9.2.1 y posteriores.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

La información de este documento se basa en el firewall Cisco ASA serie 5500-X que ejecuta Cisco ASA® Software versión 9.1.5 y versiones 9.2.1 y posteriores.

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. If your network is live, make sure that you understand the potential impact of any command.

Antecedentes

En las versiones 9.1.5 y 9.2.1 de ASA, se introducen estas mejoras de SNMP:

- Se agrega soporte para 128 hosts SNMP.
- Se agrega compatibilidad con los identificadores de objetos SNMP (OID) cpmCPUTotal5minRev.
- Se agrega soporte para mensajes SNMP de 1,472 bytes.

Compatibilidad con 128 hosts SNMP

Esta función permite al ASA soportar más de los 32 hosts SNMP actuales.

Propósito

Actualmente, el ASA tiene un límite de hardware de 32 hosts SNMP en total. Esto incluye hosts que se pueden configurar para trampas y para sondeo. En las secciones siguientes se describen los efectos que esta función tiene en los modos de contexto único y múltiple.

Modo de contexto único

- Permite configurar un número significativamente mayor de entradas (hosts totales), más de 4096. Sin embargo, de estas entradas, sólo se pueden utilizar 128 para trampas.
- Para fines de configuración de sondeo, se permite configurar hasta 4096 hosts de sondeo y 128 hosts de trampa. Sin embargo, el número real de servidores que sondean el sistema debe limitarse a menos de 128, ya que los impactos de rendimiento de un mayor número de hosts se desconocen y no se soportan.

Modo multicontexto

- A efectos de configuración, se permiten hasta 4000 hosts por contexto y se impone un límite de 64 000 hosts totales en todo el sistema.
- De los hosts configurados totales, sólo se pueden utilizar 128 (por contexto) para trampas, y el límite total del sistema para trampas en modo multicontexto es de 32,000.

- Aunque puede configurar hasta 4000 hosts totales por contexto, el número real de servidores que sondean cualquier contexto debe limitarse a 128.

Descripción

Es posible que prefiera monitorear los dispositivos de red desde un gran grupo de hosts SNMP. Idealmente, desea la capacidad de especificar un rango de IP o una subred de las direcciones IP que pueden monitorear los dispositivos de red. El ASA actualmente no proporciona esa flexibilidad y limita el número máximo de hosts SNMP a 32.

La compatibilidad con esta función implica dos aspectos:

- Proporcione la capacidad para que ASA gestione hasta 128 hosts SNMP.
- Proporcione los comandos de configuración requeridos para que pueda configurar un número significativamente mayor de hosts, como se detalla en la sección anterior a través de un solo comando.

El diseño actual en el ASA es tal que los hosts individuales se pueden configurar a través de la CLI. Para esta función, se tuvieron en cuenta estos requisitos de diseño adicionales:

- La introducción del comando CLI **snmp-server host-group** con la retención de comandos **snmp-server host** CLI.
- La capacidad para que las entradas provengan de los comandos CLI **snmp-server host-group** y **snmp-server host**.
- Para SNMP versión 3, la introducción del comando CLI **snmp-server userlist** con **snmp-server user** retención de comandos CLI.
- También se debe admitir una superposición de configuración. Por ejemplo, los comandos múltiples **host-group** se pueden dar con hosts que se superponen en los objetos de red. De manera similar, puede especificar un host con una dirección IP que se superpone con los hosts actuales o con el grupo host. Esto proporciona un mecanismo que se puede utilizar para sobrescribir los parámetros de unos pocos hosts en un grupo, sin la necesidad de reconfigurar el grupo completo.

Algunas restricciones de software y advertencias asociadas a esta función son:

- Como parte del comando **snmp-server host-group**, el valor predeterminado es **sondear** si no se especifica **[trap|poll]**. También es importante tener en cuenta que para este comando, las trampas y el sondeo no se pueden habilitar para el mismo grupo host. Si esto es necesario, Cisco recomienda que utilice el comando **snmp-server host** para los hosts relevantes.
- Puede especificar objetos de red que se superponen en diferentes comandos **host-group**. Los valores que se especifican en el último grupo de hosts surten efecto para el conjunto común de hosts en los diferentes objetos de red.

Aquí tiene un ejemplo:

```
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
```

Ingrese el comando **show snmp-server host** para ver las entradas del host:

```
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
```

A continuación se muestran algunas notas importantes sobre el uso de esta función:

- Si se elimina un grupo de host o un host que se superpone con otros grupos de hosts, los hosts se configuran de nuevo con los valores que se utilizan para los grupos de hosts configurados.
- Los valores o parámetros que están asociados con los hosts dependen del orden en que se ejecutan los comandos.
- La lista de usuarios configurada no se puede eliminar si un grupo host determinado utiliza la lista.
- El usuario SNMP no se puede eliminar si se hace referencia al usuario en una lista de usuarios determinada.
- Un objeto de red no se puede eliminar si lo utiliza el comando **host-group** CLI.

Configurar

Utilice la información que se describe en esta sección para configurar el ASA de modo que esta nueva función se implemente.

Nota: Use la Command Lookup Tool (clientes registrados solamente) para obtener más información sobre los comandos usados en esta sección.

Comandos CLI

Para SNMP versión 3, el administrador puede asociar varios usuarios a un grupo especificado de hosts. Esto es útil si el administrador desea que un conjunto de usuarios tenga la capacidad de acceder al ASA desde un grupo de hosts. Este comando CLI se utiliza para configurar una lista de usuarios para varios usuarios:

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

Para asociar la lista de usuarios con un grupo host, ingrese este comando en la CLI:

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

Con este comando único, puede especificar un objeto de red para indicar los hosts múltiples que se deben agregar. Con el objeto de red, puede especificar una máscara de subred o el rango de direcciones IP que se deben agregar, con el uso de un único comando. Todas las direcciones IP que se enumeran como parte del objeto de red se agregan como entradas de host SNMP. De manera similar, para cada uno de los usuarios especificados en la lista de usuarios, hay una entrada de host SNMP separada.

Estos comandos se utilizan para permitir que los administradores borren y vean las nuevas opciones de configuración para los servidores SNMP:

- 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

Ejemplo de configuración

Complete estos pasos para utilizar las nuevas opciones del grupo SNMP y crear un grupo host del servidor SNMP para el sondeo de la Versión 2c:

1. Crear un objeto de red:

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

2. Defina el grupo de host SNMP:

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

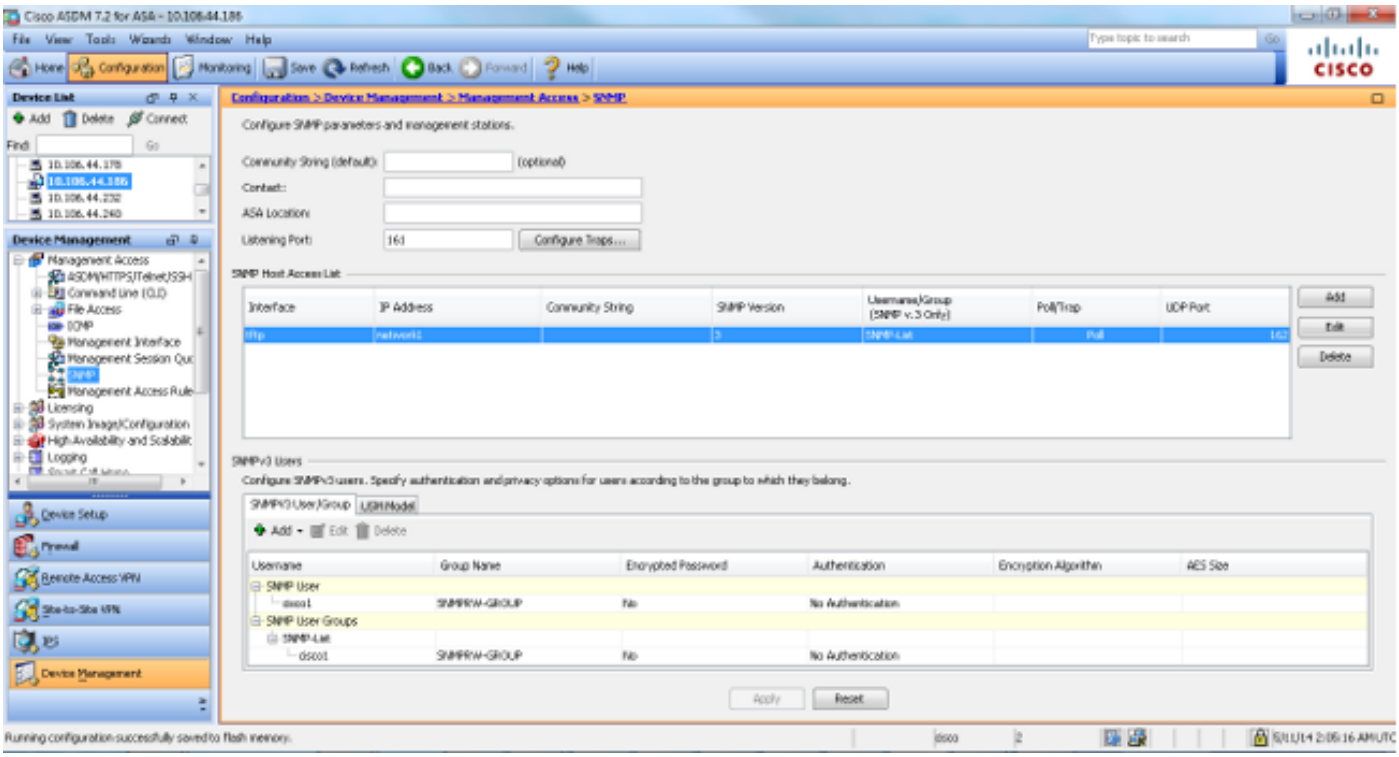
3. Defina el grupo SNMP versión 3:

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

4. Vincular los grupos a los usuarios:

```
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
```

Esta imagen ilustra los cambios que se realizan dentro del Cisco Adaptive Security Device Manager (ASDM):



Soporte para OID SNMP cpmCPUTotal5minRev

Esta función permite al ASA soportar los OID **cpmCPUTotal5minRev** SNMP.

Propósito

Esta función agrega soporte para los OID **cpmCPUTotal5minRev** y **cpmCPUTotal1minRev** en el ASA y desaprueba los OID **cpmCPUTotal5min** y **cpmCPUTotal1min** actualmente soportados. El propósito de estos OID es monitorear el uso de la CPU. Los OID admitidos actualmente oscilan entre 1 y 100, mientras que los OID admitidos recientemente oscilan entre 0 y 100. Por lo tanto, se añadió apoyo a los nuevos OID, ya que abarcan una gama más amplia.

Es importante tener en cuenta que, dado que los OID obsoletos (**cpmCPUTotal5min** y **cpmCPUTotal1min**) ya no se soportan en el ASA, si el ASA se actualiza y se sondea el OID obsoleto, el ASA no devuelve ninguna información para esos OID. Después de una actualización del ASA, ahora debe monitorear el **cpmCPUTotal5minRev** y **cpmCPUTotal1minRev** para el uso

de la CPU.

Comandos CLI

No se han introducido cambios en la CLI con esta nueva función.

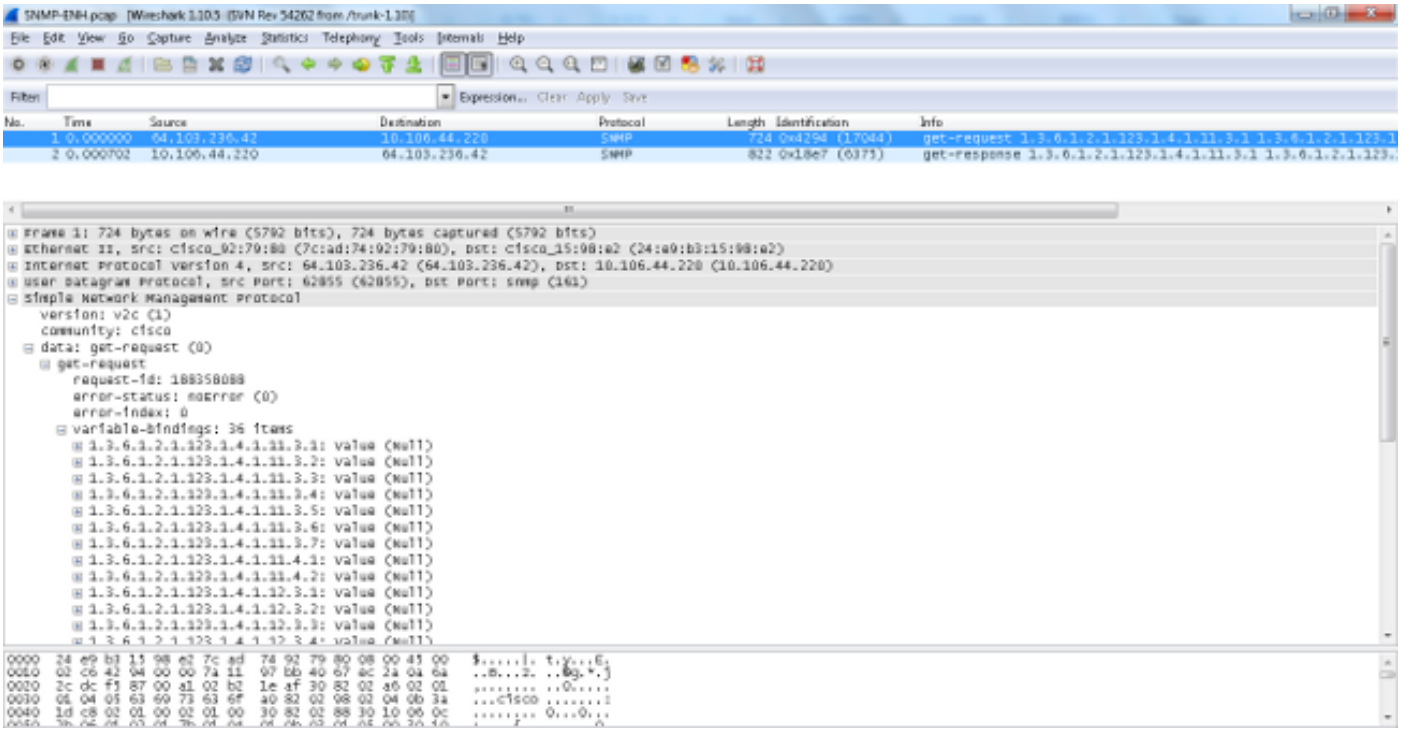
Nuevos OID

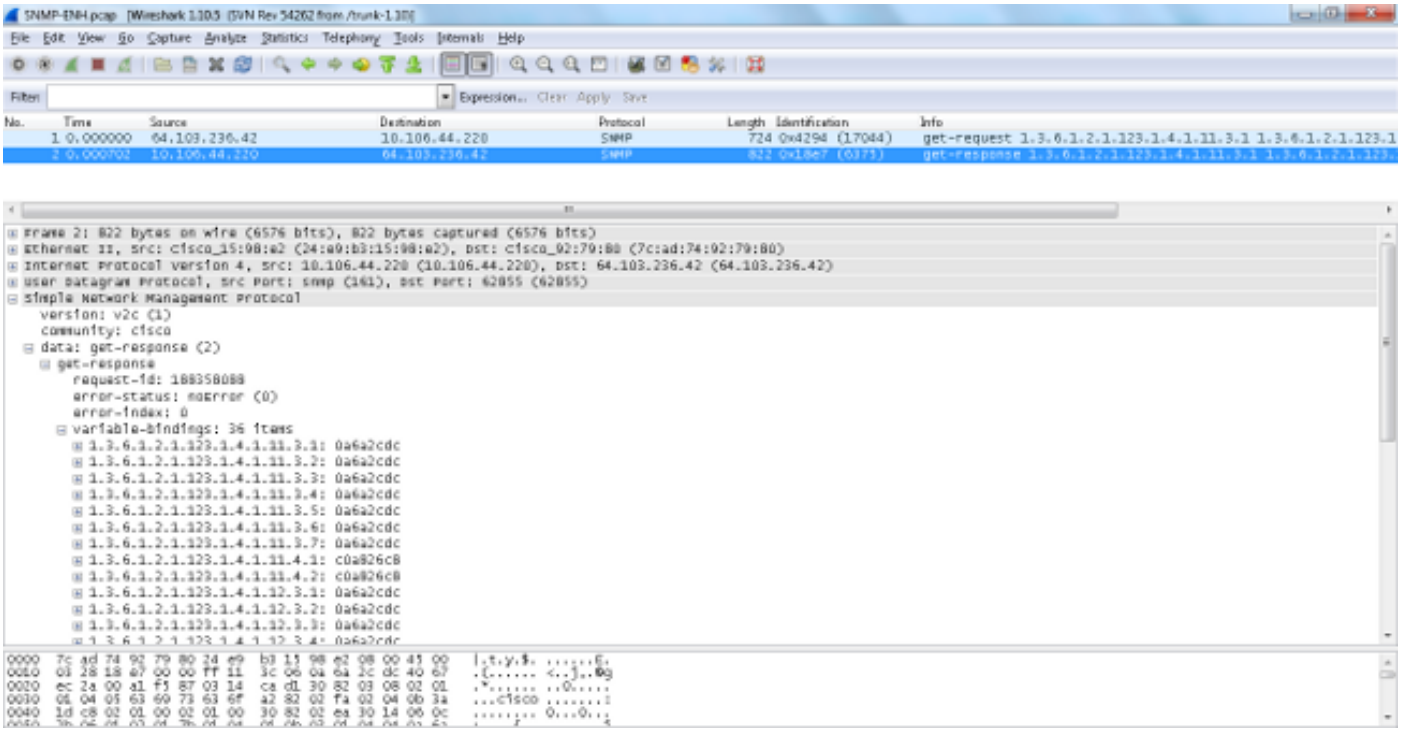
Estos son los nuevos OID que se agregan con esta función:

- **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**

Compatibilidad con mensajes SNMP de 1472 bytes

Las plataformas ASA limitan el tamaño máximo de paquete para las solicitudes SNMP a 512 bytes. Cuando realiza una consulta masiva para un gran número de OID de MIB dentro de una sola solicitud SNMP, la conexión SNMP se agota y se genera un syslog de error en el ASA. RFC3417 sugiere que el tamaño máximo de paquete para las solicitudes SNMP debe ser 1,472 bytes. Este es el tamaño de la carga útil SNMP para el paquete. Además, se deben agregar el encabezado Ethernet y el tamaño del encabezado IP para calcular el tamaño total del paquete.





Nota: Con esta función se admiten los modos de contexto único y de contexto múltiple.

Troubleshoot

Esta sección proporciona información que puede utilizar para resolver problemas del sistema en el ASA.

Comandos show

Estos comandos **show** pueden ser útiles cuando se intenta resolver problemas en el ASA:

- asa# **show run snmp-server host-group**
  snmp-server host-group inside network1 poll 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**

Este comando CLI muestra las entradas que están presentes en la tabla de direcciones del servidor SNMP, que incluye las configuraciones del host y del grupo host:

```
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
```

Como se muestra, estos comandos muestran todos los hosts configurados a través del comando **host-group**. Puede utilizar este comando para verificar si todas las entradas están disponibles y también verificar los grupos de hosts que se superponen.